Project Title:	**Advanced multi-paRametric Monitoring and analysis for diagnosis and Optimal management of epilepsy and Related brain disorders**
Contract No:	287720
Instrument:	Collaborative Project
Thematic Priority:	FP7-ICT-2011-5.1
Start of project:	1 November 2011
Duration:	36 months

Deliverable No: D 2.3
ARMOR Middleware Requirements

Due date of deliverable:	[31-08-2012]
Actual submission date:	
Version:	[1.0]
Main Authors:	**S&C, UoP, KIT, STMA, ICOM**

European Commission
Information Society and Media

Change History

Version	Date	Status	Author (Benef.)	Description
0.1	06/02/2012	Draft	Pablo Giménez (S&C)	Creation
0.2	07/05/2012	Draft	Pablo Giménez (S&C)	1st draft
0.3	20/06/2012	Draft	Pablo Giménez (S&C)	Contribution compilation from various consortium members
0.4	11/07/2012	Draft	Alberto Fernandez (S&C)	Review and contributions
0.5	11/07/2012	Draft	Alberto/Pablo (S&C)	Updates
0.6	17/07/2012	Draft	Alberto Fernandez (S&C)	Updates
0.61	19/07/2012	Draft	Artur Krukoswki (ICOM)	Review/Updates
0.62	01/08/2012	Draft	Stefan Hey, Panagiota Anastasopoulou (KIT) Irene Darmanin (STMA)	Review/Updates
0.63	10/08/2012	Draft	Korvesis Panagiotis (UoP)	Review/Updates
0.64	14/08/2012	Draft	Stefan Hey, Panagiota Anastasopoulou (KIT)	Comments
0.65	27/08/2012	Draft	Alberto Fernandez (S&C)	Clean up
1.0	19/08/2012	Final	Alberto Fernandez (S&C) Korvesis Panagiotis (UoP)	Updates & Final version

EXECUTIVE SUMMARY

This document is part of the WP 2, whose main objective is s to evaluate the most efficient body sensors available and adapt them in order to be able to collect the required physiological data and store them in a proper way

This document defines the requirements related to the middleware platform within ARMOR. From device sensors to electronic health record interface and notification applications, the middleware address the needs of the interoperability that is required among the different technologies in place within ARMOR and its functional goals.

DOCUMENT INFORMATION

Contract Number	FP7 – 287720	**Acronym**	ARMOR
Full title	Advanced multi-paRametric Monitoring and analysis for diagnosis and Optimal management of epilepsy and Related brain disorders		
Project URL	http://www.armor-project.eu		
EU Project officer	Dr. Amalia-Irina Vlad		

Deliverable	**Number**	**3**	**Title**	ARMOR Middleware requirements
Work package	**Number**	2	**Title**	Multi-parametric data collection

Date of delivery	**Contractual**	**31-08-2012**	**Actual**	
Status			final ☑	
Nature	Report ☑ Demonstrator ☐ Other ☐			
Dissemination Level	Public ☑ Consortium ☐			
Abstract (for dissemination)	This document defines the requirements related to the middleware platform within ARMOR. From device sensors to electronic health record interface and notification applications, the middleware address the needs of the interoperability that is required among the different technologies in place within ARMOR and its functional goals.			
Keywords	Middleware, interfaces, software, on-line processing			

Authors (Benef.)	Alberto Fernandez , Pablo Gimenez(S&C), Korvesis Panagiotis (UoP), Stefan Hey, Panagiota Anastasopoulou (KIT), STMA, ICOM			
Responsible Author	Alberto Fernandez		**Email**	Alberto.fernandez@sensingcontrol.com
	Beneficiary	1	**Phone**	+34 931 763 520

TABLE OF CONTENTS

1 INTRODUCTION

The principal objective of this document is to present the general requirements that should be taken into account for ARMOR's middleware (AMW from now on). The description of the requirements is divided in four levels:

i) Sensor

Within this section, all the requirements for/from sensors involved in ARMOR system and related to the middleware are described. These requirements have to be related to acquiring, processing and storing data from sensors described in D2.1

ii) Data Stream Management System (DSMS)

The DSMS is the foundation of the online analysis. Requirements describing the methods for the online management, fusion and analysis of data from sensors are pointed out within this section.

iii) Application programming interfaces

How are we going to interact with the middleware? What are the different integrations between systems and middleware for ARMOR services? These APIs and requirements are described in this section

iv) Notification services.

The middleware must ensure the communication between components. All the requirements needed to communicate events, intercommunicate processes and send data to other managed systems are described within this section.

The main source of information used to develop the ARMOR middleware requirements are D2.1 and D2.4, with main focus on the description of the services to be delivered to the users; patients and healthcare professionals, and the specification of the scenarios and use cases.

Specific sections within the deliverable D3.1 have been devoted to security issues, extracting main objectives to be accomplished at sensor/WSN and extrapolating the implications to be developed at middleware level.

2 FUNCTIONAL REQUIREMENTS

The main purpose of ARMOR Middleware is to create an isolation layer between the physical world (sensors/field devices) and high level applications.

Due to the heterogeneous nature of the physical world, it is expected to have many different field devices (which likely will include sensors and a communication system) running different protocols and communication interfaces (serial, ip (udp or tcp), etc…).

At high level side, the creation of a standardised way of accessing sensor data for online/offline processing is a key for the application developers, as they are managing the information from the point of view of service creation, hence isolating them from underlying communication and commissioning of field sensors is a must.

The path between physical world and application world is accomplished at intermediate level between the two defined interfaces. This middle layer is will run several functions supported by a data base tailored to match ARMOR services necessities.

All the requirements are described within the five levels described in the introduction.

2.1 Sensor

Code	Description	Impact
FRS01	Timestamped data. All the data must be timestamped appropiately, at a level sufficient to perform synchronisation among separate data modalities, e.g. EEG & ECG	High
FRS02	The data from Sensor(s) is (are) streamed to the AMW.	Low
FRS03	AMW drivers will collect the chunks of data from Sensor and pass them to the online data stream management system (DSMS).	Low
FRS04	Sensor will push data to AMW	Low
FRS05	AMW will pull data from Sensor (SD cards, filesystem,…)	Low
FRS06	AMW will support data input from sensors specified in [D2.1]	High
FRS07	AMW will store pulled data from Sensor locally	Low
FRS08	Alarms/Warnings can be originated by sensors (i.e. push button)	Low

2.2 Data Stream Management System (Online analysis)

Code	Description	Impact
FRSD01	Detection of abnormal values. The system must detect abnormal values due to improper use of sensors	High
FRSD02	AMW will receive a ‘start’ trigger from upper layers (GUI) to initiate the analysis of data	High
FRSD03	AMW will receive a ‘stop’ trigger from upper layers (GUI) to stop the analysis of data	High
FRSD04	The system will use variety of efficient and effective algorithms, to be able to deal with the streaming nature of data in order to perform the online analysis	High
FRSD05	The DSMS will use configuration settings to perform the analysis	High
FRSD06	Application errors will be logged to the error log.	High
FRSD07	Detection of epilleptic seizures covering scenario 4 in [D2.1]	High
FRSD08	Alarms/Warnings can be originated by DSMS	High

FRSD09	Changing of configuration parameters aplies in next run	Low
FRSD10	Detection of modalities exceeding a preset for each patient range of normal vàlues (i.e. excessive tachycardia and oxygen level excursions)	High
FRSD11	Use of activity sensor for diagnosis decisions involving cardiogenic triggers of seizures and motor seizures (including their paterns)	High

2.3 Application programming interfaces

Code	Description	Impact
FRAPI01	AMW will initiate sensor data upload to the PHR via PHR-API by notification of upper layers	High
FRAPI02	AMW will send the raw data from sensors to the PHR-API by notification of upper layers	High
FRAPI03	Configuration parameters related to FRSD05 come from the offline analysis results and are provided by upper layers (GUI)	High
FRAPI04	Configuration parameters related to FRS04/FRS05 are provided by upper layers (GUI)	High
FRAPI05	AMW will receive Patient ID from underlayed processes and services controlled by the GUI	High
FRAPI06	Alarms/Warnings can be originated by upper layers	Low

2.4 Notification services

Code	Description	Impact
FRNS01	Alarm notification. AMW must be able to pass an alarm to upper layers.	High
FRNS02	AMW will get/receive configuration parameters from upper layers (GUI)	High
FRNS03	AMW will be able to send status of operations to upper layers. (Upload progress, performing analysis, data sent, data error, mw error...)	Low
FRNS04	Application errors will be send as a notification to the upper layers (GUI)	Low

FRNS05	AMW will receive a 'send sensor data' trigger from upper layers (GUI)	High
FRNS06	AMW will notify upper layers (GUI) whether the function used is in the ON or OFF mode.	High
FRNS07	AMW will receive a 'capture sensor data' trigger from upper layers (GUI).	High

3 NON-FUNCTIONAL REQUIREMENTS

3.1 Sensor

Code	Description	Impact
NFS01	Sensor interface should allow the maximum data throughput from sensor/channel configuration defined in [D2.4]	Low
NFS02	Sensor's data will reach AMW through serial interface	High
NFS03	Sensor's data will reach AMW through ip:port	High
NFS04	Sensor's data sensor will reach AMW through local RAM memory	High
NFS05	Sensor's data sensor will reach AMW through local permanent memory (file system)	High
NFS06	The exchange data format will be unisens (streaming/logging)	High
NFS07	Storage capcity tailored for patient long term monitoring	High

3.2 Data Stream Management System (Online analysis)

Code	Description	Impact
NFSD01	Adding/Removing new sensors to the stream has to be supported during run-time without having to interrupt ongoing analysis	High
NFSD02	Stream databases technology will be used (like StreamInsight or xStream)	High

3.3 Application programming interfaces

Code	Description	Impact
NFAPI01	Message queue interfaces. AMW will provide a message system to communicate to upper layers	High
NFAPI02	Upper layers will communicate with AMW through a message queue system	High
NFAPI03	Sensor data should be compressed on transmission	Low
NFAPI04	WEB service I/F for communication from sensors to PHR NOTE: Java WEB services (preferable) or REST to be used	Low
NFAPI05	Use of Unisens/Propietary for transmitting sensor data to PHR.	Low
NFAPI06	Use of Device Profiling for standardised means of inteconencting sensor devices with PHR platform	Low
NFAPI07	Connection with API requires permanent link or a link available during periods of time	High
NFAPI08	Don't use explicit IP addresses, use friendly DNS names instead if available.	Low
NFAPI09	Java scripting API to be supported	Low
NFAPI10	DynDNS service support on the server side	Low
NFAPI11	Selection of sensor data to be transmited shall be allowed	Low

3.4 Notification services

Code	Description	Impact
NFNS01	Notification services requires permanent link or a link available during periods of time	High
NFNS02	Message queue infrastructure will be used for intercommunication.	High
NFNS03	Message format will be XML	High

4 PRIVACY & SECURITY REQUIREMENTS

As part of the non-functional requirements, within this this section the elaboration of AMW privacy and security requirements is done taking into account the global ARMOR's privacy and security requirements elaborated in deliverable 3.1 [D3.1].

Cross requirements to all subsections are specified in the following table.

Code	Description	Impact
SECG01	Storing of activity for auditing	High
SECG02	Anonymisation of patient data (AMW only knows patient IDs)	High
SECG03	Using cryptographic random number generators to generate session IDs	High
SECG04	Store credentials in an secure manner	High
SECG05	Use Strong password policies	High
SECG06	Encrypt communication channels to secure authentication tokens	High
SECG07	Authenticated API commands should be supported	Medium

4.1 Sensor

Code	Description	Impact
SECS01	Data sent to AMW is not ciphered	High
SECS02	Wirless data sent to AMW is ciphered	High
SECS03	Data sent to AMW is done locally and within an intrinsically secure channel.	Medium
SECS04	No info related to patient is sent from the sensors	High

4.2 Data Stream Management System (Online analysis)

Code	Description	Impact
SECSD01	Data through the pipe (within the AMW) is not encrypted	High

4.3 Application programming interfaces

Code	Description	Impact
SECAPI01	Use https in restful webservices	High
SECAPI02	Use ssl between communications	High
SECAPI03	Data creation, updating and deletion procedures exposed via RESTful interfaces (PHR) are authorized when possible.	High
SECAPI04	Data creation, updating and deletion procedures exposed via RESTful interfaces (PHR) will use HTTP POST requests, not HTTP GET.	High

4.4 Notification services

Code	Description	Impact
SECNS01	Use ssl between comunications	High
SECNSD02	An alarm/warning provided to upper layers is related to a patient through patient ID.	High

5 AMW ARCHITECTURE DRAFT

Given the requirements described in this document, the initial draft of the AMW architecture is drafted in Figure 1. Notice that this diagram is the tailored version fulfilling ARMOR needs from the M2M platform presented in D2.1 section 5.1.2. Figure 1 also match middleware within the ARMOR general view of ICT components (small diagram on top right of Figure 1) presented in deliverable D2.2.

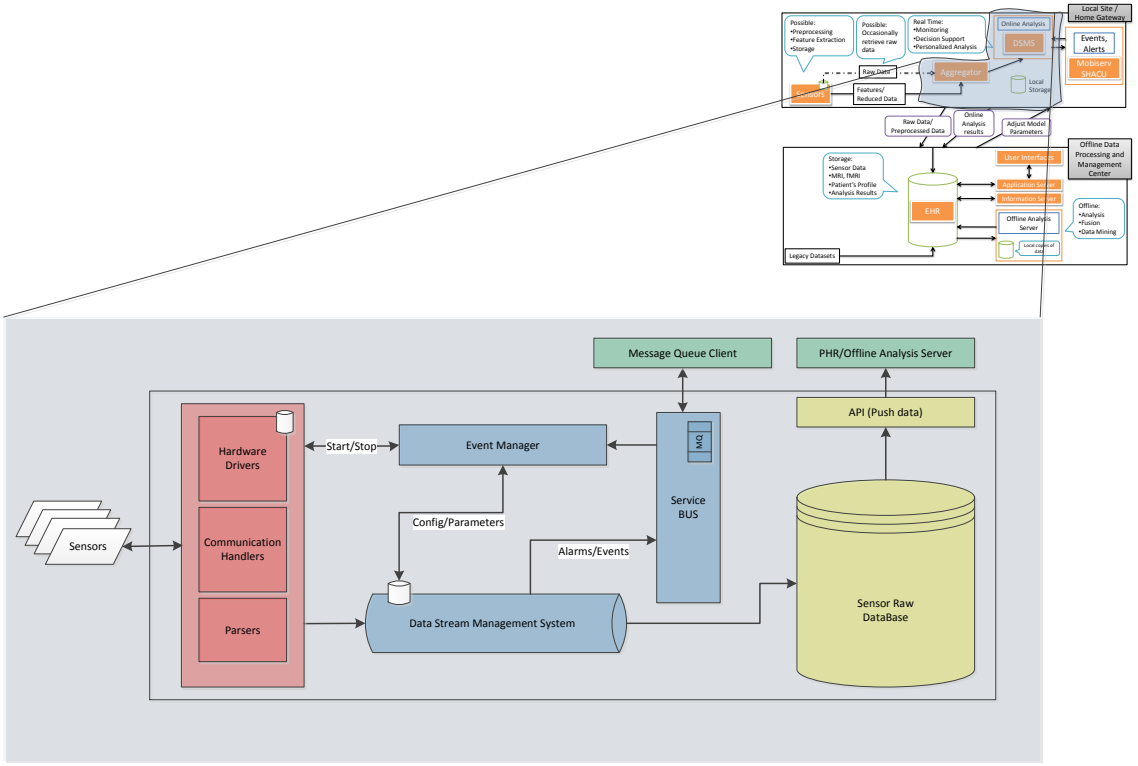

Figure 1 : ARMOR Middleware architecture.

Sensors will communicate with the AMW through the drivers and communication handlers layer (hardware interfaces in red). All the mechanisms about online analysis and interoperability between the AMW and other components (GUI, upper layers...) are within the Processing module (in blue). This layer handles all the processing/intelligence of the software. It has a built in event manager that processes messages from upper layer applications (in green), that manages communication between hardware interfaces and application service bus, automation routines and alarm/events handling based on rules.

Database layer and API (in yellow) will maintain interoperability across multiple platforms, applications and systems allowing the delivery of raw data sensors to the PHR

Protocols between AMW and “outside world” must be defined in order to communicate with devices and applications.

As described in previous sections, ARMOR MW will use two protocols to communicate with sensors and high level apps. Sensors communication protocol will be Unisens [Uni]. The communication protocol between MW and Patient Health Record will be either Unisense or Propietary, the decision will be done at design level.

6 APPENDIX 1 – ARMOR DELIVERABLE REVIEW FORM

ARMOR Deliverbale Review Form		
Deliverable:	Deliverable No: D 2.3 ARMOR Middleware Requirements	
Reviewer(s):	Stefan Hey	Vasileos Megalooikonomou
Review Date:	29-08-2012	

Does the document cover the objectives and task description stated in the DoW taking also into account the overall project vision?

Yes [x]

No [ ]

Partly [ ]

Comments:

- …
- …

Is the Executive Summary in a publishable form? (This should be no longer than 2 pages, easy to understand by people outside the project, showing scope and result achieved)

Yes [x]

No [ ]

Partly [ ]

Comments:

- …
- …

Are the structure and appearance (layout, images etc.) compliant with the Quality Plan?

Yes [x]

No [ ]

Partly [ ]

Comments:

- …
- …

7 REFERENCES

[Uni] http://www.unisens.org/

[D3.1] Deliverable No: D 3.1 Data Privacy and Security Requirements

[D2.1] Deliverable No: D 2.1 Functional and Non Functional Requirements of the ARMOR Services

[D2.2] Deliverable No: D 2.2 Real time data requirements