Project no: 234014

ATOM

Airport detection and Tracking Of dangerous Materials by passive and active sensors arrays

Instrument type: Capability Project

Priority name: TRANSPORT (including AERONAUTICS)

D8.1: Analysis of requirements for data exchange and management

Due date of deliverable: 31 January 2011
Actual submission date: 25 February 2011

Start date of project: 1st July 2009 Duration: 36 months

Organisation name of lead contractor for this deliverable: HAI

Revision [Final]

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2012)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Authors and Approvals			
Authors		**Date**	**Signature**
Name	**Company**		
Nikos Pappas	HAI		
Enrico Anniballi	SESM		
Santiago Pan	AYCO		
Giovanni Toffoli	LINK		
Reviewed by			
Name	**Company**		
Babis Kapetanidis	HAI		
Roberta Cardinali	SESM		
Miguel Moure	AYCO		
Approved by			
Name	**Company**		
Roberta Cardinali	SESM		

Modification History		
Issue	**Date**	**Description**
Draft A	26 August 2010	First issue for comments
Issue 1	28 September 2010	Draft
Issue 2	21 October 2010	Draft
Issue 3	22 December 2010	Draft
Issue 4	02 February	Draft
Issue 5	17 February	Final Draft
Final	25 February	Final Document

Contents

Figures

Tables

This Page is intentionally left blank

Glossary

3D	3 Dimensions
AES	Advanced Encryption Standard
BPSK	Binary Phase Shift Keying
BRAN	Broadband Radio Access Networks
CCK	Complementary Code Keying
CCMP	Counter mode with Cipher block chaining MAC Protocol
CCTV	Closed-Circuit Television
CDMA	Code Division Multiple Access.
DFS	Dynamic Frequency Selection
DSS	Decision Support System
DSSS	Direct-Sequence Spread Spectrum.
EAP	Extensible Authentication Protocol.
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security.
ETSI	European Telecommunications Standards Institute;
FCC	Federal Communications Commission;
FDM	Frequency-Division Multiplexing
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FH-CDMA	Frequency-Hopping Code Division Multiple Access.
FHSS	Frequency-Hopping Spread.
FSK	Frequency-Shift Keying
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile communications
IBSS	Independent Basic Service Set
ID	Identification
IEEE	Institute of Electrical and Electronics Engineer
IETF	Internet Engineering Task Force
LAN	Local Area Network
OFDM	Orthogonal Frequency-Division.
OSI	Open System Interconnection
PC	Personal Computer
PEAP	Protected EAP
PSK	Phase Shift Keying
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Access Dial In User Server
RLAN	Radio Local Area Network
SAR	Synthetic Aperture Radar
SCADA	Supervisory Control and Data Acquisition
SS	Spread Spectrum
TDMA	Time Division Multiple Access
TETRA	Terrestrial Trunked Radio
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TSA	Transportation Security Administration
Tx/Rx	Transmitter/Receiver pair
UDP	User Datagram Protocol
UWB	Ultra Wide Band
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2

VoIP	Voice over IP
VNA	Vector Network Analyzer

1 Introduction

This document concerns the network issues regarding ATOM project. It will focus on communication aspects for the ATOM system. It will show the first studies on the network that will be able to connect all the ATOM sub-systems to create a new innovative system for increasing airport security.

The document attempts to summarize the most important concepts leading to requirements formulation and therefore, is structured as follows:

In chapter 1, the basic concepts and network objectives within the project will be showed.

In chapter 2, a brief description of the ATOM subsystem will be presented. The detection systems (W band and UWB sensors), the tracking systems (active and passive) and the data center unit will be introduced in order to understand the input and the output, very useful information in the network design process.

In chapter 3 a general overview on airport infrastructure is given.

In chapter 4 a detailed description of the current communication technologies is showed in order to analyze different solutions that could be exploited within ATOM project.

In chapter 5 a detailed analysis of some application scenarios is performed in order to analyze the network load.

In chapter 6 the constraints and restrictions that are imposed in a airport environment will be analyzed, as, for example, the initial care to not to irritate airports' normality, procedures and security functions and standards. These issues are considered within the ATOM project, too.

Based on the previous analysis, in chapter 7 the network requirements will be showed.

Finally chapter 8 will focus on the study of a preliminary network architecture as starting point for deliverable D8.2 "Network Architecture Proposal Document" to be submitted on month 23.

In chapter 9 the conclusions and recommendations will be given.

1.1 ATOM Network objectives

ATOM network concept rises from the need to interconnect different subsystems and assure smooth information flow, until its final destination or the security operators. More precisely, aim of ATOM network is to provide the appropriate infrastructure for managing the various information flows and enabling constant tracking (throughout their movement in the airport area) of people carrying materials regarded as dangerous, while providing real time feedback to security men located in a central control station or scattered within the airport area.

2 Subsystems communication architecture

This section presents the ATOM subsystems that comprise the carriers of security related information in the airport and the components of the communication network that will convey this information. The focus is not so much on the structural components of the connected

subsystems, as in their parts used for communication and their produced output, in terms of content, format and other parameters, important for networking. Concentration of all these elements indicates a substantial subset of our proprietary or general purpose LAN.

2.1 W band sensor subsystem

2.1.1 Description and Communication of W band subsystem

W band subsystem is a radar utilizing the microwave part of the spectrum, known as W band, with a central frequency of about 94 GHz and a bandwidth varying between 3 GHz and 6 GHz. Its hardware includes the mechanical setup (needed for the mechanical and electrical steering, radar, data acquisition and data transmission lines). Its software functions include radar steering and signal processing (performed by a SAR). The subsystem functions on the concept of rotating platforms, which was analyzed thoroughly in D2.1 (Figure 1).

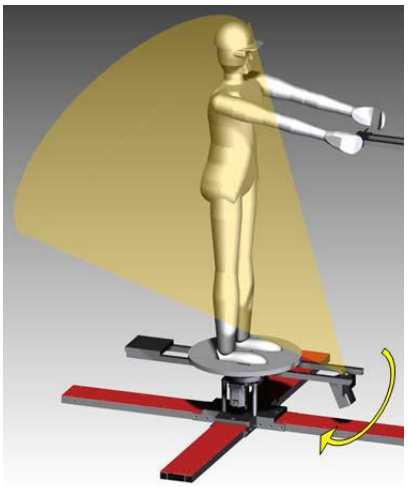

Figure 1 — Preliminary setup for screening persons by rotating radar

Indicative average dimensions of the W band radar are 3m x 3m for the scanner and additionally 1m x 1m for the steering hardware. After an initial internal signal digitization and processing of raw data, the produced output is a radar image, stored as MATLAB figure or .jpg format. Subsequently, the subsystem communication needs are rather simple, since the above image has to be transferred to the Data Centre unit ("default" case) or imported into UWB subsystem, in case a cooperation of the two scanners is realized. The output volume is 2 MB per image and the transfer can be implemented through a standard LAN protocol, e.g. Ethernet. The usage of an average of 5 W band scanners in the airport environment is the developer's logical hypothesis.

2.2 UWB sensor subsystem

2.2.1 Description and Communication of UWB subsystem

UWB imaging sensor subsystem, as a part of the ATOM Detection unit, scans the airport and produces 3D images of persons and dangerous items (if any). The raw data is processed to achieve object's shape reconstruction using suitable algorithms, with the most prominent being Frequency-wavenumber domain imaging algorithm. The subsystem includes the imaging

sensors (2-4), a mechanical scanner equipped with Tx/Rx antennas (performing SAR measurements) and a Vector Network Analyzer (VNA) (Figure2).

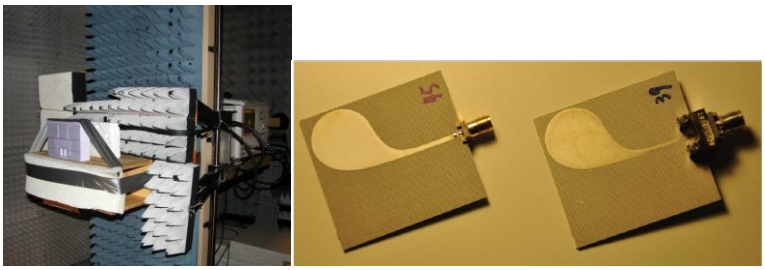

Figure 2 — SAR measurement setup and antipodal Vivaldi antenna

The subsystem's interface to "outside world" depends on the selection of data fusion method and on network topology. In case the information processing is internal, this gateway could be a PC or laptop, connected to ATOM LAN. In case of a less distributed approach, the Data Centre unit can serve as the concentrator of raw data from UWB block and its communicating interface, simultaneously.

2.3 Active radar subsystem

2.3.1 Description and Communication of Active radar subsystem

As a typical block of Active radar is considered the structure of four to six sensors transmitting raw data to a Central Node, which in turn, supplies the Active Tracker with input, called Designations. The latter are data messages which can contain several types of information, such as X,Y positioning, timestamps, designation IDs and other (under agreed convention). Complementary information serves as input to the Active Tracker also, in the format of control data consisting of timing and housekeeping data (on/off, reset, logging, status requests), of which probably the time synchronisation is the most significant. Active Tracker enhances these designations and delivers detections (plots, tracks or tracklets). The Central Node also acts as the main gateway of the active tracking system towards the external world.

2.4 Passive radar subsystem

2.4.1 Description and Communication of Passive radar subsystem

Although the Passive sensor subsystem output will be considered as input for the Tracking subsystem, it is worthwhile making a short reference about its communication interface. As a typical average block of Passive radar subsystem is considered the structure of sixteen sensors. Its interface is a RJ-45 connector, for Ethernet connectivity, used to transfer three measured parameters, *distance*, *velocity* and *direction of arriva*l, accompanied with related information, such as *signal strength*, per reporting person. More details on the format and characteristics of this information are mentioned in the corresponding paragraph 7.1.3. The connections of the subsystem can be summarized into two major categories: Passive sensors supply Tracking subsystem central unit (in which the sensors belong) with data and receives tracking requests from the Detection subsystem.

2.5 Data Centre unit

2.5.1 Description and Communication of Data Centre unit

The Data Centre unit is the core of the ATOM system. This block will manage all the information coming from the different types of sensors located in airport area: both detection and tracking systems. A relevant role is taken by the communication network that will be responsible for transporting data from a sub-system to another. The input for the management block system are also all data coming from collaborative people, e.g. operators, position of the security man, etc., that can be useful for handling of possible emergencies. The output of the data management block is information for the security man. In case of detection of suspicious people, the system provides different alarm levels with a classification of the threat and the track of the dangerous item introduced in the area.

Data Centre unit used for ATOM simulations, being the core of the system, is a workstation. It will perform a series of functions, mainly of two categories: a) data management, which is data collection from the different radar subsystems and possible data fusion, as well as b) interface or gateway for some of the subsystems (e.g. W band scanner). The main information about the work station is listed in

Table 1:

Information about the workstation for ATOM simulations:	
OS:	Windows 7 Professional
Producer	Hewlett-Packard Company
Model	HP Z200 SFF Workstation
Processor	Intel® Core™ i5 CPU 650 @ 3.20GHz 3.33GHz
RAM	12GB
System Type	OS 64 bit

Table 1 – Information about the workstation for ATOM simulations

A block diagram of the data management structure, with the input and the output, can be seen on Figure 3. This block can be seen as composed of three different blocks, each specialized in a particular task, but not relevant in this document, dealing with the connection through the network of the various subsystems. More details on this block will be given in the dedicated deliverable (D7.1: “Management of information from ATOM system”). Here we focus our attention on the inputs and outputs highlighted in red in the figure: in fact the red arrows show a connection through the network.
In the following the inputs and the outputs of this block will be described in more detail:

- The input coming from the different types of detection sensors (numbered with 1 in Figure 3) represents the biggest load for the network, because this information flow is very large and

complex (in fact an image can be represented by a high number of pixels). In particular, we expect input traffic of the following types:

- **Image**: this is an image provided by the sensors located in the area under test with the suspected person. It could be very large. It represents the major contribution for the network load, also considering the fact that each type of sensor must send this information to the management block
- **Classification**: this is information that indicates the type of dangerous tool detected by the sensors. It can be obtained, for example, by a database where are included the materials that cannot be introduced at the airport
- **Confidence of classification**: this is the probability that the detected dangerous materials are actually the identified ones

- The input coming from the tracking sensors (numbered with 2 in Figure 3) are in the following:
  - **Position**: each tracking sensor should send the coordinates of the people (x,y) inside the area under test. It is a low load for the network
  - **Velocity:** each sensor should send the estimated velocity of the people (V_x,V_y)
  - **Reference time**
- The input numbered with 3 in Figure 3 represents all the information coming from the airport environment. It is useful in this block, for the situation awareness in particular, for the decision to take in case a dangerous tool is detected. In particular here arrives information about:
  - **Position of the security man:** this is the position of the security man (x,y) located in the airport terminal. It is a very useful information because in case of alarm the man closest (one or more depending on the alarm level) to the detected threat is addressed to the specific area
  - **Finish alarm:** this information is sent by security operators when an alarm finished. This is useful to decide when tracking has to be stopped. In case of positive value the situation returns to normal

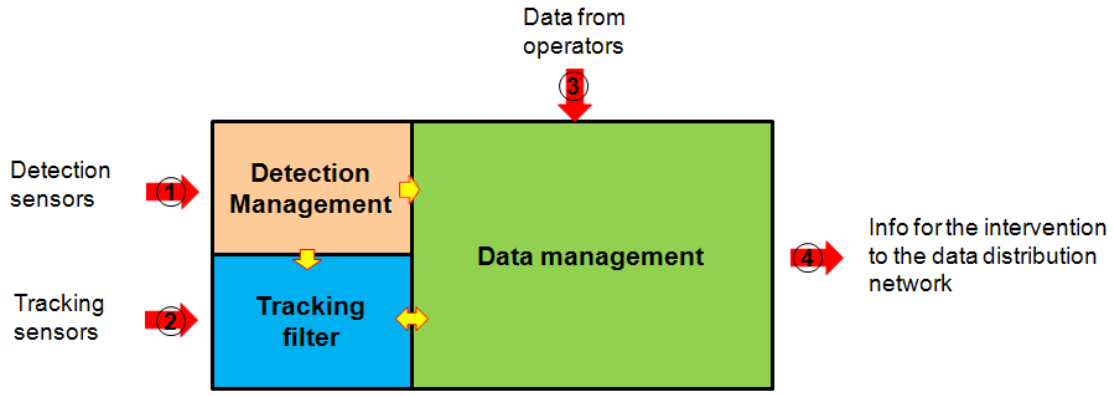

Figure 3 – Input and output of data centre unit

- The output of the data centre unit (numbered with 4 in Figure 3) contains information for the intervention in case of detected alarm: this information has to be sent to the security men that are involved in stopping the threat. As the security men are located throughout the airport area

and they are free to move inside, they need a wireless connection from the central unit. The fields of information to be sent is in the following:

- **Track identification number :** this is the track identifier of the suspected person in the airport area
- **Target position**: (x, y)
- **Target velocity**: (V_x, V_y)
- **Security men position:** (x, y) This information contains the position of the security men involved to stop the threat
- **Alarm level:** It represents an alarm level on a defined scale

3 Airport infrastructure

3.1 General Overview

The two airport companies of the ATOM project consortium allow the latter to work more analytically on the goal of airport awareness and security enhancement, since they present a significant number of heterogeneous characteristics: their size (passenger flow and provided services), their geographical dispersion in Europe and their different policies in security mechanisms, among others. The last and more important feature derives from the fact that Romania does not yet adhere to Schengen states. This diversity provides our research with a potential of a greater degree in generality and more issues to be studied and faced. From information collected by airport partners we can refer to general infrastructure descriptions for the two cases, to the extent that this input is *provided* and the sensitivity of its *privacy* is not violated.

Having a concrete knowledge of the already installed infrastructure in airports, along with the current research and market trends in security communication systems, as well as, in commercial communication systems, possibly used by passengers in such an environment, is essential for ATOM. It will assist the consortium defining the field of the proposal's benefits and setting the functional limits of ATOM network subsystem. Indicatively we can refer to limits imposed by used frequencies, hardware of sensors, radars and antennas, range and resolution requirements etc.

3.2 Security Communications

In general, as regards with the security related communication systems that one can meet at an airport infrastructure, surveillance coverage increase has become a research and practice goal. ATOM attempts to follow this trend, as it is one of the project's main objectives and desired added value. Surveillance has been expanded to surrounding and remote airport areas, including parking lots, metro stations and roads. CCTV circuits seem to play a key role, conveying video and data inputs (mainly) from baggage control and runway systems. The cameras can be interconnected, form a network and augment their communicating and supervising capabilities, by the use of suitable telecommunication hardware, such as modems, Ethernet bridges or wireless connectivity devices and multiplexers. Thus, video and audio data are transmitted to central stations and from there to concerning personnel. The resemblance of this scheme, a network of cameras backed by a seamless communication network and the provision of IP-based services, with ATOM networking purposes is obvious. The difference lies in the interconnected subsystem, being in ATOM novel detection and tracking techniques. Implementation rests on the study and adjustments of specific applications, where ATOM network could be incorporated or act complementary, offering a greater degree of security level.

Targu Mures airport (treated as a non-Schengen airport and for as long as it remains such) has discriminated flows for national and international flights, separate terminals with their own security systems and two security points for each departure terminal. Only baggage security system is the same for both terminals. Connecting point with our research programme is the use of a network for data distribution within the airport facilities and the intention to connect it or expand it with ATOM LAN. The already installed network serves the surveillance of public and restricted areas in terminals and also of airside (fence perimeter). In this way, more or less, the area beyond passenger terminals is covered, leaving "ground" to security optimization, through cooperation with ATOM network. There is, currently, no dedicated wireless network for security purposes, whereas is worthwhile referring that the airport authorities plan firstly to replace existing copper based network with wireless infrastructure and secondly to expand the network spatial coverage.

Amsterdam Airport Schiphol is an international airport with 436,000 aircraft movements in 2007 (Kolkman and Korteweg, 2009). In 2006, Schiphol handled 46,065,719 passengers, ranking fourth in Europe behind London, Paris and Frankfurt; almost 35% of its passengers travelled on intercontinental flights.

The entire airport is below sea level. It is built as one large terminal split into three large departure halls, the most recent having been completed in 1994; there are plans for further terminal expansion. During the inbound and outgoing daily peaks the airport operates at maximum capacity where at most 2 runways are in simultaneous use for take-off and 2 runways are used for landing. The peak hour capacity is currently 112 aircraft.
The main high level requirements that Schiphol contributed to the ATOM Project can be found in Deliverable D2.1 "ATOM system architecture". Here below we add some additional information related to airport security and relevant infrastructures.

RESTRICTED AREAS AND ACCESS CONTROL

Amsterdam Airport Schiphol is proud of making outstanding efforts to improve security; both passengers and staff, including security staff, are screened at various points in the airport. The airport has a number of different types of security areas:

Area	**Level of Control**
Public area	None
Company secure area	100% Access control
Airside Non-SRA	100% Access control
Airside SRA (Security Restricted Area)	100% Access control and Security Control on a random basis
Airside SRA-Critical Part	100% Access control and 100% Security Control

The company secure area is only open to holders of a company pass or Schiphol Pass. Included in this area are the baggage claim halls, Schiphol-East Business Park and the Transportstraat and Expeditiestraat.

In addition to the public area and company secure area, there are also a number of protected areas, which include Airside Non-SRA, Airside SRA and Airside SRA-Critical Part:

- The Airside non-SRA area is located inside the terminal and includes Lounges 2 and 3, the first floor of Pier D and Piers E, F and G. Anyone intending to enter this protected area must show a valid access pass; passengers must show a ticket and staff must show their Schiphol Pass

- The Airside SRA-Critical Part area is also referred to as the Clean Area. This area is inside the terminal and includes Lounge 1, Piers B and C, the second floor of Pier D, and Piers M and H. A security check is carried out at the gate in the case of flights departing from gates on the first floor of Pier D and from Piers E, F and G. The gate then qualifies as the Clean Area. Perimeter roads, aprons and baggage basements are also part of the Airside SRA-Critical Part and thus of the Clean Area. The area can only be accessed by staff in possession of a valid Schiphol Pass

AIRPORT LAN AND SECURITY

The Schiphol LAN was implemented in 2002 by Vosko Networking, as a high-performance system able to control all the critical operations in the airport, including flight information, baggage handling, office automation and other core processes.

Currently the LAN reaches full 10 Gigabit Ethernet capacity, thanks to the use of Cat. 6 S/FTP cables, that shield the network from heavy electromagnetic interferences due to a high concentration of radio traffic, aircraft navigation systems, radars, hotspots, GSM and other wireless communication.

Some 2500 airport staff rely on the data systems for office automation; these are connected to the airport LAN, as are most of the airport facilities, some of which are listed here below:

- One of the areas facing large expansion at Schiphol is that of security cameras (CCTV). Currently there are about 1200 video cameras around the airport, monitoring people and luggage throughout the three terminals. Over the next two years, the airport's security managers plan to increase the number of cameras to about 4,000. This will create a situation where all areas in the airport will be covered by cameras

- About 20 fixed CCTV cameras cover the active airside area of the airport, intended to prevent accidental or malicious intrusion onto runway and hangar area; they are connected to the control room extending the fiber network using a fault tolerant wireless mesh network

- Today, Schiphol processes sixty thousand accesses per day to restricted areas, across 110 access control points with an average throughput of eight seconds and a rejection rate of less than one percent. Schiphol pioneered the use of biometric-based access control to secure restricted areas within the airport environment, ensure efficient airport operations and comply with all appropriate regulations by the most cost effective means possible

- Since May 2007, body scan is used at Amsterdam Airport Schiphol for passenger security and Customs control procedures; the Security staff members view the images in a closed space and are unable to see the person in the scan. Schiphol's latest people screening pilot project includes 15 units of SecuriScan mm wave threat detection portals by L3 Communications. According to airport officials, the current cost of screening a passenger (including checked luggage and hand baggage) is about $7.00

- A new pilot self-service luggage check-in facility is undergoing tests. This is a cavernous system that "swallows" the passengers' suitcases, saving the airline agents the need to heft, weight and tag each suitcase as they ticket the passenger. If the pilot succeeds, the centralization and self-service orientation of the new system will enable a total redesign of the agent's counters, saving much needed space

3.3 Other Communication Systems

Airport authorities are in charge of a great volume and type information, circulating in the premises. This telecommunication traffic concerns, apart from the security staff mentioned previously, passengers, airlines and airport businessmen and may be served by multiple technologies and topologies (point-to-point, chain, star, ring etc.)

A non-exhaustive categorization of these communication services follows:

Cellular networks
Serves passengers' mobile telephony needs, through GSM and its evolution.

Airport ground communications
A series of ground services and activities need to be served by communication networks, which have evolved through time from analogue radio to TETRA networks. Their efficient management incorporates specialized telecommunication SW and HW, such as multiplexers and usable interfaces. These services include:

- Market for the airport users
- Design and development of products that meet airline companies' needs
- Value added services for users
- Management of aircraft's replenishment procedures
- Special treatment for people with moving difficulties

Internet access
Offering broadband access passengers is a self-evident airport feature. Airport users tend to spend (in average) significant time waiting in lines or passing in transit and use their laptops for leisure, work or to accomplish flight procedures (check in, e-ticket etc.). Therefore the provided Internet access should be of high quality, dispersed in lounges and cafes, served by wireless stations and Ethernet links, throughout the infrastructure.

Flight information display system
It is another example of an airport network expanding to include more areas and thus, to respond to more stringent security requirements. Travellers need to be informed for flight modifications details (cancellations, changes of gate), regardless their varying position, inserting the need for networking equipment, such as modems and repeaters.

Air traffic control
Air traffic management information load is a very critical, for safety, type of communication traffic, especially considering the increasing amount of flights in nodal world airports. The corresponding centers may need to handle heterogeneous information formats and rates, such as, voice, high/low speed data, SCADA, radio and video.

All the aforementioned types and volumes of services, network traffic and equipment should be estimated in designing ATOM LAN, as they impose many technical considerations ("Interference", to say the first and least).

Schiphol: Other Communication and Control Networks

Air Traffic Control the Netherlands (ATC-NL; the Dutch acronym is LVNL) is responsible for the correct use of the approach paths to and from Amsterdam Airport Schiphol and the Netherlands' regional airports and for the safety of aircraft taxiing at Amsterdam Airport Schiphol itself. Schiphol Airport has three control towers: the main control tower at the centre of the airport, satellite tower (Tower-West) near runway 18R/36L and an emergency tower; the main tower, with a height of 101 metres, was the tallest in the world when constructed in 1991.

Currently the connections between the ATC-NL locations in the Netherlands are based on dedicated leased lines per signal and system; in the close vicinity of Schiphol Airport a ring structured fibre optic network is used (the AORTA Network). The upcoming renewal of several systems demands packet based connections with higher bandwidths than possible with the current infrastructure.

Schiphol Airport is equipped with a mode S surface movement system; aircraft operators should ensure that the mode S transponders are able to operate when the aircraft is on the ground according to ICAO specifications (Annex 10, volume IV, 3.1.2.8.5.3 and 3.1.2.10.3.10).

Meteorology is a crucial factor that determines the maximum capacity of an airport: in 2004, the average peak hour capacity at Schiphol for inbound flights was about 35 percent lower than under optimum weather conditions. The meteorological observation infrastructure of the Royal Netherlands Meteorological Institute (KNMI) at Schiphol is based on a redundant network of sensors connected to the "AORTA" fibre optic infrastructure of the LVNL.

The airport trunked radio system used by operations personnel, operating at 180 MHz, has been working for around eight years; the in-building system is based on a central base station and the coverage is provided by a distributed antenna system. Another radio system used by the police operates at 450 MHz; this also is based on a central base station and a distributed antenna system.

A newer upgraded airport radio system based on Tetra at 415 MHz is based on RF distribution over fibre from the base station to the slaves being connected to the antennas.
An indoor GSM mobile network covers all plane terminals; the departure lounge and the shopping area; the arrival lounge, the baggage claim area and visitor waiting area; the underground train station; rental car and parking garages. The modular construction of the airport, the radio propagation environment, and the transmit power limitations require a large number of access points distributed in all the covered areas.

Schiphol Airport, in collaboration with KPN, offers wireless (Wi-Fi) Internet throughout the airport; you can even access the Internet right up to the gates. Time-restricted service is available free for all passengers.

4 Communication technologies

4.1 LAN technologies

4.1.1 Wi-Fi

4.1.1.1 Wireless networks and Wi-Fi

A wireless network combines two kinds of communication technology: data networks, that make it possible to share information among two or more computers/devices, and radio - or wireless - communication, that uses electromagnetic radiation to move information from one place to another.

The three most widely used technologies for wireless data exchange are 3G cellular service, Wi-Fi and WiMAX. The term Wi-Fi is short for Wireless Fidelity and is meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, and so on. The term originated from the Wi-Fi Alliance, which is the friendly name for WECA (Wireless

Ethernet Compatibility Alliance), an industry group that includes all major manufacturers of wireless Ethernet equipment.

The 802.11 standard refers to a family of specifications developed by the IEEE for wireless LAN technology. It specifies an over-the-air interface between a wireless client and a "base station" or between two wireless clients.

IEEE 802.11 is the most widely used wireless communication technology and probably the one that will ensure easier compatibility with existing infrastructure since it is IP based. As such it arises as the most suitable candidate for the ATOM network.

Most wireless LANs today utilize "infrastructure" mode that requires the use of one or more access points. With this configuration, the access point provides an interface to a distribution system (e.g. Ethernet), which enables wireless users to utilize corporate servers and Internet applications. As an optional feature, however, the 802.11 standard specifies "ad hoc" mode, which allows to operate in what the standard refers to as an independent basic service set (IBSS) network configuration. With an IBSS, there are no access points: devices communicate directly with each other in a peer-to-peer manner.

4.1.1.2 Wi-Fi and the ISO-OSI network model

The Open System Interconnection (OSI) network model was proposed by the International Organization for Standardization (ISO) a few decades ago; it is usually portrayed as a stack of seven layers, with each layer acting as a foundation for the layer directly above it; from the top:

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data Link layer
- Physical layer

It isn't worth to summarize here the definition of the upper layers, since it doesn't make any difference to these layers whether they are moving packets through wires, fiber optic lines or radio links.

Wi-Fi specifications concern the way data move through the Physical layer, and it defines a Media Access Control (MAC) layer that handles the interface between the physical layer, and the rest of the network structure.

4.1.1.2.1 The Physical layer

This layer deals mainly with modulation/demodulation and with low-level synchronization. In an 802.11 network the radio transmitter builds a "frame" that encapsulates the core data packet (the "payload"); it adds to the latter

- a 144-bit preamble, of which 128 bits are used by the receiver to synchronize with the transmitter, and 16 bits are a start-of-frame field
- a 48-bit header that contains information about the data transfer speed, the length of the data packet and an error-checking sequence

Since the header specifies the speed of the data that follow it, the preamble and the header are always transmitted at 1 Mbps. There is an optional alternative that uses a 72-bit (56+16) preamble in order to reduce the overhead inherent in transmitting it; this shorter preamble isn't compatible with very old hardware.

4.1.1.2.2 The MAC layer

The MAC layer is a subset of the Data Link layer of the ISO-OSI model. The MAC layer deals mainly with low-level authentication, encryption, and the sharing of the Physical link among competing transmitters (traffic control).

As to traffic control, when more than one node in the network tries to transmit data at the same time, a set of rules called "Carrier Sense Multiple Access / Collision Avoidance" (CSMA/CA) are used to instruct all but one of the conflicting nodes to give way and try again later.

The MAC layer deals also with several settings of the network and/or of a Network Adapter; we list here just a few ones:

- a network can support two power modes: Continuous Aware mode and Power Saving mode; in the first mode, the radio receiver is always on and consuming power; in the latter, the radio is idle much of the time, and periodically it polls the Access Point for new messages
- the Service Set Identification (SSID) is simply the name of the network; as a basic means to keep unauthorized user out of the network, an Access Point uses the SSID: each network node must have the SSID programmed into it or the Access Point won't "associate" it
- the "MAC address" is a unique string of characters that identifies each network node; an optional table of MAC addresses can restrict access to nodes whose addresses are not on the list

Just two remarks: obviously, some notions mentioned in relation with Wi-Fi can apply also to other communication technologies; the two simple access control expedients based on checking SSID and MAC addresses can be spoofed very easily, and cannot really be considered authentication techniques.

4.1.1.3 802.11 family of standards

There are several specifications in the 802.11 family of standards:

802.11	Applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS).
802.11a	An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5 GHz band. 802.11a uses an Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme rather than FHSS or DSSS.
802.11b	Also known, at its appearance as 802.11 High Rates, an extension to 802.11 that provides 11 Mbps transmission with fallbacks to 5.5, 2, and 1 Mbps in the 2.4 GHz band. 802.11b uses only DSS. 802.11b, was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
802.11g	Provides 20+ Mbps in the 2.4 GHz band; it is fully compatible with 802.11b.

802.11n — This recent amendment improves upon the previous 802.11 standards by adding Multiple-Input Multiple-Output antennas (MIMO) - up to 4 streams - and many other newer features. It provides 20/40 Mbps in the 2.4 GHz or 5.0 GHz band.

Protocol	Release	Frequency GHz	Bandwidth Mhz	Data rate per stream (Mbit/s)	Modulation	Indoor range (m)	Outdoor range (m)
-	1997	2.4	20	1, 2	DSSS, FHSS	20	100
a	1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
b	1999	2.4	20	1, 2, 5.5, 11	DSSS	38	140
g	2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM, FHSS	38	140
n	2009	2.4 / 5	20 / 40 per channel (up to 4)	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 / 15, 30, 45, 60, 90, 120, 135, 150 per channel	OFDM	70	250

Table 2 – 802.11 family of standards

While 802.11b was the first wireless networking technology to become popular in the United States with the Wi-Fi name, the faster 802.11a standard gained some ground as vendors attempted selling wireless products to comply with European regulations; similarly 802.11n could benefit from being able to exploit the 5 GHz band.

The 802.11g specification was designed to combine the best features of both 802.11a (higher speed) and 802.11b (greater signal range).

4.1.1.4 Wi-Fi modulation schemes

***Glossary of families of Wi-Fi transmission techniques*:**

SS — Spread Spectrum; spread-spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic or acoustic signal) generated in a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth; these techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, to prevent detection and to limit power flux density (e.g. in satellite downlinks).

DSSS	Direct-Sequence Spread Spectrum; DSSS phase-modulates a sine wave pseudorandomly with a continuous string of pseudonoise (PN) code symbols called "chips", each of which has a much shorter duration than an information bit. Therefore, the chip rate is much higher than the information signal bit rate. DSSS uses a signal structure in which the sequence of chips produced by the transmitter is known a priori by the receiver. The receiver can then use the same PN sequence to counteract the effect of the PN sequence on the received signal in order to reconstruct the information signal.
FHSS	Frequency-Hopping Spread Spectrum is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. It is utilized as a multiple access method in the FH-CDMA.
FDM	Frequency-Division Multiplexing is the method of transmitting multiple data streams over a common broadband medium; each data stream is modulated onto multiple adjacent carriers within the bandwidth of the medium, and all are transmitted simultaneously.
OFDM	Orthogonal Frequency-Division Multiplexing is an FDM scheme, where a large number of closely-spaced orthogonal sub-carriers are used to carry data; the data are divided into several parallel data streams or channels, one for sub-carrier; each sub-carrier is modulated with a conventional modulation scheme (such as QPSK or PSK) at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth. In OFDM, the sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other, meaning that cross-talk between the sub-channels is eliminated. This greatly simplifies the design of both the transmitter and the receiver. The orthogonality allows for efficient modulator and demodulator implementation, using the FFT algorithm on the receiver side and inverse FFT on the sender side. Although the principles and some of the benefits have been known since the 1960s, OFDM is popular for wideband communications today by way of low-cost digital signal processing components that can efficiently calculate the FFT.

Glossary of multi-user access schemes
To allow multiple users to be multiplexed over the same physical channel:

TDMA	Time Division Multiple Access divides access by time; it allows several users to share the same frequency channel by dividing the signal into different time slots: the users transmit in rapid succession, one after the other, each using his own time slot. TDMA is a type of time-division multiplexing, with the special point that instead of having one transmitter connected to one receiver, there are multiple transmitters.
FDMA	Frequency Division Multiple Access divides access by frequency; FDMA is not vulnerable to the timing problems that TDMA has: since a predetermined frequency band is available to a source for the entire period of communication, stream data can easily be used with FDMA.
CDMA	Code Division Multiple Access employs SS technology and a special coding scheme, where each transmitter is assigned a code.
FH-CDMA	Frequency-Hopping Code Division Multiple Access is one of two basic modulation techniques used in spread spectrum signal transmission; it is the

repeated switching of frequencies during radio transmission, often to minimize the effectiveness of the unauthorized interception or jamming of telecommunications.

Glossary of keying schemes applying to various transmission techniques

PSK	Phase Shift Keying is a digital modulation scheme that conveys data by changing or modulating, the phase of a reference signal (the carrier wave).
BPSK	Binary Phase Shift Keying, also sometimes called PRK (Phase Reversal Keying) or 2-PSK, is the simplest form of PSK; it uses two phases which are separated by 180°.
QPSK	Quadrature Phase Shift Keying is a PSK scheme that uses four points on the "constellation diagram", equispaced around a circle; with four phases, QPSK can encode two bits per symbol; it uses gray coding (a binary numeral system where two successive values differ in only one bit) to minimize the bit error rate.
CCK	Complementary Code Keying consists of a set of 64 eight-bit code words; as a set, these code words have unique mathematical properties that allow them to be accurately distinguished from one another by a receiver even in the presence of substantial noise and multipath interference (e.g. interference caused by receiving multiple radio reflections within a building).
FSK	Frequency-Shift Keying is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave.
GFSK	Gaussian Frequency Shift Keying is a type of FSK modulation that uses a Gaussian filter to smooth positive/negative frequency deviations, which represent a binary 1 or 0.

4.1.1.4.1 Use of DSSS and FHSS

The original 802.11 standard specified two different spread spectrum transmission techniques: DSSS and FHSS. All radio equipment use the 2.4 GHz ISM (= Industrial, Scientific and Medical) band and systems based on the original 802.11 standard provide data rates up to 2 Mbps. This is possible because DSSS utilizes an 11-bit chipping code called the Barker Sequence for signal spreading with modulation being achieved using either BPSK or QPSK techniques. (For FHSS, GFSK is employed.)

FHSS was dropped from the 802.11b specification because it was felt that "direct spread" could handle the tradeoff between wireless devices coexisting with other users in connection with severe band separation rules proposed by the FCC. Subsequently the FCC abandoned the stance for the peaceful "coexistence of equipment" requirement (interference rejection) in favor of support for greater wireless network capacity (higher bit-rate). Therefore, for high bit rates above 2 Mbps (5.5 Mbps to 11 Mbps and higher) 802.11b's purely spread spectrum techniques have been supplanted by CCK modulation so as to provide 4 or 8 bits per transmission symbol. The combination of QPSK and CCK is what enables 802.11b's maximum data rate of 11 Mbps. Lower data rates are accommodated through a dynamic rate shifting scheme. 802.11g supports CCK modulation so as to provide backwards compatibility with 802.11b.

4.1.1.4.2 Use of OFDM

The IEEE 802.11a/g/n standards are based on OFDM. OFDM is a broadband multicarrier modulation method that offers superior performance and benefits over older, more traditional single-carrier modulation methods because it is a better fit with today's high-speed data requirements and operation in the UHF and microwave spectrum.

Conceptually, it has been known since at least the 1960s and 1970s; originally known as multicarrier modulation, as opposed to the traditional single-carrier modulation, OFDM was extremely difficult to implement with the electronic hardware of the time; so, it remained a research curiosity until semiconductor and computer technology made it a practical method. OFDM has been adopted as the modulation method of choice for practically all the new wireless technologies being used and developed today; it is perhaps the most spectrally efficient method discovered so far and it mitigates the severe problem of multipath propagation that causes massive data errors and loss of signal in the microwave and UHF spectrum.

4.1.1.5 Wi-Fi operation

In computer networking, a wireless access point (WAP) is a device that allows wired communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a router and can relay data between the wireless and wired devices on the network. A Hot Spot is a common public application of WAPs, where wireless clients can connect to the Internet without regard for the particular networks to which they have attached for the moment.

Wi-Fi operates as a non-switched Ethernet network. Every 100 ms (typical period), Wireless Application Protocols (WAPs) broadcast service set identifiers (SSIDs) using "beacon" packets. Clients who receive these beacons can opt to wirelessly connect to the WAP. This determination is usually established by some combination of the following factors:

- whether or not the client has been configured to connect to the broadcasted SSID
- the signal strength of the WAP. In particular, a client might receive two beacons from two different WAPs, each one broadcasting the same SSID. In this instance, the client should opt to connect to the WAP demonstrating the stronger signal
- the level of encryption offered by a WAP

Each beacon is broadcast at 1 Mbps, ensuring that any client who receives the beacon at a minimum supports communication at this speed. All of the area to which a WAP beacon can be received is referred to as a hotspot; though Wi-Fi hotspots can be several miles long, such an implementation requires multiple WAPs to overlap their individual hotspots using the same SSID.

Wi-Fi can also be used in peer-to-peer mode, allowing mobile devices to communicate with one another in the absence of a wireless network. Although this method of operation does not provide any sort of connectivity to the Internet, it does lend itself to other applications such as backing up data or gaming.

4.1.1.5.1 WAP Limitations

One IEEE 802.11 WAP can typically communicate with 30 client systems located within a radius of 100 meters. However, the actual range of communication can vary significantly, depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, other electronic devices that might actively interfere with the signal by broadcasting on the same frequency, type of antenna, the current weather, operating radio frequency, and the power output of devices. Network designers can extend the range of WAPs through the use of

repeaters and reflectors, which can bounce or amplify radio signals that ordinarily would go un-received.

Most jurisdictions have only a limited number of frequencies legally available for use by wireless networks. Usually, adjacent WAPs will use different frequencies (Channels) to communicate with their clients in order to avoid interference between the two nearby systems. Wireless devices can "listen" for data traffic on other frequencies, and can rapidly switch from one frequency to another to achieve better reception. However, the limited number of frequencies becomes problematic in crowded downtown areas with tall buildings using multiple WAPs. In such an environment, signal overlap becomes an issue causing interference, which results in signal droppage and data errors.

4.1.1.6 Wi-Fi security

There are two major components to Wi-Fi security: encryption and authentication: encryption keeps the communications secret and authentication ensures that only authorized users are allowed to access the network. When most people think about Wi-Fi security, they first think about encryption; because Wi-Fi authentication requires more network infrastructure, the vast majority of home networks only use Wi-Fi encryption. Wi-Fi authentication is more complex: with encryption, there are only three major methods to choose from; with authentication, there are dozens; fortunately, usage seems to be converging on just a couple of methods: EAP-TLS and PEAP.

4.1.1.6.1 Encryption

The airborne nature of Wi-Fi inherently makes it susceptible to security risks. No longer hindered by the need to gain access to a wire, malicious users attempting to capture data transfers must only gain proximity to the intended victim. As such, several encryption protocols have been coupled with Wi-Fi in order to secure the data transferred using Wi-Fi.

WEP	Initially Wireless Equivalent Privacy (WEP) was used to secure Wi-Fi communications. It uses RC4 or ARCFOUR, stream cipher to provide confidentiality. Additionally, WEP employs a 33-bit cyclic redundancy check (CRC-32) to ensure data integrity. Due to a number of shortcomings, WEP has been outdated by Wi-Fi Protected Access (WPA and WPA2).
WPA	Wi-Fi Protected Access; created by the Wi-Fi Alliance, WPA also employs a pass phrase concept similar to that of the WEP implementation. However, WPA can use also distributed private keys administered by an 802.1X authentication server. Data encryption is again provided through the RC4 stream cipher, which uses a 128-bit key and a 48-bit initialization vector. Security is increased by inserting dynamic key changes using the Temporal Key Integrity Protocol (TKIP). Data integrity is guaranteed using the Message Integrity Code (MIC) algorithm, also called Michael's algorithm. While this increased security implementation compensates for the faults found previously with WEP, cryptoanalysts have still found weaknesses in the WPA architecture. Specifically, Michael's algorithm was chosen because it allowed mobile devices using WPA to communicate with access points still using WEP and vice versa. However, the algorithm is still susceptible to packet forgery attacks. To combat this, WPA was enhanced and expanded into WPA2.
WPA2	In Wi-Fi Protected Access version 2 (WPA2), Michael's algorithm is replaced by the Counter Mode with Cipher Block Chaining Message Authentication

Protocol (CCMP). Because CCMP provides both data integrity and key management using the Advanced Encryption Standard (AES, also known as Rijndael) it combines both the data integrity and confidentiality functions of WPA into one protocol. CCMP is considered secure at a very high degree.

4.1.1.6.2 WPA encryption modes

When choosing WPA encryption for an Access Point, the setup program usually will offer the choice between two encryption modes:

RADIUS	Remote Authentication Dial-In User Service (RADIUS); in large networks WPA uses an authentication server, usually wired to the Access Point to verify the identity of each network user; the server uses the RADIUS protocol, that provides centralized Authentication, Authorization, and Accounting (AAA) management and EAP (described hereinafter) to exchange encryption keys with the nodes in the wireless network.
PSK	Pre-Shared Key (PSK); not to be confused with the PSK modulation technique; small networks, such as home networks and networks lacking an authentication server, use a passphrase stored in the Access Point. A PSK network uses the passphrase to set up the initial connection between a client and the Access Point; once the connection is in place, the TKIP assigns new encryption keys to every data packet or group of packets.

4.1.1.6.3 Authentication

The security specifications for Wi-Fi are defined by 802.11i (2004), being incorporated in the IEEE 802.11-2007 standard; WPA2 fully implements 802.11i, while WPA only a subset of it.

The most complete authentication setting includes three subjects, as in the traditional RADIUS scheme: the Wi-Fi client station, the AP, acting as the authenticator and an authentication server. But mutual authentication and key exchange processes were added to the 802.11i standard: as a first step, the AP needs to authenticate itself to the client station; these additions allowed the authentication process to scale and also provided for dynamic key creation and updating, providing faster client authentication and roaming.

Four primary phases are required to establish secure communications (four-way handshake): Discovery-Negotiation, Authentication, Key Management, exchange of keys for Data Confidentiality and Integrity. During the Authentication phase the AP can forward to an authentication server (possibly on a wired network) the credentials provided by the client station; this server will authorize or deny access to the network; in addition the authentication server may return configuration information to the AP, such as placing the Wi-Fi user in a specific VLAN.

The first building block that led up to 802.11i was EAP.

EAP	Extensible Authentication Protocol is a framework providing a number of authentication methods to be used for the generation, transport and usage of keying material and parameters. There are several types of EAP methods used today; seven of these types are approved for interoperability by the Wi-Fi Alliance; three are mentioned below.
EAP-TLS	EAP-Transport Layer Security requires a server-site certificate and a client-site certificate for credentials. EAP-TLS is the original, standard wireless LAN EAP authentication protocol. Although it is rarely deployed, it is still

considered one of the most secure EAP standards available and is universally supported by all manufacturers of wireless LAN hardware and software. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength.

EAP-TTLS — EAP-Tunneled Transport Layer Security is the second most popular type: a user must have a server-site certificate and uses just a user name and password. This greatly simplifies the setup procedure as a certificate does not need to be installed on every client.

PEAP — Protected EAP is probably the most commonly deployed type. In this method, the server-site certificate is required, the client-site certificate is optional and a standard user name and password is used. Advantage of PEAP is that it can leverage user name and passwords already defined in an Active Directory.

4.1.1.7 Wi-Fi versus WiMAX

Comparisons and confusion between WiMAX (Worldwide Interoperability for Microwave Access) and Wi-Fi are frequent because both are related to wireless connectivity and Internet access.

- WiMAX is a long range system, covering many kilometers, that uses licensed or unlicensed spectrum to deliver connection to a network, in most cases the Internet
- Wi-Fi uses unlicensed spectrum to provide access to a local network; is more popular in end user devices; runs on the Media Access Control's CSMA/CA protocol, which is connectionless and contention based, whereas WiMAX runs a connection-oriented MAC

WiMAX and Wi-Fi have quite different quality of service (QoS) mechanisms:

- WiMAX uses a QoS mechanism based on connections between the base station and the user device. Each connection is based on specific scheduling algorithms
- Wi-Fi uses contention access - all subscriber stations that wish to pass data through a wireless access point (AP) are competing for the AP's attention on a random interrupt basis. This can cause subscriber stations distant from the AP to be repeatedly interrupted by closer stations, greatly reducing their throughput

Both 802.11 (which includes Wi-Fi) and 802.16 (which includes WiMAX) define Peer-to-Peer (P2P) and ad hoc networks, where an end user communicates to users or servers on another Local Area Network (LAN) using its access point or base station. However, 802.11 supports also direct ad hoc or peer to peer networking between end user devices without an access point, while 802.16 end user devices must be in range of the base station.

Wi-Fi and WiMAX are complementary. WiMAX network operators typically provide a WiMAX Subscriber Unit which connects to the metropolitan WiMAX network and provides Wi-Fi within the home or business for local devices (e.g. Laptops, Wi-Fi Handsets, smart phones) for connectivity. This enables the user to place the WiMAX Subscriber Unit in the best reception area (such as a window) and still be able to use the WiMAX network from any place within their residence.

4.1.1.8 Embedded Wi-Fi design considerations

Wi-Fi networking is becoming more popular for embedded applications; dedicated ICs and chipsets are available more and more; but implementing Wi-Fi networking for embedded systems poses some special challenges for the systems designer.

4.1.1.8.1 Choosing the standard

The most popular Wi-Fi devices for embedded systems are based on 802.11b and 802.11g. 802.11g is compatible with 802.11b devices and provides a much higher maximum data rate at a cost dropping fast. Both 802.11b and 802.11g use the 2.4 GHz operating frequency; this frequency could be crowded by other devices, both Wi-Fi and not: if interference is an issue, 802.11a should be considered, since it uses the relatively uncrowded 5GHz frequency band; but 802.11a availability is relatively low in the embedded space and has limited deployment in the consumer space: if you aren't in control of the makeup of the Wi-Fi network and need to integrate into existing Wi-Fi networks, 802.11b or 802.11g would be definitely better. Support for 802.11n is still poor: although 802.11n has the highest data rate available, it has very little presence in the embedded world.

4.1.1.8.2 Type of interface of the Wi-Fi device

Many Wi-Fi devices for embedded systems provide only serial-to-Wi-Fi functionality; the idea is that the Wi-Fi device has preloaded firmware and you use a serial port on your embedded device to interface with the Wi-Fi device; this option works well for applications that need only one connection (or socket) at a time. It is especially well-suited for allowing a serial port to be accessed over the network. An increasing number of single-board computers and core modules are available that have Wi-Fi integrated as a native network interface; typically this allows full socket-level access so that you can run a full networking system; this can make for an overall cheaper solution (at production time) since a separate device is not needed; of course, if you are adding Wi-Fi capabilities to an existing system, the serial-to-Wi-Fi devices will be much easier to implement.

4.1.1.8.3 Security features

In general, the more Wi-Fi authentication methods are supported, the better. Note that support for Wi-Fi encryption and authentication with ad-hoc mode networks (that is, networks with direct device-to-device communication without an access point) is generally poor; this is not a condition unique to the embedded world; support is spotty everywhere; for this reason, you should consider only infrastructure mode (with an access point) if you need Wi-Fi security.

4.1.1.8.4 Power consumption

Wi-Fi was not designed to be especially frugal with its power usage unlike other wireless technologies like Bluetooth or 802.15.4 (used for ZigBee); however, many Wi-Fi applications, require a leaner power profile. You will want to know how much power the Wi-Fi device uses when transmitting, which should give an idea of the upper bound; some typical values would be around 300 to 500 mA at 3.3V. You will also need to know how much power it uses when the Wi-Fi interface is idle; some embedded Wi-Fi devices allow you to turn off the Wi-Fi subsystem when not in use; for applications that perform some data collection and then periodically upload the data over the Wi-Fi network, this could be an acceptable solution. If the device needs to be remotely accessible at all times, the 802.11 specification help address this: it includes support for power-saving features; devices can notify an access point when they are entering power-down mode; the access point will then buffer any data destined for that device; once the device powers back up, it notifies the access point and can then receive any buffered data; typically, a device is only down for about 300 ms before checking back in with the access point.

4.1.1.8.5 Performance

The type of Wi-Fi network (such as 802.11b or 802.11g) can give you a rough indication of the performance of a Wi-Fi device, but just because a device has a theoretical data rate of up to 54Mbps does not mean it will achieve that performance. First of all, typical throughput for any Wi-Fi device is usually less than half that of the maximum data rate; furthermore, embedded devices tend to have lower performance; also, the maximum typical throughput that you can expect will vary widely depending on the embedded solution you choose: serial-to-Wi-Fi devices would typically have lower throughput just because the data must first be stuffed through a serial connection; but even integrated Wi-Fi solutions could have relatively low performance. Furthermore, some of the security options you choose can affect your performance; unlike encryption, Wi-Fi authentication does not typically affect your data throughput; it does, however, affect how long it takes your device to join the Wi-Fi network.

4.1.1.8.6 Long-term availability and support

Until recently, it was difficult for manufacturers of embedded devices to integrate Wi-Fi support; Wi-Fi chipsets were targeted more towards the consumer market, which meant chipsets were frequently introduced and EOL'd (end-of-lifed). It t's important to consider the long-term availability of your Wi-Fi solution: if you're using a serial-to-Wi-Fi-style device, it probably includes "canned" firmware that is installed at the factory; therefore, if the manufacturer finds that they need to change the Wi-Fi chipset used, they can change the installed firmware at the factory before they even sell you the device; however, if you're using an embedded device with an integrated Wi-Fi chipset, you should more carefully consider what a change to the Wi-Fi chipset means for you.

4.1.1.8.7 Wi-Fi certification

As intentional radiators, Wi-Fi devices must be qualified by regulatory agencies for specific regions; in the United States, the Federal Communications Commission (FCC) must qualify the device. If the solution you're using is a boxed product (such as a serial-to-Wi-Fi device), it's pretty simple--the device needs to be certified for the regions in which you're interested. If you're integrating a core module or other device into your product, it's a bit more complex; ideally, you would want the module certified in such a way that you won't need to certify your product; fortunately, most regulatory agencies have a form of modular certification that allows just this. You want your device's Wi-Fi certification to ride on that of the Wi-Fi device manufacturer; doing your own Wi-Fi certification testing is complex and expensive, so you want to avoid this if at all possible. Furthermore, the software or firmware for the embedded solution needs to provide ways to set the current regulatory region; this involves changing which Wi-Fi channels are available for use, as well as, the maximum transmit power. An option for configuring a device to conform to regional regulations is to use functionality provided by the IEEE 802.11d specification; this allows access points to broadcast the local regulatory domain so that a Wi-Fi client can automatically detect this and comply.

4.1.1.8.8 Other considerations

Wi-Fi often requires the placement or positioning of some sort of antenna. What options does your solution provide? Is there an internal antenna? If so, does it provide satisfactory performance (particularly with the range)? If the antenna is external, are you allowed to use an antenna of your choice? Wi-Fi devices are generally certified for use with specific antennas; use of other antennas could be a violation of local regulations.
Finally, you might need to consider how the Wi-Fi device performs when roaming from one access point to another. For infrastructure mode networks, multiple connected access points are often used to canvass a larger area than a single access point could cover. Some embedded devices might "lock on" to a single access point, even when another access point becomes a

better choice. Ideally, a device would be able to switch from one access point to another very quickly with minimal interruption in communication.

4.1.1.9 Wi-Fi standard and regulation bodies

The FCC (Federal Communications Commission, http://www.fcc.gov/) is a US regulatory body responsible for governing inter-state communications by radio, television, wire, satellite and cable.

The IEEE (Institute of Electrical and Electronic Engineers, http://www.ieee.org/) is an international body that specifies industry standards for power, consumer electronics, and computers, including computer communications.

The ETSI (European Telecommunications Standards Institute, http://www.etsi.org/) is a European body that specifies standards used by telecommunications networks operating within 56 European countries.

The IEEE defines standards like 802.11b that WLAN vendors implement worldwide. The FCC defines rules about radio use in the US; for example, 802.11b WLANs can be operated without a license in the 2.4 GHz ISM band. ETSI defines standards like ETSI Broadband Radio Access Networks (BRAN) and HIPERLAN implemented in products sold primarily within Europe. ETSI and IEEE are collaborating to harmonize BRAN and 802.11a standards because both operate in the 5 GHz band.

4.1.1.10 Channels and international compatibility

802.11 divides each of the above-described bands into channels, analogously to how radio and TV broadcast bands are sub-divided, but with greater channel width and overlap. For example the 2.4000–2.4835 GHz band is divided into 13 channels each of width 22 MHz but spaced only 5 MHz apart, with channel 1 centered on 2.412 GHz and 13 on 2.472 GHz to which Japan adds a 14th channel 12 MHz above channel 13.

Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various services. Now, almost all European countries follow the European model of allowing channels 1 through 13.

Besides specifying the centre frequency of each channel, 802.11, also, specifies a spectral mask defining the permitted distribution of power across each channel. The mask requires that the signal be attenuated by at least 30 dB from its peak energy at ±11 MHz from the centre frequency, the sense in which channels are effectively 22 MHz wide. One consequence is that stations can only use every fourth or fifth channel without overlap, typically 1, 6 and 11 in the Americas, and in theory, 1, 5, 9 and 13 in Europe although 1, 6, and 11 is typical there too. Another is that channels 1-13 effectively require the band 2.401–2.483 GHz, the actual allocations being, for example, 2.400–2.4835 GHz in the UK, 2.402–2.4735 GHz in the US etc.

4.1.1.11 Wi-Fi regulations in Europe: DFS and TPC compliance

DFS stands for "Dynamic Frequency Selection", TPC for "Transmit Power Control".
Europe (ETSI) allows Wi-Fi operation on several channels in the 5GHz band. The main idea was to make additional capacity available to Wi-Fi technology. In Europe, EN 301 893 defines regulatory requirements for Wireless Access Systems operation in the 5GHz band. The ETSI allows Wireless Access Systems including WLAN devices to use the Unlicensed National Information Infrastructure UNII-1, UNII-2 and UNII-3 bands - specifically, channels in the 5.15GHz to 5.25GHz, 5.25GHz to 5.35GHz (UNII-2) and 5.47GHz to 5.725GHz (UNII- 3) bands. The allowance especially in the UNII-2 and UNII-3 comes with an important caveat - DFS Compliance.

DFS is required to allow the co-existence of WLAN systems with military and weather radar systems. A DFS certified AP is required to detect the existence of new radar in UNII-2 or UNII-3 bands and quickly move any interfering transmission to other channels, clearing the path for the radar. In 2009 new EN 301 893 v1.5.1 requirements also called DFS-3 Compliance will be enforced affecting 802.11 APs operating in Europe. As of the date of this Advisory (November 2009) the DFS-3 compliance affects APs operating on 5GHz channels only in Europe.
The regulatory requirements for DFS, along with requirements for Transmit Power Control (TPC) and uniform channel loading, have been adopted in Europe, the United States of America, and many other geographical areas. In the (following) I hope to provide an overview of the current and proposed DFS requirements for Europe, the current DFS requirements for the USA and how they relate to requirements in Canada, Taiwan, Australia, and Japan.

4.1.1.11.1 General Overview of DFS

Standards that incorporate DFS define various requirements for the detection of radars using the following terms:

Channel Availability Check Time
: The time a system shall monitor a channel for presence of radar prior to initiating a communications link on that channel. This is also referred to by the acronym CAC.

Interference Detection Threshold
: The minimum signal level, assuming a 0dBi antenna, that can be detected by the system to trigger the move to another channel.

Channel Move Time
: The time for the system to clear the channel and measured from the end of the radar burst to the end of the final transmission on the channel.

Channel Closing Transmission Time
: The total or aggregate transmission time from the system during the channel move time.

Non-Occupancy Time
: A period of time after radar is detected on a channel that the channel may not be used.

Master Device
: Device that has radar detection capabilities and can control other devices in the network (e.g. an Access Point would be considered a master device).

Client Device
: Device that does not initiate communications on a channel without authorization from a master device (e.g. a laptop Wi-Fi card - note that a Wi-Fi card that supports ad-hoc mode would be considered a master device).

Radio Local Area Network (RLAN) or Wireless Local Area Network (WLAN)
: Generic terms for wireless systems such as 802.11a and 802.11n that operate in the 5GHz unlicensed bands.

The operation of a system with DFS capability takes the following:

- The master device selects a channel and monitors that channel for potential radar interference for a minimum listening time (channel availability check time). No transmissions can occur during this period. If interference is detected then the

system has to go and select another channel and repeat the channel availability check on the new channel (the original channel is added to a list of channels with radar)
- Once a channel has been selected and passes the channel availability check interference the network starts to use that channel
- While using the channel the network's master device continuously monitors for potential interference from a radar source (this is referred to as in-service monitoring). If interference is detected then the network master device issues commands to all other in-network devices to cease transmissions

While master devices are required to employ interference detection capabilities, client devices generally only need to be capable of responding to the master device's instructions to clear the channel. This means that client devices cannot employ active scanning techniques to find a network but must rely on passive scanning (listen-only) to find a network to join.

Point-to-point communication links operating in the DFS bands need to consider the implications of the radar interference potential at one end of the link will be very different from the interference potential at the other end of the link. For this reason it is expected that both ends of the link should be performing radar detection functions. The ETSI technical report TR 102 651 V1.1.1 (1) provides additional guidance in implementing a DFS strategy for various wireless network configurations.

4.1.1.11.2 DFS in the European Union

ETSI standard EN 301 893 V1.5.1(2), the European Union's harmonized radio standard for unlicensed devices operating in the 5150-5350 MHz and 5470-5725 MHz frequency bands, contains DFS requirements. This version of the standard superseded the V1.4.1 version on June 30, 2010. It specifies the types of waveforms that systems operating in the 5250-5350 MHz and 5470-5725 MHz bands should be able to detect, the maximum allowed values for closing and move times and the minimum channel availability check time. EN 301 893 does not require this feature for client devices provided that they:

- operate below a power level of 200mW
- are not capable of initiating communication on a channel (in effect, this prohibits them from using active scanning to detect a wireless network)
- only operate on a channel under control of a device with the detection capability (master device)
- respond to the commands to move to another channel from the master device
- meet the channel move time and channel closing transmission time

4.1.1.12 Wi-Fi in the TSA Guidelines

TSA stands for the USA "Transportation Security Administration".
The FCC has set aside several frequency bands for unlicensed operations. The most popular commercial bands are the so-called Wi-Fi frequencies developed for wireless local area networks (WLANs); those in the 802 are described in Table below.

Radio Band (frequencies)	Description and Application
2.400 to 2.483 GHz	IEEE 802.11 b/g Wireless LAN, also known as Wi-Fi IEEE 802.15 Bluetooth also uses this band
5.150 to 5.350 GHz 5.250 to 5.350 GHz 5.750 to 5.875 GHz	IEEE 802.11a Wireless LAN, also known as Wi-Fi

Table 3 — Most popular Wi-Fi frequencies

Wi-Fi systems are generally considered to operate over relatively short ranges because of FCC restrictions on radiated power and because, as a shared medium, as the number of users increases the range for all users decreases. With the proper equipment, however, video transmission over ranges of 20 miles or more have been demonstrated.

Since it is difficult, and in some cases impossible, for airports to control Wi-Fi operations, using Wi-Fi frequencies for airport operations requires special attention to what functions should be permitted over wireless links and how to secure them over the network. Most video surveillance imagery is perishable in time, in which case transmitting it without encryption may be permitted if the network is adequately secured. That will not, however, protect such transmissions from interference. In principle, video imagery and other security information which must be delivered should not use the Wi-Fi bands, however, if an airport and its tenants can agree to reserve the 802.11 a band solely for airport use this problem can be mitigated.

Issues of Wi-Fi interference and transmission security will require close cooperation between airport security and the airport IS/IT department.

Many airports already have 802.11 wireless local area networks (WLANs) installed, either by airport management or by airport tenants. Since these WLANs operate in unlicensed bands, any user can install equipment that meets FCC standards for transmitted power levels. The proliferation of this equipment and the resulting potential for mutual interference, poses a challenge for airports in view of the FCC reaffirming that it alone can regulate radio operations.

Airports can seek to limit interference through voluntary agreements with tenants, who face the same problems and can also restrict tenants from attaching Wi-Fi antennas to airport property, but under existing FCC rulings airports cannot otherwise prohibit a tenant from operating Wi-Fi equipment.

4.1.2 Ethernet and Gigabit Ethernet

4.1.2.1 Ethernet network

Ethernet was developed by the Xerox Corporation's Palo Alto Research Centre (known colloquially as Xerox PARC) in 1972 and was probably the first true LAN to be introduced.

In 1985, the Institute of Electrical and Electronic Engineers (IEEE) in the United States of America produced a series of standards for Local Area Networks (LANs) called the IEEE 802 standards. These have found widespread acceptability and now form the core of most LANs. One of the IEEE 802 standards, IEEE 802.3, is a standard known as "Ethernet". This is the most widely used LAN technology in the world today. Although IEEE 802.3 differs somewhat from the original standard (the "blue book" defined in September 1980) it is very similar, and both sets of standards may be used with the same LAN.

The IEEE standards have been adopted by the International Standards Organization (ISO) and are standardized in a series of standards known as ISO 8802-3. ISO was created in 1947 to construct world-wide standards for a wide variety of engineering tasks. Adoption of ISO standards allows manufacturers to produce equipment which is guaranteed to operate anywhere it is finally used. ISO standards tend to be based on other standards (such as those produced by the IEEE), the only problem is that the ISO standards tend to be issued later and are therefore less up to date.

The simplest form of Ethernet uses a passive bus operated at 10 Mbps. The bus is formed from a 50 Ohm co-axial cable which connects all the computers in the LAN. A single LAN may have up to 1024 attached systems, although in practice most LANs have far fewer. One or more pieces of coaxial cable are joined end to end to create the bus, known as an "Ethernet Cable Segment". Each segment is terminated at both ends by 50 Ohm resistors (to prevent reflections from the discontinuity at the end of the cable) and is also normally earthed at one end (for electrical safety). Computers may attach to the cable using transceivers and network interface cards.

Frames of data are formed using a protocol called Medium Access Control (MAC), and encoded using Manchester line encoding. Ethernet uses a simple Carrier-Sense Multiple Access protocol with Collision Detection (CSMA/CD) to prevent two computers trying to transmit at the same time (or more correctly to ensure both computers retransmit any frames which are corrupted by simultaneous transmission).

100 Mbps networks may operate full duplex (using a Fast Ethernet Switch) or half duplex (using a Fast Ethernet Hub). 1 Gbps networks usually operate between a pair of Ethernet Switches.

Ethernet LANs may be implemented using a variety of media (not just the coaxial cable described above). The types of media segments supported by Ethernet are:

- 10B5 Low loss coaxial cable (also known as "thick" Ethernet)
- 10B2 Low cost coaxial cable (also known as "thin" Ethernet)
- 10BT Low cost twisted pair copper cable (also known as Unshielded Twisted Pair (UTP), Category-5)
- 10BF Fiber optic cable
- 100BT Low cost twisted pair copper cable (also known as Unshielded Twisted Pair (UTP), Category-5)
- 100BF Fiber Fast Ethernet
- 1000BT Low cost twisted pair copper cable (also known as Unshielded Twisted Pair (UTP), Category-5)
- 1000BF Fiber Gigabit Ethernet
- 10000BT Category 6 (Unshielded Twisted Pair (UTP), Category-6)
- 10000BT Fiber 10 Gigabit Ethernet

There is also a version of Ethernet which operates fiber optic links at 40 Gbps and at 100 Gbps. Many LANs combine the various speeds of operation using dual-speed switches which allow the same switch to connect some ports to one speed of network and other ports at another speed. The higher speed ports are usually used to connect switches to one another.

Ethernet has also evolved to provide network Operations and Management (OAM) functions. These standards allow operators to manage the network (Connectivity Fault Management, CFM) and to validate the performance of the service. Standards such as 802.3ah manages a single-hop link, other standards extend this to multi-segment networks.

Some of the main elements in a Ethernet network are:

- DTEs (Data Terminal Equipment)
- Hubs
- Switches
- Routers
- Media converters

4.1.2.1.1 DTE

Ethernet DTEs are devices such as computers which are trying to communicate on the Ethernet network.

4.1.2.1.2 Hub

Hubs are used in Ethernet bases 10 and bases 100. Hub is the simplest concentrator. It is practically only one repeater. It amplifies the signal to be able to transfer it towards all connected PC. All information arriving on the equipment is thus transmitted on all the lines. In the case of important networks by the number of connected PC or the importance of the flow of transferred information, hub can not be used. Indeed, as soon as a PC says something, everyone hears it and when each one starts to transmit, speeds decrease directly.

According to the standard, the maximum number of hubs in cascade (connected port to port, by stackable types) is limited to 4 between 2 stations for the 10 base T and to 2 for the 100 base T. This is related on the maximum travel time of an Ethernet signal before its disappearance and to the time of detection of the collisions on the cable. It could be that the collision is not detected in time and that the second transmitting station sends the message by thinking that the way is free.

This does not stand for the switch "blind and forward" which records the screens before sending them and segment the network according to connections, avoiding these collisions.

4.1.2.1.3 Switch

Ethernet Switches are a simple way to increase the number of nodes, extend network distances while introducing the smallest amount of latency. Hubs don’t examine the Ethernet packets for destination information so they deliver the packets even more quickly than a switch. All messages received by the hub are sent out on all legs to all the connected devices. A switch recognizes the various computers, servers, routers, printers and firewall connected on the network. By receiving information, it decodes the heading to know the recipient and sends it only towards this one in the case of a connection PC towards PC. This reduces the traffic on the complete network.

There are mainly two kinds of switches (managed and unmanaged):

Unmanaged Ethernet switches are a plug and play installation. Switches increase the number of nodes and the length of the LAN. They are designed to divide the network into separate collision domains. This reduces overall traffic on a LAN, improving communication speed and reducing errors.

Switches route communication to the desired end device instead of broadcasting the communication to everyone connected to the LAN. This is accomplished by the bridge’s ability to set up a table of device addresses connected to each leg of the switch. With this information the bridge knows where to send each Ethernet packet once it is received.

Managed Ethernet switches allow advanced control of the LAN. They usually include software to configure the network and diagnostic ports to monitor LAN traffic. If communications fail, most managed bridges will alert the manager via e-mail or by closing a relay to trigger an audible signal or flash a light. Another feature available on managed bridges is QoS (Quality of Service) programming which prioritizes messages ensuring important data receives the highest priority on the LAN segment.

While hubs could isolate some aspects of Ethernet segments, such as cable breakages, they still forwarded all traffic to all Ethernet devices. This creates practical limits on how many machines could communicate on an Ethernet network. The entire network was one collision domain and all hosts had to be able to detect collisions anywhere on the network. This limited

the number of repeaters between the farthest nodes. Segments joined by hubs had to all operate at the same speed, making phased-in upgrades impossible.

To alleviate these problems, switching was created to communicate at the data link layer while isolating the physical layer. With switching, only well-formed Ethernet packets are forwarded from one Ethernet segment to another; collisions and packet errors are isolated. Prior to discovery of network devices on the different segments, Ethernet switches work somewhat like Ethernet hubs, passing all traffic between segments. However, as the switch discovers the addresses associated with each port, it forwards network traffic only to the necessary segments, improving overall performance. Broadcast traffic is still forwarded to all network segments. Switches also overcame the limits on total segments between two hosts and allowed the mixing of speeds, both of which became very important with the introduction of Fast Ethernet.

4.1.2.1.4 Router

A router is similar in a switch in that it forwards packets based on address. But, instead of the MAC address that a switch uses, a router can use the IP address. This allows the network to go across different protocols.

The most common home use for routers is to share a broadband internet connection. The router has a public IP address and that address is shared with the network. When data comes through the router it is forwarded to the correct computer.

4.1.2.1.5 Media Converters

Media Converters change Ethernet twisted pair copper wires into fiber optic signals. Fiber optic is often preferable because it is impervious to interference that can disrupt the signals being carried by copper. Because fiber can extend the distance of a network up to 2 km in each segment, media converters can also increase the range of a network.

4.1.2.2 Secure Ethernet network

The trend toward using Ethernet as the sole communications network for business and industry has raised concerns about security. While proprietary networks for building or factory automation have major drawbacks in terms of limiting information flow and higher cost, their separation from other systems provides a measure of protection against unauthorized access.

4.1.2.2.1 Create a secure environment

A comprehensive security plan must protect against unauthorized access from both internal and external sources. Methods of security can range from technologies based within the infrastructure itself such as physical connection paths and Virtual Local Area Networks (VLANs) to hardware and software-based devices such as firewalls and security management servers.

The most secure network, of course, is one that has no connections to other systems. But that defeats the major advantage of Ethernet--its easy connectivity to other Ethernet networks or the Internet for information sharing.

One of the most often-overlooked security measures is physically securing switches and wiring closets. Something as simple as enclosing devices in a lockable cabinet or closet and limiting access to authorized persons can prevent tampering or accidental de-coupling of a device link. In addition to physically preventing unauthorized access, it also makes sense to secure a backup copy of switch configurations using TFTP (Trivial File Transfer Protocol), a feature found in many switches, each time a change is made. This is not only a security measure but also a recovery method if a device should fail and require replacement.

Another method of easily securing infrastructure devices such as switches is password protection. Out of the box, most switches can be accessed using a serial DB9 console connection. This management interface is used to assign an IP address for remote TCP/IP-based telnet management.

Default passwords for switches may be standardized across a manufacturer's entire product line and are published in product documentation and on the web. Many users, including IT organizations, fail to change the default passwords and permissions. If an unauthorized user reaches an unsecured switch, he or she would be in complete command of the switch with the ability to change configurations or disable ports. It is therefore essential, even without an Ethernet connection to the corporate LAN or Internet, that physical security and password protection is part of any security program.

As the sophistication of an Ethernet network for building or factory automation grows, features once found only in enterprise class devices are finding their way into daily use at the workgroup level. Access control features can be configured in some switches and routers to allow only specific workstations to access a device or pass through to a target.

4.1.2.2.2 Physical Security

Physical security is crucial to a secure operating environment. Switches and routers must be held in place in a secure and sturdy fashion, preferably installed in a rack or enclosure in a secure area. Network equipment is usually equipped to be restored to factory defaults should a password be forgotten. For this reason, all ports including console and auxiliary ports should be secured by a lock or located in a lockable enclosure to prevent unauthorized access.

4.1.2.2.3 Port-based security

Port security on a switch can prevent unauthorized users from plugging in devices, such as workstations or printers. Devices like these could disrupt network operations by introducing excessive amounts of traffic and possibly errors. Administratively disabling unused ports will prevent traffic from entering the network if an unauthorized device is plugged in.

Additionally, port-based hardware address (MAC address) management may be used on a switch in order to deny access to a non-authorized device. Service will not be provided if a non-configured MAC address is sensed. This can also be used as a precaution against connecting more than the allotted number of workstations or devices to a port. If a device is replaced with one having a different MAC address, the port assignment must be appropriately re-assigned by the network administrator.

Access lists can also be utilized on supported switches and routers to permit or deny users from gaining access to specific network devices or specific resources on network devices. This is commonly known as packet and service filtering and is placed on certain interfaces. Using access lists ties up processor resources, however, and has to be locally administered on each interface within each routing device.

4.1.2.2.4 Virtual LANs

Virtual LANs are a grouping of Ethernet ports on an IEEE 802.1Q compliant switch or a grouping of switches. A VLAN may be used to help isolate packet and broadcast traffic on a factory automation network, for example, from the IT network. Measures like this are generally reserved for isolating extraneous traffic such as broadcasts that may interfere with control communications, but can also be implemented as security tools.

Switches can be divided into VLANS that could render devices on separate VLANs unreachable. The downside to switch port-based VLANS as a security strategy is management, since a port can belong to multiple VLANs extending across multiple switches.

Multi-layered VLANS can be challenging to administer. For multiple VLANs to span multiple switches, the Spanning Tree Protocol, STP, may have to be disabled as well. For example, if two VLANS exist on each of two switches, each VLAN needs a connection to the corresponding VLAN on the other switch, requiring two links between each switch. STP will disallow multiple links between devices to prevent loops.

VLANs can also be used to segment broadcast domains within a network. Since VLANs are logically segmented local area networks, physical areas do not restrict them. Utilizing VLANS reclaims network bandwidth by breaking down broadcast domains and segments one network of devices from another within the same switch.

VLAN segmentation is accomplished by assigning the ports of a device into separate VLAN memberships. For example, ports 1 and 2 may be assigned to VLAN1. Ports 3 and 4 may be assigned to VLAN2. Ports 1 and 2 will not see broadcasts or traffic from ports 3 and 4, and vice versa. This separation is accomplished at OSI layer 2. If a third VLAN were created using ports 1, 2, 3, 4 and 5, then a device on port 5 would see all broadcast traffic from ports 1, 2, 3 and 4.

4.1.2.2.5 Firewall Technologies

A firewall is a device that is implemented on a network to provide security from potential intruders. A firewall has more granular control over what can and cannot be accessed from outside the secure network than an access list can provide. A firewall can be a network appliance or a piece of software on a stand-alone server or router equipped with multiple network adapters or interfaces. A firewall provides this granular control by using its own protocol stack and, depending on the firewall, it checks each level of the stack for erroneous information.

A firewall works by examining each packet that passes between the two adapters and by comparing access rules at several different levels before allowing that packet to pass. Once a packet has been validated by all of the requirements to pass through, the firewall applies network address translation (NAT). NAT is used to hide the internal network IP addresses by substituting the actual source address with the outside address of the firewall. This acts to hide the original internal address of the sender inside the firewall.

Firewalls allow filtering on MAC addresses, IP addresses, port numbers or even certain commands and services. Each firewall offers a different level of security depending on the vendor, features and costs. Selecting and implementing a firewall into any infrastructure requires research, planning and feature/cost comparison.

Every vendor offers a different set of features, such as authentication support, logging, additional memory and performance classes. The more security checks performed, for example, the slower transactions will take place. Some firewall management suites also allow rules to be downloaded and applied to other network devices such as routers that may be internal or external.

4.1.2.3 QoS over Ethernet network

Quality of service is the ability to provide different priority to different applications, users, or data flows or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, video streaming, since these often

require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource.

A network or protocol that supports QoS may agree on a traffic contract with the application software and reserve capacity in the network nodes, for example during a session establishment phase. During the session it may monitor the achieved level of performance, for example the data rate and delay, and dynamically control scheduling priorities in the network nodes. It may release the reserved capacity during a tear down phase.

When looking at packet-switched networks, quality of service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, Grade of Service etc.

Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver:

Throughput
Due to varying load from other users sharing the same network resources, the bit-rate (the maximum throughput) that can be provided to a certain data stream may be too low for real time multimedia services if all data streams get the same scheduling priority.

Dropped packets
The routers might fail to deliver (drop) some packets if their data is corrupted or they arrive when their buffers are already full. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

Errors
Sometimes packets are corrupted due to bit errors caused by noise and interference, especially in wireless communications and long copper wires. The receiver has to detect this and, just as if the packet was dropped, may ask for this information to be retransmitted.

Latency
It might take a long time for each packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. This is different from throughput, as the delay can build up over time, even if the throughput is almost normal. In some cases, excessive latency can render an application such as VoIP or online gaming unusable.

Jitter
Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.

Out-of-order delivery
When a collection of related packets is routed through a network, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of sequence.

For Ethernet network two levels of QoS are available:

QoS in layer 2: Ethernet switches support the IEEE 802.1 Q/p standard for providing QoS. This standard allows a service provider to attach special tags, called VLAN IDs, to all incoming

frames from a customer. It consists of adding 4 bytes to the Ethernet frame. The first 2 bytes are the type protocol identifier. This identifies the frame as a tagged frame. The second byte is the VLAN tag and is used to identify the frame as belonging to a specific group on the network. When the frames go through the Ethernet network, the different switches along the way will read the VLAN tag and determine where the frame should be delivered. The first 3 bits of the VLAN tag are used to identify the priority of the frame.

By doing this, the service provider can have multiple customers using the same circuit, but still maintain a separation between them. Each customer's traffic is identified by a different VLAN tag. The method also allows for the addition of a priority value to be associated to the VLAN tag. By using the priority field, the service provider can offer different classes of service to their customers.

QoS in layer 3: There are currently two QoS standards available for the IP level. The first standard is the RFC-791, which defines the Type of Service (ToS). The second standard is RFC-2475, which defines Differentiated Services Code Point (DSCP). Both of these standards use the same field in the IP packet header to identify the level of service for the packet. The RFC-791 was the original standard but was replaced by the newer standard RFC-2475.
The IP ToS field is an 8-bit field in the IP datagram. The first 3 bits of the field are the Precedence field. This prioritizes packets within a queue. Packets with a higher priority value are transmitted before others. The other 5 fields that are present also act as routing criteria. These fields are: Delay, Throughput, Reliability, Cost and Future.

Early work used the "IntServ" philosophy of reserving network resources. In this model, applications used the Resource reservation protocol (RSVP) to request and reserve resources through a network. While IntServ mechanisms do work, it was realized that in a broadband network typical of a larger service provider, Core routers would be required to accept, maintain, and tear down thousands or possibly tens of thousands of reservations. It was believed that this approach would not scale with the growth of the Internet and in any event was antithetical to the notion of designing networks so that Core routers do little more than simply switch packets at the highest possible rates.

Differentiated services (DiffServ) is a more recent model in which traffic is treated with relative priorities based on the same type of services (ToS) field in the IP datagram. The DiffServ standard supersedes the original specification for defining the packet priority described in RFC 791. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. The first 6 bits of the ToS field are defined as the differentiated services code point (DSCP). There exists a number of class models for DSCP, some of them are described in the following RFCs: RFC2697, RFC 2698, and RFC 2598. Router companies also have their own automatic standard DSCP values. The last 2 bits of the ToS field in this case are not used for QoS. The ECN field is used for explicit congestion notification (RFC 3168).
In response to priority markings, routers and switches use various queuing strategies to tailor performance to requirements. (At the IP layer, differentiated services code point (DSCP) markings use the 6 bits in the IP packet header. At the MAC layer, VLAN IEEE 802.1Q and IEEE 802.1p can be used to carry essentially the same information).

Routers supporting DiffServ use multiple queues for packets awaiting transmission from bandwidth constrained interfaces. Router vendors provide different capabilities for configuring this behaviour, to include the number of queues supported, the relative priorities of queues, and bandwidth reserved for each queue.

In practice, when a packet must be forwarded from an interface with queuing, packets requiring low jitter are given priority over packets in other queues. Typically, some bandwidth is allocated by default to network control packets, while best effort traffic might simply be given whatever bandwidth is left over.

This newer standard gives the service provider more flexibility in configuring different QoS parameters for customers. These different QoS parameters (either for Layer 2 or 3) are stored as part of the overhead in the frames that are transmitted.

4.1.2.4 Integration with airport network

The major advantage of Ethernet network is its easy connectivity to other networks. This fact makes the challenge of integrating with the general purpose airport network an easy task. In any case there are some considerations that must be taken into account.

Security:
No mater how secure the ATOM network might be, if the airport network is not secure enough, the interconnection with it will transform the ATOM network into a non secure network too. Even if isolation mechanics are implemented to control the access from the airport network to the ATOM network, the data that are travelling through the ATOM network will be safe, but any other data that have to be sent through the airport network will be exposed to risks depending on that network security.

Data overload:
ATOM network will generate extra data that will be added to the current airport network data traffic. This may cause that the networks wouldn't be able to ensure enough resources to manage that amount of traffic.

4.1.3 PLC

4.1.3.1 PLC technology

Power line communication is a system for carrying data on a conductor also used for electric power transmission. Electrical power is transmitted over high voltage transmission lines, distributed over medium voltage and used inside buildings at lower voltages. Power line communications can be applied at each stage. Most PLC technologies limit themselves to one set of wires (for example, premises wiring), but some can cross between two levels (for example, both the distribution network and premises wiring). Typically the transformer prevents propagating the signal, which requires multiple PLC technologies to be used to form very large networks.

At high frequencies (1 MHz to 30 MHz), the power line channels are characterized by variable attenuation with frequency as a result of physical attenuation and delay spread (multipath) due to impedance mismatches. While a typical channel may present an average attenuation of approximately 40 dB, it is not uncommon for portions of the bands to experience attenuation greater than 60 dB. Similarly, while most in-home power line channels have a delay spread of 1 μs to 2 μs, some channels may exhibit a delay spread of larger than 5 μs. The major sources of noise on the power line are from electrical appliances, which generate noise components that extend into the high frequency spectrum. One of the unique characteristics of this man-made noise is its cyclic variation with respect to the ac line cycle. Electric appliances may turn on and off and/or draw electric power as a function of the ac line cycle. During this process, they generate noise that also changes with the ac line cycle. Typically, the least amount of noise is present at the ac line cycle zero crossing, while the ac line cycle peaks experiences the highest amount of noise. Impulse noise is common over power lines. Furthermore, the location of impulse noise is generally tied to the underlying ac line cycle.

Because much of the noise experienced by each node may be highly localized due to attenuation, power line channels typically are not symmetric. In addition to noise from appliances, induced radio frequency (RF) signals also impair certain frequency bands. Apart from dealing with the harsh channel conditions, PLC systems must operate with regulatory

constraints on the frequency band to use and the maximum transmit power. For example, within the United States, PLC systems operate under FCC Part 15 rules using the frequency band between 1.8 MHz to 30 MHz, at a maximum power spectral density (PSD) of –50 dBm/Hz. Several sub-bands within this range have to be notched out to prevent interference with licensed services. Moreover, the regulatory environment is in flux: aeronautical bands may be added in the United States, power levels are under debate in Europe and Japan is considering introduction of regulation that would allow PLC. This unstable international regulatory environment requires that PLC systems be flexible to adapt with changing regulations.

All power line communications systems operate by impressing a modulated carrier signal on the wiring system. Different types of power line communications use different frequency bands, depending on the signal transmission characteristics of the power wiring used. Since the power wiring system was originally intended for transmission of AC power, in conventional use, the power wire circuits have only a limited ability to carry higher frequencies. The propagation problem is a limiting factor for each type of power line communications. A new discovery called E-Line that allows a single power conductor on an overhead power line to operate as a waveguide to provide low attenuation propagation of RF through microwave energy lines while providing information rate of multiple Gbps is an exception to this limitation.

Data rates over a power line communication system vary widely. Low-frequency (about 100-200 kHz) carriers impressed on high-voltage transmission lines may carry one or two analogical voice circuits or telemetry and control circuits with an equivalent data rate of a few hundred bits per second; however, these circuits may be many miles long. Higher data rates generally imply shorter ranges; a local area network operating at millions of bits per second may only cover one floor of an office building, but eliminates installation of dedicated network cabling.

4.1.3.1.1 Interferences

The original concept of electric power networks did not foresee its use as a communication channel and power lines present a harsh environment for communication signals. Besides, the cable infrastructure works as a radiating system, representing a potential source of interference for radio communication services operating at the 1.7-80 MHz frequency band.

These issues remain a challenge to widespread PLC adoption, predating the IEEE standards and G.hn for in-home use. All new power line modems are supposed to detect the existence of SW-Radio services at the location and time of operation by monitoring the ground noise at the socket where the modem is connected but in reality this is not being implemented.

Questions remain on how effectively an interference-avoidance system will meet the requirements of SW-Radio services where reception is the first concern. Frequency avoidance schemes cannot adapt to the very low signal levels necessary for a radio receiver to operate reliably. By far, most SW-Radio services are receiving sites and not transmitting sites, so the interference issue remains significant. Current detection schemes are dependent upon transmitted signal levels as the triggering event to force equipment into a frequency avoidance scheme.

The most significant advantage of broadband power line communication (BPL) systems over their wired competition (e. g. xDSL and cable modem) is that they do not require an entirely new infrastructure. The most serious technical challenges to PLC systems have been found to be first, attenuation due to junctions such as taps, connected elements such as transformers and the lack of matched transmitter/receiver impedances, second, relatively high (and very frequency dependent) background noise usually due to induced radio broadcast signals, and third, legal limits on electromagnetic emissions from these unlicensed systems. The first causes the attenuation rate for high frequency signals to be quite high and very frequency dependent and (together with background noise and input power limitations due to the latter two) results in possibly unacceptable limits on the range of the system. Reduction of the attenuation to more

reasonable levels through system conditioning may require a financial investment that is incompatible with the requirement that the system be profitable.

4.1.3.1.2 Home Plug AV

HomePlug AV is a power line communication technology developed by the Powerline Alliance, aiming to distribute high-quality multimedia content in in-home networks. It utilizes existing AC wiring at home which makes extra wiring unnecessary. At the MAC layer, both prioritized and parameterized QoS are provided. A single Central Coordinator (CCo for short), works as the central manager in the HomePlug AV network. CCo broadcasts Beacon frames periodically to synchronize all network stations and schedule both contention-based and contention-free traffics. The Beacon Period is synchronized with the AC line cycle. Each Beacon Period is divided into three regions) as shown in Figure below:

- Beacon Region
- CSMA Region (for contention-based traffic)
- Contention-Free Region (for contention-free traffic)

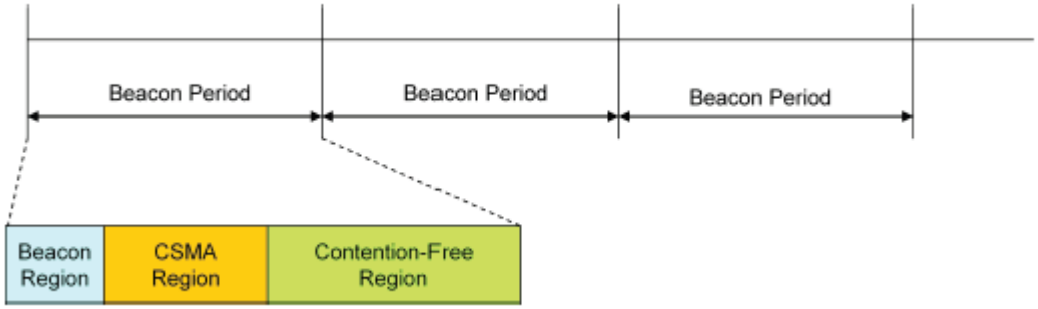

Figure 4 — Beacon Period of HomePlug AV

CSMA/CA
Based Prioritized Service: This is a connectionless contention-based service. Four priority levels are defined: CA0, CA1, CA2 and CA3 in increasing order of priority.

TDMA
Based Parameterized Service: This is a connection-oriented contention-free service. A traffic stream initiated by a higher layer should request CCo first with a Connection Specification (CSPEC). The CCo then determines how much time should be allocated to the traffic and if current network condition allows the request, TXOPs will be granted to the traffic stream. Each traffic stream can be delivered in its TXOPs at the Contention-Free Region. CSPEC is similar to TSPEC of WLAN, although the format differs.

HomePlug AV could be applied to an airport environment, but the target telesurveillance application brings a new, more stringent set of requirements: higher data rates are required to provide support for multiple HDTV streams, Quality of Service metrics must be met in terms of latency, jitter and very low frame error rates (for video and voice applications) etc. The brute speed achievable by HomePlug AV (maximun PHY datarate is 189 Mbit/s) may be too limiting.

4.1.3.1.3 Gigabit PLC

Gigabit PLC is the next step in PLC communication technology. Gigabit PLC devices uses the Mediaxtream band that provides a very high performance PLC channel capable of achieving

PHY rates up to 1Gbps. It also includes a HomePlug AV band, which is compliant with the HomePlug AV specification Version 1.1 and is fully interoperable with existing HomePlug AV products.

There are two technologies developed under this device, mediaxtreamTM and xtendnetTM technologies. MediaxtreamTM technology delivers raw throughput data rates of up to 1Gbps at the PHY level, sufficient for the most performance demanding home multimedia networks.

With xtendnetTM technology, each node added to a network can function as a repeater, increasing the overall range of the signal, assuring whole building coverage and improving throughput between distant devices.

mediaxtreamTM technology
This switch is the only wire line communications device with true dual band architecture. The dual band architecture provides a HomePlug AV compliant 200 Mbps capacity PHY supporting up to thirty two meshed networking nodes with “Simple Connect” push button encryption and mediaxtreamTM 1Gbps capacity PHY. This dual band approach, combined with an advanced parameterized/prioritized QoS agent and intelligent CSMA/CA-TDMA MAC provides for adequate flexibility, reliability and performance. This dual band approach is provided through the mediaxtreamTM band. Moreover, the mediaxtreamTM interfaces coexists with existing services on the wire lines such as xDSL, CATV, MoCA etc.

xtendnetTM technology
Through xtendnetTM, the Gigabit Ethernet and Powerline Network Switch support mesh networking and data repetition, to extend coverage.

4.1.3.2 Secure PLC

Admission control procedures ensure that only permitted devices are allowed into the PLC network. A station’s ability to maintain multiple security keys allows it to participate in multiple AVLNs.

All data traffic and nearly all control traffic within the network —the exception being a strictly limited set of control messages that simply cannot be encrypted—is secured by 128-bit AES encryption, providing a high level of security. This encryption uses the Network Encryption Key (NEK) and is performed on individual segments as the MPDUs are created. The NEK may be automatically and dynamically changed.

In order to join a PLC network, a station must obtain a Network Membership Key (NMK). If it already possesses an NMK it may join the network immediately; otherwise is must be provided with the NMK. This provisioning may occur in a variety of ways, including:

- Using the default NMK that is programmed into all PLC stations. While this default NMK provides a seamless, plug and play experience for the user when the equipment is initially installed, it does not provide any privacy since it is known by every HPAV-certified station
- The user can define and enter a Network Password (NPW) directly into a new station. This NPW is hashed to create the NMK, a 128 bit AES encryption key. The user must enter a NPW on at least one station to initially define the NMK for the AVLN
- All AV stations are also programmed with a unique Device Access Key (DAK). The user may enter this key into any suitably programmed station already in the network and that station will use the DAK to encrypt the NMK and broadcast it. Since only the new station has the DAK, it will be the only station that is capable of decrypting the broadcast message and so it and only it will receive the new NMK
- Using asymmetric Public/Private Key encryption, the PLC stations may provide the user the ability to join the new station to the network without needing to remember or enter passwords. This may be as simple as having the user press a button or make a menu selection on the new station and on a station already in the network

When a station has the correct NMK and actually joins the network, it will be given the current Network Encryption Key (NEK) which is used to encrypt data during segmentation in the MAC.

The design also permits encryption key management by higher layer Security and Authentication Standards such as 802.1x and EAP

4.1.3.3 QoS over PLC

PLC devices support a rich set of programmable Quality of Service (QoS) policies. These are some of the policies that are supported:

Classifier rules: Forward and reverse rules with the following matching rules: Ethernet destination address, Ethernet source address, VLAN user priority, VLAN ID, IPv4 type of service, IPv4 protocol, IPv4 source address, IPv4 destination address, IPv6 traffic class, IPv6 flow label, IPv6 source address, IPv6 destination address, TCP source port, TCP destination port, UDP source port and UDP destination port.

QoS and MAC parameters: Forward and reverse rules with the following constraints: Number of TXOPs per beacon, Rx window size, average number of 520 byte PBs per TXOP, maximum number of PBs per TXOP, PPB threshold, surplus bandwidth, connection descriptor, smallest tolerable average number of PBs per TXOP, original average number of PBs per TXOP, maximum MSDU average delay, maximum MSDU average jitter, average MSDU size, maximum data rate, maximum time between two Tx opportunities, exception policy, maximum inactive time for a connection, transmission band.

Connection information: Forward and reverse rules with the following parameters: MAC service type (Contention free (TDMA), Contention based (CSMA), Contention free preferred). User Priority (0 to 3).

The MAC layer in the HomePlug AV system supports both Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access.

Collision Avoidance (CSMA/CA) based channel access, which is controlled by the Central Coordinator (CCO). The contention free TDMA access technique provides strict QoS guarantees for connections with particular bandwidth and latency requirements by periodical allocation of transmission opportunities. Prioritized QoS is also supported in the connectionless CSMA/CA channel access mode, which supports up to four priority levels through prioritized contention. The Higher Layer Entity (HLE) uses the Connection Specification (CSPEC) to specify its QoS requirements, which includes the features such as guaranteed bandwidth, quasierror free service, fixed latency and jitter control. The Connection Manager (CM) resides at the CCO evaluates the CSPEC and decides whether it is able to accommodate the connection. On both ends of a connection, the Convergence Layers (CLs) provide sufficient information to the CMs that it can monitor the level of service quality being provided to ensure that the QoS guarantees for each connection are being met.

If any QoS violation occurs, the CM will take corrective measures specified by the CSPEC to reschedule the transmission opportunities. With the advanced network management functions, the HomePlug AV system supports plug-and-play configurations, that introduces great flexibility for users. In a HomePlug AV PLC network, the stations could be automatically configured as user terminal or CCO, which ensures that the most appropriate node is considered as the CCO to schedule channel resources in the network. This feature provides sufficient support for the nomadic users in the hospital environment.

4.1.3.4 PLC integration with other networks

Integration between PLC network and other networks is an easy task. In a hybrid network, although there are QoS mechanisms defined in both interconnected networks, there is no mapping of those mechanisms between them. The non-matching QoS features may lead to decrease of the end to-end performance. Therefore, a QoS broker would be needed to provide QoS mapping between the two networks, with a special concern on the high priority data.

A QoS broker consists of admission control and QoS mapping functions. If there is bandwidth request from the PLC network to the other network, the QoS broker works in line with the Base Station Connection Admission Control module (BS CAC), to decide whether it could accommodate the connection or suggested a set of lower but acceptable transmission parameters. And the QoS broker works in the reverse direction to Central Coordinator if there is traffic request to the PLC network from the other network as well.

The mapping of QoS parameters in the hybrid networks works on connection level. Upon network sets up, the QoS broker collects the service flow information from both networks, and creates a database. After that, the QoS broker monitors the incoming packets, and transfers it into the corresponding connections in the other network.

5 Application scenario

This chapter aims to show an example of scenario to estimate how the network could be stressed in case of data transmission. The attention will be focused on the worst case. To calculate the network load, a terminal area in the rush hour with a crowd of people fairly high will be considered. In the following, two different situations will be analyzed: Firstly, a small airport will be examined (e.g. Targu Mures), with a low number of passengers (250 pax/h) and secondly, a big airport (e.g. Schiphol) with a larger number of passengers (5000 pax/h).

To better understand the procedure used for calculation, some issues are listed in the following:

The network load is mainly due to the images provided by the detection sensors;

Under this condition it is possible to ignore the load due to the tracking sensors, that transmit only the plot of suspicious person (few kB) and other secondary information.

Taking into account the previous points, the adopted scheme for data transmission is showed in the following figure:

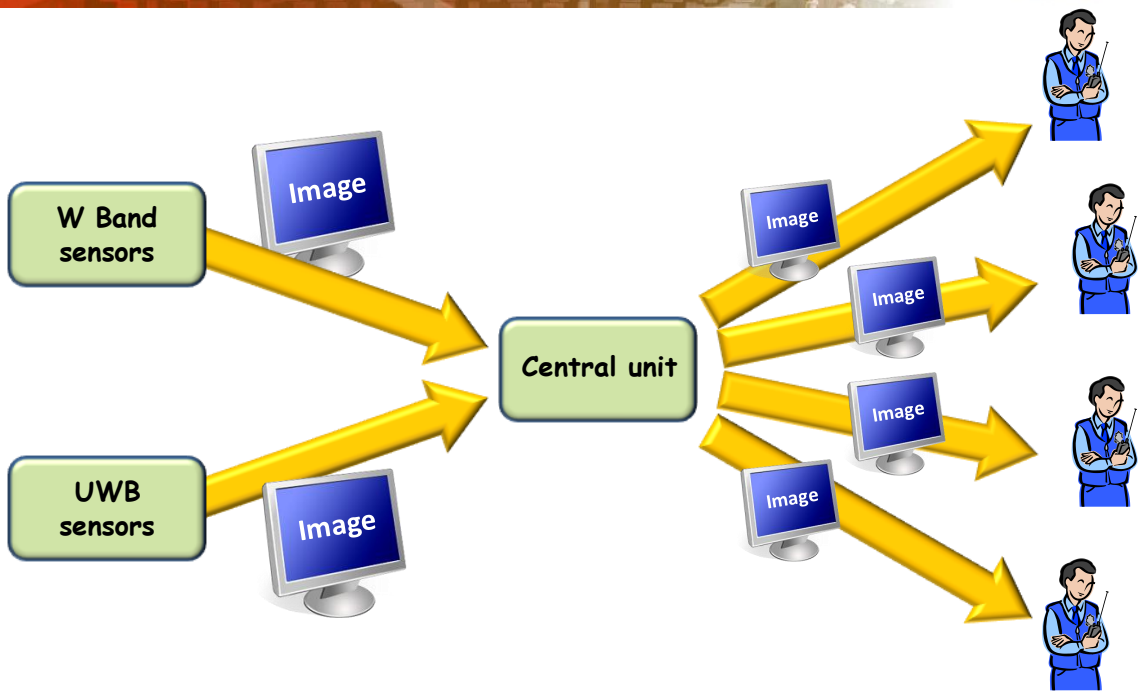

Figure 5 - Main data flow in ATOM network

Each detection sensor transmits an image to the central unit, which in turn, analyzes and merges all the images in a single one that contains more useful information. After this, the central unit transmits the image to the members of the security staff if a suspicious situation is detected. It should be noted that images coming from the sensors to the central unit are bigger in terms of MBs when compared to the images coming from the central unit to the security staff. This fact can be justified considering that the central unit needs more information to perform an operation of data fusion. As a result the images must contain a high number of pixels to achieve this objective. Once the threat has been identified, the image for the security staff can contain less information, for example only the type of threat and its position.

In the following section a more detailed analysis of the problem will be dealt.

5.1 Use cases networking

In this paragraph two scenarios will be showed to understand the load of the network when the ATOM sensors detect an anomalous situation. In the first case it is taken into account a small airport with a mean passenger flow in the rush time equal to 250 passengers/hour. In the second case a bigger airport will be considered with a passenger flow equal to 5000 passengers/hour.

As we said in the previous paragraph, we have to distinguish between the two types of images (different due to their size). Let's call I_{SC} the image transmitted from the sensors to the central unit; let's call I_{CS} the image from the central unit to the security staff.

In our scenario, an image is transmitted to the central unit from both sensors either when a dangerous tool is detected or when a false alarm occurs. As the probability that there is a real threat at the airport (by triggering a real alarm) is much lower than the one of a false alarm, in our calculations it is possible to consider only P_{fa}. Let's call φ the passenger flow at the airport expressed in terms of passengers per seconds. As a consequence, the bit-rate in input to the central unit for a single sensor is as follows:

$$B_{ss} = I_{SC}\, P_{fa}\, \varphi$$

Now considering a number of sensors n_s the overall bit-rate in input to the central unit is

$$B = n_s\, I_{SC}\, P_{fa}\, \varphi$$

Once the images I_{SC} arrive to the central unit, they are fused in a new image I_{CS} and sent to the police man. By assuming a number of police men equal to n_p, the overall bit rate C from the central unit to the police men can be computed as in the previous one, i.e.:

$$C = n_p\, I_{CS}\, P_{fa}\, \varphi$$

The number of police men necessary for the surveillance depends on the frequency of control, on the control duration t_d and on the number of police men for each control (n_{pc}):

$$n_p = \varphi \cdot P_{fa} \cdot t_d \cdot n_{pc}$$

An important issue to consider is the following: the bit rate depends also on the number of access points inside the airport area. For big airports it is obvious to assume that they have several access-points. With this consideration, if we assume a number of access points equal to m and the passenger flow equally distributed in the airport, the overall bit-rate for the network load decreases by a factor m.

Thanks to the previous considerations, the overall load for the network is expressed by the following relationship:

$$\Gamma = \frac{B + C}{m} = \frac{P_{fa}\, \varphi\, (n_s I_{sc} + n_p I_{cs})}{m}$$

5.1.1 Case studies

In this section two different case studies will be analyzed. It will be showed how the passenger flow is an important parameter for the overall load of the network. The initial analysis is performed by considering a small airport with a reduced passengers flow.
In both cases, suppose that I_{SC} consists of a number of pixels equal to $6x10^6$ and each pixel is represented from 8 bit. As a consequence we have:

$$I_{sc} = 6 \times 10^6 [pixel] \times 8 \left[{}^{bit}/_{pixel} \right] = 48\, Mb$$

On the other hand, for the reason explained in the previous section, let's suppose that I_{CS} consists of less pixels than I_{SC}, let's say 106 pixels. As a consequence the overall size of I_{CS} is expressed by the following relationship:

$$I_{CS} = 10^6\, [pixel] \times 8 \left[{}^{bit}/_{pixel} \right] = 8Mb$$

The following table summarizes all the parameters adopted to estimate the load of the network:

Parameter	Value
l_{SC} *(image from sensors to the central unit)*	48 Mb
l_{CS} *(image from central unit to security staff)*	8 Mb
P_{fa} *(probability of false alarm)*	20%
n_s *(number of sensors)*	2
n_{pc} *(number of policemen per control)*	2
t_d *(duration of a control)*	5 minutes
m *(number of access points)*	1
φ *(passenger flow)*	0.07 s^{-1}

Table 4 - Parameters adopted for the case study

Based on the previous considerations and the parameters showed in Table 4, the overall load for the network can be computed as follows:

$$\Gamma = 0.2 \cdot 0.07 \left(2 \cdot 48 \cdot 10^6 + 8.33 \cdot 8 \cdot 10^6\right) =$$

$$= 2.26 \cdot 10^6 \, {bit}/{s} \cong 2.3 \, {Mb}/{s}$$

If a different passenger flow is considered, for example, a big airport is taken into account, the load of the network radically changes. If we substitute the value φ=1.4s^{-1} we obtain:

$$\Gamma = 0.2 \cdot 1.4 \left(2 \cdot 48 \cdot 10^6 + 166 \cdot 8 \cdot 10^6\right) =$$

$$= 397 \, {Mb}/{s}$$

As can be seen from the previous case studies, the passenger flow greatly affects the network load. Due to the fact that this is a fixed parameter, determined by the type and characteristics of the airport, the most suitable parameter to change for a correct sizing of the network is I_{CS} and I_{SC}. In the Figure 6 it is represented the network load Vs passenger flow for different values of I_{CS} for a number of access point equal to m=1. Figure 7 shows the same figure with a value of *m*=5.

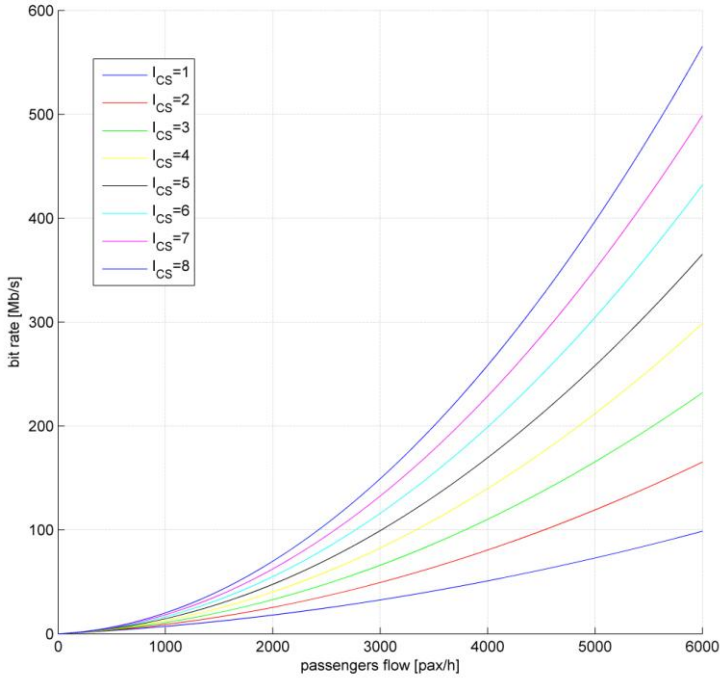

Figure 6 – Network load Vs passenger flow (@ l_{CS})

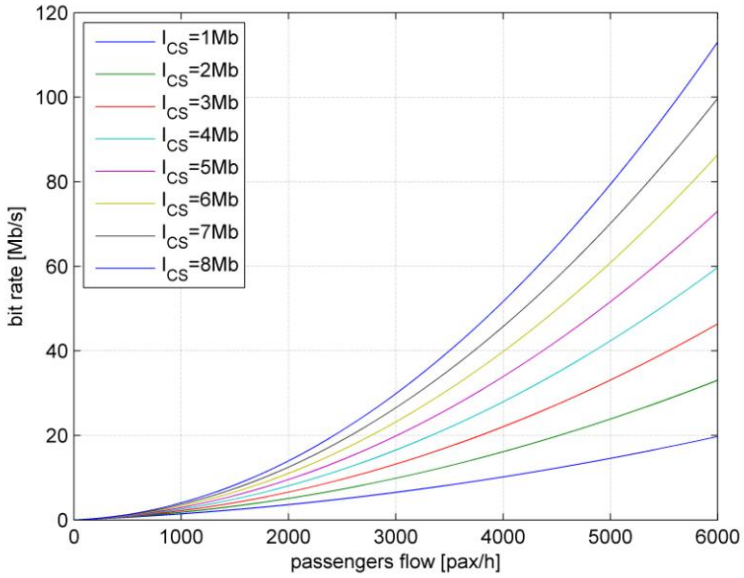

Figure 7 – Network load Vs passenger flow for *m*=5 (@ l_{CS})

6 Constraints

For a network development process, as the one attempted in the framework of ATOM project, the initial care should be not to irritate airports' normality, procedures and security functions and standards. The majority of restrictions imposed by the environment relate to an extent to airports' spatiotemporal conditions. Special thought and study should be spared on how the project will offer a solution that will optimize safety awareness, in a highly dynamic complicated context where a plethora of individuals and structures coexist and function. As a part of the network requirements formulation, the present chapter tries to consider the basic limits and pitfalls, categorizing them into two categories: a) the physical restrictions prescribed by the system itself, b) the communication network restrictions and hazards.

6.1 System boundaries and restrictions

Resources
Chapter 4, *Communication Technologies*, indicates in detail the software and hardware resources which are vital or possibly necessary for constructing a LAN. Hubs, switches, routers, bridges, access points, gateways, terminals/displays, servers, firewalls, databases etc. are elements that should be registered not only as network components, but also, as material cooperating and collocating with existing infrastructure.

Deployment
The answer to the new network placement problem is a particularly application specific issue. It should be estimated in conjunction with the more general subsystems' spatial functional specifications. For example, UWB system sensing capabilities are in proportion with the small distance (in the order of centimeters) of the target.

Coverage/Connectivity
Again, depending on the application, the nature and number of structural network components is decided ("how many WAPs do we need? Is this feasible?").

Hierarchy/Users
A cautious organization of network privileges is necessary, to guarantee effectiveness of ATOM network. We should take into account that its users are, already, handling security information (which is going to be augmented) and working under strict rules, with specific authorities in a framework of specific hierarchy.

6.2 Network vulnerabilities, interferences and attacks

Wireless channel vulnerability
The open broadcast nature of wireless medium makes its security by default sensitive. We ought to ensure that the addition of ATOM network will not increase this vulnerability. The appropriate measures will be taken, since the construction of a secure LAN is standardized through adherence to recommended practices.

Interference
The simultaneous existence of various networks in the airport premises (wireless network for passengers, internal LANs, ATOM, GSM, security operators' handheld devices etc.) indicate as evident the need for special treatment on the issue of interference of many types. In fact, the factor of interference might play a significant role in the selection of ATOM LAN communication techniques.

Attacks

The long list of physical and software LAN attacks is augmented with airport related offensive actions and should be addressed, to strengthen passenger and infrastructure security. The threats vary greatly in type and in the way they affect the network. Therefore, the security scheme, which will be adopted in ATOM network implementation, depends on the selected priorities of attacks category list we wish to confront. The major categories, concerning wireless infrastructure, along with a short description, are listed in the table below:

Threat Category	Description
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials
Man-in-the-middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges
Message modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it
Message reply	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants

Table 5 – Common attacks to wireless infrastructure

7 Network requirements

ATOM project wishes to present a solution of additive value in the area of airport security and increase authorities' awareness and passengers' safety in an increasingly unstable environment. To do so, it utilizes the assistance of subsystems and blocks, physically or logically discriminated, which form a demanding architectural structure and are analyzed in detail in previous deliverables. ATOM network concept rises from the need to interconnect these subsystems and assure smooth information flow, until its final destination, the security operators. The possibility of transmitting information through a general purpose or proprietary network will be examined. Critical prerequisite, apart from the desired efficiency and performance, is that the LAN will not hinder normal life conditions in the airport or burden current infrastructures and procedures with additional overhead.

7.1 Architectural requirements

7.1.1 Hardware

The necessary network equipment results from the concentration of subsystems' communication interfaces and other possible common hardware needed to construct a LAN (routers, access points, laptops etc.).

Data Centre unit is a PC, being the core of ATOM system and performing a series of functions, mainly of two categories: a) data management, which is data collection from the different radar subsystems and possible data fusion, as well as b) interface or gateway for some of the subsystems (e.g. W band scanner).

Active tracking sensors' output device (and thus gateway to ATOM LAN) will be either a Central Node that will act as a base station communicating with several nodes or a Client of the active tracker (e.g. a laptop).

Similarly, a Centralized Unit (PC or laptop), is the interface and the data pre-processor of UWB radar. An alternative combination, regarding UWB and W band scanners, is using W band data as an input to UWB, if we want to pre-filter some images and reduce the workload of UWB. In that case (or points in network), UWB Centralized Unit acts as the communication interface for the whole Detection subsystem.

The sixteen sensors of Passive radar subsystem communicate with the world (Detection system and internally with the Tracking system centre) with a RJ-45 connector, for Ethernet connectivity.

UWB radar subsystem comprises of three basic elements: the imaging sensors (2-4), a mechanical scanner equipped with Tx/Rx antennas (performing SAR measurements) and a Vector Network Analyzer (VNA). With regard to the communication network, a computer is utilized as a gateway, being either the generic Data Centre unit or a local central machine in the Detection block.

7.1.2 Communication Software

Since our communication environment concerns LANs, utilization of IEEE 802 family standards is expected. The exact implementation and combination of protocols and amendments depends on a series of factors and is the outcome of our study, the final implementation or demonstration.

W band scanners, UWB scanners and Data Centre unit may communicate alternatively with 802.3 a/b or 802.11a/g/n. This group of standards applies for the intra-communication between nodes in the Active tracking system, also, and possibly the communication between their gateway and other subsystems. Similarly, Passive sensors subsystem uses Ethernet to interface with the related blocks.

7.1.3 Data

7.1.3.1 Format

W band scanner produces, after internal processing, a complete radar image. The image is stored as a Matlab figure or a .jpg file.

The processed output of UWB radar is, also, a .jpg image (3D).

Raw data from Active tracking sensors is concentrated and processed in Central Node and subsequently forwarded to Active Tracker in the form of data messages (Designations). The latter produces the subsystem's output in the format of enhanced designations, plots and tracks.

Passive sensors subsystem produces measurements in the form of 16bit binary floating point numbers.

7.1.3.2 Volume

W band radar image is about 2 MB, whereas the corresponding one from UWB radar is in the order of 400 MB or 1MB, the difference reflecting the stages before and after raw data processing.

Active tracking subsystem output data volume is low. Indicatively, a Designation message is expected to have a size of 47 bytes.

Passive sensors subsystem output data volume is in the class of 20KB per sensor's output (including the three measurements and the related information).

7.1.3.3 Throughput/Rate

Data rate is not of interest for W band radar image, due to internal pre-processing.

Active tracking subsystem output data rate is low, in the order of 10 Kbps.

Passive sensors subsystem output data throughput is 0.32 Mbps (see 7.1.3.2, sixteen sensors multiplied with 20KB per sensor's output).

7.1.4 Dimensioning

As the ATOM system (and therefore the ATOM network) is intended to be settled in airports, deployment and dimension considerations play a critical role. Drawing the complete picture, at this study phase, is tricky. However a parameterization, based on most important factors, can be attempted:

- Airport dimensions (application specific)
- Network (desirable) coverage
- Selection of communication technology
- Ease of deployment / no interference in airport's normality

W band scanner developers foresee an average space occupation of 3m x 3m for the scanner, plus 1m x 1m for the steering hardware.

Every Passive sensor achieves about 50 meters coverage range.

UWB scanner subsystem has as a functional prerequisite the small distance between the sensors and the examined person. This assumption results from the synthetic aperture radars' functional requirement which states that the distance of the scanned object must be in the order of wavelength and dimensions of the sensing aperture. In our case the sensor deployment consists of two or four imaging sensors, placed on the sides of a narrow corridor in a scheme resembling < >, where each inclined stroke stands for a sensor. From the fact that UWB radar is a centimeter wave sensing technology, derives that an airport passenger should pass or stand as close as less than a meter to the sensors.

Airport dimension is a parameter necessary for the network design, coverage, development and deployment. Targu Mures, as a local airport, serves a flow of 9500 passengers per month (8300 international and 1200 national), with a mean flow during rush hour being 250 passengers per hour, whereas the mean air traffic corresponds to about 410 flights per month (290 international and 120 national).

ATOM subsystems have a very different degree of expected development (from simulations to small prototypes and sizeable systems), making the generalization effort to produce a complete collaborative network, a very challenging task.

7.2 Functional requirements

7.2.1 Connecting subsystems

The dominant functional requirement of ATOM network summarizes its basic concept of existence and operation: to interconnect different ATOM subsystems for the configuration of a proprietary or general purpose LAN. This task performs the necessary connection of blocks and terminals that have to communicate with each other, e.g. the interaction scheme between Tracking System and Data Management for the activation and termination of tracking, incorporating all the special communication capabilities and interfaces these heterogeneous subsystems have.

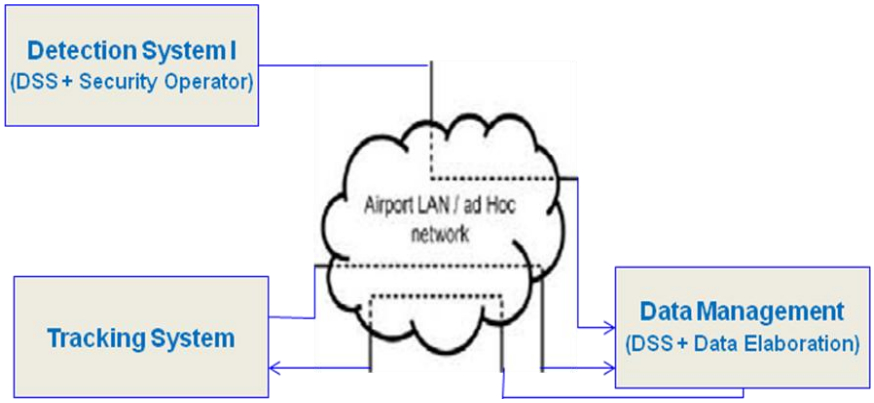

Figure 8 — ATOM LAN connecting subsystems

7.2.2 Information flow

In addition to the basic subsystem communication support, further communication needs may exist in the application environment and, therefore can be (serviced by and) embodied in ATOM network. Examples are (from the ATOM architecture block diagram) the communication between Decision Support Centre and Security Operator or between Security Operator and Alert Handler. Main and complementary services of data transmission summarize the vital need that ATOM network should serve: the unhindered information flow towards security operators, for enhancing airport situational awareness, taking into consideration that every Airport already has a settled infrastructure for passenger control and that ATOM does not wish to cause obstructions or interfere with it, but to enhance it.

7.3 Non-Functional requirements

7.3.1 Usability

ATOM network should offer ease of use and efficiency to its users, the airport authorities and security personnel. It should be fully functional, without causing irritations in the normal airport life.
Although it is not easy to distinguish usability issues specific to the network from those pertaining to the overall ATOM system, special attention should be given to the following ones:

- easy setup and maintenance: it should be easy to install, access and configure the (elements of the) ATOM network; this requires a clear identification of the hardware and software items making up the network, besides the sensors and the data center, a clear specification of the physical interfaces, of the protocols and of tolerances, of limitations concerning topology, distance and obstacles; a detailed setup procedure
- self checking and monitoring: it should be easy for different classes of users to understand when unavailability or reduced reliability of the ATOM system should be imputed to a fault or to low performance of the communication network

7.3.2 Performance

Network performance should be optimum. There should be accurate time synchronisation and little latency between the involved interconnected parts.

As for many other requirements, we have to distinguish between different targets; for example:

- in a prototype configuration, needed to demonstrate in a real but simple scenario the capabilities of the ATOM concept, most of the dimensioning parameters mentioned in section 7.1.4 will have been fixed: it should be relatively easy to adjust the other ones in order to ensure a network performance not jeopardizing the overall system performance
- in a more general scenario, say a big airport comprising of terminals with different geometries and levels of traffic, in order to meet the required performance, it could be necessary at some point to consider alternative choices, with reference to architecture (e.g. topology), technology (e.g. wired Vs wireless) and so on

7.3.3 Reliability

The LAN should be available and reliable to its users.

In system engineering, reliability can be defined as "The ability of a system or component to perform its required functions under stated conditions for a specified period of time".
Issues pertaining to security and integrity will be considered below, in section 7.4. Performance, which has been addressed just above, as a separate requirement, impacts also reliability, since relevant delay in exchange of the data could make them unusable to the receiver subsystem.
A pre-condition of reliability is availability, measured as the time a subsystem stays online in a certain time interval. While in general it is difficult to evaluate how the degree of fulfilment of a requirement by a sub-system can impact the overall system, for availability a well established theory exists. High availability and more general high reliability should be obtained by a mix of:

- quality of components and knowledge of statistical parameters on their life
- redundancy and ability to exploit it; redundancy consists in duplication of critical components of a system; in the case of a network, an important contribution to redundancy is the availability of multiple communication paths, possibly relying on additional nodes with only relaying an routing functionality
- adequate maintenance plans and maintenance resources (spare parts, trained personnel etc)

The communication interfaces used by the ATOM sensors, at this stage and presumably at the time that the ATOM Demonstrator will be setup, are commercial components such as the Ethernet adapters included in any PC. More evolved and compact versions of them, e.g. of those inside the tracking subsystems, could include embedded network interfaces, possibly based on dedicated Wi-Fi chipsets; in such a case, long-term availability considerations could be relevant for maintainability (see section 4.1.1.8.6).

7.3.4 Robustness

The network should be fault tolerant and be able to continue its function under abnormal circumstances.

Examples of abnormal circumstances:

- damage to cables due to mechanical stress
- abnormal crowding of the wireless band in use
- fault of a wireless base station

Redundancy, together with dynamic re-configurability could be a way to improve robustness. Examples of redundancy:

- dual (or multi-) network cabling to interconnect critical equipment and platforms
- multiple wireless base stations
- multiple wireless bands available for use
- multiple interface adapters per connected subsystem

7.3.5 Scalability

Given the different dimensions from airport to airport premises, the dynamicity of airport environment and the fact that ATOM study relies on generalization of small prototypes, the network should be scalable.

Scalability is an important property for our cause, which allows manufacturers and users to adjust and extend product's capabilities; a scalable network is able to handle increased load either with the same resources, at cost of acceptable performance degradation or by allowing to add/replace resources without changing the basic architecture.

A slightly different, but belonging in the same "family" of size related properties, requirement is Capacity. It is, also, a clear networking property. The network volumes (and therefore the passenger traffic it can serve) should be well considered.

7.3.6 Airport environment

The physical environment of our application (airports), besides impacting operational and assistance-related requirements, will also impose a number of restrictions (see Chapter 6). For example, wireless communication links should be safe for people, should not interfere with those used for other airport functions and with services offered to airport users; if part of the ATOM network will exploit the already existent or planned common communication infrastructure of the airport, it shouldn't load it more than agreed upon.

7.4 Security requirements

Security considerations are critical when implementing a LAN, let alone in the context of an airport establishment, where the network is responsible for this level of confidential data transmission. Practically, when a network is not secure its own existence is questionable and thus, security requirements are treated as a special category in this study. ATOM LAN security selection specifications rely on the overall communication architecture and the standards that implement it. For example, the most popular WLAN set of standards, family 802.11, is lately accompanied with amendment 802.11i, which enhances security. In general, methodology for "building" a secure LAN is codified and recommended practices are indicated per application, technology, environment etc.

Interconnectivity between networks and, in particular, connectivity to the public Internet, exposes non-public networks to a hostile environment of rapidly evolving threats. Connections to other networks (such as to public data carriers or the public Internet) provide convenient channels through which external entities can imperil internal end-systems. In addition, internal network users can deliberately or inadvertently threaten the network and its end-systems through their actions. If an internal node on the airport network is compromised, it can become a threat to the rest of the network.

Network security is the measures taken to reduce the susceptibility of a network to these sorts of threats. Broadly speaking, network security has three fundamental objectives:

- Protect the network service
- Reduce the susceptibility of end-systems and applications to threats originating from the network
- Protect data during transmission across the network

Network security counters both external and internal threats with a full suite of security safeguards to address risks to the network. These safeguards include the following:

- Physical and environmental safeguards to protect network equipment and media
- Technical controls within the network infrastructure to reduce its susceptibility to security threats
- Controls applied within lifecycle processes to limit the vulnerability of the network infrastructure to security threats
- Information security operations to detect, contain, respond to and recover from security incidents

Network security controls threats from external networks primarily through safeguards deployed at external network interfaces. Inside the network security perimeter, safeguards that are designed to detect, contain, respond to, and recover from attacks control threats from insiders and provide in-depth defence against external threats.

Network security protects data in transit by controlling access to network media, by deploying cryptographic security measures within the network and by facilitating the deployment of cryptographic security measures within application systems and the distributed computing environment.

Network security can reduce the susceptibility of end-systems to threats from external and internal entities by filtering malicious software and invalid network traffic, detecting suspicious traffic patterns, raising alarms and blocking or terminating threatening connections. However, valid data streams often carry threats to the information infrastructure. In these cases, there is a limit to the ability of network security controls to mitigate risks to end-systems because those controls can address threats only if they can detect threats in the network traffic. Platform safeguards, distributed computing safeguards and application security safeguards should be deployed to address the additional threats.

As referred in the ISO/IEC 27002 information security standard, the objective of communication security is the preservation of three principles:

- Confidentiality: the communication data are only disclosed to authorised subjects
- Integrity: the data in the communication retain their veracity and are not able to be modified by unauthorised subjects
- Availability: authorized subjects are granted timely access and sufficient bandwidth to access the data

Under this perspective we try to cite the more important network requirements, adjusted in ATOM's special case studies and applications:

7.4.1 Network Security Requirements

7.4.1.1 Identification

The requirement applies when a (new) user claims his identity to the network.

7.4.1.2 Authentication and Authorization

Authentication is the well defined specification of airport employees with granted access to the network. Authorization is the allocation of rights to categories of people, a “who can do what” list of network functions.

7.4.1.3 Non-Repudiation

Originator of communications can’t deny it later. The user cannot deny that he is the individual who made a particular transaction.

7.4.1.4 Availability

The network should ensure legitimate users to have access when they need it.

7.4.1.5 Integrity

Airport authorities should provide the specification of desirable level of integrity, for the databases of traded, through the network, information.

7.4.1.6 Privacy

The network function should ensure respect of privacy for the individuals about whom it stores information.

7.4.1.7 Confidentiality

The network should ensure protection from disclosure to unauthorized persons.

7.4.1.8 Accountability and Auditing

The system should be able to determine the actions of a user. The network should retain records or log files of its operation and events. This requirement links to Non-Repudiation.

7.4.1.9 Network Protection

Under this category are the requirements with which the network should comply, in order to raise a strong “shield” against attacks, infections and harmful software.

7.4.1.10 People Safety

Safety requirements concern quantification of the perceived risk to damage people, property or the environment.

7.4.2 Security Threats

Some of the possible threats that the network is exposed could be:

- Information disclosure/information leakage
- Integrity violation
- Masquerading
- Denial of service
- Illegitimate use
- Generic threat: backdoors, trojan horses, insider attacks
- Most Internet security problems are access control or authentication ones. Denial of service is also popular, but mostly an annoyance

7.4.3 Attack types

There are two possible main attack types, passive and active:

- Passive attack can only observe communications or data
- Active attack can actively modify communications or data. This kind of attack is often difficult to perform, but very powerful:
  - Mail forgery/modification
  - TCP/IP spoofing/session hijacking

7.4.4 Security Mechanisms

For network security purposes three basic building blocks can be used:

- Encryption must be used to provide confidentiality, can provide authentication and integrity protection
- Digital signatures must be used to provide authentication, integrity protection, and non-repudiation
- Checksums/hash algorithms must be used to provide integrity protection, can provide authentication

One or more security mechanisms can be combined to provide a security service.

7.4.5 Network Security Zones

The Zones are defined to minimize network complexity, to ensure effective and efficient delivery of network services, to promote interoperability and to provide a consistent level of security for services provided within and across Zones. A Network Security Zone is a construct to implement security consistently across an interconnected network environment. It demarcates a logical area within a networking environment with a defined level of network security. Zones define the network boundaries and their associated perimeter defence requirements. This is achieved by:

- Defining the entities which populate Network Security Zones
- Identifying discrete entry points
- Filtering network traffic at entry points
- Monitoring the state of the network
- Authenticating the identity of network entities
- Monitoring network traffic at the entry points

The concept of Network Security Zones is limited to the network environment. The use of the Zones is intended to reduce the threat to end-systems and applications. A Zone is not intended to meet all of the information management and information technology requirements to

safeguard end-systems, applications or data. To achieve a sound overall security posture, Zones must be used in conjunction with additional safeguards such as platform, application, and administrative security controls. Within a Zone, these additional safeguards can be implemented based on assumptions about the network security environment, including:

- The level of trust in entities present in the network environment
- The nature of network traffic entering and exiting the environment
- The nature of traffic within the environment
- The security services available to protect communications
- The robustness of the network environment

The airport network zones can be divided into seven different zones:

- Public Zone
- Public Access Zone (PAZ)
- Operations Zone (OZ)
- Restricted Zone (RZ)
- Highly Restricted Zone (HRZ)
- Restricted Extranet Zone (REZ)
- Special Access Zone (SAZ)

7.4.5.1 Public Zone

The Public Zone is entirely open and includes public networks such as the public Internet, the public switched telephone network, and other public carrier backbone networks and services. Restrictions and requirements are difficult or impossible to place or enforce on this Zone because it is normally outside the control of the airport as a system owner. The Public Zone environment is assumed extremely hostile. Any systems delivered in or interfacing with, the Public Zone should be hardened against attack.

7.4.5.2 Public Access Zone (PAZ)

A PAZ mediates access between operational airport systems and the Public Zone. The interfaces to all airport online services should be implemented in a PAZ. Proxy services that allow airport personnel to access Internet-based applications should be implemented in a PAZ, as should external e-mail, remote access, and extranet gateways.

A PAZ is a tightly controlled environment that protects internal airport networks and applications from the hostile Public Zone. The PAZ also acts as a screen to hide internal resources from the Public Zone and limit the exposure of internal resources.

7.4.5.3 Operations Zone (OZ)

An OZ is the standard environment for routine airport operations. It is the environment in which most end-user systems and workgroup servers are installed. With appropriate security controls at the end-systems, this Zone may be suitable for processing sensitive information; however, it is generally unsuitable for large repositories of sensitive data or critical applications without additional strong, trustworthy security controls.

Within an OZ, traffic is generally unrestricted and can originate internally or from authorized external sources via the PAZ. Examples of external traffic sources include remote access, mobile access and extranets. Malicious traffic may also originate from hostile insiders, from hostile code imported from the Public Zone or from undetected malicious nodes on the network (e.g., compromised host, unauthorized wireless attachment to the Zone).

7.4.5.4 Restricted Zone (RZ)

An RZ provides a controlled network environment generally suitable for business-critical information technology services (i.e., those having medium reliability requirements, where compromise of the information technology services would cause a business disruption) or large repositories of sensitive information (e.g., in a data centre). It supports access from systems in the Public Zone via a PAZ. All network-layer entities in an RZ are authenticated, either explicitly through the implementation of a peer-entity authentication service or implicitly through a combination of physical security and configuration control. The RZ reduces the threats from system insiders by limiting access and through administrative monitoring. Data confidentiality services are implemented in an RZ to protect Zone traffic from eavesdropping by unauthorized nodes. These services may be implemented in the network or through media security.

7.4.5.5 High Restricted Zone (HRZ)

An HRZ provides a tightly controlled network environment generally suitable for safety-critical applications or extensive repositories of sensitive information. Only other Zones controlled by the airport may access an HRZ (i.e. there is no access by systems in the Public Zone). All network-layer entities in an HRZ are authenticated, either explicitly through the implementation of a peer-entity authentication service or implicitly through a combination of physical security and rigorous configuration control. In general, the HRZ has more stringent requirements for end-systems than the RZ does. It also imposes stricter controls on system insiders to address threats from that source. Data confidentiality services, suitable for protecting sensitive information, are also implemented in an HRZ to protect Zone traffic against eavesdropping by unauthorized nodes. These services may be implemented at either the network or physical layer. Measures may be required to protect against unauthorized access to electronic emissions.

7.4.5.6 Special Access Zone (SAZ)

A SAZ is a tightly controlled network environment suitable for special processing needs. Requirements for a SAZ would be developed on a case-by-case basis to meet the special processing needs of the environment. Measures may be required to protect against unauthorized access to electronic emissions. Limitations in security technology may prohibit network connections to other Zones.

7.4.5.7 Restricted Extranet Zone (REZ)

A REZ supports directly connected extranet services with highly trusted partners. This Zone can be viewed as a logical extension of internal Zones to organizations external to the airport. The requirements and practices for this Zone would be developed on a case-by-case basis and enforced through agreements with partners.

7.5 Scenario Requirements

At this section a set of requirements is set, stemming from the processing of networking needs of an airport, as the latter is represented in ATOM project from the application fields of Targu Mures and Schiphol. It is obvious, that by taking into consideration use cases induced by the larger airport, we are able to provide our system with greater generality and requirements variety. Instead of naming, we depict these requirements in Table 6 by description and association with critical properties of the network. ATOM network should:

Requirement description	Property
Support **traffic load** imposed by (each time) sensors subsystems. Load could have an indicative size of 400 Mbps, according to simulation results of § 5.1.1	Magnitude, Scalability, Efficiency
Be easily **manageable** of airport's staff	Usability
Not degrade greatly from **interference**	Robustness
Be constantly **available** to its users	Reliability
Fit without problems in already installed infrastructures. This concerns **spatial** considerations, as well as, **communication protocol** selection issues	Flexibility, Communication Protocol
Provide **connectivity** between new subsystems, data centres, security operators, suitably adjusted per application	Connectivity, Adaptability
Be based on communication protocols with strong **security** services. Sense of "security" is two fold, concerning not only ATOM network, but its conjunction with existing infrastructure (as explained in § 4.1.2.4)	Security

Table 6 – Network Application Requirements

8 Preliminary Network Architecture

In the current deliverable an analysis for airport security information management and exchange was attempted. We tried to incorporate all possible network elements, parameters, restrictions and peculiarities, setting the basis for the architectural network proposal, which is the final goal of WP8 and the objective of deliverable 8.2. Linking the two works, we are in the position to "draw" the framework of what a communication network, conveying data from ATOM sensors to airport authorities and security personnel, could be like and to refer to the most prominent candidate security mechanisms for this network's protection.

8.1 ATOM Network

Summarizing from above, it is clear that in the ATOM network area four intercommunicating subsystems can be identified: Detection, Tracking, Data Center and Security. Figure 3 depicts the information flow and its directions. The main data volume is expected during the "feeding" of Data Center with images from the Detection subsystem. Important role is played by UWB sensor island's capability of processing the images or not. The two cases present a difference, in terms of produced information magnitude, in the order of hundreds of MBs. Detection subsystem can either send data directly to Data Center or to Tracking subsystem. In case of tracking procedures activation, Data Center interacts with Tracking subsystem, establishing a duplex communication mode. Data Center informs airport Security personnel, whenever such a need arises.

Regarding the implementation phase of ATOM Network, the above study and formulation of requirements lead to a network structure, which cannot be considered "final", but positively a strong solution candidate. Work in WP8 is continued: further simulations will be conducted, integration of ATOM Network with existing infrastructure will be examined and the potentials for

more advanced transmission features will be investigated, optimizing network architectural proposal.

A fundamental role in our design is played by the combination of networking protocols, which will be selected to carry out wireless (and wired) communications, throughout several parts of the network. In paragraph 4.1.1.8.1, a brief analysis of the considerations imposed by the environment, when choosing the communication standard, is presented. Important factors, such as *interference* and *capability of control/intervention* in the new shaped environment, are weighed (or their in-between trade off is estimated). With this procedure and concentrating the information from all components, we ***tend to*** conclude in the use of elements out of the stack of 2 communication standard families, covering wired and wireless network sections: IEEE 802.3 and its expansions or amendments (802.3 a/b/ab) and IEEE 802.11 with its family of standards (802.11a/b/g/n), correspondingly.

In this context, an indicative and simplified ATOM LAN topology is illustrated below (the presence - or not - of specific network elements in this diagram is not exhaustive and is supposed to depict the variety or options of network structure):

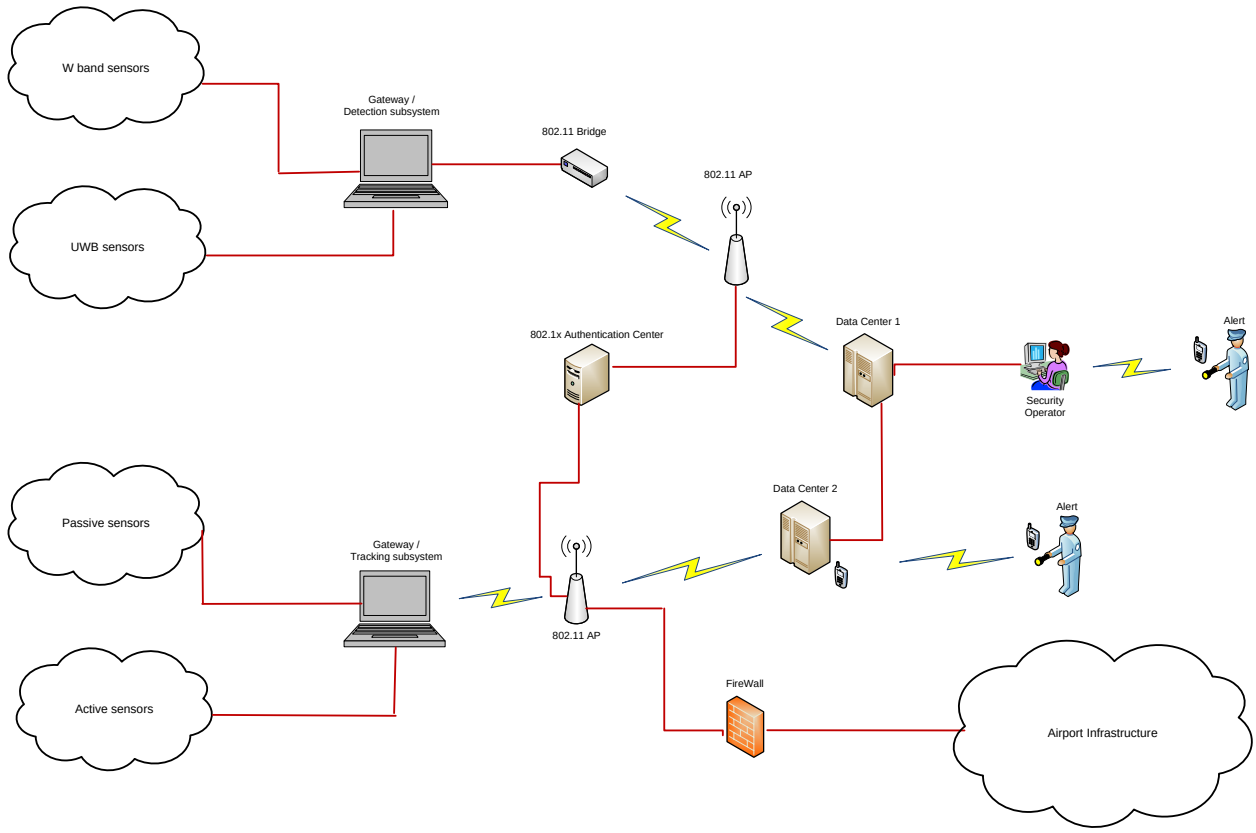

Figure 9 — ATOM LAN

8.2 ATOM Network Security

Following the term definitions and requirements of paragraph 7.4, some interesting notions about ATOM LAN Security candidate scheme can be introduced:

8.2.1 Network access

Primarily, a user needs to be authenticated, granted with access rights and authorized to perform several actions in the network. While many references are made in chapter 4 (state of the art study), some of the enabling technologies for access control are filtered below:

RADIUS
Remote Access Dial In User Server is a protocol by IETF for authentication, authorization, accountability and configuration information. RADIUS packets are carried over UDP, while a Network Access Server (NAS) is required to perform the authentication procedure, carrying messaging between the Client (C) requesting access and the Authentication Server (AS).

Diameter
Diameter protocol is based on RADIUS and used for applications as IP mobility. It improves RADIUS in many points, including failover, confidentiality, reliability of transmission and roaming support.

EAP
EAP may be used on a variety of topologies, dedicated links or switched circuits, wired or wireless links. From ATOM perspective is interesting that it has been implemented with access points, using IEEE 802. EAP encapsulation on IEEE 802 wired media is described in IEEE-802.1x and encapsulation on IEEE wireless LANs in IEEE-802.11i.

IEEE 802.1x
802.1x specifies the port-based network access control for wired and wireless networks. As mentioned right above, IEEE 802.1x uses EAP as an auxiliary protocol to transmit the authentication data. Giving an example of the scheme C-NAS-AS (see RADIUS above) in the 802.1x framework, we have: Client-Access Point-RADIUS server.

8.2.2 LAN security

Following authentication and association of a user with a network, let's have a look on the important "stations" of network confidentiality development, as they are filtered out from our study (chapter 4) in chronological and quality (in the sense of complement, enhancement and improvement) order.

WEP
Wired Equivalent Privacy was one of the first attempts to enhance confidentiality, compared with the one provided by a wired network. It was based on the use of the same shared private encryption key among all stations on a WLAN and on cipher algorithm $RC4^2$. In consequence, when a station is compromised, the whole LAN is compromised. WEP was also vulnerable to eavesdropping, since it could be easily cracked by public domain tools and an attacker passively monitoring communications. The effort to overcome these and other drawbacks led to TKIP.

TKIP
The Temporal Key Integrity Protocol was designed to improve WEP protocol without causing significant performance degradations, using mainly the same algorithms and hardware. The security related fields mentioned below were strengthened:

- Confidentiality protection, using RC4 algorithm
- Integrity protection, using the Message Integrity Code (MIC) based on the Michaels algorithm
- Replay prevention, using a frame sequencing technique
- Use of a new encryption key for each frame

Table 7 summarizes its basic characteristics:

Characteristic	Security Attribute
Two 64-bit message integrity keys are used for MIC. The MIC is computed over the user data, source and destination addresses, and priority bits	Integrity
A monotonically increasing TKIP Sequence Counter (TSC) is assigned to each frame. This provides protection against replay attacks	Integrity
A key-mixing process produces a new key for every frame. It uses the Temporal key and the TSC to generate a dynamic key	Confidentiality
The original user frame, the MIC and the source address are encrypted using RC4 using the per-frame key	Confidentiality

Table 7 – TKIP summary

Counter Mode with Cipher Block Chaining MAC Protocol
CCMP is similarly targeted, but more flexible in hardware implementation, compared with TKIP. It is based on a generic authenticated encryption block cipher mode of the Advanced Encryption Standard (AES) Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC) (CCM) mode. Its use is mandatory in WPA2 implementation. CCMP enables integrity and confidentiality protection that allow for easier detection of a wrong packet.

9 Conclusions and recommendations

This document represents the deliverable D8.1 titled “Analysis of requirements for data exchange and management”. Its objective has been to study and investigate airport network requirements, stating from the analysis of the ATOM system, the user requirements and the available technological solutions. After a first presentation of the different sub-systems composing ATOM, focusing on the input and output provided to the central unit, further analysis has been performed. Airport infrastructures and the most common technology have been exposed. Then a detailed analysis of the traffic load has been performed by analyzing a specific scenario and considering a variable passengers flow inside the airport. Finally, after a chapter dealing of typical airports’ constraints, the network requirements have been defined. The last chapter is about the preliminary study of the network architecture. This can be considered as a starting point for deliverable D8.2, titled “Network architecture proposal document”. It will be the direct continuation of the work done until now which will conclude the study and analysis performed in WP8.

10 References

Below we list links to publications and web resources we consulted in writing the *WiFi* section:

[1] Adel-2007, Adel, 802.11's Modulation Techniques, in Wi-Fi and Wireless Technology Blog, wi-fi-wireless.blogspot.com/2007/05/80211s-modulation-techniques.html

[2] Briggs-2010, Mark Briggs (Elliott Labs), Dynamic Frequency Selection (DFS) and the 5GHz Unlicensed Band, www.elliottlabs.com/documents/dynamic_frequency_selection_and_5ghz_band.pdf

[3] IBM-2006, Lydia Parziale et alii (IBM), TCP/IP Tutorial and Technical Overview, Eighth Edition (December 2006), Redbooks

[4] Magee-2009, Owen Magee (Digi International Inc.), A designer's guide to embedded Wi-Fi (May 2009), in EE Times-Asia, www.eetasia.com/ART_8800571763_499488_TA_7175cfc9.HTM

[5] MDD-2009, Louis E. Frenzel (Mobile Dev & Design), Orthogonal Frequency-Division Multiplexing (OFDM): FAQ Tutorial, mobiledevdesign.com/tutorials/ofdm/

[6] Ross-2008, John Ross, The Book of Wireless. A painless guide to WI-FI and broadband wireless. No Stack press, 2008 (2nd edition)

[7] Trapeze-2009, Trapeze Networks, Inc., TB_DFS3_081109 - Dynamic Frequency Selection (DFS), www.trapezenetworks.com/file.cfm?content=1369&pageId=32

[8] TSA-2006, Transport Security Administration, Recommended Security Guidelines for Airport Planning, Design and Construction, Eighth Edition (Revised June 15, 2006), www.tsa.gov/assets/pdf/airport_security_design_guidelines.pdf

[9] Wikipedia, many entries of the english version of Wikipedia (en.wikipedia.org) have been consulted

[10] Xirrus-2008, Xirrus, Inc., Wi-Fi Authentication Demystified - Tutorial, www.xirrus.com/pdfs/Tutorial_Authentication.pdf

We acknowledge below some more specific credits:

- some excepts from (Ross-2008) make up the section "Wi-Fi and the ISO-OSI network model" and integrate the section "Wi-Fi security" [11]
- a large number of technical details draw heavily on (Wikipedia) [12]
- some general subsections on 802.11 have been adapted from (IBM-2006) [13]
- the section on "Embedded Wi-Fi design considerations" has been freely abridged from (Magee-2009) [14]
- most of the section on "Wi-Fi regulations in Europe" is an excerpt from (Briggs-2010) [15]
- the section on "Wi-Fi in the TSA Guidelines" has been drawn almost literally from (TSA-2006), possibly a bit obsolete [16]

Below we list links to publications and web resources we consulted in writing *Ethernet* and *PLC* sections:

Web links:

- IEEE 802 LAN/MAN Standards Committee: www.ieee802.org [17]
- A Guide to Ethernet Components and Terminology: http://www.bb-elec.com/ethernet_infrastructure.asp [18]
- Building a Secure Ethernet Environment: http://www.automation.com/resources-tools/articles-white-papers/industrial-ethernet/building-a-secure-ethernet-environment [19]

- Ethernet Security, Safety Relies on Common Sense Networking: http://www.ictglobal.com/enet_security.html [20]

- Wikipedia: http://en.wikipedia.org/wiki/Ethernet; http://en.wikipedia.org/wiki/IEEE_802.3; http://en.wikipedia.org/wiki/QoS; http://en.wikipedia.org/wiki/Power_line_communication [21]

Papers:

[22] Icns 2007, Warsaw University of Technology. On assuring QoS in Ethernet access network. Robert Janowski, Piotr Krawiec and Wojciech Burakowski. Nowowiejska 15/19, 00-665 Warsaw, Poland

[23] Anote134-ang, EXFO. Quality of service for Ethernet. Matthew Demyttenaere, Sophie Legault, www.exfo.com

[24] IEEE 2008 , Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. Field Measurements of Broadband PLC: A Case Study in the Brazilian Regulation Diana Tomimura ANATEL, V. Vellano Neto Fundação CPqD

[25] Olsen 2005, Technical Considerations for Broadband Powerline (BPL) Communication. School of EECS, Washington State University, Pullman, WA, USA, bgolsen@wsu.edu

[26] RfDesign 2006
Srinivas Katar, Manjunath Krishnam, Richard Newman and Haniph Latchman. Harnessing the potential of powerline communications using the HomePlug AV standard. www.rfdesign.com

[27] HPAV, Powerline Alliance. HomePlug 1.0 Technology White Paper

[28] IEEE 2009, A Novel Hybrid Network for Hospital Environment Incorporating IEEE802.16 and HomePlug AV Standards. Peng Wang, Keyworth Institute, University of Leeds, UK LS2 9JT, Garik Markarian Department of Communications Systems, University of Lancaster, UK LA1 4YW, George Kolev, Rinicom Ltd.Leeds, UK LS2 9AE

[29] IEEE 2003, A Comparative Performance Study of Wireless and Power Line Networks. Yu-Ju Lin, Haniph A. Latchman, and Richard E. Newman, University of Florida Srinivas Katar, Intellon Corporation

Books and Guides:

[30] IEEE, Wireless Engineering Body of Knowledge (WEBOK), G. Giannattasio, J. Erfanian, P. Wills, H. Nguyen, T. Croda, K. Rauscher, X. Fernando, N.Pavlidou, 2008 Edition

[31] Volere, Requirements Specification Template, by James & Suzanne Robertson principals of the Atlantic Systems Guild

[32] Security in Wireless LANs and MANs, T.Hardjono, L.R.Doneti

[33] Lawrence Livermore National Laboratory:
Securing WLANs using 802.11i, Ken Masica

Airport infrastructure:

[34] [ATC-Network-2011]
Tenders - 11021601 Network equipment and network services -
http://www.atc-network.com/Tender/37174/11021601-Network-equipment-and-network-services---NETHERLANDS

[35] [AAS-2010-a] Amsterdam Airport Schiphol, A/SSE/AAO. "Safety & Security. Pocket Guide 2010-2011", 2010 (pdf_internet_engels.pdf)
http://www.schiphol.nl/Vacancies/SchipholPass/SafetySecurity/PocketGuideSafetySecurity.htm

http://www.schiphol.nl/web/file?uuid=64de12cf-b969-44d4-aa69-2ec24a608684&owner=562a3b2a-da01-4c81-a03b-e2dd38ec65eb

[36] [AAS-2010-b] Internet available throughout the airport
http://www.schiphol.nl/Travellers/AtSchiphol/AirportFacilities/InternetTelephone/InternetAndPhoneAccessEverywhere.htm

[37] [AAS-2010-c] KPN Internet Centre & Zones
http://www.schiphol.nl/Travellers/AtSchiphol/AirportFacilities/InternetTelephone/KPNInternetCentreZones.htm

[38] [AAS-2010-d] Who does what at Schiphol?
http://www.schiphol.nl/web/file?uuid=8e08772b-11ae-43c0-a7d7-79189b490a75&owner=7ccedf61-a8f4-4180-b5b0-849e8def7d3e

[39] [AAS-2010-e] Safety and security
http://www.schiphol.nl/SchipholGroup/CorporateResponsibility/SafetyAndSecurity.htm

[40] [IRIS-2010] Iris ID Systems, Inc. "21st Century Airport Operations. Improving security and efficiency with iris recognition based access-control", 2010
http://www.irisid.com/download/brochure/IrisID_AirportSecurity.pdf

[41] [ISNR-2010] Schiphol Airport Security - New Screening Technologies Designed to Improve Passenger and Luggage Screening
http://www.isnrabudhabi.com/body.aspx?id=81

[42] [Moodie-2010] Schiphol Group steps up security at See Buy Fly stores after alert
http://www.moodiereport.com/document.php?c_id=6&doc_id=23469

[43] [mulder-hardenberg-2010] A new ‘home’ for 500.000 signals a month...
http://www.mulder-hardenberg.nl/en/cases/documenten/Case_IA_Schiphol.pdf

[44] [KNMI-2009] Wiel Wauben, Jan Sondij. Royal Netherlands Meteorological Institute (KNMI). "The Meteorological Observation Infrastructure at Schiphol Airport". Information Paper METG/19, September 2009
http://www.knmi.nl/~wauben/HIM/METG%5B1%5D%5B1%5D.19.IP.024.AppendixA.5.NED%20-%20Observation%20infrastructure%20KNMI%20%28ID%207294%29.pdf

[45] [bsia-2009] Airport security - CCTV takes off
http://www.bsia.co.uk/news/newsarticle/NXS342728561?backlinktype=articles

[46] [rdm-2009] R&M Solution Makes Information Fly at Schiphol Group
http://www.rdm.com/en/Portaldata/1/Resources/hq/downloads_d_e/referenzberichte_d_e/englisch/Schiphol-Group_Benelux_2009.pdf

[47] [CDM-2009] CDM Collaborative Decision Making
http://www.euro-cdm.org/library/airports/schiphol/mou_ams.pdf

[48] [nationaleombudsman-2009] Security screening at Schiphol Airport
http://rapporten.nationaleombudsman.nl/rapporten/grote_onderzoeken/2009schiphol/documents/IngenomengoederenSchipholengels.pdf

[49] [hollandtrade-2008] Dutch airport technology
http://www.hollandtrade.com/publications/made-in-holland/mih.asp?bron=airport+technology

http://www.hollandtrade.com/publications/made-in-holland/pdf/2008_01_Dutch_airport_technology_EN.pdf

[50] [KPN-2007] Full TETRA service at Schiphol Airport
http://www.tetramou.com/uploadedFiles/Files/Presentations/Argentina2007airportcasestudy.pdf

[51] [indigovision-2006] IP Video Analytics Ensures Airport Safety
http://www.indigovision.com/business_airports_schiphol.php

http://www.indigovision.com/news/press%20releases/Schiphol-PR-US.pdf

[52] [aerialfacilities-2006] Recent Projects - Schipol Airport (Netherlands)
http://www.aerialfacilities.com:1050/pdf/recent-projects.pdf

[53] [thefreelibrary-2002] Ethernet Switching from Nortel Networks Assumes Key Role at Amsterdam Airport Schiphol; Vosko Networking Implements Award-Winning Enterprise Data Solution
http://www.thefreelibrary.com/Ethernet+Switching+from+Nortel+Networks+Assumes+Key+Role+at+Amsterdam...-a085261310

[54] [Radio-Planning-Group-1998] Design Proposal for the Amsterdam Schiphol Airport
http://www.scribd.com/doc/32067826/GSM-Indoor-design-for-Schiphol-Airport

[55] [AFS-2007] ATC Fact sheet - Transponder ground operation
http://www.lvnl-ohd.nl/ATC%20Fact%20sheets/AFS%2007%20Transponder%20ground%20operations.pdf

[56] [AAS-2010-f] Innovative from the start
http://www.schiphol.nl/web/file?uuid=8b12d8b3-994f-4e95-b9a7-5a2f1d82922e&owner=7ccedf61-a8f4-4180-b5b0-849e8def7d3e