CUSTOMER SECURITY PLAN

Document No	IT.PL.01
Release Date	08/31/2023
Revision Date	-
Revision No	00

Index

1. Scope and Purpose

Customers need security documentation to perform more robust risk assessments, define configurable security controls, and better protect their systems. This document provides an overview of the following topics that can be included in customer security documentation following a potential cybersecurity attack.

- Product description
- Hardware Features
- Operating Systems
- Third-party software
- Data flow diagram
- Patch Management
- Authentication
- Physical controls
- Data Encryption
- Secure Encryption Standards
- System Retrofit Standards
- Risk Summary

2. Product Description

Magic Loggia Ultimate M infant incubators are designed to support developmental care for infant and neonates. Magic Loggia Ultimate M is intended to keep infants or neonates in a warm environment which is covered by a hood and isolated from ambient air and of which internal air temperature and humidity are controlled.

The device includes an AC- powered heater, a fan to circulate the hot air, a container for water to produce humidity, a control valve to control requested O_2 concentration.

3. Hardware Specifications

3.1 Sensor Module (Sensor Board):

The sensor module is designed to measure humidity, air temperature, skin temperature and oxygen parameters inside the cabinet. Chips and passive components are suitable to operate in the range of 40^{o}C~+125^{o}C with their very low offset values and stable offset/temperature curves.
All inputs and outputs are protected with ESD and TVS diodes. All analog signals are filtered from electrical noises by providing the necessary bandwidth. Also, with Common-Mode Choke elements input and output isolations are increased.

3.2 Main Board:

Communication Part; All inputs and outputs of this unit, which manages data transfer between all units, are isolated from each other. All inputs and outputs have thick isolation barriers as well as ESD and TVS diodes. Input and output isolations increased with Common-Mode Choke components. PCB design is made due to difficult conditions so all components are selected to operate in the range of -40^{o}C~+125^{o}C.
DC Part; Power input of the system is protected with LC low pass filter to filter out unwanted signals. This part is designed for DC regulation. All components have very stable regulation curves to operate in the range of -40^{o}C~+125^{o}C. Switch-mode regulation techniques are used to eliminate heating, furthermore, current limiters are placed at the power outputs to prevent excessive power draw. All power inputs and outputs are protected by ESD and TVS diodes additionally Schottky Barrier diodes are used to prevent reverse polarization. Filters and ferrite beads are used at the power inputs and outputs to prevent electrical noises.

AC Part; This unit, which performs heating, valve and motor driving processes, is very well insulated. Current limiting systems on the unit, which have double and reinforced insulation with ESD diodes, TVS diodes and filters, prevents excessive power draw. With the power-protected Solid State Relays potential hazards due incorrect on/off process eliminated and system upgraded to a higher level.

3.3 Com Board:

This board interconnects Main Board and Display Module. Insulation is high priority for this board so communication parts of the board separated from each other with insulation barriers. All components are suitable to operate in the range of -40^{o}C~$+125^{o}$C. All components have very low offset values. Inputs and outputs are protected strictly with ESD and TVS diodes. Electrical noise is significantly decreased with 4 layer PCB design. The Magic Loggia Ultimate M hardware list is given in Table 1 below.

PART NO	COMPONENT NAME	PCB OF COMPONENT	POSITION OF COMPONENT	SUPPLIER
1	Microcontroller	MainBoard	U18	ST Microelectronics
2	Step Down Regulator	MainBoard	U3	Texas Instruments
3	Step Down Regulator	MainBoard	U4	Texas Instruments
4	Step Down Regulator	MainBoard	U26	Texas Instruments
5	Voltage Detector	MainBoard	U5	Microchip
6	Voltage Detector	MainBoard	U23	Microchip
7	TVS Diode	MainBoard	U6	Semtech
8	TVS Diode	MainBoard	U33	Semtech
9	TVS Diode	MainBoard	U7	Semtech
10	Solid State Relay	MainBoard	U1	IXYS
11	Solid State Relay	MainBoard	U2	IXYS
12	Digital Isolator	MainBoard	U17	Analog Devices
13	Digital Isolator	MainBoard	U29	Analog Devices
14	EPROM	MainBoard	U19	Winbond
15	EMI Filter	MainBoard	U20	Murata
16	Low Offset Opamp	MainBoard	U32	Analog Devices
17	DC-DC Isolated Converter	MainBoard	U27	CUI Inc.
18	Battery Charger	MainBoard	U21	Microchip
19	Step Up Regulator	MainBoard	U22	Linear Technology
20	Linear Voltage Regulator	MainBoard	U24	Analog Devices
21	Linear Voltage Regulator	MainBoard	U28	Analog Devices
22	Ideal Diode	MainBoard	U25	Linear Technoogy
23	Analog Switch	MainBoard	U30	Texas Instruments
24	Thermocouple Amplifier	MainBoard	U31	Analog Devices
25	Inductor	MainBoard	L1	Sumida
26	Inductor	MainBoard	L2	Abracon
27	Inductor	MainBoard	L3	Abracon
28	Power Supply	--	--	MeanWell Semiconductor
29	EMC Filter	--	--	Schaffner EMC Inc.
30	Multiplexer	SensorBoard	U1	Analog Devices

31	Low Offset Opamp	SensorBoard	U3	Analog Devices
32	Low Offset Opamp	SensorBoard	U6	Analog Devices
33	Opamp	SensorBoard	U2	Analog Devices
34	Analog Digital Converter	SensorBoard	U4	Analog Devices
35	Analog Digital Converter	SensorBoard	U7	Analog Devices
36	Analog Digital Converter	SensorBoard	U8	Analog Devices
37	Multiplexer	SensorBoard	U5	Analog Devices
38	Multiplexer	SensorBoard	U9	Analog Devices
39	Transceiver	SensorBoard	U10	Analog Devices
40	Linear Voltage Regulator	SensorBoard	U12	Analog Devices
41	EMI Filter	SensorBoard	U11	Murata
42	Microcontroller	SensorBoard	U13	ST Microelectronics
43	EPROM	SensorBoard	U14	Microchip
44	TVS Diode	ComBoard	U1	Semtech
45	Digital Isolator	ComBoard	U2	Analog Devices
46	DC/DC Converter	ComBoard	U3	Analog Devices
47	Linear Voltage Regulator	ComBoard	U4	Analog Devices
48	Serial UART Interface	ComBoard	U5	FTDI
49	Transceiver	ComBoard	U6	Analog Devices

Table 1:Magic Loggia Ultimate M Infant Incubator Hardware List

4 Programming Language Requirements

Programming language requirements include program size requirements or restrictions, and information on management of memory leaks.

5 Interface Requirements

Interface Requirements include communication between system components such as;

- Control module
- Sensor module
- Display module

6 Operating System

	Magic Loggia Ultimate M Control Board	Magic Loggia Ultimate M Display Board	Magic Loggia Ultimate M Sensor Board
Operating System	C-Based Emmattressded	Linux	C-Based Emmattressded
Programming Language	C++	Java	C++
Software Version	V.1.2.2	AS.UL.04.00.00	Module Hw Ver:3 Module Maj Ver:1 Module Min Ver:0 (3.1.0)

Hardware Platform	MCU: STM32F103RBT6	CPU: Allwinner A33 Chipset	MCU: STM32F030R8T6
Hardware Interface	JTAG / SWD	USB	JTAG / SWD
Off-the Shelf Software	Not applicable	Not applicable	Not applicable
Software Type	Custom Developed (Internal Custom)	Custom Developed (Internal Custom)	Custom Developed (Internal Custom)

Table 2: Software description of Magic Loggia Ultimate M

7 Third-Party Software

Also referred to as a Bill of Materials (BOM), includes a list of third-party software and version numbers where applicable. An SBOM is effectively a nested inventory, a list of components that make up software components. The SBOM identifies and lists software components, information about those components, and the supply chain relationships between them. The SBOM graph for our product is shown in Figure 1 and the SBOM list is shown in Table 3:

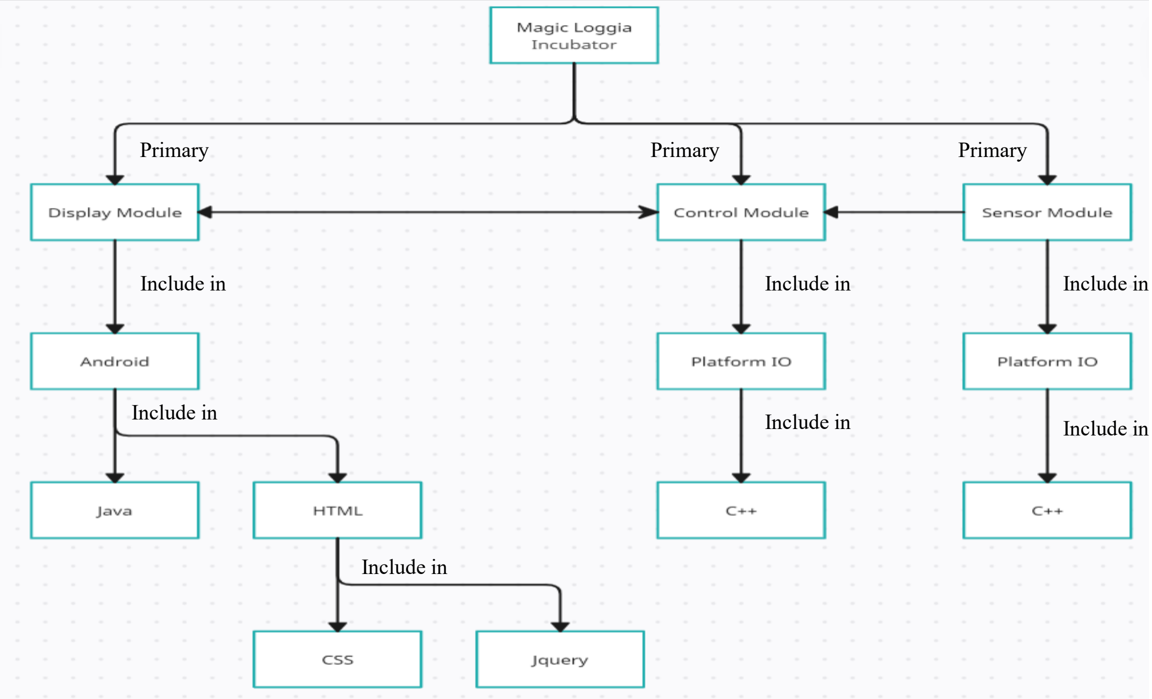


Figure 1: SBOM graph of Magic Loggia Ultimate M Infant Incubator

Component Name	Supplier	Version	Relationship
Android	Google	4.4	Primary
Java	Oracle Corporation	8	Include in
Html	WHATWG, World Wide Web Consortium	5	Include in
Jqeury	The jquery Team	1.4.3	Include in
CSS	World Wide Web	0.16.1	Include in

	Consortium (W3C)		
Control Module Platform IO	Platform IO Labs	framework-mbed 6.60600.210128	Primary
Sensor Module Platform IO	Platform IO Labs	framework-mbed 6.51506.201227	Primary
Control Module C++	Bell labs	17	Include in
Sensor Module C++	Bell labs	17	Include in

Table 3: SBOM list of Magic Loggia Ultimate M Infant Incubator

8 Data Flow Diagram

Magic Loggia Ultimate M infant incubator;

- data type: non-standard
- data flow type: export
- connection type of device : connection through gateway.

Fig. 2 shows the function evaluation use case of a device used in hospitals

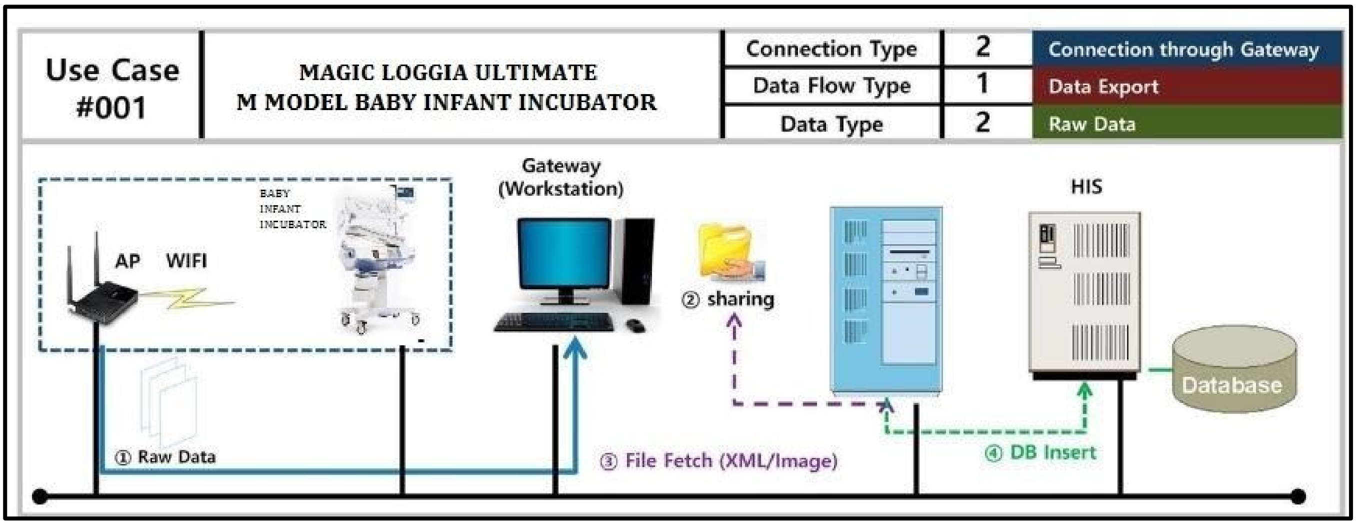


Figure 2: Function assessment use case for an Infant Incubator

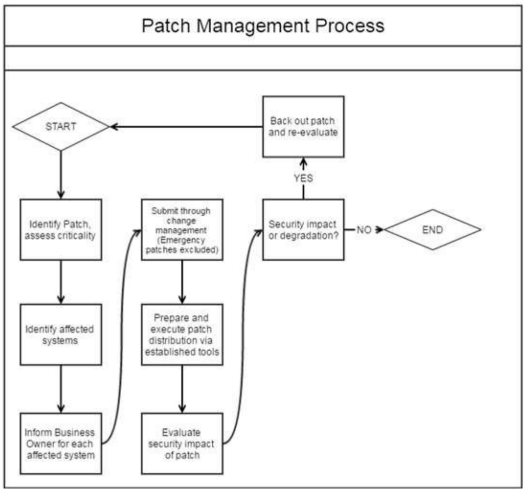
9 Patch Management

Application patching is similar to planned maintenance. Applications are upgraded (rather than patched) as part of a support programme. The steps are:

i. Evaluate upgrade
ii. Plan the implementation
iii. Perform UAT
iv. Release new version

Patch Management Process:

Due to the risk associated to security patches, timely processing is absolutely critical to ensure that the representative risk posed by the vulnerability is mitigated. Consequently, it is recommended that security related patches be treated as any other production problem. The following is a high-level workflow for the patch management process.



Patch Management Process
START
Back out patch and re-evaluate
YES
Identify Patch, assess criticality
Submit through change management (Emergency patches excluded)
Security impact or degradation?
NO
END
Identify affected systems
Prepare and execute patch distribution via established tools
Inform Business Owner for each affected system
Evaluate security impact of patch

Figure 3: Patch Management Process workflow for an Infant Incubator

10 Authentication & Authorization

- Limit Access to Trusted Users Only system
  - Limit access to devices through the authentication of users with user ID and password;
  - Automatic timed methods use to terminate sessions within the system where appropriate for the use environment
- In the user role, a layered authorization model is used according to the operator (nurse, doctor), technical service specialist and system administrator or according to the device role. Wifi access is disabled in the user interface and all authorities can use it. The technical service department can access the system via the wifi activation password. Only technical service personnel can enter this section when the system administrator gives permission.
- Wifi activation codes are not fixed codes. It changes automatically on each serial numbered device and at the time of access.

11 Encryption

Secure data transfer to and from the device is carried out by the system administrator with encryption methods.

Using the back-end microservice architecture policy on the front-end helps break up the application into smaller components, with each front-end (or client-side) application having its own back-end component. This partitioning prevents vulnerabilities in the public part of the application from damaging or compromising the server or user information.

12 Secure Coding Standards

a) CERT Coding Standards

b) CVE is a list of cybersecurity vulnerabilities and exposures found in a specific software product

13 System Hardening Standards

a) CLSI, AUTO11-A - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard.

b) IEC, TR 80001-2-2 Edition 1.0 2012-07 - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.

c) AAMI/ANSI/IEC, TIR 80001-2-2:2012, - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls.
d) IEC, /TS 62443-1-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.
e) IEC, 62443-2-1 Edition 1.0 2010-11 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
f) IEC, /TR 62443-3-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems.
g) ISO 14971:2019 - Medical devices — Application of risk management to medical devices
h) ISO 13485:2016 - Medical devices — Quality management systems — Requirements for regulatory purposes
i) IEC 62304:2006 - Medical device software — Software life cycle processes
j) H.R.7667 - Food and Drug Amendments of 2022
k) UL 2900-1:2017 - UL Standard for Safety Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
l) IEC 810001-5-1: 2021 - Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

14 Risk Summary

Penetration tests, static code analysis and risk analyses are regularly performed for devices and applications. No findings have been encountered in this context.

15 Revision Level History

Date	Revision Number	Description of Change	Responsible
08/31/23	00	First release	Nursel ŞAHİN

Approvals

Author(s):

The information herein is complete and accurate to the best of my knowledge.

Nursel ŞAHİN/R&D and Quality Manager/Electrical - Electronics Engineer 08/31/2023

Name/Title Date

Reviewer(s)

I have reviewed the document and agree with its contents.

Dr. Soner ÇELİK /Cyber Security Consultant / System Engineer 08/31/2023

Name/Title Date