D3.3 Preliminary Pilot III Integration: Air Quality Monitoring System use case.

WP 3. Integration of CIPSEC solution to transportation, health and environment pilots

CIPSEC

Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 31-October-2017

Actual submission date: 31-October-2017

HORIZON 2020. WORK PROGRAMME 2014 – 2015			Project No 700378
Call			Instrument Innovation action
Digital Security: Cybersecurity, Privacy and Trust			Start date May 1st, 2016
Secure societies. Protecting freedom and security of Europe and its citizens			Duration 36 months
DS-03-2015: The role of ICT in Critical Infrastructure Protection			Website www.cipsec.eu
Public	Confidential	Classified	Lead contractor Atos Spain S.A.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

This deliverable has been endorsed by Security Advisory Board.

Document contributors

Editor	Barbara Lunel (CSI)	
Contributors		**Reviewers**
Ilias Spais	AEGIS	
Antonio Álvarez, Joaquín Rodríguez, Rubén Trapero	ATOS	
Ciprian Oprisa	BD	
	COMSEC	
Barbara Lunel, Isabella Vespa, Vittorio Vallero, Francesca Raimondi	CSI	
	DB	Dominik Renkel, Christian Schlehuber
Panagiotis Sifniadis	EMP	
Christos Papachristos, Sotiris Ioannidis, Manos Athanatos	FORTH	Manos Athanatos
	HCPB	
	TUD	
Xavi Masip	UPC	
Apostolos Fournaris	UOP	
Carlos Valderrama	WOS	

Document history

Version	Date	Author	Notes
0.1	07-04-2017	Joaquín Rodríguez (ATOS), Antonio Álvarez (ATOS), Barbara Lunel (CSI), Isabella Vespa (CSI), Vittorio Vallero (CSI)	Preliminary Table of Contents and comments
0.2	11-07-2017	Antonio Álvarez (ATOS), Joaquín Rodríguez (ATOS), Carlos Valderrama (WOS), Apostolos Fournaris (UOP) Panagiotis Sifniadis (EMP) Ciprian Oprisa (BD), Xavi Masip (UPC), Sotiris Ioannidis (FORTH)	Input to section 2 on defining the elements of a robust security solution for the environmental pilot
0.3	11-07-2017	Antonio Álvarez (ATOS), Joaquín Rodriguez (ATOS), Carlos Valderrama (ATOS), Apostolos Fournaris (UOP), Christos Papachristos (FORTH), Panagiotis Sifniadis (EMP), Ciprian Oprisa (BD),	

		Ilias Spais (AEGIS)	
0.4	17-07-2017	Apostolos Fournaris (UOP), Manos Athanatos (FORTH)	Input to section 2
0.5	02-08-2017	Rubén Trapero (ATOS), Antonio Álvarez (ATOS)	Slight modification to section 2 approach
0.6	09-08-2017	Antonio Álvarez (ATOS)	Minor update in section 3
0.7	10-08-2017	Antonio Álvarez (ATOS)	Minor updates
0.8	28-08-2017	Barbara Lunel (CSI)	Input to section
0.9	11-09-2017	Barbara Lunel (CSI)	Minor updates
1.0	20-09-2017	Barbara Lunel (CSI)	Added contributions of: FORTH, EMP, ATOS,UOP,UPC,AEGIS, WOS
1.1	10-10-2017	Barbara Lunel (CSI)	Modified diagram and general review
1.2	22-10-2017	Barbara Lunel (CSI)	General review
1.3	31-10-2017	ATOS	Quality check

Index

Glossary

AQDRS	Air Quality Detection Regional System
ARPA	Agenzia Regionale per la Protezione Ambientale. Regional Agency for the Environmental protection
NetApp SAN	NetAPP Storage Area Network
RUPAR	Rete Unitaria della Pubblica Amministrazione del Piemonte o Unitary net of the Public Administration of the Piedmont
OC	Operations Centre

1 Executive summary

In the CIPSEC project the Task 3.3 aims to integrate the CIPSEC framework into an air quality domain CI. The implementation will take place through the close collaboration between CSI and ARPA and the solution providers and related services that are part of the CIPSEC consortium. This report will describe the steps needed to get the preliminary integration.

Project partners have offered their top solutions that, conceived for specific security issues, play their role in contexts and scenarios that are very different from each other and are not specifically designed for our Pilot. The hypothesis of using a part or all of the tools proposed is linked to a deepening of the characteristics of the Environmental Pilot and an overview is required that facilitates the specific vision that suits our scenario.

The Air Quality Analysis and Monitoring is becoming ever more important as pollution-related phenomena are closely linked to public health. As a result of exceeding the thresholds for polluting elements (eg pm10), restrictive measures have been taken to the movement of private means as well as the temperature of buildings and the technology used for heating.

The Regional Air Quality Detection System deals with the management and coordination of air quality monitoring systems in the Piedmont Region, which is an integrated system that enables the centres to acquire data from stations, applications, application services, Internet sites designed for planning, managing, communicating and disseminating environmental data.

The communication technologies used by the stations are different, depending partially on the historical period in which the station was installed and by the nature of the station itself of which:

56 are fixed stations that have different connection types, 38 using ISDN connectivity, 2 using the ADSL, 10 using a 3G connection, while the mobile stations are still 6 of the 3G type and are used for extraordinary campaigns or in emergency situations such as forest fires or fires of industrial structures or in case of outbreaks of toxic substances.

The assessment of air quality is useful to ensure the protection of the health of the population and the protection of ecosystems.

This evaluation is conducted through:

- continuous monitoring of the most significant pollutants;
- estimation of the spatial distribution of pollutants through modelling of dispersion, transport and transformation into atmosphere.

The integration of measured data from the monitoring network with those estimated through the dispersion models provides information on the levels of air quality with a great spatial and temporal detail across the regional territory. Data estimated through the models, besides producing useful elements for describing the levels of pollution even in areas not covered by the monitoring network, allow to estimate the possible impacts on air quality resulting from variations in the emissivity framework such as, for example, new production facilities, modification of the car park or use of new fuels.

Pollutants can originate from productive activities, and more generally human, or derive from natural phenomena. Atmospheric pollutants can be classified as:

PRIMARY: their presence in the environment is directly derived from a specific emission, for example carbon monoxide comes directly from incomplete combustion of carbon compounds (e.g. fuels or wood);

SECONDARY: their production comes only from transformations of compounds that can be of natural origin or anthropic; for example, ozone is a typical example of secondary pollutant.

There are also pollutants, such as particulate PM10 or PM2.5, whose components can be variable primary and secondary.

The detected environmental data reach central systems on which are analyzed, validated and finally published on the portal of the public administration.

Based on the characteristics of the air quality detection infrastructure and with the aim of securing the infrastructure, a framework has been defined that may include certain peculiarities of the Environmental Pilot and can be extended to any similar critical infrastructure.

The various solutions that make up CIPSEC could facilitate network management by securing transmitted data, controlling access to stations or applications, and verifying the integrity of data in central and peripheral data banks.

Proposed solutions include SIEM, a virtualized version of Honeypot, the HSM system for data encryption, an intrusion detection system on wireless networks, and the use of antivirus.

The expected capabilities of the CIPSEC solution will soon be released and will be available to be deployed in environmentally-friendly environments for infrastructure testing.

2 Introduction

WP3 deals with the adaptation of the CIPSEC security framework into the pilots that participate in the project. In particular, it deals with the adaptation of the reference security architecture design defined in Task 2.1, part of WP2, by the Environmental monitoring Critical Infrastructure. WP3 aims at applying three specific security enhancing solutions with capabilities to improve the resilience of each of the respective critical infrastructures. The outcomes of WP3 are to be tested in the context of WP4 in a clear interplay between the two WPs.

This deliverable reports the work done in the Italian environmental monitoring pilot, in the context of Task 3.3, from the beginning of the task (M10, February 2017) to the release of the document (M18, October 2017).

To produce the present report, a methodology has been introduced with a sequence of steps being followed. This workflow is replicated in the document structure:

1) Understanding the pilot. The documentation generated in the context of WP1 and reflected in D1.2 is revisited and the most important aspects of the pilot are highlighted (see section 3.1)
2) A list of security features is accurately defined. Then, for each security feature, the product owners describe how their tools can provide each one (provided that the proposed tools can do so). This is done in section 3.2.
3) Then, the pilot owners select the security features that are applicable to them based on their respective devices / resources, justifying their choice (see section 3.2).
4) In the next step it is expected that partners, in response to the choices and needs of each single Pilot, will provide the most appropriate security features; (see the table in section 3.3). This is the result of the pilot choices and the analysis of the partners. Solution providers with prospective participation in the environmental pilot, will be presented in paragraph 3.3, each one within a specific subsections.
5) Through the coverage analysis and the security features provided by each security solution, the pilot owner can choose which products are to be used to secure the critical infrastructure in question (see section 3.4).
6) An introduction to the actual Air Quality System and a description of the preliminary efforts carried out to integrate the CIPSEC framework into Pilot III (section 4.1) is presented.
7) The solutions' providers specify the hardware and software requirements of each product (presented in section 4.2).
8) Then the pilot analyses the feasibility of using the products on the infrastructure in question, according to the specs obtained in the previous steps. In the event that some of the products that are part of the framework proposed by the Consortium have characteristics that are not adaptable to the Pilot Infrastructure, it may be necessary to get it out of the solution and look for an alternative if the intended security features were not covered as a result of the exclusion. As a next step, the pilot proceeds to adapt their infrastructure to accommodate the solutions. This includes OS updates and the definition of a virtual test environment (see section 4.3)
9) Subsequently, the pilot produces the final detailed definition of the infrastructure map with all the associated technical details (see section 4.4).
10) Then both pilot and providers work together to determine how and where the different selected products are going to be deployed within the pilot infrastructure (see section 4.5).
11) Finally, the connection between the final deployment and the reference architecture is documented, as well as the role of the CIPSEC services in the pilot is addressed (see section 4.6).

3 Defining the elements of a robust security solution for the environmental pilot

3.1 Understanding the pilot

D1.2 offers an extensive and detailed description of the environmental pilot. This chapter offers a summary of that description, highlighting its most relevant aspects and linking with its main security needs, which act as input to define the security requirements for the different assets of the pilot.

In the context of WP1, a fine-grain scenario breakdown was obtained as a result of a thorough analysis of the pilot. The pilot consists of five main functional areas:

- The air measurement equipment
- The PC Stations
- The OC Operations Centre used for the data acquisition and the PC station remote control
- The OC Database Servers
- The ARPA Enterprise Infrastructures

The figure below shows the internal schema of a measuring station. It depicts how it interfaces to the rest of the pilot infrastructure. This measuring station is composed by the air measurement equipment and the PC station (first two bullets of the list above). It adopts the shape of an insulated container where the analysers are placed and connected in three different ways:

1) Analog output which is transformed into digital by means of an A/D converter;
2) LAN port
3) Serial Port.

These analysers acquire information on the main pollutant parameters. Air conditioning, anti-intrusion systems, fire control systems, UPS, maintenance and cleaning equipment are included. Each station has a PC which is connected to the A/D converter and to a switch that sends information to a router / modem by means of LAN port. The data are sent to a concentrator, which implements the post-processing required by law (validation, averages and exceedances calculation) and stores the data on the regional database.

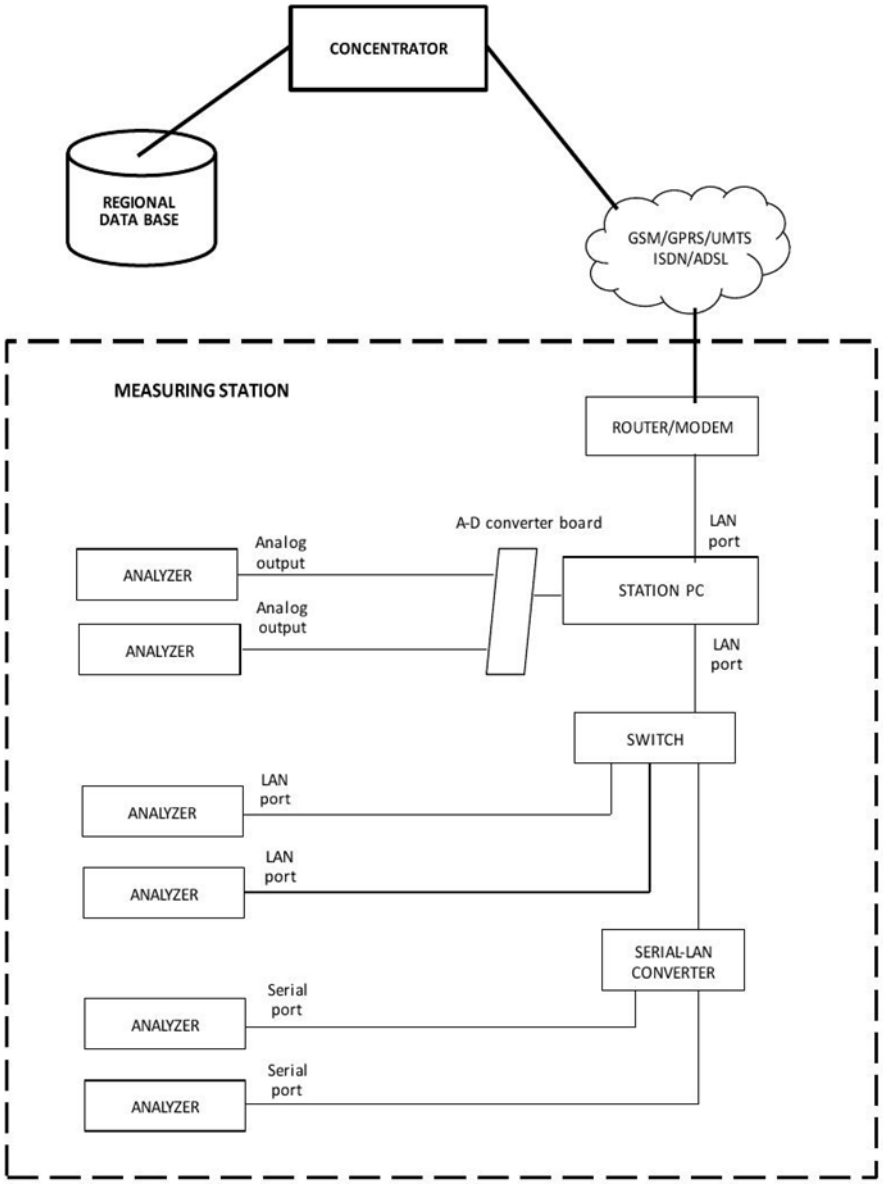

Figure 1 - Schema of an environmental monitoring station

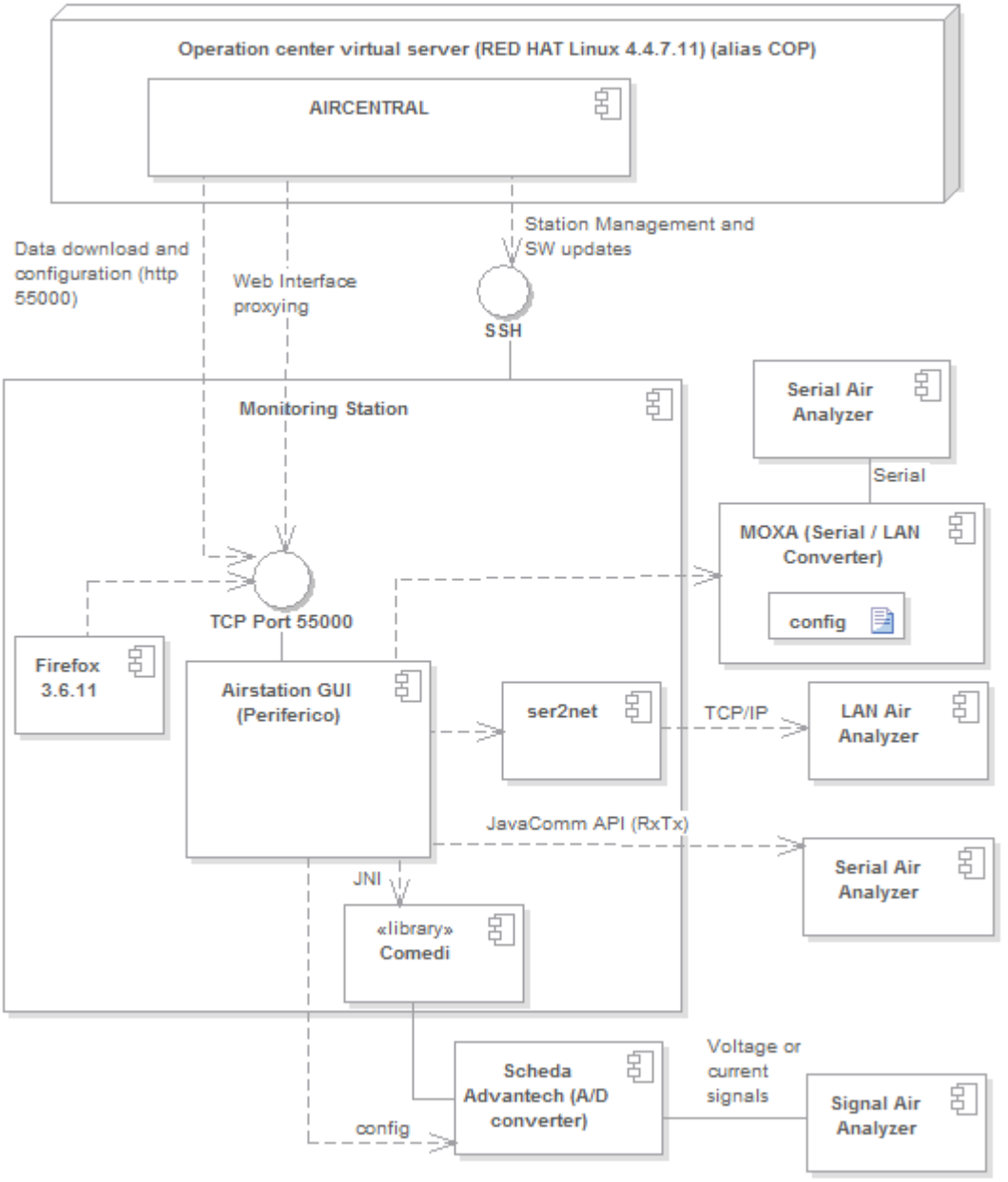

Figure 2 - Schema of an environmental monitoring station - Diagram View

The information is sent to the Concentrator using different technologies which depend on how advanced the technology used in the station is. The stations using ISDN send the information to the ISDN Access Server of the ARPA Network. Those stations using GSM/GPRS/UMTS are connected through the Internet to the corporate proxy servers of both ARPA and CSI. This is also the case for the stations using ADSL. Both machines are in turn connected to the ARPA Virtualization Server that includes the Operation Centre Virtual Server for data acquisition (third bullet of the list above) and the Operation Centre Databases where the measurements are properly stored (fourth bullet of the list above). The figure below depicts this.

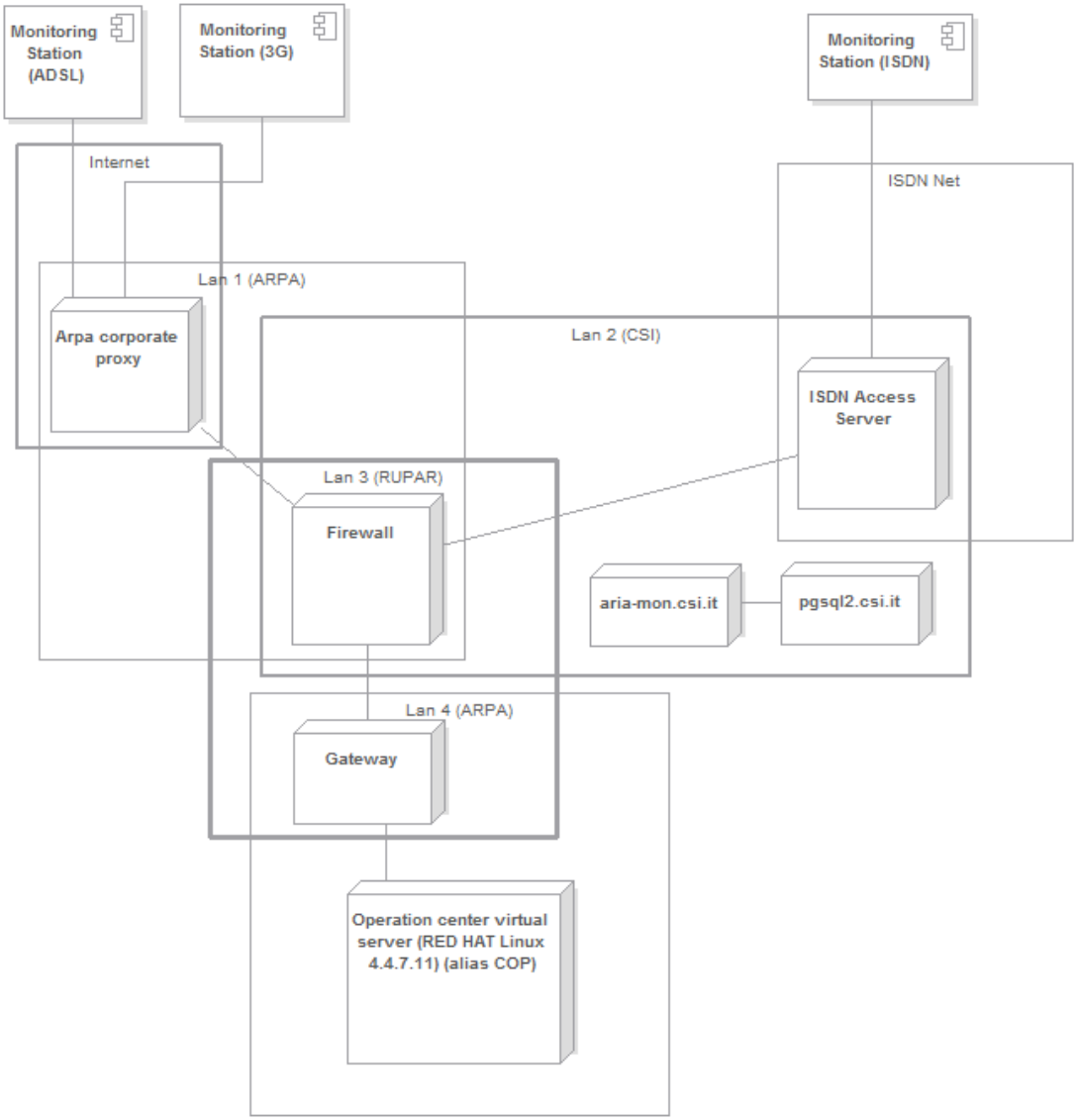

Figure 3 - Physical view of the operation centre[1]

The ARPA Enterprise Infrastructure (fifth point of the list above) is composed by the Operation Centre, the proxy and the access server described above, and all the client machines that relay the information, using HTTP connections to the Operation Centre or directly connecting to the individual monitoring stations through the ARPA Proxy. In order to see the whole picture, it is necessary to consider the CSI Network itself, where the client machines can connect to ARPA Network by means of RUPAR[2], which is the private network of public

[1] CIPSEC D1.2: Report on Functionality Building Blocks, section 4.1.3

[2] http://archivio.cnipa.gov.it/site/it-IT/Attivit%C3%A0_-_Archivio_storico/Sistema_Pubblico_di_Connettivit%C3%A0_%28SPC%29/RUPA/

administration. Likewise, the client machines in CSI Network can leverage the CSI Proxy to access directly the monitoring stations. The figure below reflects this.

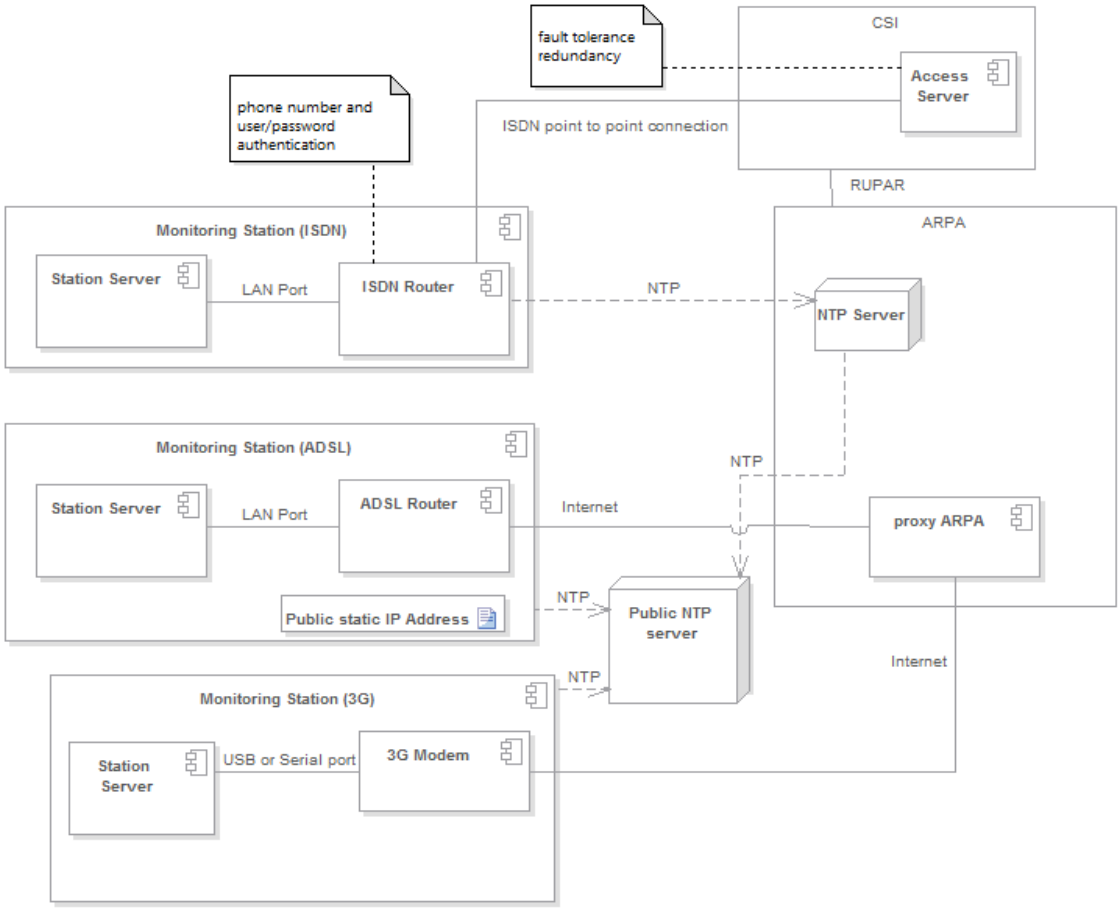

Figure 4 - Environmental pilot overall network - Component Diagram

3.2 Definition of required security features

Leveraging the extensive pilot description documented in WP1, an early definition of requirements per scenario was identified[1]. When WP3 activities started in M10 (February 2017), an interplay with the system design presented in WP2 took place in order to refine this requirements' definition. It was translated into choosing one or more security features per resource / logical group of resources within the pilot. These security features have been formally defined for the sake of coherence and the establishment a common ground.

The following tables describe each security feature, along with the proposed tools/services of the CIPSEC framework that are able to provide them with a description of their applicability.

[1] See sections 4.2 and 4.3 of CIPSEC D1.2: Report on Functionality Building blocks.

Table 1. Availability description

Availability		
The probability that a system will work as required during the period of a task/activity/session (as described in a system's manual/specifications, under specific circumstances, and/or in relevant SLAs). Also, defined as the stability of the system –regarding its ability to work for long periods without problems or possible "bugs".		
Tool	**Partner**	**How**
Sensors	*ATOS*	*Sensors can detect DoS attacks, preventing system breakdowns and contributing to maintain the availability of the system high. There are some events generated by the devices that could be used by the XL-SIEM to define rules that allow identification of anomalous behaviour in the CPU usage, load average or memory that could be considered as potential DDoS attacks* *Also, the Host Intrusion Detection Sensors are capable of monitoring the OS logs, the domain logs, the OS events registered, website activities or access occurrences.*
XL-SIEM	*ATOS*	*This asset leverages the information obtained by the sensors to generate events and alarms that are relevant for protecting the availability of information.*
Real-Time detector for jamming attacks	*WOS*	*Apart of being external and autonomous, our sensors act in a non-intrusive way and they only "listen" to detect Denial of Services to the wireless networks in form of jamming attacks, which are the easiest, cheapest and the most impactful attacks to critical infrastructure wireless elements, not only affecting the interconnection of the devices but also allowing cyber attackers to impersonate wireless elements and infiltrate the entire network in a stealthy way.*
Total Defender / Gravity Zone	*BD*	*The asset will continuously protect a host from attacks, keeping it available for normal usage. In some rare conditions, a system reboot might be required for a complete clean-up.*
Honeypot	*FORTH*	*The DDoS attacks detection system is able to provide information about potential DDoS attacks that are active on the Internet. The results produced can be used by system and network administrators. The accuracy of the produced results is proportional to the amount of the dark IP address space monitored and the amount of honeypot VM instances deployed.* *The solution enables the user to remotely install and configure a new honeypot virtual machine and thus to easily create and maintain a distributed infrastructure of DDoS detection systems (sensors).*
AEGIS Agents	*AEGIS*	*AEGIS Agents can monitor and record system status values (CIPIs) like CPU usage, disk usage, network load and communications, and other parameters.* *This data, together with critical status data, can be used to have a real-time status overview of all monitored devices.*
Forensics Service	*AEGIS*	*The service contributes to the availability of a system by providing visualisation of CIPIs whose irregular values can indicate a problem and therefore alert the operators to take*

		some actions in order to ensure the system's availability.
AEGIS Forensics AVT	*AEGIS*	*The visualisation part of AEGIS forensics service can be used to show the status of the systems monitored by AEGIS agents and other tools.*
Hardware Security Module	*UoP*	*The HSM provides a series of cryptography and security operations that are executed within a controlled, secure and trusted environment inside the HSM embedded processor. Therefore, the executed functions are dedicated to the HSM functionality and thus there are no manipulation point to reduce their availability. Thus, the HSM will be able to always respond to Host requests and will always be available. This enhances a Host System's availability since Host security operations that are migrated to the HSM will always work regardless of the Host's status.*

Table 2. Robustness description

Robustness		
Robustness is the ability to tolerate perturbations that might affect the system's normal functionality. The ability of a system to work as expected (according to system's specifications under pre-defined conditions), and to resist a change with no need to adapt its initial stable configuration. The persistence of a system's characteristics after perturbation (includes mutational robustness and environmental robustness).		
Tool	**Partner**	**How**
Total Defender / Gravity Zone	*BD*	*Bitdefender will protect from software attacks like malware, without disturbing the system functionality and remove any malware traces, restoring the system to the pre-attack state.*
Honeypot	*FORTH*	*The honeypot can detect attacks against communication / transfer protocols: FTP, TFTP, HTTP, HTTPS, TELNET, DNS, SMTP, MS Windows RPC, SMB.* *The tool provides support for IPv4 and IPv6 protocols.*

Table 3. Reliability description

Reliability		
Probability that a device will perform its required functions when needed (as probably described in a system's manual/specifications, under specific circumstances, and/or in relevant SLAs). It can also be defined as the consistency of the product when used under constant conditions.		
Tool	**Partner**	**How**
Sensors	*ATOS*	*Network Intrusion Detection Sensors can satisfy this requirement. Network traffic and events registered are key to provide this.* *Host Intrusion Detection Sensors capabilities can be leveraged to provide the reliability in a similar way to that providing availability.*
Real-Time detector for	*WOS*	*The asset can monitor the wireless network physical layer with*

Jamming Attacks		*external sensor to detect jamming attacks to 3G/GPRS network.*
HSM	*UOP*	*HSM has integrity and encryption handling properties, with impact on the reliability. The HSM can provide cryptographic primitive acceleration to handle secure communications.*
Total Defender / Gravity Zone	*BD*	*The asset prevents malware or potentially unwanted applications. BD will ensure that the device performs its required functions when needed.*
Honeypot	*FORTH*	*The honeypot can detect attacks against communication / transfer protocols: FTP, TFTP, HTTP, HTTPS, TELNET, DNS, SMTP, MS Windows RPC, SMB.* *The tool provides support for IPv4 and IPv6 protocols.*
Forensics Service	*AEGIS*	*The forensics service can prove via the CIPIs monitoring that the system performs reliably and that no significant change happened at certain points or periods of time where specific circumstances or conditions were met.*

Table 4. Usability description

Usability		
Ease of use and learnability of the product by its users/operators. The efficiency and satisfaction the users may achieve when running tasks.		
Tool	**Partner**	**How**
AEGIS Forensics AVT	*AEGIS*	*The visualisation part of AEGIS tools can be easily used to show an overview of the assets monitored or drill-down to a specific group of assets or a single asset.* *An intuitive mechanism allows the user to focus on a specific period that includes the current time or be entirely in the past.*
Total Defender / Gravity Zone	BD	Bitdefender will contribute to usability, by providing a low system impact. The Endpoint Security will only inform the user when a threat is detected, running in background the rest of the time. The Control Center will ensure usability by allowing the system administrator to perform the common operations in an easy and intuitive manner.
Real-Time detector for Jamming Attacks	WOS	DoSSensing helps to the usability of the framework by presenting in real time the alerts of jamming attacks in a visual and comprehensive way.

Table 5. Effectiveness description

Effectiveness		
The capability of the product to produce the desired result. The ability of the product to "do the right thing".		
Tool	**Partner**	**How**
Total Defender / Gravity Zone	*BD*	*Bitdefender will block any intrusion in the normal operation, enabling the system to produce the desired result*

Table 6. Privacy description

Privacy		
The ability of the product to provide its users with the capacity to have some control on their personal information.		
Tool	**Partner**	**How**
Data Privacy Tool	*UPC*	*The data privacy tool will provide anonymization of sensitive data stored/exchanged in CIs. The two main services provided to CIPSEC are:* *- Anonymization of personal data of clients/users of CI. The main functionality in this case is protecting personally identifiable information through data anonymization. Here, the tool will provide a statistical disclosure control methodology endowed with a series of privacy-enhancing algorithms. Furthermore, the tool can give as an output various level of utility, depending on the privacy level required by the application.* *- Anonymization of cybersecurity data relative to attacks and security incidents that are exchanged between SIEMs. In this case, anomaly activities (i.e., malicious ip address, time of attack, etc.,) will be anonymized (suppressed or generalized or pseudonymized) before being shared by third parties.* *These features are not necessary in the Environmental Pilot because of the nature itself of the managed data*

Table 7. Response time description

Response-Time		
The ability of the product to complete assigned tasks within a given time according to specification and relevant SLAs under specific conditions. The ability of the product to reply to users' requests in a timely manner.		
Tool	**Partner**	**How**
HSM	*UOP*	*HSM can handle cryptographic operations related to needed security protocols in case the existing equipment cannot handle cryptography fast enough*
Secocard	*EMPELOR*	*The device is able to respond to a smart card in a timely manner.*

Table 8. Integrity description

Integrity		
Integrity can be offered in two flavours: • Data Integrity: assures that information and programs are changed only in a specified and authorized manner. • System Integrity: assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.		
Tool	**Partner**	**How**
XL-SIEM	*ATOS*	*Data coming from integrity sensors may be used by XL-SIEM as part of the process to detect manipulations in the communication. Detecting any manipulation in measured values or injection of commands to change configuration parameters or reading values which could mean a hacking attempt. One particular case in this group is to preserve system dataflow integrity.* *Detecting illegal modifications in the firmware to avoid intentionally wrong commands sent to devices, wrong answers on commands received from its, or combination of both. Particular use cases in this group are to preserve system integration by detecting physical intruder attempts in the field or in other words, potential hacking attempts.* *There are several events generated in this environment at different levels related to the firmware update that could be used by the XL-SIEM in order to detect suspicious misbehaviour and generate an alert.* *To avoid false alarms in the attack detection, the XL-SIEM could use those events in conjunction with other events that could mean that someone is trying to hack a device, or with other context information provided (for example to know if there is a scheduled field intervention to apply a new firmware).*
HSM	*UOP*	*The asset can handle cryptographic operations related to needed security protocols (e.g., HTTPS, IPSEC, TLS). HSM can also provide identification / authentication*
Secocard	*EMP*	*Secocard as an advanced card reader that authenticates the user to the host. So, it will provide data integrity protection indirectly by restricting unauthorized users from entering the system.*
Total Defender / Gravity Zone	*BD*	*Bitdefender will provide both data integrity, by protecting against ransomware and system integrity, by blocking system changes performed by malicious software.*
Honeypot	*FORTH*	*The honeypot detects attacks against databases: MSSQL, MySQL, ORACLE, POSTGRES.* *The tool provides LDAP user authentication*
Forensics Service	*AEGIS*	*The forensics service can reveal and expose potentially unauthorised actions or indications of data integrity violation via*

		relevant monitored CIPIs, e.g. unforeseen number of connected users at the same time

Table 9. Confidentiality description

Confidentiality		
Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. In short, access must be restricted to those authorized to access the data.		
Tool	**Partner**	**How**
XL-SIEM	*ATOS*	*XL-SIEM shall capture and analyze relevant log files of OT components, IT infrastructure components to allow detection of known threats. The objective is to detect attempts of forced entrance in the enterprise network through OT Components that might be dangerous for the confidentiality of the information.*
Forensics Service	*AEGIS*	*The forensics service can reveal potential confidentiality problems via the monitoring of relevant CIPIS, e.g. more than expected user connections to a monitored machine.*

Table 10. Auditing description

Auditing		
Network auditing is the set of collective measures used to analyse, study and gather data about a network with the purpose of ascertaining its proper functionality in accordance with the network/organization requirements. Network auditing primarily provides insights on what effective network control practices are, i.e. its compliance to internal and external network policies and regulations. Auditing is useful when further analysis of security incidents is needed in order to identify the root cause and apply appropriate protection mechanisms to similar systems		
Tool	**Partner**	**How**
Sensors	*ATOS*	*Sensors monitoring the network usage can be deployed, in addition specific sensors meant to detect network-based intrusion attempts can be deployed as well. Specific examples are Snort / Suricata, Ntop, tcptrack, Nagios3 ot DNS Traffic sensor.* *Host Intrusion Sensors like OSSEC bring specific auditing features such as OS logs or domain logs.*
XLSIEM	*ATOS*	*This asset can be used to detect interruptions in the communication. Potential causes of an interruption in the communication could be the application of a Faraday cage around a meter, jamming in the mobile signal or a mechanical interruption in the communication channel.* *XL-SIEM builds on information brought by both network and host intrusion sensors to contribute to the auditing task.*
Total Defender / Gravity Zone	*BD*	*Bitdefender will produce logs that will help in the auditing process.*

Forensics Service	*AEGIS*	*Forensics main goal is to exactly provide auditing and help investigators find the root cause of security incidents or malfunctions.*
AEGIS agents	*AEGIS*	*Agents monitoring the network usage can be deployed, in addition specific sensors meant to detect network-based intrusion attempts can be deployed as well. Specific examples are Ossec, Netflow and Nagios3*
AEGIS AVT	*AEGIS*	*In the instances where auditing tools produce relevant data, the AEGIS AVT can offer to the auditor detailed and dynamic viewpoints of varying granularity to act upon in a manner that improves systems compliance with the organizational requirements.*

Table 11. Alerting description

Alerting		
Ability to report any unusual and potentially dangerous or difficult incidents. When an alert is produced, a notification, that a particular event (or series of events) has occurred, is generated which is sent to responsible parties for spawning an action.		
Tool	**Partner**	**How**
XL-SIEM	*ATOS*	*Produces alerts based on correlations of events of different kinds generated thanks to the process of the information coming from different sensors. The more information available, and the more complex the filtering and correlation rules are, the more specific the alarms become.*
Real-Time detector for Jamming Attacks	*WOS*	*External sensors can contribute to the alerting feature by alerting to the command and control when jamming attacks are present*
Total Defender / Gravity Zone	*BD*	*Bitdefender will provide alerts about suspicious events.*
Honeypot	*FORTH*	*The tool provides alerting mechanisms for custom IP addresses or range of IP addresses.*
Cloud based security tool	*FORTH*	*The solution is able to monitor the traffic that is exchanged through VMs (Virtual machines) which reside in the same physical hosts. The solution is based on Single Root I/O Virtualization technology and is able to identify possible attacks between co-located VMs in the Cloud. Alerts are presented via a web interface.*
Forensics Service	*AEGIS*	*The service is capable to produce alerts through the real-time forensics analysis*

In the light of the definitions above, the table below indicates and justifies the security features that must be in place for the different resources existing in the environmental pilot.

Device / Resource	Description	Technical details	Security Features	Justification
1 - Air measurement equipment	Takes samples of air quality, quantifies their chemical composition (especially hazardous toxic agents), and expresses the values in form of analog / digital signals	LAN Serial Port Analog Output	Availability	The air measurement data should be acquired 24 hours a day
			Reliability	The alarms produced from the equipment depends on the correct operation of the instrument.
			Integrity	The instruments contained in the monitoring stations, sensors, PCs, ethernet switches, etc., should not be manipulated by unauthorized players and be free from deliberate or involuntary unauthorized manipulation.
2 - PC Stations	Acquisition of the measurements and status info from the air quality analyzers Computation of aggregated data Communication with Operation Centre	Two LAN Ports PCI card with A/D converters ISDN ADSL 3G / GPRS Web interface	Availability	The PC Stations are used to transmit the data recorded by the tools, and must ensure the same 24 hours, availability of the tools they manage
			Reliability	PCs must be up and running, otherwise the recorded data cannot be stored or transferred to OP
			Alerting	It is necessary to receive warning signals to know if PCs operate properly or not and to act when needed
			Usability	the PC's correct usability can easily provide less intervention to the technicians who act in the station to solve any problems

			Robustness	A robust system guarantees the accuracy of the detected data and ensures the correct functioning of the whole infrastructure even in the event of an attack
			Response-Time	The response time of the station PC must be consistent with the related tools and periodic or extraneous requests of the OP
			Integrity	Tools should not be manipulated by unauthorized actors, and should be free from deliberate or inadvertent unauthorized manipulation of the system.
3 - OC Server (Data Acquisition)	Protect the node that acquires data from environmental stations	See section 4 in D1.2 for extended details	Usability	Correct usability of the OC can easily require less intervention by ARPA technicians who keep in check the overall situation of all the stations connected to it
			Availability	The OC is used to receive the data transmitted by PCs Station, and must ensure the same 24 hours ,availability.
			Reliability	The OC must be up and running otherwise the detected data received cannot be analyzed.
			Alerting	It is necessary to receive warning signals to know if the OC operate properly or not and to act when needed

			Auditing	Audit is required to ensure the proper functioning of the system in accordance with the requirements of the organization and to produce a status report to the clients
			Robustness	A robust system guarantees the accuracy of the detected data and ensures the correct functioning of the whole infrastructure even in the event of an attack
			Effectiveness	it must be guaranteed in order to get proper communication between OC and PC and vice versa
4 - OC Database	DB Air Central DB	See section 4 in D1.2 for extended details	Availability	The OC database is used to store the data transmitted by PC Stations, and must ensure the same 24 hours, availability.
			Response time	Response times must be consistent with requests from applications
			Robustness	A robust system guarantees the accuracy of the detected data and ensures the correct functioning of the whole infrastructure even in the event of an attack
			Usability	The Data Base Usability guarantee the correct operation of the whole system
5 - ARPA Enterprise	ARPA Access Server (for ISDN)	See section 4 in D1.2 for	Availability	The ARPA Enterprise Infrastructure must

Infrastructure	ARPA Workstations ARPA Internet Proxy (for HTTP)	extended details		ensure the availability 24 hours.
			Response time	Response times must be consistent with requests from applications
			Auditing	Audit is required to ensure the health of the system in accordance with the requirements of the organization and to produce a status report to the clients
			Robustness	A robust system guarantees the accuracy of the detected data and ensures the correct functioning of the whole infrastructure even in the event of an attack
			Usability	The ARPA Enterprise Infrastructure Usability guarantees the correct operation of the whole system
			Integrity	The information must remain unchanged from the source and only modified by authorized personnel
			Effectiveness	it must be guaranteed in order to get proper communication between OC and PC and vice versa

Table 12. Choice of security features per resource / group of resources

The CSI in agreement with ARPA (the regional client) decided to prepare a testing environment on which the first test of the CIPSEC Framework will be carried out. The virtualized environment is comprised of two parts: the monitoring station (1 and 2 in the table above) and the Operation Centre (3, 4 and 5).

3.3 Analysis of security features covered per product

The partners playing the role of solution providers have made an extensive analysis of what their products can offer in terms of coverage of the demanded security features in the context of the environmental pilot. The table below shows the coverage of each required security feature per product:

- XL-SIEM and sensors (ATOS)
- Real-Time Detector for Jamming Attacks (WOS)
- Hardware Security Module / FPGA cryptographic device (UoP)
- K-Anonymization Tool (UPC)
- Honeypot / Cloud security tool (FORTH)
- Secocard (Empelor)
- Total Defender / Gravity Zone (BD)
- Secure Hardware and Safety Process know-how (TUD)
- Forensics Support Analysis Visualization Tool (AEGIS)

Device / Resource	Security Features	ATOS	WOS	UOP	UPC	FORTH	EMP	BD	TUD	AEGIS
1 - Air measurement equipment	Availability	X		X			X			
	Reliability	X		X			X			
	Integrity			X			X			
2 - PC Stations	Availability	X	X	X		X		X		X
	Reliability	X	X					X		X
	Alerting	X	X			X		X		
	Usability		X					X		X
	Robustness					X		X		
	Response-Time		X	X						
	Integrity	X		X		X	X	X		X
3 - OC Operations Centre Server (Data Acquisition)	Usability							X		X
	Availability	X		X		X		X		X
	Reliability	X		X				X		X
	Alerting	X				X		X		
	Auditing	X						X		X
	Robustness					X		X		
	Effectiveness							X		

4 - OC Operations Centre Database	Availability	X		X		X		X		X
	Response time			X						
	Robustness					X		X		
	Usability							X		X
5 - ARPA Enterprise Infrastructure	Availability	X						X		
	Response time									
	Auditing	X						X		X
	Robustness							X		
	Usability							X		X
	Integrity	X						X		X
	Effectiveness							X		

Table 13. Coverage of demanded security features by product provided

3.3.1 ATOS XL-SIEM and sensors

3.3.1.1 ATOS Sensors

Sensors will be configured and installed on Pilot infrastructure at the network or end-point layer level. This will require a limited interaction between the CIPSEC support team and the Pilot. The XL-SIEM sensors will pre-process, analyze and correlate the collected data in order to produce a pre-elaborated output. The pre-processing will already give the possibility to detect attacks and vulnerabilities.

Some of the most common standard sensors which could be used (depending technical dependencies) in XL-SIEM are sniffing or monitoring tools such as:

- Snort / Suricata (network based intrusion detector)
- ARPwatch (ARP activity monitor)
- Ntop (network usage monitor)
- OSSEC (host based intrusion detection system)
- tcptrack (Monitor TCP connections on the network)
- openVAS-Client (the client part of the OpenVAS Security Scanner)
- nagios3 (Network/systems status monitoring daemon)
- p0f (Identify remote systems passively)
- DNS traffic sensor and analyzer
- Netflow sensor for behavioral analysis

As reflected in D2.1, using the appropriate sensors data and setting up the right security policy rules, these are some uses cases where XL-SIEM could be useful:

1) Interruption in the communication

Potential causes of an interruption in the communication could be the application of a Faraday cage around a meter, jamming in the mobile signal or a mechanical interruption in the communication channel.

2) Manipulation in the communication

Detecting any manipulation in measured values or injection of commands to change configuration parameters or reading values which could mean a hacking attempt. One particular case in this group is to preserve system dataflow integrity.

3) Manipulation in system integrity

Detecting illegal modifications in the firmware to avoid intentionally wrong commands sent to devices, wrong answers on commands received from its, or combination of both. Particular use cases in this group are to preserve system integration by detecting physical intruder attempts in the field or in other words, potential hacking attempts.

There are several events generated in this environment at different levels related to the firmware update that could be used by the XL-SIEM in order to detect suspicious misbehaviour and generate an alert.

To avoid false alarms in the attack detection, the XL-SIEM could use those events in conjunction with other events that could mean that someone is trying to hack a device, or with other context information provided (for example to know if there is a scheduled field intervention to apply a new firmware).

4) Network intrusion attacks

The objective is to detect attempts of forced entrance in the enterprise network through OT components preserving integrity of the network and its components. XL-SIEM shall capture and analyze relevant log files of OT components, IT infrastructure components to allow detection of known threats.

5) Denial of Service (DDoS) attacks

There are some events generated in the devices that could be used by the XL-SIEM to define rules that allow identifying anomalous behavior in the CPU usage, load average or memory that could be considered as potential DDoS attacks

6) Illegal use/access of/to security credentials

For the detection of this type of attack, the log file of the master keys database should be available and securely retrievable by the XL-SIEM. Besides, it would require the capability of monitoring on cells in the database what could be out of the scope of the XL-SIEM features on CIPSEC project.

Summarizing, all these sensors are capable of detecting several types of attacks within the pilot's network, some examples come below:

- Denial of Service
- Sniffing
- Man in the middle
- Spoofing
- Malware introduction
- SPAM
- Botnets

3.3.1.2 ATOS XL-SIEM

XL-SIEM is the reasoner in charge of raising events and alarms out of the information collected by the agents. This is done based on filtering and correlation rules applied. The detection capabilities of the XL-SIEM rely on the quantity and variety of the information made available coming from the sensors, on the one hand, and the expertise of the person in charge of implementing the reasoning rules being applied by the XL-SIEM.

Concerning the coverage of the security features by the assets brought by ATOS, it is summarised as follows:

- The availability and reliability features required by the air monitoring equipment are satisfied only in the case of the LAN analysers, thanks to the monitoring and detection provided by the NIDS sensors. Network traffic and events registered are key to provide this.
- The availability, reliability and alerting features required by the PC Stations are satisfied thanks to the NIDS sensors, which monitor the network traffic, the OS logs, the domain logs, the OS events registered, website activities or access occurrences.
- Concerning the OC Operations Centre Server:
    - The usability requirement is covered by different dashboard capabilities
    - The availability, reliability, auditing and alerting features are satisfied by means of the NIDS sensors, which monitor the network traffic, the OS logs, the domain logs, the OS events registered, website activities or access occurrences. Also, the monitoring and detection capabilities of the NIDS sensors which watch over the network traffic play a relevant contribution, as well as the events registered.
- The availability and response time required by the OC Operations Centre Database are fulfilled by the monitoring and detection capabilities of the NIDS sensors (network traffic and events registered)
- The availability, response time and auditing required by the ARPA Enterprise Architecture are covered by the monitoring and detection provided by the NIDS sensors (network traffic and events registered).

3.3.2 WOS Real-Time detector for Jamming Attacks

WOS sensors are external to the LAN, wireless LAN, servers and computers, which is an advantage for the pilots that are affected by restrictions on installing software or hardware to protected and/or closed equipment.

Apart of being external and autonomous, our sensors act in a non-intrusive way and they only “listen” to detect Denial of Services to the wireless networks in form of jamming attacks, which are the easiest, cheapest and the most impactful attacks to critical infrastructure wireless elements, not only affecting the interconnection of the devices but also allowing cyber attackers to impersonate wireless elements and infiltrate the entire network in a stealthy way.

The coverage provided by this asset brought by WOS is the following:

The availability, reliability, usability, response time and alerting required by the PC Stations are addressed by monitoring the wireless network physical layer with external sensor to detect jamming attacks to 3G/GPRS network and alerting to the command and control.

3.3.3 UOP Hardware Security Module / FPGA cryptographic service

The specific adaptations to the asset brought by UOP addresses are explained below:

- The reliability and integrity demanded by the air measurement equipment are addressed in collaboration with Empelor Secocard. Secocard can act as a local collection point and the associated HSM can handle data integrity and encryption if needed by the pilot’s security plan

- The response time and integrity required by the PC Stations are also satisfied in collaboration with Secocard. HSM individually or through the Secocard can handle cryptographic operations related to needed security protocols (e.g. HTTPS, IPsec, TLS) in case the existing equipment can't handle crypto fast enough.
- Concerning the availability, reliability, usability and effectiveness, the OC server can identify and authenticate MS devices using the integrity quotes provided by HSMs connected to MS hosts. The HSM can provide cryptographic primitive acceleration to the OC server to handle secure communications through security protocols like HTTPS, IPsec, TLS.

3.3.4 UPC K-Anonymization tool

This asset does not cover any requirement posed by the environmental pilot.

3.3.5 FORTH Honeypot and cloud security tool

3.3.5.1 FORTH Honeypot

The first tool FORTH is planning to use is an already existing solution of a cloud based honeypot implementation (The DDoS attacks detection system). FORTH's solution is able to provide information about potential DDoS attacks that are active in the Internet. The results produced can be used by system and network administrators. The accuracy of the produced results is proportional to the amount of the dark IP address space monitored and the amount of honeypot VM instances deployed.

It can provide solutions to the following areas, in the context of CIPSEC project:

- Detection of DDoS attacks.
- Prevention with the assistance of a firewall that will apply ACLs produced by the honeypot system.

Also by emulating a number of production services our solution is able to detect and prevent:

- Attacks against databases: MSSQL, MySQL, ORACLE, POSTGRES.
- Attacks against communication/transfer protocols: FTP, TFTP, HTTP, HTTPS, TELNET, DNS, SMTP, MS Windows RPC, SMB

The above services are almost present in every critical infrastructure due to the basic functionality that they offer to all computing systems. Also many of the aforementioned services are a popular target for internet attacks.

The tool also provides:

- Support for IPv4 and IPv6 protocols.
- Alerting mechanisms for custom IP addresses or range of IP addresses
- LDAP user authentication

Furthermore, the solution enables the user to remotely install and configure a new honeypot virtual machine and thus to easily create and maintain a distributed infrastructure of DDoS detection systems (sensors). Our cloud based honeypot implementation comprises of two subsystems. The first subsystem comprises of the virtual machines which contain the detection software which is a combination of low and medium interaction honeypots specialized for the detection of specific protocol attacks and DDoS attacks. Every sensor uses a log engine to gather information about the detected attacks and runs appropriate services to securely transfer the results to a centralized database. The second subsystem is the control panel which provides a graphical interface for the administration and visualization of the results and is interconnected with the centralized database.

The system provides the following core functionality:

1. Sensor registration.
2. Sensor management.
3. User registration.
4. Services monitoring

The users and the administrators of the system, are able to view statistics on the aggregated attack results. The user can look up and get information about a specific IP address or a specific protocol by using predefined or custom search rules. Statistics are also provided about the top attack destinations and the activity of the top attackers.

Due to restrictions posed by the Italian law, honeypots cannot be used in this pilot, so the honeypot features cannot contribute to address the required security features.

3.3.5.2 FORTH Cloud based security tool

FORTH will bring in to the consortium a cloud based security solution. The solution is able to monitor the traffic that is exchanged through VMs (Virtual machines) which reside in the same physical hosts. The solution is based on Single Root I/O Virtualization technology and is able to identify possible attacks between co-located VMs in the Cloud. The amount of traffic exchanged within a machine with many VM instances could be enormous and in really high speeds. The challenge for the solution is to be able to monitor all that traffic produced and try to identify potential incoming and/or outgoing DDoS attacks. The solution that will be contributed is based on SR-IOV (Single-root input/output virtualization).

This tool will be able to protect any cloud or VM based tools running in the pilot from attacks within the same cloud or virtual environment.

3.3.6 EMP Secocard

This asset brought by Empelor addresses the security features in the following way:

- As far as the air measurement equipment is concerned, Secocard could be used for data integrity. However, after carefully taking into consideration the requirements that are necessary to connect to the air measurement equipment it is best to use the card reader functionality of the device to provide user authentication in the PC stations as explained below.
- Regarding the PC stations, Secocard will be used as an advanced and programmable card reader providing authentication services to the host. The user will use a smart card that contains a chip with the user's private key and public key certificates. The user inserts the smart card into the Secocard, which is attached to the PC station and then provides the pin when requested. The smart card in combination with the smart card reader will provide user authentication and indirectly data confidentiality and data integrity.

3.3.7 BD Total Defender / Gravity Zone

This asset brought by Bitdefender addresses the security features in the following way:

- In the air measurement equipment, to address the demands on availability, reliability and integrity the solution cannot be directly installed on this device. By installing it in other hosts in the same network, it will be protected indirectly.
- In the PC Stations:
    - Concerning availability, Bitdefender will continuously protect a host from attacks, keeping it available for normal usage. In some rare conditions, a system reboot might be required for a complete clean-up.

- As for reliability, Bitdefender can take care of it, by preventing malware or potentially unwanted applications, Bitdefender will ensure that the device performs its required functions when needed.
- Regarding usability, Bitdefender asset has no interference with normal usage.
- In the case of robustness, Bitdefender will protect from software attacks like malware, without disturbing the system functionality and remove any malware traces, restoring the system to the pre-attack state.
- As for the response time, Bitdefender will not affect the system response time, due to the low performance impact demonstrated in various tests.
- Regarding integrity, Bitdefender will provide both data integrity, by protecting against ransomware and system integrity, by blocking system changes performed by malicious software.
- Related to alerting, Bitdefender will provide alerts about suspicious events.

- In the OC Operations Centre Server (Data Acquisition):
  - Robustness: Bitdefender will protect from software attacks like malware, without disturbing the system functionality and remove any malware traces, restoring the system to the pre-attack state.
  - Availability: Bitdefender will continuously protect a host from attacks, keeping it available for normal usage. In some rare conditions, a system reboot might be required for a complete clean-up.
  - Reliability: by preventing malware or potentially unwanted applications, Bitdefender will ensure that the device performs its required functions when needed.
  - Usability: No interference with normal usage.
  - Effectiveness: Bitdefender will block any intrusion in the normal operations, enabling the system to produce the desired result.
  - Alerting: Bitdefender will provide alerts about suspicious events.
  - Auditing: Bitdefender will provide logs that will help in the auditing process.
- In the OC Operations Centre Databases:
  - Robustness: Bitdefender will protect from software attacks like malware, without disturbing the system functionality and remove any malware traces, restoring the system to the pre-attack state.
  - Availability: Bitdefender will continuously protect a host from attacks, keeping it available for normal usage. In some rare conditions, a system reboot might be required for a complete clean-up.
  - Usability: No interference with normal usage.
  - Integrity: Bitdefender will provide both data integrity, by protecting against ransomware and system integrity, by blocking system changes performed by malicious software.
  - Response time: Bitdefender will not affect the system response time, due to the low performance impact demonstrated in various tests.
- In ARPA Enterprise Infrastructures:
  - Robustness: Bitdefender will protect from software attacks like malware, without disturbing the system functionality and remove any malware traces, restoring the system to the pre-attack state.
  - Availability: Bitdefender will continuously protect a host from attacks, keeping it available for normal usage. In some rare conditions, a system reboot might be required for a complete clean-up.
  - Usability: No interference with normal usage.

- Integrity: Bitdefender will provide both data integrity, by protecting against ransomware and system integrity, by blocking system changes performed by malicious software.
- Response time: Bitdefender will not affect the system response time, due to the low performance impact demonstrated in various tests.
- Effectiveness: Bitdefender will block any intrusion in the normal operations, enabling the system to produce the desired result.
- Auditing: Bitdefender will provide logs that will help in the auditing process.

3.3.8 TUD Safe Hardware and Safety Process know-how

This asset does not cover any requirement posed by the environmental pilot.

3.3.9 AEGIS Forensics Support Analysis Visualization Tool

The AEGIS forensics solution offers intuitive and detailed visualizations of Critical Infrastructure Performance Indicators (CIPIs) that can help investigators perform detailed forensic analysis in critical infrastructure that was affected by an attack or a malfunction. Moreover, through the real-time forensics analysis it facilitates situations awareness and can help to an immediate response to an incident that is detected at the moment that it is happening.

In the concept of this pilot, AEGIS agents that measure CIPIs will be configured and installed on the Pilot infrastructure on the measurement station PCs, on the Operations Center Server, on the Operations Center Database, and at the ARPA Enterprise Infrastructures.

The AEGIS Forensics AVT will be configured and installed at the OC on a separate PC or under a Virtual Machine on an existing PC. The solution, when deployed, will be able to collect operating data at all the points of operation, from the air quality measurement stations to the database at the Operations Centre.

In all the zones, the AVT can be used to give an overview of the status of the monitored assets. In the case of an event report from Anomaly Detection Reasoner or any other tool included in the CIPSEC framework separately, AVT can be used to analyze and visualize current or historic data collected by the agents and all the other tools, in order to aid the operator, pinpoint the sequence of events that led to an alert or a malfunction.

3.4 Choice of products to be used in the environmental pilot

Based on the analysis done in section 3.3, and as reflected in Table 13, there is at least one product addressing all the requirements posed by the environmental pilot. The list of products to be used in the pilot is the following:

- XL-SIEM and sensors (ATOS)
- Real-Time Detector for Jamming Attacks (WOS)
- Hardware Security Module / FPGA cryptographic device (UoP)
- Honeypot / Cloud security tool (FORTH)
- Secocard (Empelor)
- Total Defender / Gravity Zone (BD)
- Forensics Support Analysis Visualization Tool (AEGIS)

With this information, the next step is adapting the reference architecture defined in D2.2 to the specific case of the environmental pilot and find out the appropriate mapping and integration of the products in the existing topology.

Device / Resource	ATOS	WOS	UOP	UPC	FORTH	EMP	BD	TUD	AEGIS
1 - Air measurement equipment	X		X			X			
2 - PC Stations	X	X	X		X	X	X		X
3 - OC Operations Centre Server (Data Acquisition)	X		X		X		X		X
4 - OC Operations Centre Database	X		X		X		X		X
5 - ARPA Enterprise Infrastructure	X						X		X

Table 14. Application of products to pilot resources

4 First phase of the implementation of the CIPSEC Security Platform in the environmental pilot

In the previous section, an effort was done to understand how the pilot works and the security needs associated to the daily operation of this environmental critical infrastructure. These security features have been coupled to what the different solutions brought by the partners . As a result, a subset of the offered products has been selected to be applied to the different parts of the pilot infrastructure.

With this input, the following step is to analyse the hardware and software requirements of the products to ascertain that their installation and deployment on the pilot is feasible. If it is not, it would be necessary to check if the unavailability of the product in question leaves some security feature uncovered. If that is the case, some alternative solution (including third party products) would have to be explored to ensure a complete protection of the infrastructure.

Once the compatibility of the products has been checked, it is necessary to study the pilot infrastructure adaptation to accommodate the products. Then, a final and stable infrastructure map definition is necessary, presented in a higher level of detail, which enables the mapping, installation and deployment of the products within the infrastructure, with all the needed information in place. In addition, it will be also necessary: 1) to show a clear instantiation relationship between the pilot secured infrastructure and the CIPSEC reference architecture and 2) to define how the pilot will benefit from CIPSEC services portfolio.

4.1 The preliminary efforts carried out to integrate the CIPSEC platform into Pilot III

The activities carried out to adapt Arialinux were as follows:

- A virtual machine was created on ariasrv1.csi.it to host the new version of Arialinux.
- The operating system was updated to the Ubuntu 14.04.5 LTS version with Linux version 3.13.0-91-generic.
- The latest version of the Periferico 3.3.0 software was installed, and all the drivers were hooked up for the current acquisition cards developed: api, lspm10, modbus, mode04, nira, opsis, swam, synspec and tecora.
- The Comedi driver for the dialog with the acquisition cards was recompiled and also the Comedi modules were blacklisted for the correct configuration.
- The sudoers file was updated by entering the necessary users.
- Arialinux version number was updated in the reference file.
- The srqauser user was added to the dip and dialout group so that they had the same Periferico's user groups.
- The rules for uploading GPS drivers (Garmin and Telit) from modprobe and the module file have been updated.
- Updated iptables files for ISDN and GPRS.

A Test Cop was prepared on a virtual machine (always on ariasrv1.csi.it) where Central software is installed. The test station with the new Arialinux installed was configured on the Central software. Testing is performed over LAN because the two virtual machines reside on the same physical machine.
Polling is done correctly, but there is no data downloaded because the virtual test station is not linked to analysers.

The next step would be, after we have acquired the necessary hardware, install the new Arialinux operating system on the test machine that will be located in Collegno Station (test solution a) or to create a complete Virtual Infrastructure (test solution b) to set up all the needed tests avoiding any eventual problems on the Real Production Environment resulting from test activities.
Connect the analysers already in the station by analog mode for acquiring test data and check through the test cop that the data acquisition is done correctly using ADSL as communication channel. The connection between the analysers and the test environment could be real if we choose the test solution a) instead would be simulated if we choice the test solution b).

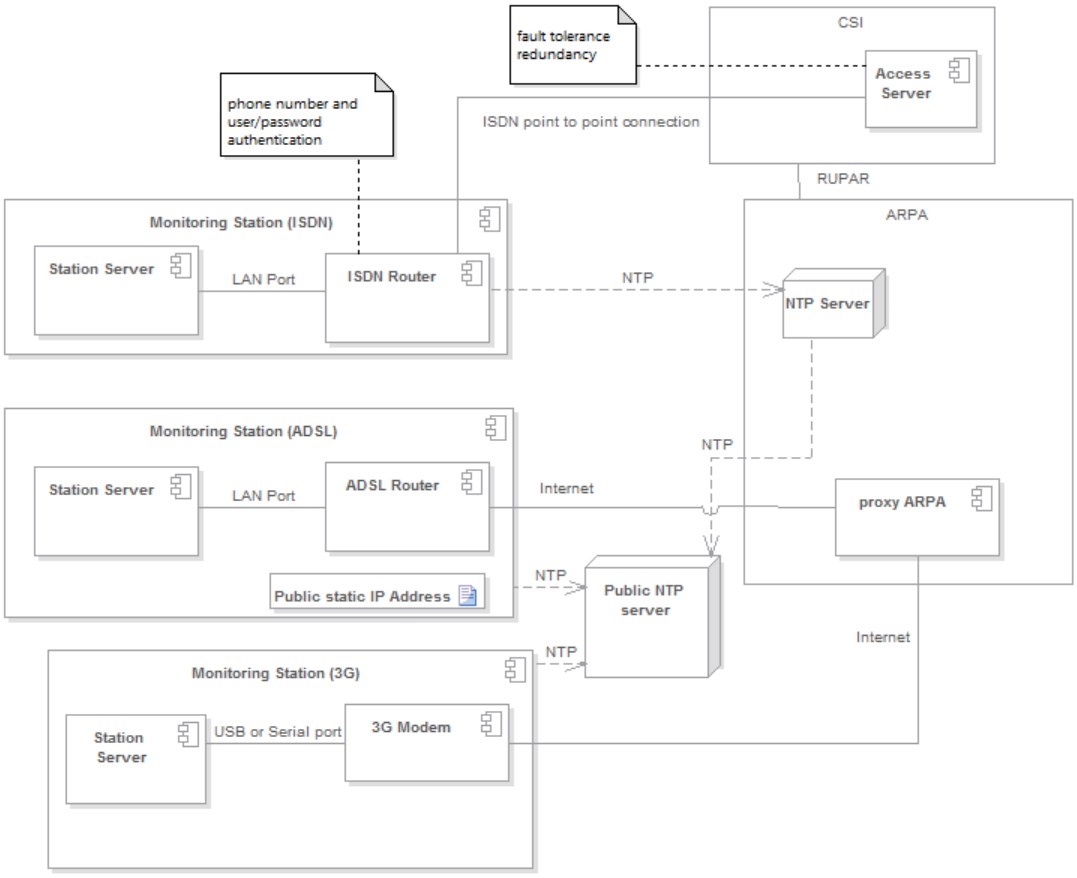

Figure 5. Communication between stations and Operation Center – without security equipment

4.2 Analysis of hardware and software requirements posed by the products

4.2.1 ATOS XL-SIEM and sensors

4.2.1.1 ATOS sensors

Sensors will be configured and installed on Pilot infrastructure at the network or end-point layer level. This will require a limited interaction between the CIPSEC support team and the Pilot. The XL-SIEM sensors will pre-process, analyse and correlate the collected data in order to produce a pre-elaborated output. The pre-processing will already give the possibility to detect attacks and vulnerabilities.

4.2.1.2 ATOS XL-SIEM

XL-SIEM agents can run both Ubuntu 12.04 or 14.04. XL-SIEM Server is deployed as a virtualized image. So it's required a dedicated machine with enough hardware resources (16 GB RAM memory and a CPU with at least 4 cores (i5 or i7 with quad core CPU architecture)) to manage the hypervisor.

4.2.2 WOS Real-Time detector for jamming attacks

Worldsensing are going to use their own hardware infrastructure to deploy their solution. The only constraint is to have local or external network connectivity with Atos XL-SIEM Agents to send its jamming attack events.

Specifications:

- Reliability: 98%
- Discovery latency: real-time
- Protected protocols:
    - NB-IoT, Lora, Sigfox, UNB, Weightless-N (700 MHz – 900 MHz)
    - GSM/UMTS/LTE
    - WiFi-802.11b/g, RPMA, Bluetooth, ZigBee (2.4 GHz)
- Processing: 64bit ARMv7 Quad Core 1.2 GHz
- Memory: 1GB RAM
- Software defined radio module
    - 1 MHz to 6 GHz operating frequency
    - Half-duplex transceiver
    - SMA female antenna connector
    - SMA female clock input and output for synchronization
- Supported sample rate: 5 Mbps
- Communication: Ethernet, 3G WiFi
- Power supply: 5V (3000 mA)
- Power consumption: -W
- Box size: 276 x 272x 96.5 mm (HxLxW)
- Weight: around 2 Kg
- Operating temperature: -20 to +55ºC
- Operating humidity: 10-95%.

4.2.3 UOP Hardware Security Module / Cryptographic service

The requirements are the following:

- Communication interface
    - USB based Serial interface (UART)
- Protocols
    - Custom API to host device
- The unique hardware requirement is to have appropriate communication interface which is serial UART (RS232) that can be handled through a usb-to-serial driver. There is a need for a usb port availability
- The UoP HSM communication requires that the Host device can support usb host mode. This mode is always available in Personal Computers and Servers but it may not be available in embedded system devices.

- Appropriate drivers must be available in the Host device for UART communication (FTDI-based drivers). In Windows and Linux Machines, such drivers are usually part of the operating system or are automatically installed.
- The UoP HSM can operate in an unencrypted (unsecure channel) with the Host machine using the standard RS232 (UART) communication (FTDI-based drivers). In that case, the HSM can provide very basic services like symmetric key encryption and Hashing.
- In order to fully take advantage of the UoP HSM full spectrum of security services (e.g. local attestation, data integrity) then a secure channel must be established between the Host and the HSM. To achieve that a client software must be executed in the Host device. This is a C programming language based software that when executed it establish secure communication and encrypts/decrypts all data transactions (HSM commands and responses) between Host and HSM.
- The UoP HSM is a passive device so it will not initiate any communication or provide any data unless the Host requests it. A Host user can provide HSM commands through a terminal based serial communication channel initialized in the Host device. The HSM commands are text based.
- In case the Host device does not support USB-to-serial communication, a bridge device will be needed to transmit commands from the host system to the HSM and collect replies. The bridge can be any COTS device that fits the required role or it can be Empelor's Secocard if this product functionality allows it.

4.2.4 FORTH Honeypot and Cloud Security Tool

Due to restriction of the Italian law FORTH Honeypot tool cannot be deployed in the CSI Pilot.

Cloud security tool requires 8GB RAM memory and CPU with at least 4 cores (i5 or i7 with quadcore CPU architecture) to manage the hypervisor and the IDS tool.

4.2.5 EMP Secocard

When Secocard is connected to a PC running either Windows or Linux a serial port will appear. This has been tested in Windows 7, 8, 8.1 and 10 as well as Ubuntu 14.04. In some Windows installations, a driver installation is necessary during the first time that the device is connected. If Secocard is successfully recognized by the operating system, then for all practical purposes the operating system will expose a serial port where applications or terminal programs can be used to communicate with Secocard. An application capable of communicating with serial devices would be necessary in order to implement the use case described above. Secocard has not been tested with other operating systems such as Android.

Secocard has an internal battery which is adequate if the device needs to be operated shortly but for the purposes of the CIPSEC project it should stay connected to a standard USB port. The device both communicates and is powered by the USB port. A USB 2.0 port should be adequate in most cases (especially if the internal battery is full) but a USB3.0 port is recommended so that the device can draw more current if necessary.

4.2.6 BD Total Defender / Gravity Zone

The table summarizes the operating systems and virtualization solutions for which the product is compatible:

Workstation operating systems	Windows 7, 8, 8.1, 10 Windows Vista (SP1, SP2), Windows XP (SP3) Mac OS X Lion (10.7.x), Mountain Lion (10.8.x), Mavericks (10.9.x), Yosemite (10.10.x), El Capitan

	(10.11.x)
Table and embedded operating systems	Windows Embedded Standard, POSReady, 2009, 7 Windows Embedded Enterprise 7 Windows XP Embedded (SP 2), Tablet PC Edition
Server operating systems	Windows Server 2012, 2012 R2 Windows Small Business Server (SBS) 2008, 2011 Windows Server 2008, 2008 R2 Windows Small Business Server (SBS) 2003 Windows Server 2003 (SP 1), 2003 R2 Windows Home Server Red Hat Enterprise Linux / CentOS 5.6 or higher, Ubuntu 10.04 LTS or higher, SUSE Linux Enterprise Server 11 or higher, OpenSUSE 11 or higher, Fedora 15 or higher, Debian 5.0 or higher, Oracle Solaris 11, 10 (only in VMware vShield environments)
Mobile operating systems	Apple iPhones and iPad tablets (iOS 5.1+) Google Android smartphones and tablets (2.2+)
Virtualization solutions	VMware vSphere 6.0. 5.5, 5.1, 5.0 P1 or 4.1 P3 ESXi 4.1, 5.0, 5.1, 5.5 VMware vCenter Server 6.0, 5.5, 5.1, 5.0 or 4.1 VMware vShield Manager 5.5, 5.1, 5.0 VMware vShield Endpoint VMware vCNS 5.5 VMware Tools 8.6.0 build 446312 VMware View 5.1, 5.0 Citrix XenDesktop 5.5, 5.0 Citrix XenServer 6.0, 5.6 or 5.5 including Citrix Xen Hypervisor Citrix VDI-in-a-Box 5.x Microsoft Hyper-V Server 2012, 2008 R2 including Microsoft Hyper-V Hypervisor Red Hat Enterprise 3.0 including Red Hat KVM Hypervisor Oracle VM 3.0

The Gravity Zone Control Centre (the “server”) comes as a virtual appliance (OVA, XVA or VHD) and there are no special hardware requirements.

4.2.7 AEGIS Forensics Support Visualization Tool

The product needs a high-end workstation with the following specs

- Windows 10
- Core i7 Intel processor, 6th generation minimum
- High end graphics card supporting two displays
- 16GB memory (RAM) and 2TB disk.
- Two monitors, 24 inch. Minimum.
- It also has to have access to the Anomaly Detection Reasoner so as to retrieve necessary information for the visualizations

4.3 OS Update and Virtual test environment available for testing purposes

The operating system of the PC Station has been updated to the Ubuntu 16.04.LTS version. Currently, the test infrastructure is on a managed virtualization system on a single physical machine namely ariasrv1.csi.it. Specifically, there is a virtual machine that represents the COP and a virtual machine that represents the PC Station. In this configuration, the communication between COP and PC Station is via LAN.

In the second phase, we will add to our infrastructure a real pc to test in a real monitoring station the solution proposed or we will create a Virtualized Infrastructure which also includes a virtualization of the connectivity.

In the third phase if the solution passes all the test it would be deployed in a Real Production Environment.

4.4 Final detailed definition of the pilot infrastructure map

Below a diagram on the different solutions supplied by the partners related to the SRRQA system infrastructure

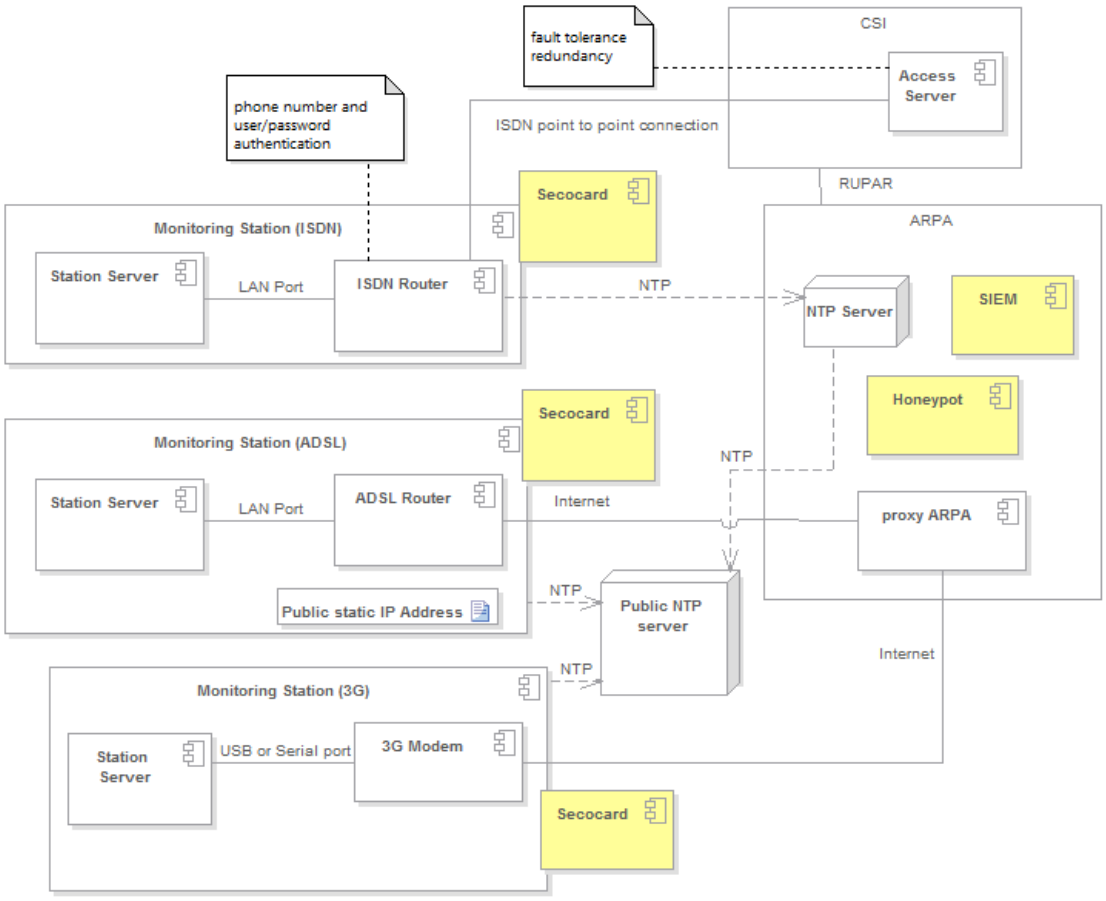

Figure 6 - Communication between stations and Operation Center - with hypothesis of security equipment

4.5 Provision of secured environmental monitoring infrastructure by including the chosen products

On the Station PC, the related parts of Total Defender/Gravity Zone, EMP Secocard, UOP HSM and WOS jamming detector should be added.

On the OC virtual machine the related part of UOP should be added.

It is necessary to set up a new machine to accommodate the features offered by XL-SIEM and FORTH.

It is necessary to set up a new machine to accommodate the features offered by AEGIS.

Machine	Existing features	Added features
Machine for XL-SIEM and FORTH		24 GB RAM memory and a CPU with at least 4 cores (i5 or i7 with quad core CPU architecture)
Pc Station	• Processor X86-64bit – 2 core • Motherboard with bus SATA2 with possibility	Total defender/Gravity zone EMP Secocard UOP HSM

	RAID 1,5 , 0, 1+0 • RAM 4Gb DDR2 • 2 Hard disk 500 Gb SATA2	WOS anti-jamming detector
OC – virtual machine (KVM)	• Processor X86-64bit – 1 core • RAM 4Gb • Hard disk 250Gb	UOP HSM
Machine for AEGIS		Windows 10, Core i7, 16GB RAM, 2TBdis

4.6 The secure solution as an instantiation of the reference architecture and role of services

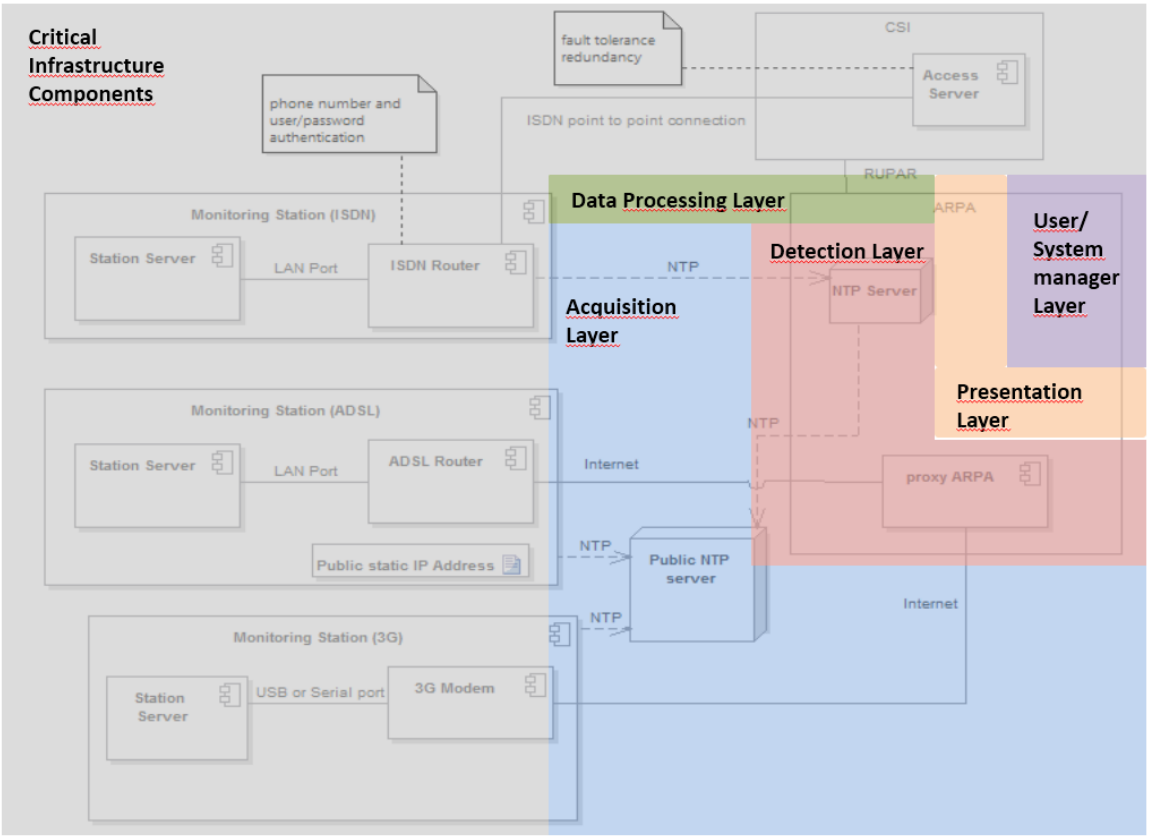

Figure 7 - CIPSEC Solution Reference Architecture

5 Conclusion and next steps

In this document, we have described what the necessary requirements must be satisfied for the CIPSEC solution to be applied to the SRRQA system.

By pursuing this objective, we have described in detail the possible security systems and how these should be assigned to the equipment of the pilot.

Later, we defined which solutions could provide the necessary features, and we have made a choice on the proposed solutions to create the most complete security framework possible, to secure the critical infrastructure of the Environmental Pilot. Always with the ultimate aim of securing the infrastructure, the solution providers have hypothesized where to place the individual elements of the solution into the existing infrastructure.

It was considered the opportunity to acquire new HW and SW to install and test the proposed solutions. A new phase of acquisition of material for the full integration of the CIPSEC framework distribution is expected and at the same time several updates of ARPA and CSI infrastructures. The changes should be completed in the first quarter of 2018.

It is supposed to act for subsequent increments based on completing the previous steps to begin in November to adopt Total Defender and Bitdefender Gravity Zone, by the end of 2017 instead we count on adding UOP HSM to securely transmit and encrypt the data channel in storage systems and subsequently will be added to all the other preview components. Each implementation will monitor the system response and test the various pre-existing features as a result of new systems introduced as well as system and network functionality.

In order to test malicious attacks on the SRRQA infrastructure and interconnected infrastructures, a system will be introduced that simulates them, in a replication testing environment of the real one, and we will highlight if the adoption of the CIPSEC framework mitigated the consequences of these attacks. In the event that the attacks and / or their consequences cannot be mitigated, a risk analysis for the assess will be carried out, to decide whether they can be accepted or whether a further framework development iteration or whether the adoption of further safety items not previously taken into account is needed.

As an additional test phase, on the security system, we have provided a penetration test to be performed against our critical infrastructure that can provide additional evaluation elements to the partners that provide the services.

6 References

[1] 20161025 D1.2 Report on Functionality Building Blocks.pdf