



FP7-ICT-SEC-2007-1  
Contract no.: 225186  
www.wsan4cip.eu



# WSAN4CIP

## Deliverable D1.1

### Definition of critical performance and reliability parameters through radio coverage, energy and CIP process time tomography

Editor:	Evgeny Osipov, LTU
Deliverable nature:	R
Dissemination level: (Confidentiality)	PU
Contractual delivery date:	30/09/2009
Actual delivery date:	30/09/2009
Suggested readers:	Consortium
Version:	1.0
Total number of pages:	55
Keywords:	CIP scenario analysis, CIP performance bounds

---

#### *Abstract*

This deliverable describes an assessment methodology for WSN installation sites in applications connected to protection of critical infrastructures. A methodology for identification of critical performance parameters through performing tomography (or in other words analysis) of properties of the particular installation site and envisioned CIP application in radio, energy, time, reliability, and security domains is presented. Being equipped with the presented methodology a developer has means to systematically analyse critical parameters of the future application. These parameters are further formulated as application requirements on the protecting ICT system. When selecting hardware and software components according to the parameters of the site and the application, a new set of parameters critical for system performance is introduced. This time it is parameters of the functional blocks of the communication system itself (topology, selected hardware, software components). In this document most important parameters of this kind are identified. On examples of two project's demonstrator scenarios the suggested tomography process of radio properties of the environment, energy sources and timing of particular CIP processes is described.

---

---

## Disclaimer

---

This document contains material, which is the copyright of certain WSAN4CIP consortium parties, and may not be reproduced or copied without permission.

*In case of Public (PU):*

All WSAN4CIP consortium parties have agreed to full publication of this document.

*In case of Restricted to Programme (PP):*

All WSAN4CIP consortium parties have agreed to make this document available on request to other framework programme participants.

*In case of Restricted to Group (RE):*

The information contained in this document is the proprietary confidential information of the WSAN4CIP consortium and may not be disclosed except in accordance with the consortium agreement. However, all WSAN4CIP consortium parties have agreed to make this document available to <group> / <purpose>.

*In case of Consortium confidential (CO):*

The information contained in this document is the proprietary confidential information of the WSAN4CIP consortium and may not be disclosed except in accordance with the consortium agreement.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the WSAN4CIP consortium as a whole, nor a certain party of the WSAN4CIP consortium warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

## **Impressum**

Wireless Sensor Networks for the Protection of Critical Infrastructures

WSAN4CIP

WP1 CIP Requirements and methodologies

Selected communication protocols for target applications

Evgeny Osipov, LTU

## **Copyright notice**

© 2009 Participants in project WSAN4CIP

## Executive summary

Developing communication system for applications related to protection of critical infrastructures (CIP) is a complex process which demands systematic approach starting from early design stages. On the one hand, WSAN technology is an ideal technological building block to improve the reliability of critical infrastructures; on the other hand WSANs themselves become part of a critical infrastructure, i.e. of the information system. Deploying WSAN in the control loop of critical infrastructures adds another level of complexity and a point of failure. Nothing is more dangerous than an ICT control system which is not extremely reliable. It is by far not trivial to bring the right level of automation as well as information and communication technology to a CI aiming at the ultimate goal of a dependable control and monitoring system for the CI.

Being able to correctly identify critical parameters for particular CIP system performance metrics and the factors that affect their behavior is essential for the design of the *dependable* communication systems.

This document describes a methodology for identification of critical performance parameters through performing tomography (or in other words analysis) of properties of the particular installation site and envisioned CIP application in radio, energy, time, reliability, and security domains. Being equipped with the presented methodology a developer has means to systematically analyse critical parameters of the future application. These parameters are further formulated as application requirements on the protecting ICT system. When selecting hardware and software components according to the parameters of the site and the application a new set of parameters critical for system performance is introduced. This time it is parameters of the functional blocks of the communication system itself (topology, selected hardware, software components). In this document we identified most important parameters of this kind.

It is important to note that understanding the degree of influence of certain parameter of the *software part* on particular system-level performance metric (i.e. the *criticality* of a parameter) is a challenging task. The *criticality* (or in system identification terminology - *significance*) of a parameter for system performance should be studied systematically through an extensive set of experiments (or simulations) and applying analysis methodology used for identification of complex systems. This question is, however, considered in the scope of a different research activity inside the project. In particular Milestone 1.1 and the following up Deliverable 1.3 documents will present the results of such analysis. In this document we opt at identification of a set of parameters of communication protocols along with their possible interdependencies with the potentially affected performance metrics for a general case WSANs. Filling software parameters with the specific values is outside the scope for this deliverable.

The methodology for the site and application assessment through multidimensional tomography presented in the first part of this document is further applied on examples of particular CIP applications. We focused on the CIP scenarios which further will be adopted for the project demonstrators.

## List of authors

<b>Company</b>	<b>Author</b>
INOV	António Grilo
IHP	Steffen Peter
BME	Levente Buttyan
LTU	Evgeny Osipov

## Table of Contents

Executive summary .....	3
List of authors.....	4
Table of Contents .....	5
List of tables .....	6
1 Introduction .....	7
2 Analysis methodology of critical for CIP applications parameters.....	8
2.1 Environmental parameters as input for communication system configuration.....	10
2.2 System level performance metrics in time, reliability and security domains.....	10
2.3 Parameters imposed by the structure of the communication system and their criticality for WSAN4CIP performance. ....	12
2.4 Security threat analysis and threat enabling parameters .....	14
2.4.1 Methodology.....	14
2.4.2 Application types .....	14
2.4.3 Adversary models .....	15
2.4.4 Attack mechanisms .....	16
2.4.5 Risk assessment .....	17
2.4.6 Summary .....	22
3 Considered CIP scenarios.....	24
3.1 Site 1 description.....	24
3.1.1 Scenario #1 – Circuit breaker trip coil condition active status monitoring .....	27
3.1.2 Scenario #2 - Power Transformer oil temperature active monitoring .....	31
3.1.3 Scenario #3 - Neutral Reactance oil temperature active monitoring .....	34
3.1.4 Scenario #4 - Neutral Resistor coil box temperature active monitoring.....	37
3.1.5 Scenario #5 - Power line current active monitoring per tower and per phase .....	40
3.1.6 Scenario #6 - perimeter unauthorized intrusion detection .....	44
3.1.7 Scenario #7 - MV/LV power station video surveillance and hotspot detection .....	47
3.2 Site 2 description.....	50
3.2.1 Scenario description.....	51
4 Summary .....	54
References .....	55

## List of tables

Table 1. Classification of critical environmental parameters .....	9
Table 2. System level performance domains.....	11
Table 3. Classification of critical parameters of communication system .....	13
Table 4. Risk estimation in the case of control loop application with poor attacker.....	18
Table 5. Risk estimation in the case of control loop application with clever attacker .....	18
Table 6. Risk estimation in the case of control loop application with rich attacker.....	19
Table 7. Risk estimation in the case of surveillance application with poor attacker.....	20
Table 8. Risk estimation in the case of surveillance application with clever attacker.....	21
Table 9. Risk estimation in the case of surveillance application with rich attacker .....	22
Table 10. Summary of the risk analysis .....	23
Table 11. Critical environmental parameters for EDP Power Substation .....	25
Table 12. Critical environmental parameters for EDP 15KV power distribution lines.....	26
Table 13. Critical environmental parameters for EDP MV/LV power station.....	26
Table 14. Scenario #1 - Summary of function description.....	28
Table 15. Scenario #1 - System level performance requirements for the application .....	29
Table 16. Scenario #1 - Scenario-specific parameters of communication system .....	30
Table 17. Scenario #2 - Summary of function description.....	32
Table 18. Scenario #2 - System level performance requirements for the application .....	32
Table 19. Scenario #2 - Scenario-specific parameters of communication system .....	33
Table 20. Scenario #3 - Summary of function description.....	35
Table 21. Scenario #3 - System level performance requirements for the application .....	35
Table 22. Scenario #3 - Scenario-specific parameters of communication system .....	36
Table 23. Scenario #4 - Summary of function description.....	38
Table 24. Scenario #4 - System level performance requirements for the application .....	38
Table 25. Scenario #4 - Scenario-specific parameters of communication system .....	39
Table 26. Scenario #5 - Summary of function description.....	41
Table 27. Scenario #5 - System level performance requirements for the application .....	43
Table 28. Scenario #5 - Scenario-specific parameters of communication system .....	43
Table 29. Scenario #6 - Summary of function description.....	44
Table 30. Scenario #6 - System level performance requirements for the application .....	45
Table 31. Scenario #6 - Scenario-specific parameters of communication system .....	46
Table 32. Scenario #6 - Summary of function description.....	48
Table 33. Scenario #6 - System level performance requirements for the application.....	48
Table 34. Scenario #6 - Scenario-specific parameters of communication system.....	49
Table 35. Classification of critical environmental parameters .....	51
Table 36. Summary of function description .....	52
Table 37. System level performance requirements for FWA CIP application .....	52
Table 38. Scenario-specific parameters of communication system.....	53

# 1 Introduction

Developing communication system for applications related to protection of critical infrastructures (CIP) is a complex process which demands systematic approach starting from early design stages. On the one hand, WSAN technology is an ideal technological building block to improve the reliability of critical infrastructures; on the other hand WSANs themselves become part of a critical infrastructure, i.e. of the information system.

On the other hand, whenever another layer of complexity is added to a system, this opens new possibilities for system failures, misuse or malicious attacks. However, almost all modern critical infrastructures are equipped with an ICT control system to continuously monitor the critical infrastructure's status. It is by far not trivial to bring the right level of automation as well as information and communication technology to a CI aiming at the ultimate goal of a dependable control and monitoring system for the CI.

Things become even more delicate, when the ICT system contains Wireless Sensor and Actuator Networks. On the one hand due to its sensing capabilities and wireless characteristics they are an almost mandatory building block to continuously monitor various real-world phenomena on a large scale, and give valuable feedback about the CI status to the control system. On the other hand, nothing is more dangerous than an ICT control system which is not extremely reliable.

Being able to correctly identify critical for particular CIP system performance metrics and the factors that affect their behavior is essential for the design of the *dependable* communication systems. This document describes a methodology for identification of critical performance parameters through performing tomography (or in other words analysis) of properties of the particular installation site and envisioned CIP application in radio, energy, time, reliability, and security domains. Being equipped with the presented methodology a developer has means to systematically analyse critical parameters of the future application. These parameters are further formulated as application requirements on the protecting ICT system. When selecting hardware and software components according to the parameters of the site and the application a new set of parameters critical for system performance is introduced. This time it is parameters of the functional blocks of the communication system itself (topology, selected hardware, software components). In this document we identified most important parameters of this kind.

The structure of the document is as follows. We first describe an assessment methodology in Section 2. Further in Section 3 the description of the CIP scenarios related to project's demonstrators are presented along with the results of the multidimensional tomography performed according to the presented methodology. Section 4 summarizes the deliverable.

## 2 Analysis methodology of critical for CIP applications parameters

Systematic analysis of a CIP application is a multidimensional problem and the essential step towards designing functionality of a dependable communication system as part of the critical infrastructure. The interdependencies of the design process are illustrated in Figure 1.

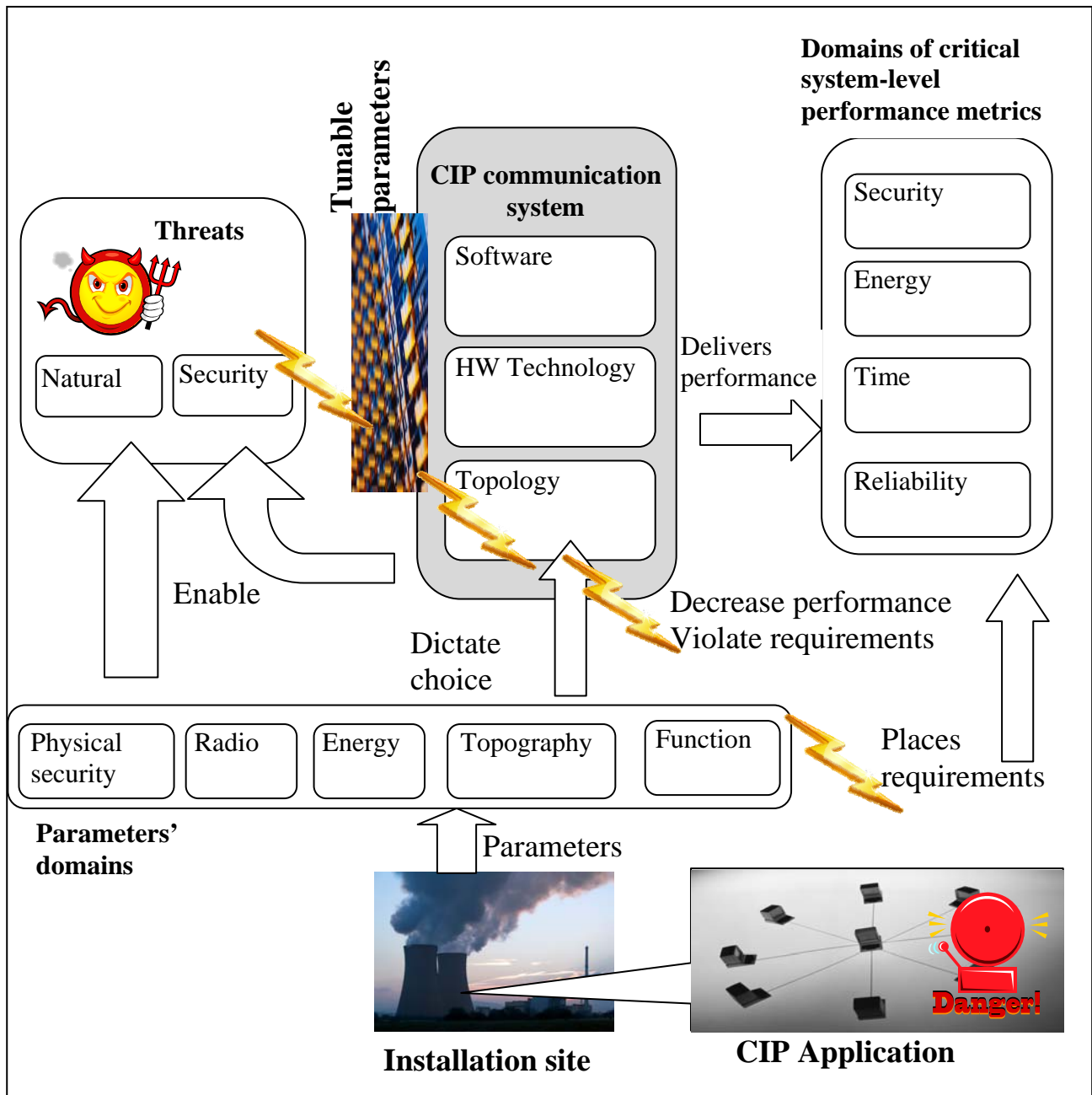


Figure 1: Interdependencies during the CIP application design process.

A specific critical infrastructure is in the root of the analysis and design chain. The parameters of the particular installation site characterize both the physical environment of the site and the infrastructure protection function to be implemented by WSN. We identified five classes of environmental parameters,

which describe: Physical security procedures; Radio properties of the environment, Energy properties, topography and CIP function. Table 1 presents particular critical parameters in each class.

These parameters are assessed at the first stage of the WSAN design process. This is because the environmental parameters play dual role in the design chain. On the one hand they dictate specific configuration of the communication system along layout, hardware and software axes. Some of the parameters (e.g. Functional) place also requirements on the performance characteristics of the WSAN based communication system. On the other hand site's properties are natural enablers of different types of natural and security threats.

**Table 1. Classification of critical environmental parameters**

Class	Parameters	Comment
Physical security	Access control	Level of accessibility of third party persons to the critical infrastructure site
	Physical surveillance	Level of other security means that limit access to CI site.
	Tamper resistance	Level of tamper resistance of the WSAN nodes and sensors. Level of tamper resistance can range from no tamper resistance through tamper evidence to passive tamper resistance and active tamper detection and reaction. These levels correspond to the 4 levels defined in FIPS 140 (The Federal Information Processing Standardization 140 (FIPS) are series of publications numbered 140 which are a U.S. government computer security standards that specify requirements for cryptography modules.).
Radio	Degree of interference	Characterization of radio noise in absence of the useful signal [1 .. 5]. The value of 1 indicates low interference, 5 represents complex interference picture.
	Propagation of radio signal	Type of signal propagation (open space line of sight, shadowing propagation, etc.).
	Transmission power	Legal restrictions on transmission power
	Bandwidth	Legally available radio bandwidth
Energy	Availability of sources	
	Type of sources	Solar, infrastructure, etc.
	Continuity	Per cent of one day
	Voltage level	
	Current level	
Topography	Type	Open space, urban, rural
	Scale	CI area in square meters, max distance, min distance between objects, etc.
Function	Type of application	Surveillance, control loop
	Type of critical data	Voice, video, data
	Frequency of critical event	Percent of day, month, year
	Data importance class	[1 ..5] The value of 1 indicates low priority, 5 represents highest priority.
	Data distribution pattern	Type of communication flows [multicast, convergecast, unicast]
	Reliability type	<None, Partial (average =x%), Guaranteed (minimum = X%), Full>

## 2.1 Environmental parameters as input for communication system configuration

The choice of particular components for dependable communication system is naturally driven by the properties of the installation site and the type of the protection function. The critical in this respect parameters fall in Radio, Energy, Topography and Function domains. The choice of particular radio technology depends on its tolerance to the background electro-magnetic noise which would interfere with the radio transmission. The selection of the transmission energy value depends on the signal propagation properties in a particular environment. The latest parameter should be assessed by the result of the topography parameter analysis. Indeed, the placement of the monitored objects, the presence of the interfering constructions directly affects the radio propagation properties.

Availability of energy sources is critical for most WSN installations and the functional content of the communication stack. Whenever stable sources of energy are available long duty cycle protocols are preferred to achieve better system performance in time domain. On contrary different energy optimal solutions should be deployed when the CI WSN is operating on autonomous energy sources in order to prolong the network lifetime and as the result the overall system reliability.

The parameters describing topographical properties directly affect the choice of the network topology which in turn implies usage of different network solutions in order to deliver the function of the WSN application.

Finally, the parameters describing properties of the WSN function are further mapped into the technical performance requirements of the entire application in Time, Reliability, Energy and Security domains. This issue is further elaborated in Section 2.3.

## 2.2 System level performance metrics in time, reliability and security domains

The set of system-level performance metrics is in fact well defined in the domain of the wired Internet. The known metrics of network performance to be used by network operators, end users or independent testing groups include *connectivity* [6], *delay* [1][3], *delay variation (or jitter)* [4], *loss patterns* [5], *packet delivery ratio (delivery reliability)*, *packet reordering* [8], *throughput (or bulk transfer capacity* [7]), *energy consumption index*, *fairness index*. For wireless sensor and actuator networks this set of metrics must be extended as well with *degree of autonomy* reflecting the lifetime of the installation without human maintenance. For purposes of further discussion we classify these metrics into three domains of system properties: Security, Time, Reliability and Energy as shown in Table 2.

While requirements in Time, Energy and reliability domains are self-explainable, the application requirements on security need some extra clarification. The particular application may require not only presence of specific security services (confidentiality, integrity, authentication, non-repudiation) but also different levels of their strengths. The strength's level depends on the one hand on the type of envisioned attack (see section 2.4) and on the criticality of the specific data class. The choice of the particular security solution is then performed by finding a trade-off between the desired level of security service and computational and communication capability of each sensor device and the WSN system as a whole. For example the highest strength of confidentiality could be achieved by using advanced encryption technique and large keys, this however implies selection of hardware with appropriate characteristics which potentially is able to implement this requirement.

**Table 2. System level performance domains**

<b>Performance domain</b>	<b>Performance metrics</b>	<b>Comment</b>
Security	Confidentiality	Hiding the content of messages, or message parts, from unauthorized access. A binary performance metric indicating whether the system provides confidentiality or not.
	Integrity	Detection of unauthorized intentional modifications of messages. A binary performance metric indicating whether the system provides integrity or not.
	Authentication	Unforgeable identification of message sources. A binary performance metric indicating whether the system provides authentication or not.
	Non-repudiation	Proving to a third party who the sender and/or the receiver of a message were. A binary performance metric indicating whether the system provides non-repudiation or not.
Time	Throughput	The minimum acceptable data rate observable at the receiver.
	Jitter	Delay variation between subsequent messages in a flow. The maximum value observable at the receiver.
	Delay	The maximum end-to-end delay observable at the receiver.
	Fairness index	The value observable in the network.
Energy	Energy consumption index	The maximum value of the energy consumption for a specific node in operation.
	Energy consumption pattern	The allowed distribution of energy consumption in the network during its operation.
Reliability	Packet loss	A minimum percentage of packages correctly received (relative to all sent packets) over a specific time (per hour, day, or month).
	Information integrity	A minimum percentage of packages that are correct, relative to all received and accepted packets.
	Degree of autonomy	Life time of the network when it delivers specified functionality.
	Spatial resolution	Number of information samples needed to successfully reconstruct the measured phenomenon.

The metrics specified in Table 2 are filled with the particular values based on the analysis during the site and application assessment (using Table 1). The security requirement part is filled in with the values taking into account risks for particular types of threats presented further in Section 2.4 in taken into account properties of the particular site and the application. Each metric is then used both to suggest the initial choice of particular content of the WSA communication system and to benchmark the correctness of its parameters' configuration, i.e the system's performance (see next subsection).

These metrics can further be mapped into a higher-level performance metrics meaningful for end-users of the network (i.e humans), for example reliability level, accuracy etc. Applications of different types place different requirements either on the whole set of metrics or its subset. For example, an application prioritizing high data reliability over other characteristics would demand maximization of end-to-end delivery ration even by the cost of reduced life time due to non-optimal energy consumption and other performance characteristics. In this document we, however, do not further discuss the tradeoffs of simultaneous optimization of different system-level performance metrics.

## 2.3 Parameters imposed by the structure of the communication system and their criticality for WSAN4CIP performance.

As it is described in Section 2.1 the environmental parameters shape the structure of the WSAN4CIP communication system. This structure includes the topology, hardware architecture and the functional content of the communication stack. The communication system in its turn exposes a set of parameters critical for performance of the system as a whole. The most important parameters in this class are presented in Table 2. We classify these parameters into three categories according to Figure 1: Topology parameters, Hardware parameters and Software parameters. Changing the values of these parameters leads to changes in the overall system performance. In the previous section we presented system performance metrics critical for wireless sensor and actuator networks in the context of critical infrastructures' protection. In Table 3 we identify the domains of the system performance metrics affected by changes in parameters of communication system.

In Table 3 the parameters described in the shaded part are parameters statically linked to environmental variables. The developer may uniquely identify the type of topology and the needed hardware by analyzing the characteristics of the installation site and the CIP application (see Table 1). In this document we present specific values for particular CIP scenarios considered for project's demonstrators in these two classes.

It is important to note that understanding the degree of influence of certain parameter of the *software part* on particular system-level performance metric (i.e. the *criticality* of a parameter) is a challenging task. The *criticality* (or in system identification terminology - *significance*) of a parameter for system performance should be studied systematically through an extensive set of experiments (or simulations) and applying analysis methodology used for identification of complex systems [9]. This question is, however, considered in the scope of a different research activity inside the project. In particular Milestone 1.1 and the following up Deliverable 1.3 documents will present the results of such analysis. In this document we opt at identification of a set of parameters of communication protocols along with their possible interdependencies with the potentially affected performance metrics for a general case WSANs. Filling software parameters with the specific values is outside the scope for this deliverable.

**Table 3. Classification of critical parameters of communication system**

Part of communication system	Parameters		Values range	Affected domain of system performance characteristics
Topology	Type		Single cell, mesh, star, tree, etc.	Energy
	Density of nodes		<MIN(r), NOM(r), MAX(r)>	Energy, Time, Reliability
	Number of hops		<MIN(h), NOM(h), MAX(h)>	Time, Energy
Hardware	Heterogeneity		Low-energy only, high energy only, mixed, etc.	Time
	Power consumption for communication activities for every used technology.		<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	Energy, Reliability, Time.
	Sensitivity threshold		<MIN(SNR), NOM(SNR), MAX(SNR)>	Energy, Reliability
	Tamper resistance		<no protection, tamper evidence, passive tamper resistance, active tamper detection and response>	Security, Reliability, Energy
Software	Transport layer	Xcast support	<Broadcast, Multicast, Convergecast, Geocast, Anycast>	
		Retransmission Strategy	None, Hop-by-hop, end-to-end	Time, Energy
		Size of retransmission unit	<MIN(CWND), NOM(CWND), MAX(CWND)>	Time, Reliability,
		QoS support	None, Bounded delay, differentiated priority	
		Security services	<Confidentiality, Integrity, Authentication>	Security, Time, Energy
	Network/routing layer	Type	Reactive, proactive	Time, Energy, Reliability
		Route age	<MIN(RT), NOM(RT), MAX(RT)>	
		Route maintenance strategy	None, local, end-to-end	Time, Reliability, Energy
		Security services	<Confidentiality, Integrity, Authentication>	Reliability, Security, Energy
	MAC	Type	Low duty-cycle, synchronous, asynchronous, etc	Energy, time
		Maximum payload	<MIN(PL), NOM(PL), MAX(PL)>	Energy, reliability, time
		Preamble length	Lpre	Time
		Back-off time	<MIN(PL), NOM(PL), MAX(PL)>	
		Security services	<Confidentiality, Integrity, Authentication>	Reliability, Security, Energy

## 2.4 Security threat analysis and threat enabling parameters

While the application of wireless sensor and actuator networks in critical infrastructures have many potential advantages mainly due to cost efficiency, as well as ease of deployment and maintenance, it also has potential disadvantages related to the reduced reliability and security of the communications between the sensors, the actuators, and the back-end control center. In particular, it is well-known that wireless communication channels are more vulnerable to environmental noise, and hence, less reliable, in general, than wired links. Moreover, wireless channels are also vulnerable to attacks, such as jamming, injection of forged data, and eavesdropping and replay of communications that are more difficult to carry out in a wired environment, where access to the communication links is physically limited. Naturally, it is important to identify and understand all these vulnerabilities, but it is equally important *to put them into perspective* by carefully estimating their risk, where the risk associated with vulnerability is usually determined by the amount of effort needed to exploit it by an attack and the potential damage that such an attack may cause. In other words, not all vulnerabilities may need to be eliminated (that would possibly be too expensive, anyway), but one should rather focus on those vulnerabilities that are easy to exploit and that can potentially cause a large amount of damage.

Therefore, the objective of this section is to carry out a threat analysis of wireless sensor and actuator networks in the context of critical infrastructure applications, which includes *both* the identification of vulnerabilities related to this communication technology and the estimation of their risk of being exploited. It is important to understand that we are considering potential applications of wireless sensor and actuator networks in critical infrastructures in general, and not a particular, well-specified system. In other words, we are not analyzing an already existing system, but to some extent, we are looking into the future, and investigate how such a system may potentially look like and what vulnerabilities it may entail. Consequently, the analysis will be rather high level. Still, at this stage of the project, such an analysis is useful, or even indispensable for an informed decision on where to put the emphasis in the technical work packages that aim at developing specific mechanisms to enhance the reliability and the security of wireless sensor and actuator networks in the context of critical infrastructure applications.

### 2.4.1 Methodology

It is well-known in the IT security community (although, most of the times, ignored outside of it) that “nothing useful can be said about the security of a mechanism except in the context of a specific application and environment.”<sup>1</sup> Here, environment refers to the environment in which the mechanism operates, and thus, it includes an adversary who may interact with the mechanism. This means that for the purposes of our threat analysis, we must first identify the potential applications of WSA technology in the context of critical infrastructures, and we must come up with some adversary model, before attempting to carry out any analysis of vulnerabilities and estimation of risks. Therefore, as a first step, we identify application types and attacker models. Next, we identify possible attack mechanisms, and finally, for each combination of application types and attacker models, we identify the potential objectives of the given type of adversary with respect to the given type of application, and estimate the risk of the various attacks that we think are relevant and feasible in the given context. In the risk estimation, we limit ourselves to three levels of risk: low (L), medium (M), and high (H), because in this high level analysis and without the specific details of the critical infrastructure application and the wireless sensor and actuator network in use, it is impossible to really quantify the risk at a more fine grained manner (e.g., in thousands of Euros).

### 2.4.2 Application types

We identify two types of applications of WSANs in the operation of critical infrastructures. First, and perhaps most straightforwardly, wireless sensors and actuators could be used to replace the wired sensors and actuators that are used in today’s operations. Indeed, the operation of many critical infrastructures is

---

<sup>1</sup> Actually, this has first been articulated by Robert H. Courtney Jr., one of the first computer security professionals, and hence, it is often referred to as Courtney’s first law.

based on a control loop, where system parameters are measured by sensors, the collected data is continuously reported to a control center, where it is processed, and if needed, some actuators are activated to modify the system parameters. For instance, in a drinking water supply system, the level of water in the reservoirs is monitored continuously, and if it falls below some threshold, then some valves are opened, and more water is pumped in the system in order to increase the level in the reservoirs. Thus, sensors and actuators are routinely used already today, but those are communicating with the control center via wired connections. The motivations to replace these wired connections with a wireless communication technology include the cost reduction and the easier deployment and maintenance of the system.

The second type of application is the use of WSANs as part of a surveillance system that aims at detecting physical intrusions and attacks against the critical infrastructure facilities. The motivation for this type of application is twofold. First, such physical intrusions and attacks may have fatal consequences, especially if carried out by organized terrorist groups. For instance, shutting down the electric power system in a given geographical area by sabotage against some towers or substations is very much undesirable, just like the poisoning of the water in the drinking water supply system. The second motivation is that traditional surveillance systems do not scale up to the physical size of many critical infrastructure facilities. For instance, traditional video surveillance is not feasible for several hundreds of kilometers of power lines or pipelines. Of course, terrorist attacks and sabotage cannot be fully excluded by any kind of surveillance system, but due to the above mentioned scalability problem, today, large parts of the critical infrastructures are not monitored *at all*, and we argue that WSANs could be used to improve this situation. Indeed, this is the only technology we know of that can serve as the basis of such large scale surveillance systems.

The two application types identified above induce different requirements on the WSAN. In the first application, the WSAN becomes part of a control loop, where it is important to continuously and reliably deliver data from the sensors to the control center, and from the control center to the actuators. In the second application, continuous monitoring of very important facilities may be required, but less important parts of the infrastructure may not have such stringent requirements. In particular, in the second application, one may think of the use of off-line sensor network islands that do not report surveillance data continuously, but instead they store those data in a reliable manner, and the data are read by a mobile reader that shows up at the off-line island occasionally. Such an off-line surveillance network cannot raise an alarm immediately; however, it may record the traces of some suspicious activities. Hence, such an off-line WSAN can still be useful in detecting the preparations of sabotage or in forensics.

### 2.4.3 Adversary models

We distinguish different classes of adversaries in terms of their available resources. In particular, we identify the following three classes of adversaries depending on the amount of resources that they can invest into attacking the system:

**Poor** – Poor adversaries have no or very limited amount of resources both in terms of technical knowledge and money to invest. In terms of equipment, they may obtain commercially easily available devices, such as a laptop computer. However, they have no particular experience and knowledge in (mis)using those equipments to mount malicious attacks. As a representative of this class, one may think of kids playing around with a laptop, and trying to interfere with the operation of the system in a rather ad hoc and non-premeditated manner.

**Clever** – Clever adversaries have limited monetary resources, but they are technically highly skilled. In terms of equipment, they may obtain some special devices that are typically available in a university laboratory environment (e.g., laptops, evaluation boards, oscilloscopes, etc.) or they can craft special devices for their needs using a limited budget (e.g., a wireless sniffer with a sensitive antenna). In addition, they are fully aware of how the system operates and how the protocols used in the WSAN work. As representatives of this class, one may think of a university student or a network engineer.

**Rich** – Rich adversaries have substantial monetary resources that they can use to buy very specialized equipments and technically skilled professionals. Clearly, these are the most dangerous adversaries that can carry out premeditated, carefully organized, and large scale attacks. A representative of this class would be a criminal or terrorist organization.

#### 2.4.4 Attack mechanisms

In this section, we identify the most relevant attack mechanisms that could be used against the WSAN.

**Physical destruction of nodes** – In some cases, the sensor and actuator nodes, the wireless relays, and/or the base stations are physically easily accessible. In those cases, probably the easiest attack is to disable some of these nodes by physical destruction. In this respect, special nodes, such as base stations, and the nodes that form a vertex cut in the network are more attracting targets, because their physical destruction causes the largest amount of damage; in the worst case, disabling the base stations in an on-line WSAN shuts down the services of the network completely. On the other hand, there may be cases, where the nodes are mounted in special locations and they cannot be easily approached and destroyed. Also, in an off-line WSAN, the network can be designed to cope with the problem of disappearing nodes, while the mobile base station can be assumed to be reasonably protected against physical destruction attacks.

**Dismounting and stealing nodes** – This attack has similar effects to the physical destruction of nodes in the sense that, in both cases, some nodes completely and suddenly disappear from the network. The difference here is that nodes are actually not destroyed, but stolen, and hence we can assume that they may be reverse engineered. This means that secrets, such as cryptographic keys, can be extracted from these stolen nodes, and their software and hardware can be analyzed in order to gain a full understanding of the operation of the system. Hence, this attack can be a useful preparation step before other types of attacks listed below. For instance, a discovered bug in the software may allow a remote code injection attack on all the nodes that run the same software.

**Dismounting and relocating sensors** – In this attack, the attacker changes the location of some sensors. Thus, the victim nodes do not disappear, unlike in the previous two attacks, but they report measurements from a wrong location enforced by the attacker. Similar to the previous two attacks, the effort needed to carry out this attack depends on how easy or hard it is to physically access the sensors.

**Sensor input manipulation** – Even if sensor nodes are not easily accessible, their sensed environment may still be manipulated such that they sense and report false data. For instance, light sensors can be cheated with a pocket lamp when it is dark, and temperature sensors can also be manipulated easily with a cigarette lighter. The goal of such an input manipulation attack can be to prevent an alarm when otherwise the system should raise an alarm, or on the contrary, to provoke false alarms and undermine the operator's trust in the system (after hundred such false alarms, the next alarm will probably not be taken very seriously). In case of an off-line sensor, input manipulation results in false records that may jeopardize any later analysis.

**Jamming** – This attack consists in emitting noise on the radio channels used by the network in order to prevent the nodes to communicate with each other. More precisely, jamming usually targets a subset of the nodes, and it prevents those targeted nodes from receiving any useful signal; however, the transmissions of the jammed nodes may be received outside of the jammed area. Jamming is very easy to carry out, and have similar effects to node destruction. There are slight differences, though. First, jamming does not need physical access, and hence, it is even easier to carry out than node destruction attacks. Second, jamming has a temporary effect: when the jammer stops emitting noise, the attacked nodes can recover easily; while such recovery from a physical destruction is usually not possible. Jamming can be continuous, meaning the permanent emission of noise, and it can also be selective, where the jammer attempts to prevent the victims from receiving particular transmissions. For instance, the jammer may interpret the header information of overheard packets, and prevent the reception of certain packets whose headers satisfy some filtering criteria by interfering with those particular transmissions for a sufficiently long time, but not continuously emitting noise. Such a sophisticated jammer is much harder to detect and cope with.

**Eavesdropping** – Another attack that is easy to carry out in a wireless environment is eavesdropping. In particular, nodes in a WSAN typically use omnidirectional antennas, and therefore, the transmissions of the nodes are very easy to overhear with a well-placed receiver. Also, the radio technology and the protocols used by these networks are easily available to anyone, so eavesdropping devices can be either purchased or constructed easily.

**Replay of protocol messages** – Replay of messages consists of two steps: first eavesdropping transmissions, and then, re-injecting the same messages in the network, perhaps at a different location and later in time. Both are easy to carry out in a wireless environment with a combination of receivers and transmitters. Protocols must be prepared to detect such replay attacks, otherwise they may have devastating effects on the operation of the system.

**Injection of crafted protocol messages** – Similar to replay attacks, here as well, the attacker injects messages in the network, but those are not previously eavesdropped messages but they are crafted by the attacker (perhaps using fragments of previously eavesdropped messages). Such an attack requires a more sophisticated attacker who knows very well the protocols used in the network and their potential weaknesses.

**Corruption of stored data** – This attack is relevant only for WSANs where the nodes store sensor readings for later processing, and it consists in the manipulation of those stored data. To carry out such an attack, the attacker may need physical access to the nodes, or the attacker may exploit some weaknesses in the protocols used to manage those stored data to overwrite them remotely. In the latter case, the attacker may rely on other types of attack mechanisms such as replay and injection of messages. Hence, the complexity of such an attack very much depends on the particular protocols in use.

**Remote code injection** – This attack exploits some software bugs (e.g., a buffer overflow vulnerability) to inject some crafted code into the node and to provoke its execution. As a consequence, the attacked nodes may crash, in the best case, or they may remain operable but become fully controlled by the attacker, in the worst case. The code injection attack is executed remotely, via the wireless interface of the nodes, and the attacker code can be propagated further by the infected nodes, resulting in an epidemic-like, fast infection of the entire network. This is facilitated by the fact that most probably all the nodes run the same software stack, and thus, contain the same software bugs (which may be discovered by stealing and reverse engineering a single node). Today, remote code injection attacks require very specialized and deep knowledge of the organization of the software on the nodes; however, this situation may quickly change and become worse if WSANs become more widely deployed, their software architecture become more standardized, and exploit scripts begin to be published on the Web.

**Installing rogue software on nodes** – In this attack, the attacker installs some rogue software on some of the nodes either by physically accessing the nodes and uploading the rogue software via a standard interface, such as USB, or by exploiting weaknesses in the remote code update protocol, if such a protocol is used in the network. In the latter case, the attack may rely on other attack mechanisms including replay and injection of crafted protocol messages.

**Deployment of rogue nodes** – This attack goes one step further than the rogue software attack described above: it not only introduces new software on existing nodes, but it introduces new nodes in the network with arbitrary code. What makes this attack easy to mount is that, due to the low hardware cost of the computing and communication parts of the sensor and actuator nodes (the sensors themselves may be more expensive), it is easy to fabricate clone devices, and due to the wireless communication medium, it is easy just to place them near to the network and logically connect them into the system (at least at the physical layer).

## 2.4.5 Risk assessment

### 2.4.5.1 Case: Control loop application and poor attacker

Let us consider the case when the WSAN is used to replace wired sensors and actuators, and it operates as part of the control loop of the critical infrastructure application. A poor adversary has no resources to carry out sophisticated attacks against such a system, but his main objectives could be **vandalism** and **to disturb the operation** of the system. In view of this, the following table contains the risk estimation of the various attack types.

**Table 4. Risk estimation in the case of control loop application with poor attacker**

<b>Attack</b>	<b>Risk</b>	<b>Comment</b>
Physical destruction of nodes	M/L	Matching objectives: vandalism, disturbing the operation. If nodes are accessible, then it is relatively easy to carry out (risk is M), otherwise, it may be simply impossible to carry out (risk is L).
Dismounting and stealing nodes	M/L	Matching objective: disturbing the operation. If nodes are accessible, then it is relatively easy to carry out (risk is M), otherwise, it may be simply impossible to carry out (risk is L).
Dismounting and relocating sensors	L	Matching objective: disturbing the operation. The risk is L, because the sensors themselves are usually difficult to access physically (e.g., they may be under the ground or high on towers).
Sensor input manipulation	L	Matching objective: disturbing the operation. The risk is L, because the sensors themselves are usually difficult to access physically.
Jamming	H	Matching objectives: disturbing the operation. This attack is very easy to carry out, and there's no need to access the nodes physically.
Eavesdropping	M	This attack is very easy to carry out, but it does not really help to achieve any of the objectives of this attacker type in the given application.
Replay of protocol messages	L	Matching objective: disturbing the operation. This type of attacker has no knowledge to carry out this attack.
Injection of crafted protocol messages	L	Matching objective: disturbing the operation. This type of attacker has no knowledge to carry out this attack.
Corruption of stored data	n/a	In this application, the nodes continuously report data, and they don't store them.
Remote code injection	L	Matching objective: disturbing the operation. This type of attacker has no knowledge to carry out this attack.
Installing rogue software on nodes	L	Matching objective: disturbing the operation. This type of attacker has no knowledge to carry out this attack.
Deployment of rogue nodes	L	Matching objective: disturbing the operation. This type of attacker has no knowledge and resources to carry out this attack.

#### 2.4.5.2 Case: Control loop application and clever attacker

Let us consider again the case when the WSAN is used to replace wired sensors and actuators, and it operates as part of the control loop of the critical infrastructure application. A clever adversary has the knowledge to carry out sophisticated attacks against such a system, with the main objective of **disrupting its operation** partly or entirely. In view of this, the following table contains the risk estimation of the various attack types.

**Table 5. Risk estimation in the case of control loop application with clever attacker**

<b>Attack</b>	<b>Risk</b>	<b>Comment</b>
Physical destruction of nodes	M/L	Matching objectives: disruptions in the operation. If nodes are accessible, then it is relatively easy to carry out (risk is M), otherwise, it may be simply impossible to carry out (risk is L).
Dismounting and stealing nodes	H/L	Matching objectives: disruptions in the operation. If nodes are accessible, then easy to carry out, and for a clever attacker it provides the means for reverse engineering and preparing other attacks (risk is H), otherwise, it may be simply impossible to carry out (risk is L)
Dismounting and relocating sensors	L	Matching objective: disruptions in the operation. The risk is L, because the sensors themselves are usually difficult to access physically (e.g., they may be under the ground or high on towers).
Sensor input	L	Matching objective: disruptions in the operation. The risk is L, because

manipulation		the sensors themselves are usually difficult to access physically.
Jamming	H	Matching objectives: disruptions in the operation. This attack is very easy to carry out, and there's no need to access the nodes physically.
Eavesdropping	H	This attack is very easy to carry out, but it does not really help to achieve the objectives of this attacker type. Yet, it may provide information about the operation of the system and its protocols, which can be used in other attacks.
Replay of protocol messages	H	Matching objectives: disruptions in the operation. This attack is very easy to carry out for this type of attacker.
Injection of crafted protocol messages	H	Matching objectives: disruptions in the operation. This attack is very easy to carry out for this type of attacker.
Corruption of stored data	n/a	In this application, the nodes continuously report data, and they don't store them.
Remote code injection	M	Matching objective: disruptions in the operation. This type of attacker has the knowledge to carry out this attack, but it needs information of the internal organization of the code and a software bug to exploit.
Installing rogue software on nodes	M	Matching objectives: disruptions in the operation. This attack needs physical access to nodes or manipulation of some remote code update protocols, and hence, there are probably easier ways to achieve the objectives of this attacker.
Deployment of rogue nodes	H	Matching objectives: disruptions in the operation. This attack does not really need physical access to the infrastructure, and it can use commercially available hardware.

**2.4.5.3 Case: Control loop application and rich attacker**

Finally, we consider again the case when the WSAN is used to replace wired sensors and actuators, and it operates as part of the control loop of the critical infrastructure application. A rich adversary has the resources to carry out sophisticated attacks on a large scale against such a system. The main objectives of this adversary type could be to completely **disable the operation** of the system, to create a false impression that the system works properly when in reality it does not, i.e., **deception**, and **to gather sensitive information** about the critical infrastructure. In view of this, the following table contains the risk estimation of the various attack types.

**Table 6. Risk estimation in the case of control loop application with rich attacker**

<b>Attack</b>	<b>Risk</b>	<b>Comment</b>
Physical destruction of nodes	H/M	Matching objectives: disable operation. If nodes are accessible, then it is easy to carry out (risk is H), otherwise, it may be difficult to carry out (risk is M).
Dismounting and stealing nodes	H	Matching objectives: disable operation, gather sensitive information. If nodes are accessible, then it is easy to carry out, otherwise, it may be difficult to carry out this attack. However, stolen nodes can be reverse engineered and important information can be gathered to prepare other attacks.
Dismounting and relocating sensors	M	Matching objectives: disable operation, deception. The risk is M, because the sensors themselves are usually difficult to access physically.
Sensor input manipulation	M	Matching objectives: disable operation, deception. The risk is M, because the sensors themselves are usually difficult to access physically.
Jamming	H	Matching objectives: disable operation. This attack is very easy to carry out, and there's no need to access the nodes physically.
Eavesdropping	H	Matching objectives: gather sensitive information. This attack is very

		easy to carry out, and it may provide sensitive information about the operation of the system and its protocols, which can be used in other attacks.
Replay of protocol messages	H	Matching objectives: deception, disable operation. This attack is very easy to carry out for this type of attacker.
Injection of crafted protocol messages	H	Matching objectives: deception, disable operation. This attack is very easy to carry out for this type of attacker.
Corruption of stored data	n/a	In this application, the nodes continuously report data, and they don't store them.
Remote code injection	M	Matching objective: deception, disable operation. This type of attacker has the resources to carry out this attack. However, the attack needs exploitable software bugs in the code. In addition, this is still a complex attack, and there may be easier ways to achieve the objectives.
Installing rogue software on nodes	H	Matching objectives: deception, disable operation. This attacker may have the resources to buy some internal maintenance engineer and coerce them to install rogue software on the nodes.
Deployment of rogue nodes	H	Matching objectives: deception, disable operation. This attack does not really need physical access to the infrastructure, and it can use commercially available hardware.

#### 2.4.5.4 Case: Surveillance application and poor attacker

Let us now consider the case when the WSAN is used for surveillance of the critical infrastructure. A poor adversary has no resources to carry out sophisticated attacks against such a monitoring system, but his main objectives could be **vandalism** and **to generate false alarms** for joy. In view of this, the following table contains the risk estimation of the various attack types.

**Table 7. Risk estimation in the case of surveillance application with poor attacker**

Attack	Risk	Comment
Physical destruction of nodes	M/L	Matching objectives: vandalism. If nodes are physically accessible, then it is relatively easy to carry out (risk is M), otherwise, it may be simply impossible to carry out (risk is L).
Dismounting and stealing nodes	L	Does not really help to reach the objectives, and it may be difficult to carry out if the nodes are not accessible easily.
Dismounting and relocating sensors	M/L	Matching objective: generating false alarms. If the sensors are physically accessible, then it is relatively easy to carry out (risk is M), otherwise, it may be simply impossible to carry out (risk is L).
Sensor input manipulation	M	Matching objective: generating false alarms. It may be relatively easy to carry out by simply physically approaching the site. However, it has some risk of being caught.
Jamming	M	Does not really help to reach the objectives, but it is very easy to carry out remotely.
Eavesdropping	L	Does not really help to reach the objectives, and needs some technical knowledge.
Replay of protocol messages	L	Matching objective: generating false alarms. This type of attacker has no knowledge to carry out this attack.
Injection of crafted protocol messages	L	Matching objective: generating false alarms. This type of attacker has no knowledge to carry out this attack.
Corruption of stored data	L	Matching objective: generating false alarms (delayed for the time when data is collected and interpreted). This type of attacker has no knowledge to carry out this attack.
Remote code injection	L	Matching objective: vandalism, generating false alarms. This type of

		attacker has no knowledge to carry out this attack.
Installing rogue software on nodes	L	Matching objective: generating false alarms. This type of attacker has no knowledge to carry out this attack.
Deployment of rogue nodes	L	Does not really help to reach the objectives, and this type of attacker has no knowledge and resources to carry out this attack.

#### 2.4.5.5 Case: Surveillance application and clever attacker

Let us consider again the case when the WSAN is used for surveillance of the critical infrastructure. A clever adversary has the technical knowledge to carry out sophisticated attacks against such a monitoring system, with the main objectives of **generating a large number of false alarms** (and effectively rendering the system untrustworthy), and **denial-of-service**. In view of this, the following table contains the risk estimation of the various attack types.

**Table 8. Risk estimation in the case of surveillance application with clever attacker**

Attack	Risk	Comment
Physical destruction of nodes	H/M	Matching objectives: denial-of-service. If nodes are physically accessible, then it is relatively easy to carry out (risk is H), otherwise, it may be simply impossible to carry out (risk is M).
Dismounting and stealing nodes	M/L	Does not really help to reach the objectives, and it may be difficult to carry out if the nodes are not accessible easily (risk is L). However, if the nodes can be physically accessed, then stealing them may let the attacker to reverse engineer them (risk is M).
Dismounting and relocating sensors	M/L	Matching objective: generating false alarms, denial-of-service. If the sensors are physically accessible, then it is relatively easy to carry out (risk is M), otherwise, it may be simply impossible to carry out (risk is L).
Sensor input manipulation	H	Matching objective: generating false alarms. It may be relatively easy to carry out by simply physically approaching the site. However, it has some risk of being caught.
Jamming	H	Matching objective: denial-of-service. This attack is very easy to carry out remotely.
Eavesdropping	M	Does not really help to reach the objectives, and this attacker can carry out easily.
Replay of protocol messages	H	Matching objective: generating false alarms, denial-of-service. This type of attacker has the knowledge to carry out this attack, and it does not need physical access.
Injection of crafted protocol messages	H	Matching objective: generating false alarms, denial-of-service. This type of attacker has the knowledge to carry out this attack, and it does not need physical access.
Corruption of stored data	H/L	Matching objective: generating false alarms (with delay), denial-of-service. This type of attacker has the knowledge to carry out this attack, but it needs physical access to the nodes.
Remote code injection	M	Matching objective: denial-of-service, generating false alarms. This type of attacker has the knowledge to carry out this attack, but it needs information of the internal organization of the code and a software bug to exploit.
Installing rogue software on nodes	M	Matching objective: denial-of-service, generating false alarms. This type of attacker has the knowledge to carry out this attack, but it needs physical access to the nodes or manipulation of the code update protocol.
Deployment of rogue nodes	H	Matching objective: generating false alarms. This attack does not really need physical access to the infrastructure, and it can use commercially available hardware.

### 2.4.5.6 Case: Surveillance application and rich attacker

Finally, consider the case when the WSAN is used for surveillance of the critical infrastructure and the attacker is a resourceful organization. Such an adversary can mount sophisticated attacks at large scale against such a monitoring system. The main objectives of this adversary could be **denial-of-service**, **deception** (to let physical attacks go undetected), and **gathering sensitive information** about the operation of the system. In view of this, the following table contains the risk estimation of the various attack types.

**Table 9. Risk estimation in the case of surveillance application with rich attacker**

Attack	Risk	Comment
Physical destruction of nodes	H	Matching objectives: denial-of-service. If needed, this attacker can find and destroy nodes even if they are difficult to access physically.
Dismounting and stealing nodes	H	Matching objective: gathering sensitive information. Stealing some nodes may let the attacker to reverse engineer them and obtain important information to prepare other attacks.
Dismounting and relocating sensors	H	Matching objective: denial-of-service, deception. If the sensors are physically accessible, then it is relatively easy to carry out.
Sensor input manipulation	H	Matching objective: deception. It may be relatively easy to carry out even without physical access to the nodes.
Jamming	H	Matching objective: denial-of-service. This attack is very easy to carry out remotely.
Eavesdropping	H	Matching objective: gathering sensitive information. This attack is very easy to carry out remotely.
Replay of protocol messages	H	Matching objective: denial-of-service, deception. This type of attacker has the knowledge to carry out this attack, and it does not need physical access.
Injection of crafted protocol messages	H	Matching objective: denial-of-service, deception. This type of attacker has the knowledge to carry out this attack, and it does not need physical access.
Corruption of stored data	H	Matching objective: denial-of-service, deception. This type of attacker has the knowledge and resources to carry out this attack, even if it needs physical access to the nodes.
Remote code injection	M	Matching objective: denial-of-service, deception. This type of attacker has the resources to carry out this attack, but it needs information of the internal organization of the code and a software bug to exploit. There may be easier ways to reach the objectives.
Installing rogue software on nodes	H	Matching objective: denial-of-service, deception. This attacker may have the resources to buy some internal maintenance engineer and coerce them to install rogue software on the nodes.
Deployment of rogue nodes	H	Matching objective: deception. This attack does not really need physical access to the infrastructure, and it can use commercially available hardware.

### 2.4.6 Summary

In this section, we identified possible application types for WSANs in critical infrastructures, and different classes of adversaries. We also identified the main objectives of the different adversary classes with respect to the different application types, and various attack mechanisms that could be used to achieve some of these objectives. Finally, for each combination of application types and adversary models, we estimated the risk of the different attack types. In the risk estimation, we used three levels to quantify the risk, and we determined the level in each case, by taking into account the objectives of the given adversary in the given application type, as well as the difficulty to carry out the given attack, and its expected amount of damage. The results are summarized in the table below, where we collected the estimated risks of the attack types for each application and adversary type into a single table.

**Table 10. Summary of the risk analysis**

<b>Application type &gt;</b>	<b>Control loop</b>			<b>Surveillance</b>		
<b>Adversary model &gt;</b>	<b>Poor</b>	<b>Clever</b>	<b>Rich</b>	<b>Poor</b>	<b>Clever</b>	<b>Rich</b>
<b>Attack type</b>						
Physical destruction of nodes	M/L	M/L	H/M	M/L	H/M	H
Dismounting and stealing nodes	M/L	H/L	H	L	M/L	H
Dismounting and relocating sensors	L	L	M	M/L	M/L	H
Sensor input manipulation	L	L	M	M	H	H
Jamming	H	H	H	M	H	H
Eavesdropping	M	H	H	L	M	H
Replay of protocol messages	L	H	H	L	H	H
Injection of crafted protocol messages	L	H	H	L	H	H
Corruption of stored data	n/a	n/a	n/a	L	H/L	H
Remote code injection	L	M	M	L	M	M
Installing rogue software on nodes	L	M	H	L	M	H
Deployment of rogue nodes	L	H	H	L	H	H

As it can be seen from the table, the risk of the attacks that require physical access (e.g., destruction, stealing, and relocating nodes or sensors) depends on how easy or difficult it is to physically approach the nodes or the sensors. If physical access is possible, then these attacks are easy to carry out, and hence, they have a rather high risk; otherwise their risk is rather low. On the other hand, many of the attacks that do not require physical access, but can be carried out remotely due to the wireless communication medium, are always easy for a capable attacker to carry out, and hence, in general, they have a high risk. In particular, we must mention **jamming, eavesdropping, replay and injection of protocol messages, and deployment of rogue nodes**, which are attacks with a high associated risk in both application types given a serious adversary with knowledge or monetary resources. Modifying the behavior of the nodes by remote code injection or attacking the code update procedures is also possible, although we estimated the risk somewhat lower. In any case, making the protocols and the nodes themselves more dependable and resistant against these identified attacks is important, and it is addressed in the technical work packages of the project.

Looking at the table from another viewpoint, we can see that in face of the strongest adversary, essentially all types of attacks have a high risk. Perhaps a more informative case is the clever adversary model, where the different attacks have varying estimated risk levels. Thus, if one needs to find security engineering trade-offs, then the analysis of this case can suggest which attacks have the highest risk.

Note that some of the identified attacks depend on the critical environmental parameters identified earlier. In particular, parameters in the physical security, radio, and topography classes may have a profound effect on the feasibility of the attacks. At the same time, the attacks identified in this section affect the system level performance metrics. The performance domains of security and reliability are clearly affected, while the attacks with a denial-of-service type objective also affect the time and energy domain (e.g., decrease in throughput, and early battery depletion).

### 3 Considered CIP scenarios

The scenarios described in this section are considered for two project demonstrator sites at EDP and FWA. In this document we present how the analysis methodology presented in Section 2 is applied for tomography of particular CIP applications along radio, time, energy, reliability, and security axes. The structure of the sections below is as follows. We begin the analysis by first describing the highlights of the installation site in a free form text. At the end of each site description we summarize the results of the site tomography in filling in the site-specific values in Table 1 of Section 2. The site analysis follows by the description and the analysis of the scenario of the particular CIP application to be implemented on this site. Firstly, the scenario is described in a free form text and the result of the tomography in security, time, energy, reliability domains are summarized in Tables 2 and 3 from Section 2 filled in with values specific for the particular CIP process.

For each considered CIP scenario we identify its type (surveillance vs. control loop). Using this information the developer is able to analyse risks for security threats presented in Section 2.4.

#### 3.1 Site 1 description

The CIP site 1 comprises in fact three different sites. The first one is a Power Substation in the outskirts of the city of Setubal, Portugal, commonly known as São Sebastião Substation. The second site is used in Scenario #5, which concerns monitoring 15 KV power distribution towers located mainly in open space, starting from the São Sebastião Substation. Finally, scenario #7 shall be set at a MV/LV power station, connected to the São Sebastião Substation through the power distribution towers considered in scenario #5.

The São Sebastião Substation is an important substation in the context of the regional wider grid it belongs to.

The substation serves a large number of industrial and home clients.

Feeders High-Voltage (HV):

- 60KV bus-bar with 247Km of lines

Feeders Medium-Voltage (MV):

- 30KV bus-bar with 148Km of lines and 131 MV/LV Power St.
- 15KV bus-bar with 186Km of lines and 281 MV/LV Power St.

Clients (HV, MV and LV)

- 60KV – 4 clients (High-voltage, large industries)
- 30KV – 63 clients (Medium-voltage, factories)
- 15KV – 61 clients (Medium-voltage, factories)
- 400/230V - 37407 Clients (homes and small business)



- Legend:
1. Main building and WSAN sink/gateway location
  2. Power lines in and out the substation
  3. Power transformers, neutral reactances and neutral resistors.
  4. Circuit breakers

Figure 2: S. Sebastião substation bird’s-eye view from Visual Earth (Microsoft)

Table 11. Critical environmental parameters for EDP Power Substation

Class	Parameters	Value
Physical security	Access control	Third parties are not allowed within the substation, unless dully authorized and escorted by EDP personnel.
	Physical surveillance	Only some substations have intrusion detection mechanisms installed on the perimeter fence. No additional surveillance procedures are established.
	Tamper resistance	Tamper evidence
Radio	Degree of interference	2
	Propagation of radio signal	Mostly open space line of sight
	Transmission power	2.4GHz : 100 mW EIRP
	Bandwidth	ETSI 13 channels for 2.4 GHz band
Energy	Availability of sources	110V DC power grid accessible at active elements
	Type of sources	Infrastructure
	Continuity	100% (with backup power)
	Voltage level	110 V DC
	Current level	Unknown (capacity is enough to activate electro-mechanical devices)
Topography	Type	Suburban
	Scale	Area: 5.400 m <sup>2</sup> (90m x 60m) Perimeter: 300m Distance from main building to the centre of the premises: 50m

**Table 12. Critical environmental parameters for EDP 15KV power distribution lines**

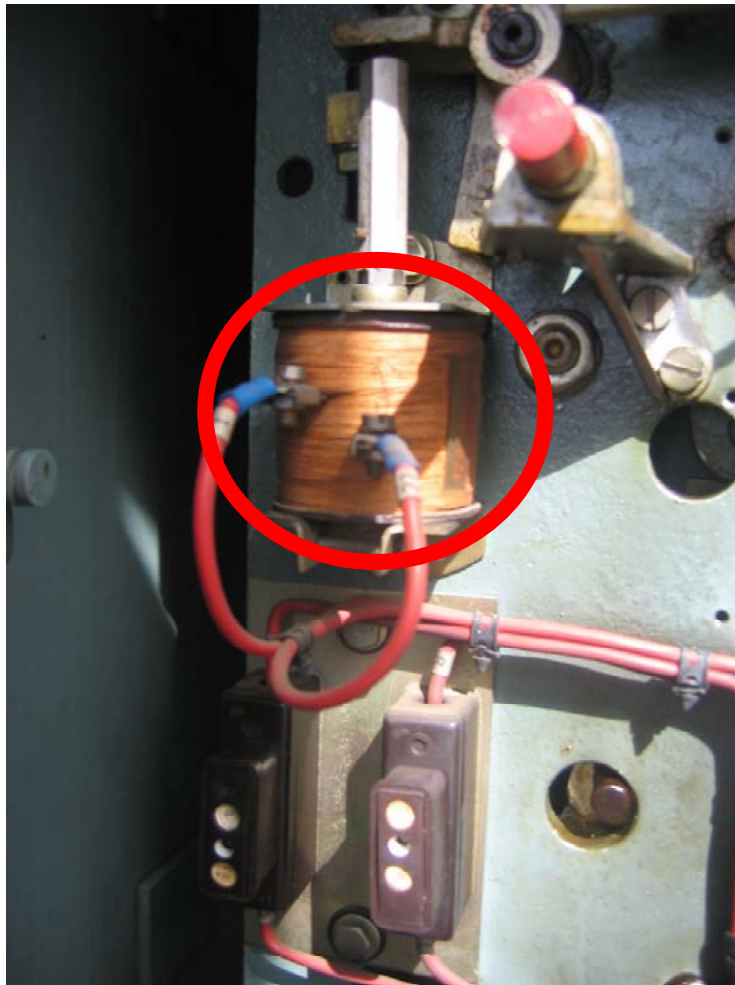
<b>Class</b>	<b>Parameters</b>	<b>Value</b>
Physical security	Access control	The power distribution towers are installed in open country without physical access barriers.
	Physical surveillance	The power distribution towers are not subject to any kind of surveillance.
	Tamper resistance	Tamper evidence
Radio	Degree of interference	1
	Propagation of radio signal	Open space line of sight
	Transmission power	2.4GHz : 100 mW EIRP
	Bandwidth	ETSI 13 channels for 2.4 GHz band
Energy	Availability of sources	No low voltage power available, but high-voltage (15 kV / 30 kV) tower lines may be used for energy harvesting
	Type of sources	Infrastructure
	Continuity	Available current lowers during nighttime
	Voltage level	15 kV / 30 kV AC
	Current level	Few to hundreds Amps
Topography	Type	Rural / Suburban
	Scale	200-700 m between towers

**Table 13. Critical environmental parameters for EDP MV/LV power station.**

<b>Class</b>	<b>Parameters</b>	<b>Value</b>
Physical security	Access control	The power stations are enclosed within a concrete building. Third parties are not allowed within the power stations, unless dully authorized and escorted by EDP personnel.
	Physical surveillance	The power stations are currently not subject to any kind of surveillance.
	Tamper resistance	Tamper evidence
Radio	Degree of interference	2
	Propagation of radio signal	Communications between the indoor and outdoor area of the power station must go through a concrete wall (1 hop only).
	Transmission power	2.4GHz : 100 mW EIRP
	Bandwidth	ETSI 13 channels for 2.4 GHz band
Energy	Availability of sources	220V AC power sources
	Type of sources	Infrastructure
	Continuity	100%
	Voltage level	220V AC
	Current level	Capacity is enough to feed a suburban or industrial area.
Topography	Type	Suburban or Industrial
	Scale	

### 3.1.1 Scenario #1 – Circuit breaker trip coil condition active status monitoring

In scenario #1 we consider a sensor and actuator for periodically evaluating the operating status of the circuit breaker trip coil element.



**Figure 3: Trip coil element on circuit breaker**

The trip coil is a fundamental component of the circuit breaker that sometimes breaks down even when under normal use. The trip coil activates the circuit breaker when a 110V DC voltage is applied at its terminals, cutting the energy supply to the power line. It happens that after activating the circuit breaker there is a chance the coil may be damaged and the circuit breaker will not function properly in the next event.

#### *Behaviour*

This scenario aims to check the working status of this component in a pro-active way. A 5V DC voltage will be applied each 60 minutes by an actuator. The magnetic field generated by the coil will be measured by a Hall-effect transistor. In the event of failure, meaning that no magnetic field is detected when a 5V DC voltage is applied, the sensor will report the failure back to the network. The sensor shall also test the coil after a trip. In an activation event, the circuit breaker coil is under an 110V DC voltage for 50 to 150ms, the Hall-effect sensor sampling rate shall be at least half of the shorter time, i.e. at least 25ms. Thus, when the activation of the breaker happens, the sensor detects it and can program an extra test shortly after the activation, checking if the circuit break remains functional for the next time it is called into duty.

The sensor shall also allow for on demand requests for immediately probing the coil and reporting back its status. The sensing and controlling of the trip coil test is done locally. The information sent back to the sink consists only of the test results.

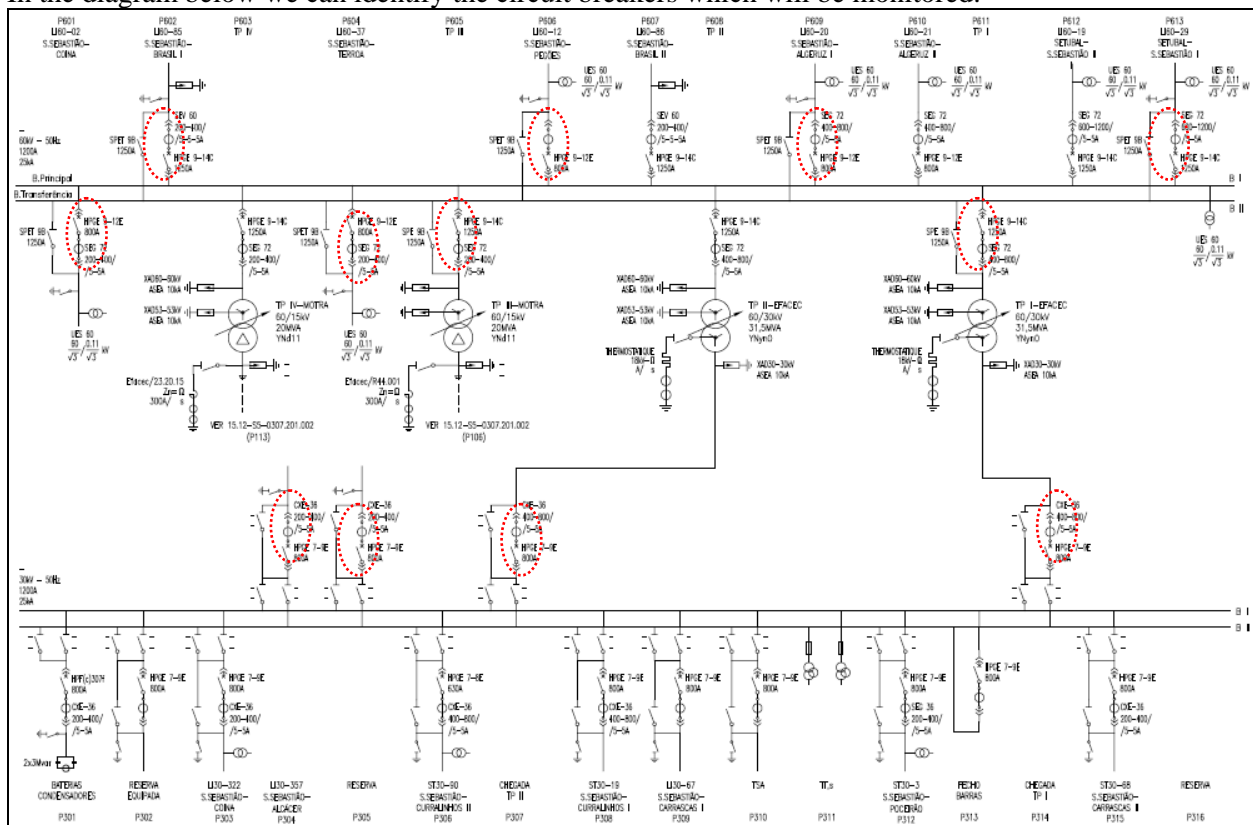
**Table 14. Scenario #1 - Summary of function description**

Function	Type of application	Control loop
	Type of critical data	Data
	Frequency of critical event	1 time per hour
	Data importance class	3
	Data distribution pattern	Sensor-to-Sink and Sink-to-Sensor Unicast
	Reliability type	Readings: Partial (average=80%) Commands: Guaranteed (100%)

**Quantities**

In EDP’s S. Sebastião substation we will monitor twelve (12) out of twenty-four (24) existing circuit breakers (50%).

In the diagram below we can identify the circuit breakers which will be monitored:



**Figure 4: Circuit Breakers under monitoring at S. Sebastião**

The total number of sensors and actuators in scenario #1 is:

- 12x Magnetic field sensors
- 12x 5VDC Power injectors actuators
- 12x 110V to 5V DC/DC converters.

*Network traffic*

The traffic generated by the sensors in this scenario is very low. Given that on demand tests are occasional, most of the messages sent in this scenario are going to be the periodic status information sent by each sensor to the sink/gateway, comprised by:

- 6-byte MAC address for identifying the sensor;
- 1-byte for identifying the type of sensor;
- 1-byte for sending the sensor status.

This gives a total of 8-byte data per sensor and per hour. For the 12 sensors we have a total of 768 bytes per hour. The network latency requirement is low. There is no immediate action that can be taken to solve the problem once it is detected; it requires a scheduled maintenance operation.

*System level performance requirements*

**Table 15. Scenario #1 - System level performance requirements for the application**

<b>Performance domain</b>	<b>Performance metrics</b>	<b>Value</b>
Security	Confidentiality	0
	Integrity	1
	Authentication	1
	Non-repudiation	0
Time	Throughput	1.8 bps (per sensor)
	Jitter	N/A
	Delay	Automatic measurement report: 1 hour On-demand request: 2 s (RTT)
	Fairness index	90%-100% (fair)
Energy	Energy consumption index	≈1W
	Energy consumption pattern	400 mW peaks allowed
Reliability	Packet loss	Readings: 90% within 1 hour Commands: 100% per 2 seconds RTT
	Information integrity	88%
	Degree of autonomy	2 years
	Spatial resolution	1 per monitored device

*Identified parameters of the communication system***Table 16. Scenario #1 - Scenario-specific parameters of communication system**

Part of communication system	Parameters	Values range	Values
Topology	Type	Single cell, mesh, star, tree, etc.	Star or Tree
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	25 / 5.400m <sup>2</sup>
	Number of hops	<MIN(h), NOM(h), MAX(h)>	<1,1,5> (may operate multihop if required)
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity

### 3.1.2 Scenario #2 - Power Transformer oil temperature active monitoring

In scenario #2 we consider using a wireless temperature sensor for monitoring the oil temperature of the Power Transformers. EDP's substation has four (4) Power Transformers; two 60KV/15KV and two 60KV/30KV. Due to the value and importance of these elements to the EDP distribution network the scenario will monitor the temperature of all (100%). A failure on one of the power transformers affects a series of power lines and all the downstream MV/LV Power Stations, meaning thousands of homes and businesses.



**Figure 5: High-Voltage Power Transformer**

#### *Installation*

The temperature sensor probe will be placed in the external side of the metallic oil tank, firmly and thermally attached to the tank external wall. The sensor probe will be isolated from the external environment with thermal foam. The sensor shall be mounted on the north side of the Power Transformer, to avoid exposure to direct sun light and consequent excessive temperatures. The sensor will be driven by a 110VDC power source from the substation DC grid.

#### *Behaviour*

Calibration of the sensor is needed and can be done by locally reading the analogue temperature gauge and the value read by the sensor.

On normal status a measure will be taken every one (1) minute (0,016Hz) but uploaded to the network only every 15 minutes. When reaching a temperature 20% below the alarm threshold of 95°C or when a 1°C or higher increase happens over consecutive readings, the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every one (1) second (1Hz).

The temperature sensor will also allow for on demand temperature reading.

**Table 17. Scenario #2 - Summary of function description**

Function	Type of application	Control loop
	Type of critical data	Data
	Frequency of critical event	1 time per second (peak)
	Data importance class	5
	Data distribution pattern	Sensor-to-Sink and Sink-to-Sensor Unicast
	Reliability type	Guaranteed (minimum=100%)

**Quantities**

This scenario will be comprised of:

- 4x External temperature sensors
- 4x 110V to 5V DC/DC converter

**Network traffic**

The maximum network traffic will occur when uploading temperature readings at 1Hz. Each temperature reading will carry the following data fields:

- 6-byte MAC address for identifying the sensor;
- 1-byte for identifying the type of sensor;
- 4-byte for the temperature reading value.

This data adds to 11-byte payload per reading. At the maximum 1Hz rate, the four (4) sensors will output data at a combined 352bps rate.

**System level performance requirements****Table 18. Scenario #2 - System level performance requirements for the application**

Performance domain	Performance metrics	Value
Security	Confidentiality	0
	Integrity	1
	Authentication	1
	Non-repudiation	0
Time	Throughput	88 bps (per sensor)
	Jitter	N/A
	Delay	< 2 s (RTT)
	Fairness index	90%-100% (fair)
Energy	Energy consumption index	1 W
	Energy consumption pattern	400 mW peaks allowed
Reliability	Packet loss	98% within 2 seconds
	Information integrity	100%
	Degree of autonomy	2 years
	Spatial resolution	1 per monitored device

*Identified parameters of the communication system*

**Table 19. Scenario #2 - Scenario-specific parameters of communication system**

<b>Part of communication system</b>	<b>Parameters</b>	<b>Values range</b>	<b>Values</b>
Topology	Type	Single cell, mesh, star, tree, etc.	Star or Tree
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	4 / 5.400m <sup>2</sup>
	Number of hops	<MIN(h), NOM(h), MAX(h)>	NOM:1 MAX:3
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity

### 3.1.3 Scenario #3 - Neutral Reactance oil temperature active monitoring

In scenario #3 we consider a temperature sensor for monitoring the oil temperature of the Neutral Reactance element. S. Sebastião substation has two (2) Neutral Reactances for phase-earth failures limitation and detection on the 15KV Power Transformers. On a typical failure event this element is under great stress, dissipating 2.6MW of power for as long as 2+2 seconds. If the defect persists the reactance may be under this heavy load several more times in a short period, causing it to overheat and rising the risk of failure to spread to other elements in the failing circuit.

Due to the importance of this element in the detection and prevention of failures on the network and the protection it grants to other equipment (like the Power Transformer), this scenario will monitor the temperature of all (100%) the Neutral Reactances.

Each reactance tank is similar to a Power Transformer tank and the methodology used to monitor its temperature is identical to the previous scenario.



**Figure 6: Reactance tank**

#### *Installation*

The temperature probe will be placed in the external side of the metallic oil tank, firmly and thermally attached to the tank external wall. The sensor probe will be isolated from the external environment with thermal foam. The sensor shall be mounted on the north side of the Neutral Reactance to avoid exposure to direct sun light and consequent excessive temperatures. The sensor will have a 110VDC power source from the substation DC grid.

#### *Behaviour*

The normal operating temperature for the Neutral Reactance is equal to the one of the Power Transformer (95°C).

On normal status a measurement will be taken every one (1) minute (0,016Hz) but uploaded to the network only every 15 minutes. When reaching a temperature 20% below the alarm threshold of 95°C or when a 1°C or more increase on consecutive readings the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every one (1) second, 1Hz.

The sensor will also allow for on demand temperature reading.

**Table 20. Scenario #3 - Summary of function description**

Function	Type of application	Control loop
	Type of critical data	Data
	Frequency of critical event	1 time per second (peak)
	Data importance class	5
	Data distribution pattern	Sensor-to-Sink and Sink-to-Sensor Unicast
	Reliability type	Guaranteed (minimum=100%)

**Quantities**

The total number of sensors in scenario #3 is:

- 2x External temperature sensors
- 2x 110V to 5V DC/DC converter

**Network traffic**

The maximum network traffic will occur when uploading temperature readings at 1Hz. Each temperature reading will carry the next data fields:

- 6-byte MAC address for identifying the sensor;
- 1-byte for identifying the type of sensor;
- 4-byte for the temperature reading value.

This data adds to 11-byte payload per reading. At the maximum 1Hz rate, the two (2) sensors will output data at a combined 176bps rate.

**System level performance requirements****Table 21. Scenario #3 - System level performance requirements for the application**

Performance domain	Performance metrics	Value
Security	Confidentiality	0
	Integrity	1
	Authentication	1
	Non-repudiation	0
Time	Throughput	88 bps (per sensor)
	Jitter	N/A
	Delay	< 2 s (RTT)
	Fairness index	90%-100% (fair)
Energy	Energy consumption index	1 W
	Energy consumption pattern	400 mW peaks allowed
Reliability	Packet loss	98% within 2 seconds
	Information integrity	100%
	Degree of autonomy	2 years
	Spatial resolution	1 per monitored device

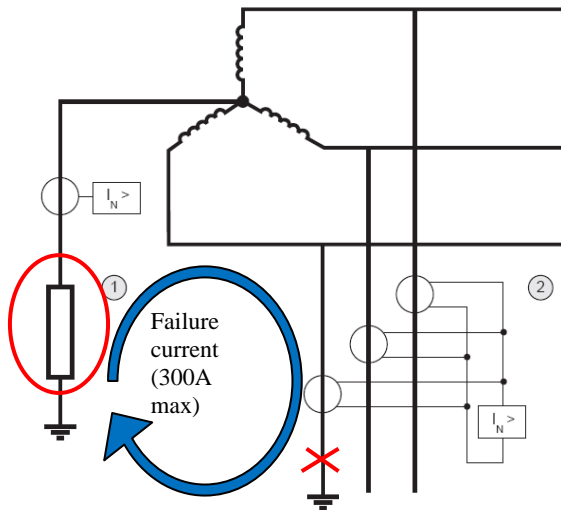
*Identified parameters of the communication system***Table 22. Scenario #3 - Scenario-specific parameters of communication system**

<b>Part of communication system</b>	<b>Parameters</b>	<b>Values range</b>	<b>Values</b>
Topology	Type	Single cell, mesh, star, tree, etc.	Star or Tree
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	2 / 5.400m <sup>2</sup>
	Number of hops	<MIN(h), NOM(h), MAX(h)>	NOM:1 MAX:3
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity

### 3.1.4 Scenario #4 - Neutral Resistor coil box temperature active monitoring

In scenario four we consider a temperature sensor for monitoring the Neutral Resistor coils. EDP’s substation has two (2) Neutral Resistors for phase-earth failures limitation and detection on the 30KV Power Transformers. The Neutral resistor limits the current in a phase-earth failure to 300A. On a typical failure event this element is under great stress, dissipating 5.2MW of power for as long as 2+2 seconds. If the defect persists the Resistor may be under this heavy load several more times in a short period, causing it to overheat and rising the risk of failure.

Due to the importance of this element in the detection and prevention of failures on the network and the protection it grants to other equipment (like the Power Transformer), this scenario will monitor the temperature of all (100%) the Neutral Resistors.



**Figure 7: Neutral Resistor circuit with failure**



**Figure 8: Neutral Resistor box**

#### *Installation*

Each Neutral Resistor box has 4-5 coils inside. An internal temperature probe shall be placed inside the Neutral Resistor box, near the top where the temperature rises quicker. An external temperature probe is needed for comparison and shall be placed on the outside of the box, in the north facing side and out of direct sun light.

#### *Behaviour*

The normal operating temperature should be the outside environment temperature, because at normal operation the potential is 0V, hence no current is flowing through the Neutral Resistor and no power (heat) is being dissipated.

On normal status a measurement will be taken every thirty (30) seconds (0,032Hz) but uploaded to the network only every 15 minutes. When reaching a temperature 20% above the external temperature or when a 1°C or more increase happens over consecutive readings the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every one (1) second (1Hz). Compensation may be needed for day-night-day shifts where the temperature inside the box may drop slowly or raise sharply triggering false alarms.

**Table 23. Scenario #4 - Summary of function description.**

Function	Type of application	Control loop
	Type of critical data	Data
	Frequency of critical event	1 time per second (peak)
	Data importance class	5
	Data distribution pattern	Sensor-to-Sink and Sink-to-Sensor Unicast
	Reliability type	Guaranteed (minimum=100%)

**Quantities**

The total number of sensors in scenario #4 is:

- 2x External temperature sensors
- 2x 110VDC to 5VDC DC/DC converter

**Network traffic**

The maximum network traffic will occur when uploading temperature readings at 1Hz. Each temperature reading will carry the following data fields:

- 6-byte MAC address for identifying the sensor;
- 1-byte for identifying the type of sensor;
- 4-byte for the temperature reading value.

This data adds to 11-byte payload per reading. At the maximum 1Hz rate, the two (2) sensors will output data at a combined 176 bps rate.

**System level performance requirements****Table 24. Scenario #4 - System level performance requirements for the application**

Performance domain	Performance metrics	Value
Security	Confidentiality	0
	Integrity	1
	Authentication	1
	Non-repudiation	0
Time	Throughput	88 bps (per sensor)
	Jitter	N/A
	Delay	< 2 s (RTT)
	Fairness index	90%-100% (fair)
Energy	Energy consumption index	1 W
	Energy consumption pattern	400 mW peaks allowed
Reliability	Packet loss	98% within 2 seconds
	Information integrity	100%
	Degree of autonomy	2 years
	Spatial resolution	1 per monitored device

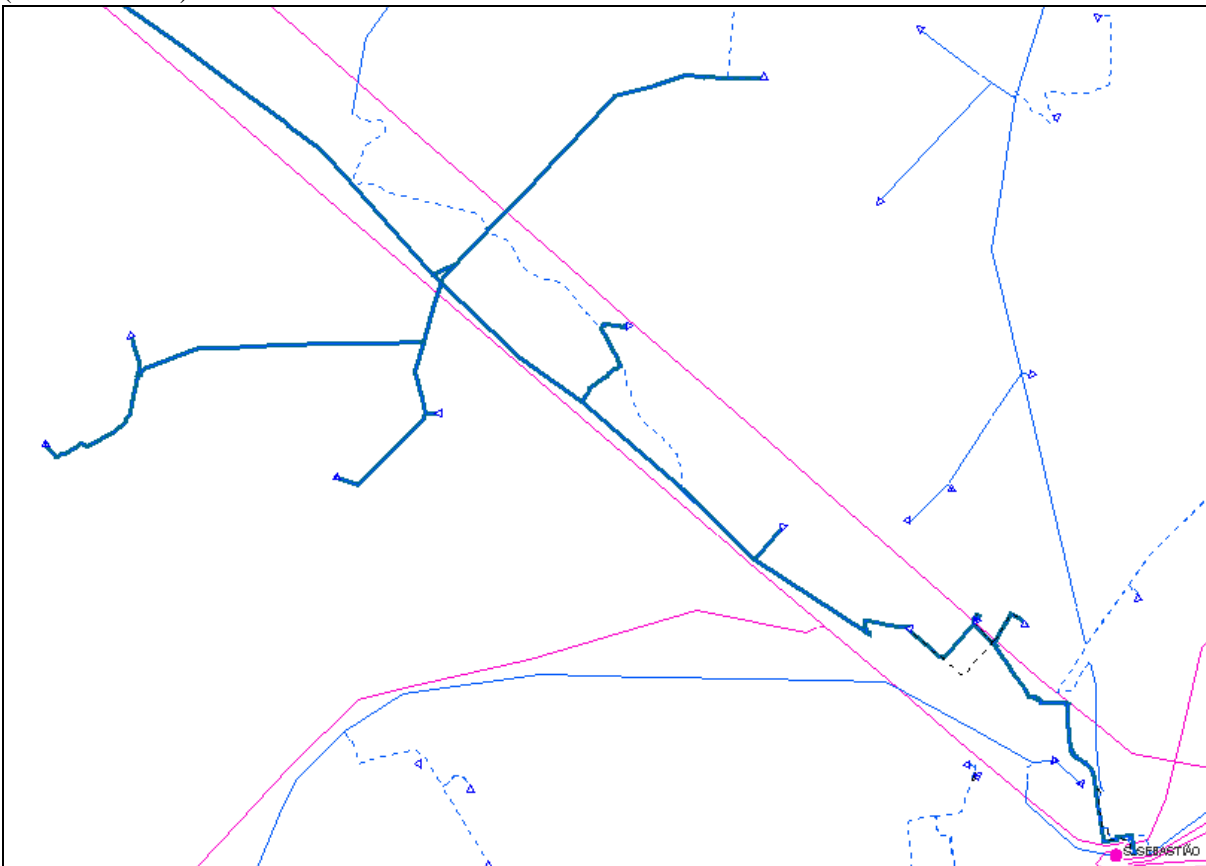
*Identified parameters of the communication system*

**Table 25. Scenario #4 - Scenario-specific parameters of communication system**

<b>Part of communication system</b>	<b>Parameters</b>	<b>Values range</b>	<b>Values</b>
Topology	Type	Single cell, mesh, star, tree, etc.	Star or Tree
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	2 / 5.400m <sup>2</sup>
	Number of hops	<MIN(h), NOM(h), MAX(h)>	NOM:1 MAX:3
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity

### 3.1.5 Scenario #5 - Power line current active monitoring per tower and per phase

The scenario presented here aims to monitor the status of a Medium-Voltage (MV) power line section, stretching from S. Sebastião substation to several MV/LV Power Stations in the vicinity of the substation (less than 5Km)<sup>2</sup>.



**Figure 9: S. Sebastião power line section (bold blue line) under surveillance**

The power line chosen is a medium voltage 15KV line that feeds a set of urban and suburban MV/LV Power Stations in the city of Setubal. The line topology is a tree shape with several branch levels, the leaves being the MV/LV Power Stations.

The power cable paths are not always aerial, in fact, in some segments the cables are buried underground, especially when the line crosses urban areas. This could pose a challenge to the wireless communications since the distance from one tower to the next could be too big for the wireless technology or line-of-sight is not available. Nevertheless, when we have a buried segment we also have a MV/LV Power Station house where a router node can be safely mounted on the outside for data routing purposes only, bridging the gap between consecutive towers.

#### *Installation*

The physical measurement to be taken is the electrical current flowing through the line (phase), a current transformer shall be used to measure its value and to derive a parasitic power source for the wireless sensor, eliminating the need for batteries on the sensor and at the same time posing no power constraints on the wireless protocols.

Each tower carries three (3) 15KV power lines (phases) in parallel, and each one needs its own sensor. We propose to monitor eighteen (18) aerial towers, and three (3) phases. Therefore, we will be placing two (3) current sensors on each tower to a total of 54 sensors. We also need three (3) router nodes for bridging buried segments along the line. These router nodes shall be installed in the outside of MV/LV Power Stations located between towers. The router shall be placed in high ground or at the end of a pole if more elevation is needed, to achieve line-of-sight to the next node site.

The diagrams below show the line segments proposed in the scenario:

<sup>2</sup> The precise location and number of towers is still under study by INOV and EDP.

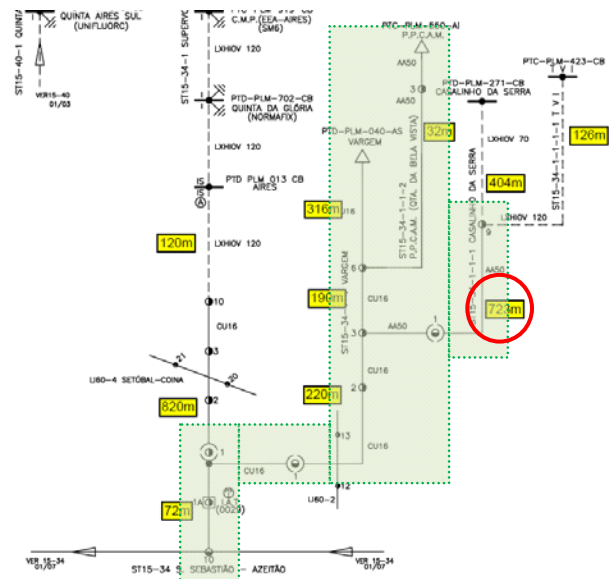
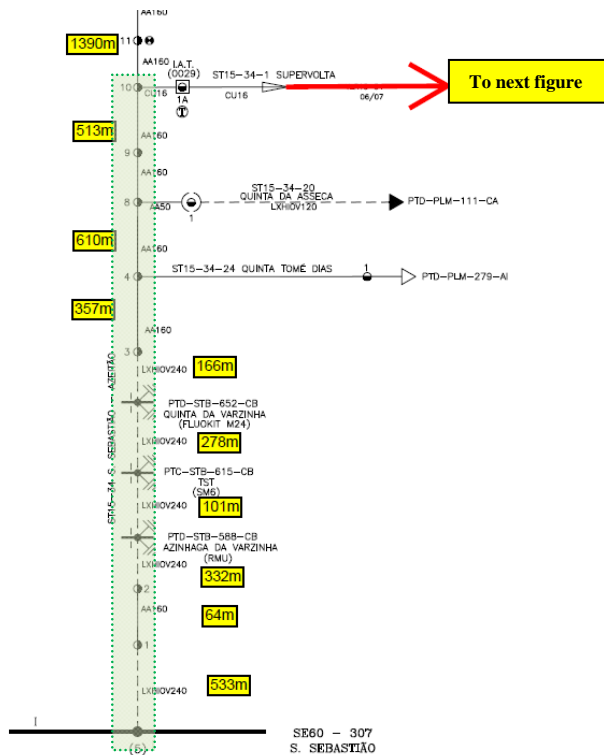


Figure 10: Main line under surveillance.

Figure 11: Line branch under surveillance.

The maximum distance between towers is 723 meters (Figure 11: Line branch under surveillance), requiring great care in the antenna choice for the sensor since contradictory requirements apply:

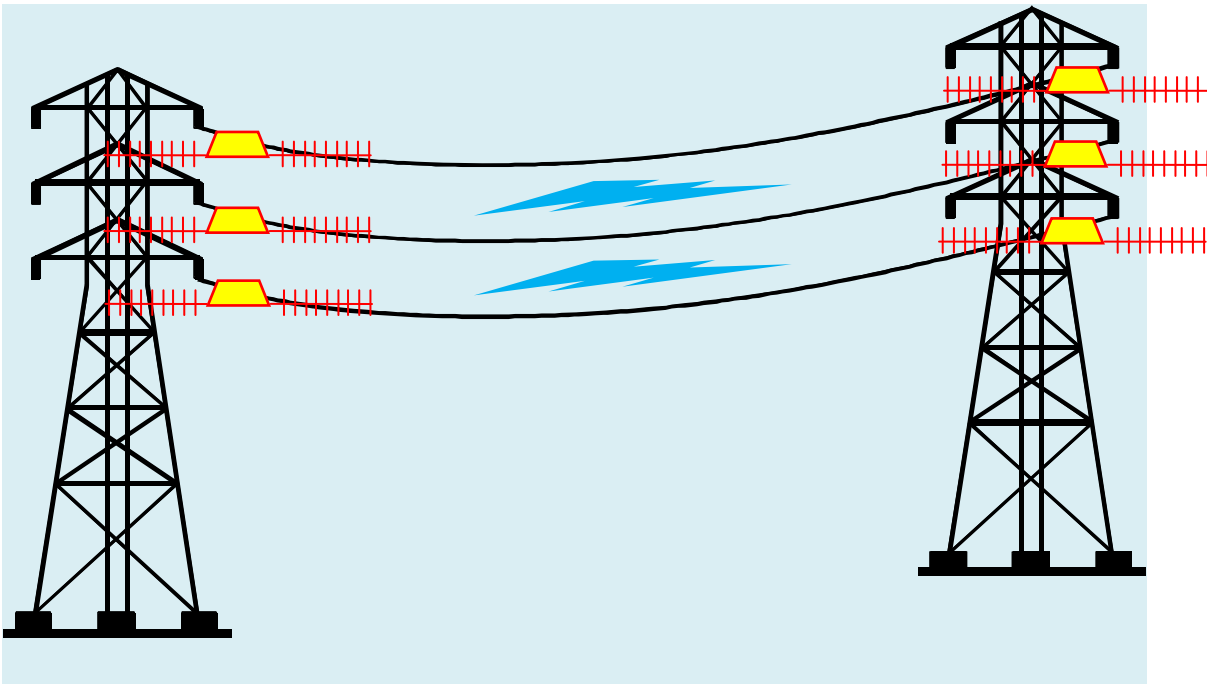
- It should be directional for increased gain and range (ex. yagi);
- It must run parallel to the power cable and should not be orthogonal to it;
- It must be small for installation easiness.

**Behaviour**

The current sensor shall sample the current on the line each 1s. The use of data aggregation techniques is still under discussion.

Table 26. Scenario #5 - Summary of function description

Function	Type of application	Surveillance
	Type of critical data	Data
	Frequency of critical event	100 Hz (peak)
	Data importance class	4
	Data distribution pattern	Sensor-to-Sink Unicast/Convergecast
	Reliability type	Guaranteed (minimum=80%)



**Figure 12: Power tower current sensor**

#### *Quantities*

The total number of sensors in scenario #6 is:

- 54x MV current sensors
- 3x Router nodes with AC power supply or PoE

#### *Network traffic*

Each data sample shall carry this data fields:

- 6-byte MAC address for identifying the sensor;
- 4-byte for the current reading value;
- (optional) 4-byte temperature reading value.

The network traffic generated by this scenario depends on the data upload policy. Sending all (1Hz) the collected samples (10-byte) translates to 8.0 bps per tower per line. Given the tree shape of the network, the last tower before the network sink would aggregate all the traffic generated in the tree. The wireless technology must accommodate for this.

*System level performance requirements***Table 27. Scenario #5 - System level performance requirements for the application**

Performance domain	Performance metrics	Value
Security	Confidentiality	1
	Integrity	1
	Authentication	1
	Non-repudiation	1
Time	Throughput	8.0 bps (per tower)
	Jitter	N/A
	Delay	10 s
	Fairness index	90%-100% (fair)
Energy	Energy consumption index	200 mW
	Energy consumption pattern	400 mW peaks allowed
Reliability	Packet loss	80% within 10 seconds
	Information integrity	85%
	Degree of autonomy	10 years
	Spatial resolution	Per tower line

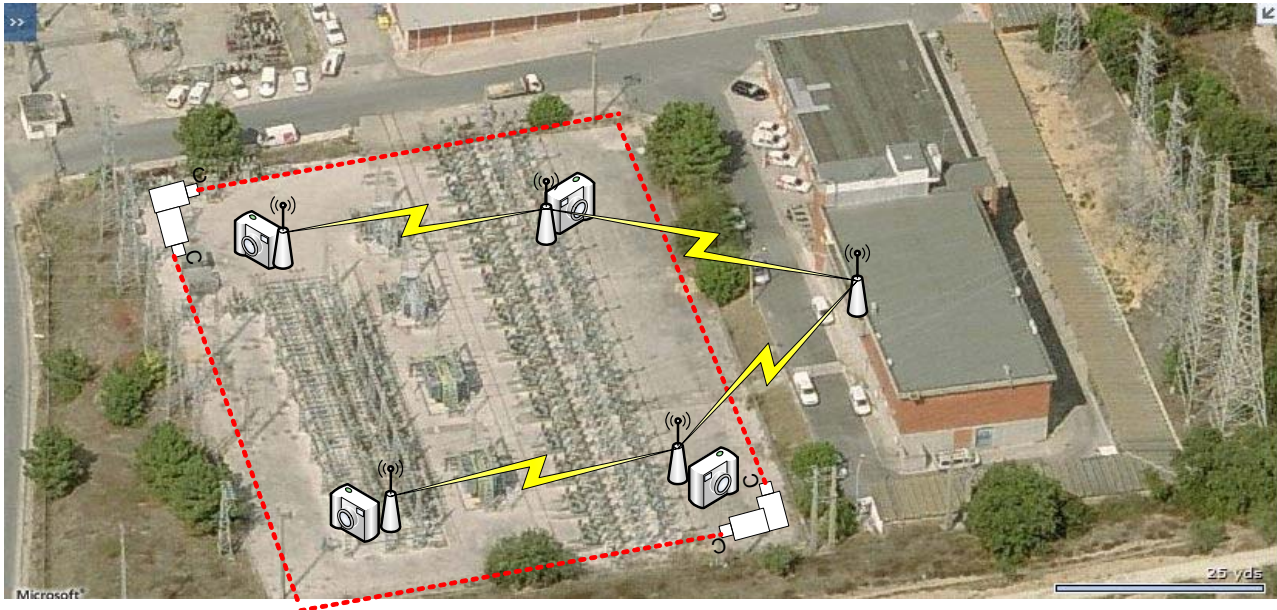
*Identified parameters of the communication system***Table 28. Scenario #5 - Scenario-specific parameters of communication system**

Part of communication system	Parameters	Values range	Values
Topology	Type	Single cell, mesh, star, tree, etc.	Tree
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	Low area density, 1-5 nodes/km
	Number of hops	<MIN(h), NOM(h), MAX(h)>	MAX:50
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity, confidentiality, non-repudiation

**3.1.6 Scenario #6 - perimeter unauthorized intrusion detection**

Scenario #7 of the EDP demo is quite different from the previous ones. It aims to maintain the substation premises secured against trespassers by detecting its presence and providing a video feed that can be served to a mobile or fixed terminal of security personnel.

Movement detectors will be used to infer the area where the intrusion is taking place. For example, a couple of sensors placed at diagonally opposed corners of the substation square (e.g. PIR or laser detectors), monitoring two orthogonal sides of the fence, can detect an intrusion from any direction and eventually measure the distance to the intruder (e.g. laser detector). The sensor can then quickly send an alarm to the network and sharply point its camera to the hot area.



**Figure 13: Perimeter surveillance.**

*Behaviour*

While no intrusion is detected, the movement detectors send keep-alive messages every five (5) seconds. Once an intruder is detected by a movement sensor, an alarm message is sent and one or more cameras are activated and start to transmit the video stream to the control center. The cameras can also be controlled remotely from the control centre.

**Table 29. Scenario #6 - Summary of function description**

Function	Type of application	Surveillance
	Type of critical data	Data + Video
	Frequency of critical event	0.2 Hz while idle, continuously during intrusion situation
	Data importance class	5
	Data distribution pattern	Sensor-to-Sink and Sink-to-Sensor Unicast
	Reliability type	Data: Guaranteed (minimum=100%) Video: Guaranteed (minimum=98%)

### Quantities

The major hardware items in this scenario are:

- 4x Outdoor Point-Tilt-and Zoom (PTZ) cameras
- 4x Outdoor Single Board Computers (SBC) with wireless communications.
- 4x Motion detectors

### Network traffic

The IP based cameras with MPEG-4 codecs will generate bitrates up to 768Kbps (CIF 352x288 at 15 frames/sec, according to the MPEG-4 Advanced Simple Profile). The MPEG-4 profile most suitable is the ASP with a reduced compression level.

### System level performance requirements

**Table 30. Scenario #6 - System level performance requirements for the application**

Performance domain	Performance metrics	Value
Security	Confidentiality	1
	Integrity	1
	Authentication	1
	Non-repudiation	1
Time	Throughput	768Kbps (per camera)
	Jitter	200 ms
	Delay	3 s
	Fairness index	Alarm data is more important
Energy	Energy consumption index	200 mW
	Energy consumption pattern	10 W peaks tolerated
Reliability	Packet loss	Data: 90% within 3 seconds Video: 95% within 3 seconds
	Information integrity	Data: 100% Video: 98% per frame <sup>3</sup>
	Degree of autonomy	2 years
	Spatial resolution	To be defined

<sup>3</sup> See ITU-T G.1070 recommendation.

*Identified parameters of the communication system***Table 31. Scenario #6 - Scenario-specific parameters of communication system**

Part of communication system	Parameters	Values range	Values
Topology	Type	Single cell, mesh, star, tree, etc.	Star
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	4 / 5.400m <sup>2</sup>
	Number of hops	<MIN(h), NOM(h), MAX(h)>	1 (may operate multihop if required)
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity, confidentiality, non-repudiation

### 3.1.7 Scenario #7 - MV/LV power station video surveillance and hotspot detection

In this scenario we propose the use of the wireless communications link build in scenario #6 to upload a video/image feed of the MV/LV Power Station house interior to the network. At the same time an infrared thermo sensor attached to the camera will sweep the Power Station critical elements, like the main switch board, for hotspots. The detection of a hotspot will trigger an alarm to the network.

This scenario also includes an actuator. The remote user shall be able to turn on the lights on the MV/LV power station house. Thus, albeit the camera shall be night and day capable, the user can get a better and coloured video stream even at night, improving on the black-and-white stream available in night mode. This feature improves the remote MV/LV power station physical security.



**Figure 14: MV/LV power station main switch board.**

#### *Behaviour*

While no intrusion or hotspot is detected by the infrared sensor, the latter sends a keep-alive messages every five (5) seconds. Once an event is detected by the infrared sensor, the latter starts sending alarms every 1 second and the camera is activated, transmitting the video stream to the control center. The lights can also be controlled remotely from the control center.

**Table 32. Scenario #6 - Summary of function description**

Function	Type of application	Surveillance
	Type of critical data	Data + Video
	Frequency of critical event	0.2 Hz while idle, continuously during an event situation
	Data importance class	5
	Data distribution pattern	Sensor-to-Sink and Sink-to-Sensor Unicast
	Reliability type	Data: Guaranteed (minimum=100%) Video: Guaranteed (minimum=98%)

### *Quantities*

The major hardware items in scenario #8 are:

- 1x indoor PTZ camera
- 2x AC/DC PSU
- 1x Indoor sensor unit
- 1x Infrared thermo probe.

### *System level performance requirements*

**Table 33. Scenario #6 - System level performance requirements for the application.**

Performance domain	Performance metrics	Value
Security	Confidentiality	1
	Integrity	1
	Authentication	1
	Non-repudiation	1
Time	Throughput	768Kbps peak (per camera)
	Jitter	200 ms
	Delay	10 s
	Fairness index	Alarm data is more important
Energy	Energy consumption index	200 mW
	Energy consumption pattern	10 W peaks tolerated
Reliability	Packet loss	Data: 90% within 10 seconds Video: 95% within 10 seconds
	Information integrity	Data: 100% Video: 98% per frame <sup>4</sup>
	Degree of autonomy	5 years
	Spatial resolution	Power Station area: 5-15 m <sup>2</sup> (1 sensor node is enough) Note: Data transmission shall be done using the network implemented in Scenario 5.

<sup>4</sup> See ITU-T G.1070 recommendation.

*Identified parameters of the communication system*

**Table 34. Scenario #6 - Scenario-specific parameters of communication system.**

Part of communication system	Parameters	Values range	Values
Topology	Type	Single cell, mesh, star, tree, etc.	Star
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	Sensor nodes: Very low Relay nodes (power distribution lines): Low area density, 1-5 nodes/km
	Number of hops	<MIN(h), NOM(h), MAX(h)>	MAX:51
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	High-energy only
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	MAX(TX)=400 mA * 3.3 V MAX(RX)=200 mA * 3.3 V MAX(Listen)=200 mA * 3.3 V
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services		Authentication, integrity, confidentiality, non-repudiation

### 3.2 Site 2 description

The FWA demonstrator concerns the fail-safe and secure data transmission for monitoring operation of water mains. Between the waterworks in Briesen and the elevated tank in Rosengarten are laid two parallel water pipes over a total length of 17,5 km. Modern protection on pipe bursts, flow rate and pressure measuring devices are build in four special stations along the pipes and permitting optimal operating and monitoring. For realizing necessary functions all components are integrated in the central process management system for supervisory control and data acquisition every 30 seconds.

#### Installation

The five measurement-delivering nodes are aligned in a line along the pipe. The distance between the nodes is up to 5km. Figure 15 illustrates the pipe and the position of its access points on an environmental map.



**Figure 15: Map of the FWA demonstrator with position of the measuring nodes. Data should be delivered to the top right FWA head station.**

In a physically protected environment (locked building, fence) each of the access points provides data (pressure, flow) as analogue data (4-20mA). These values will be gathered and transmitted by one of the measurement-delivering nodes. In the building power line supply is available.

Intermediate network forwarding nodes can be placed between the measuring nodes to reduce the hop-by-hop communication distance. The intermediate nodes will be deployed on open field and they are not physically protected. Due to the lack of infrastructure the rely nodes depend on battery power.

**Table 35. Classification of critical environmental parameters**

Class	Parameters	Value
Physical security	Access control	Sensors and measuring nodes are physically protected (inside a building) Rely-nodes are on open field only protected by their node housing
	Physical surveillance	Building for sensors is locked, no other protections or surveillance
	Tamper resistance	Tamper evidence
Radio	Degree of interference	[2] On open field low, close to villages interferences even broad band and over long time (e.g. baby phones) are possible.
	Propagation of radio signal	Open Space, with trees and hills and some buildings
	Transmission power	500mW max total (including antenna amplification)
	Bandwidth	25 kHz per channel, 250kHz max, 10% duty time
Energy	Availability of sources	240V power supply + UPS at measurement nodes Space for large batteries for network nodes
	Type of sources	Infrastructure, battery
	Continuity	<5% duty time
	Voltage level	3V
	Current level	Up to 1.0 Ampere (sending with 500mW)
Topography	Type	Tree
	Scale	Line, 17.5km, Sparse

### 3.2.1 Scenario description

It is important to note that the number of CIP applications specified for this installation site is less than that for the installation sites described in the previous section. This is due to specific requirements of the owner of the installation site.

#### *Behaviour*

Primary objective is the delivery of measured data from the measurement points to the head station every 30 seconds. Optionally an asynchronous alarm should forward directly in case critical situations are detected on sensor side.

Additionally each node should be accessible for maintenance and service requests for parameterisation and status requests. Such requests are initiated from the network head. To improve usability answering time should be reasonably low. A special maintenance use case is the remote code update of the nodes. Then partial or full code images should be transferred from head to the nodes using the network.

#### *Quantities*

The total number of nodes in this scenario is:

- 5x Data-collecting nodes with A/D-converter for the sensor signals and 220VDC power supply
- up to 8x packet forwarding nodes, battery-powered

**Network traffic**

The network traffic depends on the task the network performs.

For the default periodic data collection each sensor has to send measured values every 30 seconds. Payload will be about 20 bytes. Due to forward error correction and protocol overhead the actual traffic will be about 100 bytes. Considered the bytes are forwarded through the entire network for all 5 data collecting nodes the total network load will be 5 sensor nodes x 10 intermediate nodes x 100 bytes → 5000 Bytes/30 sec

Maintenance data are rather small packets: one from the head station to the node and one back to the head. Even with network overhead the resulting traffic is smaller than 1000 Bytes per request total network load.

Code update is a uni-directional data stream from the head to the nodes. The total data amount can be up to 100 kBytes. Since time requirements are low, the data can be sent with residue band with. Forwarding through the entire network, the total network load will be 11x100kBytes/15 minutes.

**Table 36. Summary of function description**

Function	Type of application	Surveillance, control loop
	Type of critical data	Data
	Frequency of critical event	N.A.
	Data importance class	3
	Data distribution pattern	Converge cast for sensed data Unicast for service requests Multicast for code update
	Reliability type	Partial, 98% per month

**System level performance requirements****Table 37. System level performance requirements for FWA CIP application**

Performance domain	Performance metrics	Value
Security	Confidentiality	1
	Integrity	1
	Authentication	1 (derived from the high integrity requirement)
	Non-repudiation	1
Time	Throughput	1 kB/s
	Jitter	not critical
	Delay	<2 seconds end to end
	Fairness index	90-100% while respecting packet priorities
Energy	Energy consumption index	50 mWh per hour
	Energy consumption pattern	peaks with up to 500mW
Reliability	Packet loss	98% per month
	Information integrity	99.9999% (1 per 1 mio packets may be wrong)
	Degree of autonomy	3 Months
	Spatial resolution	1

**Table 38. Scenario-specific parameters of communication system**

<b>Part of communication system</b>	<b>Parameters</b>	<b>Values range</b>	<b>Values</b>
Topology	Type	Single cell, mesh, star, tree, etc.	Tree
	Density of nodes	<MIN(r), NOM(r), MAX(r)>	<5;8;12>
	Number of hops	<MIN(h), NOM(h), MAX(h)>	<4;8;12>
Hardware	Heterogeneity	Low-energy only, high energy only, mixed, etc.	Equal hardware, Mixed sensors, mixed power supply
	Power consumption for communication activities for every used technology.	<MIN(TX), NOM(TX), MAX(TX)>; <MIN(RX), NOM(RX), MAX(RX)>; <MIN(Listen), NOM(Listen), MAX(Listen)>	Send: <0.1W,3W,5W> Listen: <0.1W,0.2W,0.2W>
	Sensitivity threshold	<MIN(SNR), NOM(SNR), MAX(SNR)>	N/A
	Security services	Confidentiality, integrity, authentication, non-repudiation	ALL

## 4 Summary

Deploying WSA in the control loop of critical infrastructures adds another level of complexity and a point of failure. Developing communication system for applications related to protection of critical infrastructures (CIP) is a complex process which demands systematic approach starting from early design stages. Being able to correctly identify critical for particular CIP system performance metrics and the factors that affect their behavior is essential for the design of the *dependable* communication systems.

In this document we described a methodology for identification of critical performance parameters through performing multidimensional tomography of the particular installation site and envisioned CIP application. We identified critical parameters in radio, energy, time, reliability, and security domains.

Being equipped with the presented methodology a developer has means to systematically analyse critical parameters of the future application. These parameters are further formulated as application requirements on the protecting ICT system. When selecting hardware and software components according to the parameters of the site and the application a new set of parameters critical for system performance is introduced. This time it is parameters of the functional blocks of the communication system itself (topology, selected hardware, software components).

We applied the developed methodology for the site and application assessment on samples of particular CIP applications. We focused on the CIP scenarios which further will be adopted for the project demonstrators.

## References

- [1] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Delay Metric for IPPM. RFC 2679, 1999.
- [2] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way packet loss for IPPM. RFC 2680, 1999.
- [3] G. Almes, S. Kalidindi, and M. Zekauskas. A round trip Delay Metric for IPPM. RFC 2681, 1999.
- [4] C. Demichelis and P. Chimento. IP Packet Delay Variation Metric for IP Performance Metrics IPPM. RFC 3393, November 2002.
- [5] R. Koodli and R. Ravikanth. One-way Loss Pattern Sample Metrics. RFC 3357, August 2002.
- [6] J. Mahdavi and V. Paxson. IPPM Metrics for Measuring Connectivity. RFC 2678, 1999.
- [7] M. Mathis and M. Allman. A Framework for Defining Empirical Bulk Transfer Capacity Metrics. RFC 3148, July 2001.
- [8] A. Morton, L. Ciavattone, G. Ramachandran, S. Shalunov, and J. Perser. Packet Reordering Metrics. RFC 4737, November 2006.
- [9] Miguel Castaño and Wolfgang Birk. New methods for structural and functional analysis of complex processes. In To be presented at the IEEE Multiconference on Systems and Control, in St. Petersburg, 2009.