PANTHORA Industrial IoT Gateway, Applications & Security

TELCOSERV

Harris Avgoustidis

h.avg@telcoserv.gr

Presentation Agenda

Section 1

- The Panthora Industrial IoT Gateway
- Applications & Installed base

Section 2

- Industrial IoT Security Challenges
- The H2020 CHARIOT Project & Applications

Section 1: The Panthora IoT Gateway

PANTHORA Monitoring & Management

PANTHORA

REMOTE MONITORING SYSTEM

PANTHORA solution designed by TELCOSERV, is a powerful network management system allowing monitoring and controlling of site related unattended infrastructure, all in a single proactive and intuitive platform. TELCOSERV has designed and developed the following indicative innovative solutions:

- PANTHORA SOFTWARE
- PANTHORA REMOTE MONITORING SYSTEM HW + SENSORS
- PANTHORA LOCK HW – PHYSICAL ACCESS CONTROL

PANTHORA Indicative Applications

Environmental

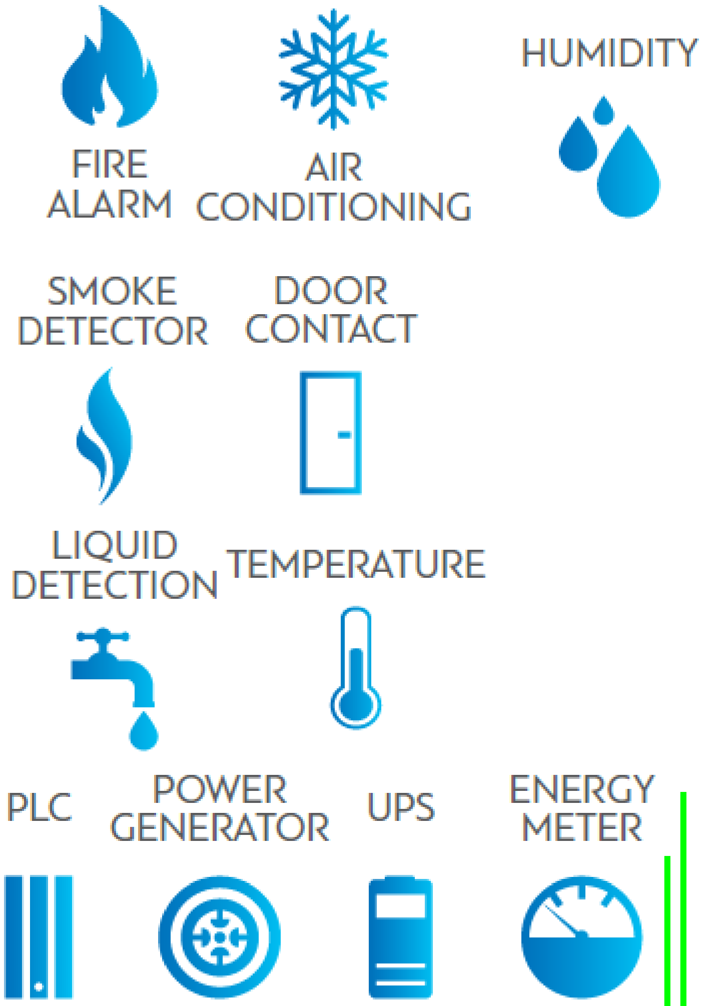
- Water presence / flood
- Temperature and Humidity
- Atmospheric Pressure/ Differential Pressure

Security

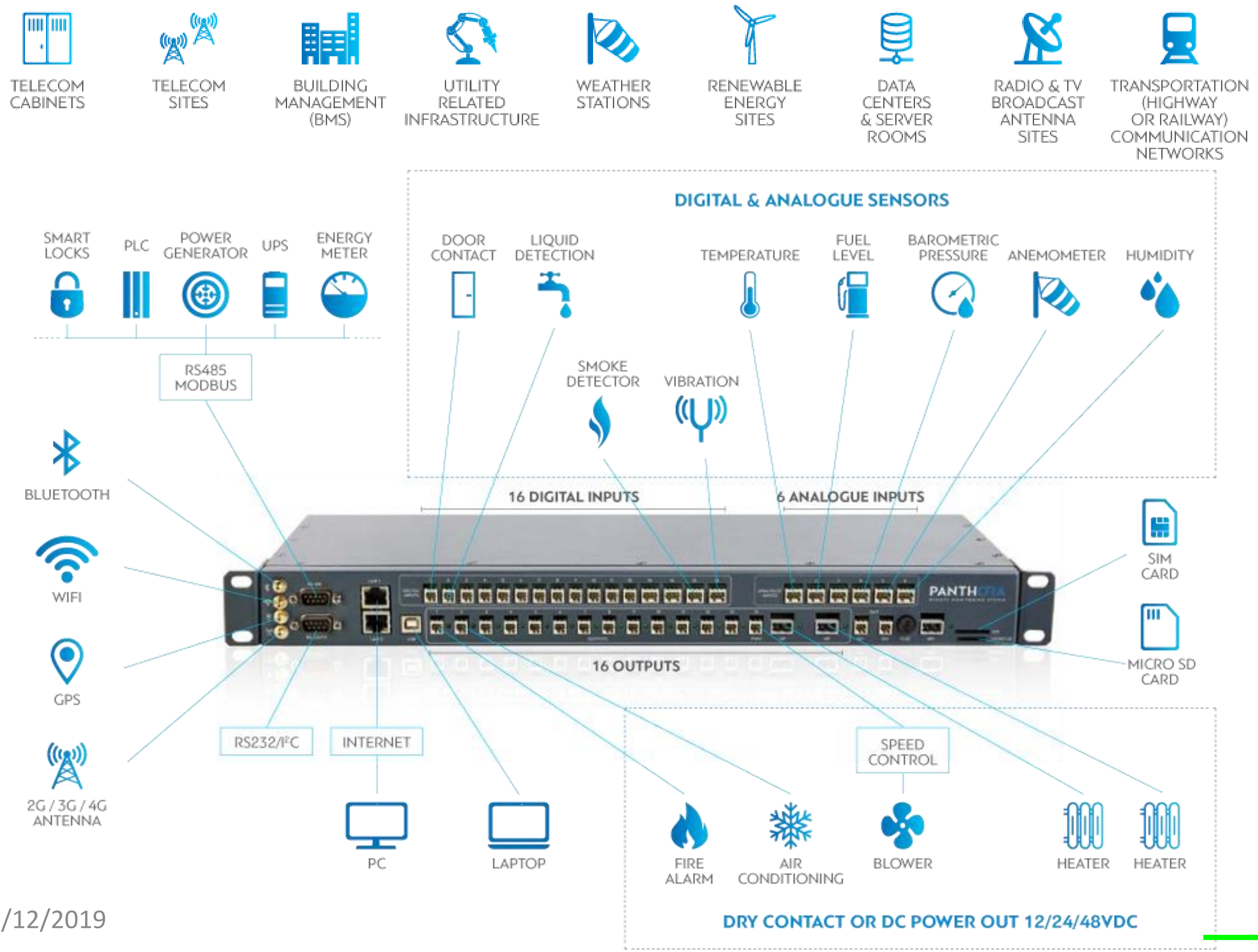
- Physical Access Control
- Break-in Door / Window
- Motion detection
- Smoke / fire detection

Critical Infrastructure

- Generators and tank fuel level monitoring
- UPS / HVAC / PSU
- Power consumption
- Automation Systems (PLCs, SCADA)
- Equipment Status Monitoring



Applications & Interfaces



PANTHORA RMS Features

- Monitoring and Management of the infrastructures concerning Operational, Security, Access and Environmental conditions (temperature, humidity, tank fuel levels, water/fluids presence/levels, motion, intrusion, vibration, etc)
- Alarm signals creation with customized input parameters
- Control of different devices from multiple vendors (e.g. air conditions, power generators, rectifiers etc.) remotely
- Power Management, Fuel Control, Management of Energy Consumption
- Access Authorization System capability
- Operation and configuration capabilities and web interface
- Data collection 24x7, storage and presentation using graphs and reports
- Alerts for any monitored environmental condition exceeds a user-specified range
- Customizable to specific requirements

Benefits

- Increase the availability of the system, decreasing the downtimes
- Overall reduction in OPEX
- Decrease downtime by identifying the root cause and allocating the appropriate personnel with the appropriate materials
- Proactively monitoring so to identify possible problems before they actually happen
- Avoid cost due to unnecessary visits with result to reduce the staff requirements
- Avoid tank fuel theft
- Better use of the systems in the site as you have full information during the whole lifecycle protecting your CAPEX
- Improve the physical security of the sites
- Fully customized solution, easily adaptable to the customer environment

Installed base

Broadcast Operator in Greece improving their site intelligence and eventually intensifies site security whilst at the same time will reduce operating costs. Monitoring and Management of the remote sites:

- Concerning specific Environmental conditions (temperature, humidity, air pressure).
- Monitor and Control all the critical support equipment (UPS, Generator, ATS, Power meter, A/C).

Benefits with the use of PANTHORA:

- OPEX reduction (less on site visits 60 %, less personnel, energy consumption control, prevent major failures)
- Improved reliability and offered SLA (less failures, less time to correct, quick response on power failures)
- Improved security (alarms, logging, controlled access, fuel theft monitoring)
- 1-year ROI

Installed base

National Meteorological Service, performs:

- Environmental monitoring in different spaces/racks of the **Data Center** having for each place different thresholds for producing alarms
  - ➢ Temperature
  - ➢ Humidity
- Power monitoring
- Check if different racks are powered on
- Security conditions (doors & move sensor)

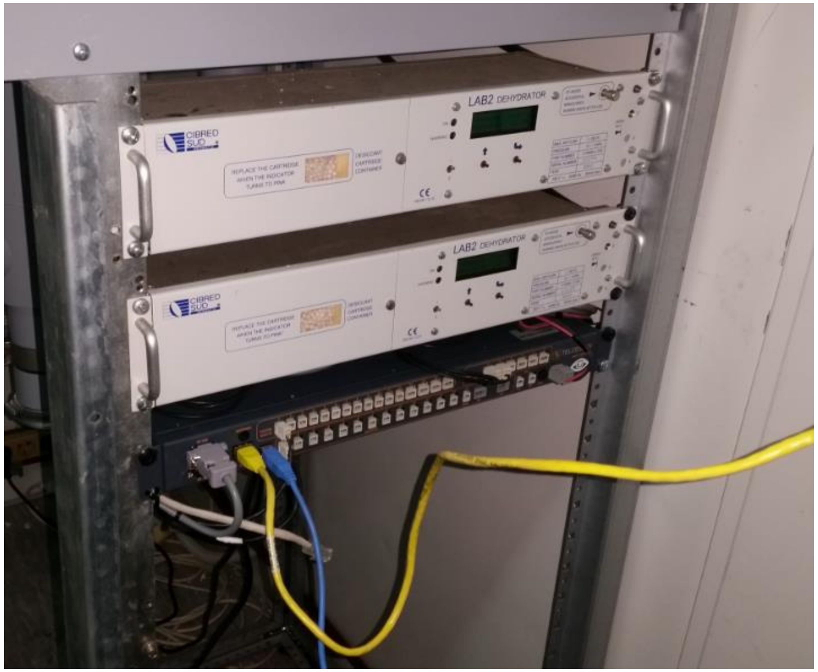
Installed base

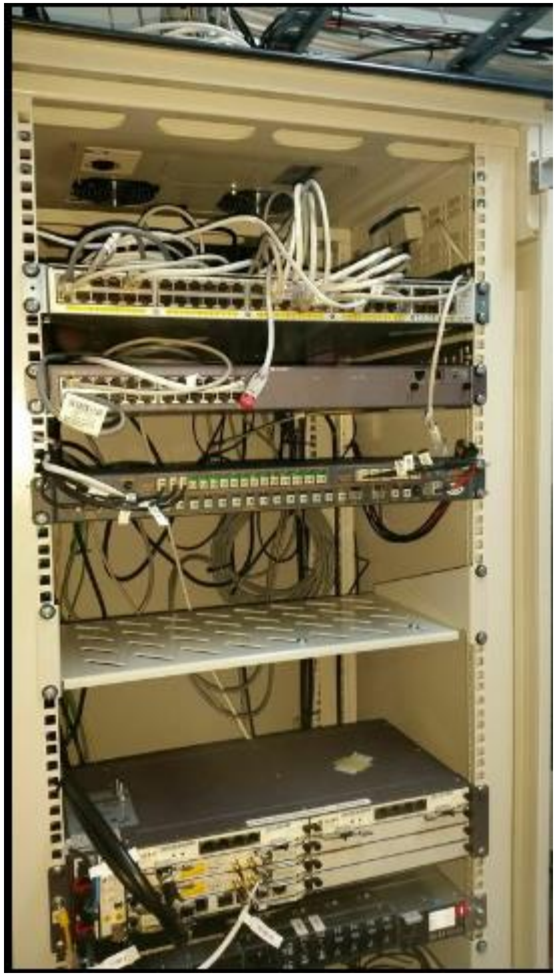
Mobile Operator in Albania aiming to the reduction of avoidable site visits, improving their site intelligence and at the same time reducing the operating costs.

- Monitoring and Management of the remote sites
- Monitoring of Environmental conditions (temperature, humidity, air pressure).
- Monitor and Control the critical support equipment of the site (Power Supply, Generator, Power meter, A/C).

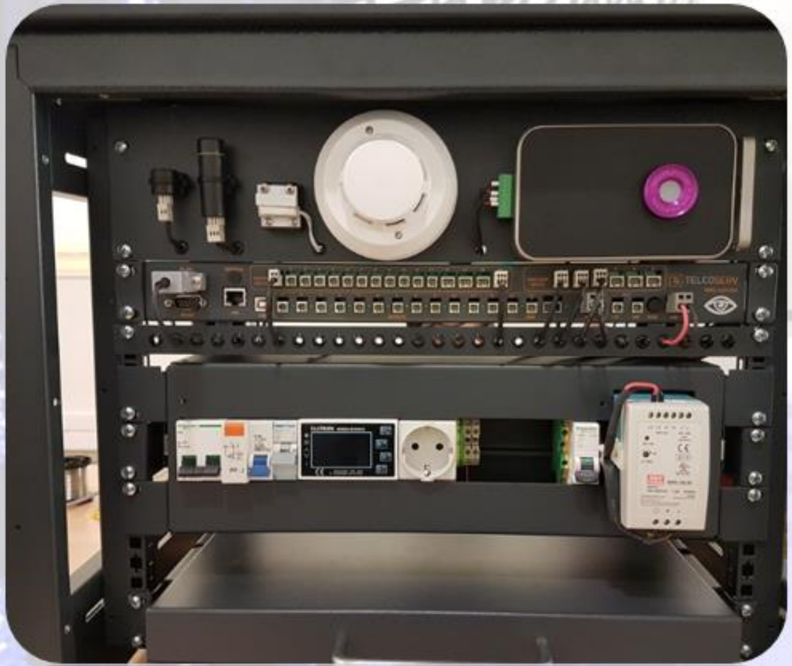
Installation in Telecom Cabinets

Installation in Racks





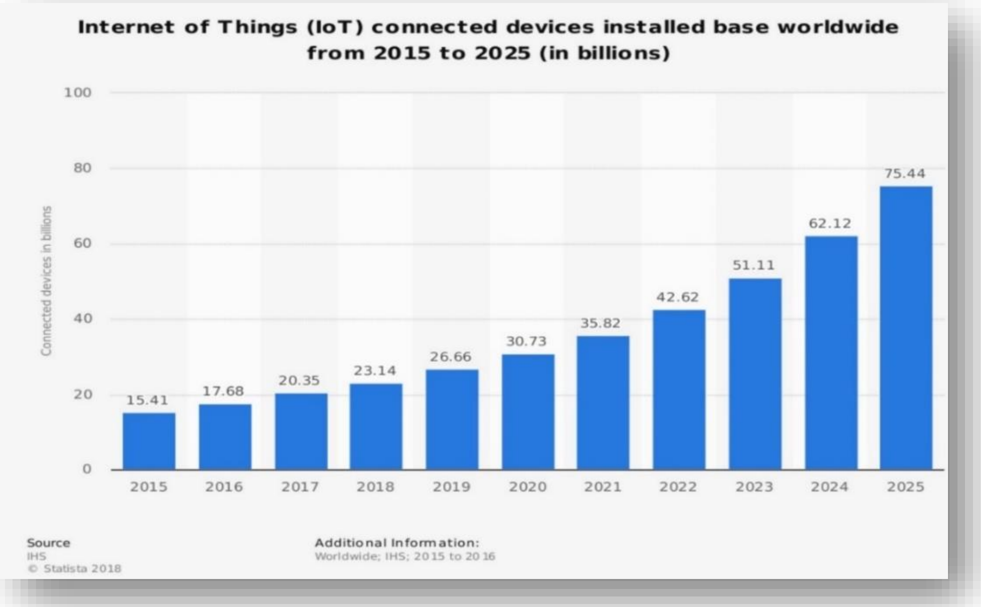
Installation in Racks



Section 2: The H2020 CHARIOT Project

CHARIOT – Industrial IoT Challenges

- By 2025 it is anticipated that there will be **75 Billion IoT-connected devices World Wide**
- **Spending on IoT devices and services reached $2 trillion in 2017**, with China, North America, and Western Europe accounting for 67% of all devices (Gartner Inc)
- Growth in connected devices is anticipated accelerate due to a **rise in adoption of cross-industry devices** (LED lighting, HVAC systems, physical security systems and lots more)
- In recognition of this, **Secure IoT** is now becoming a more important focus of attention



Source
IHS
© Statista 2018

Additional Information:
Worldwide; IHS; 2015 to 2016

CHARIOT – Industrial IoT Challenges

- **Internet of Things (IoT) security breaches have been dominating headlines** recently
  - WikiLeaks’s trove of CIA documents revealed that internet-connected televisions can be used to secretly record conversations
  - Trump’s advisor (Kelly-Anne Conway) believes that microwave ovens can spy on us (through microwave cameras which can be used for surveillance)

- **96% of security professionals expect an increase in IoT breaches this year** (Forbes 2017)

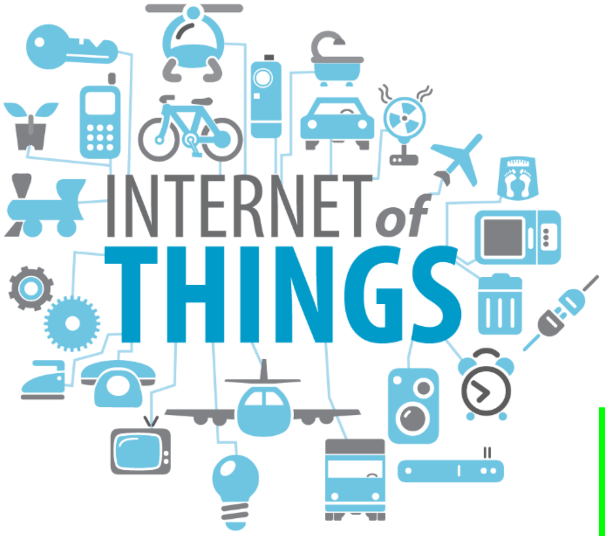
- Recently, ISP Dyn came under attack – **cyber-criminals commandeered a large number of internet-connected devices** (mostly DVRs and cameras) to serve as their helpers

- Requests for government regulation of the IoT, asserting that **IoT manufacturers and customers are not paying attention to the security of IoT devices** (Bruce Schneier, Cybersecurity expert)

CHARIOT Factsheet

Cognitive Heterogeneous Architecture for Industrial IoT "CHARIOT"

Topic:	IoT-03-2017 - R&I on IoT integration and platforms
Type of Action:	Research and Innovation (RIA)
Funding:	4,928,562.50 €
Duration:	36 months
Start Date:	1/1/2018



18

The CHARIOT Consortium

No	Participant organization name	Short	Role	Country
1.	Inlecom Systems (Coordinator)	ILS	Project management, IoT governance	BE
2.	IBM	IBM	Cognitive Architectures & Platforms for IoT	IE
3.	CEA	CEA	Static source code analysis tools for IoT	FR
4.	Athens International Airport - AIA	AIA	Airport LL	GR
5.	eBOS Technologies Ltd	EBOS	Analytics Prediction models and Dashboard development	CY
6.	VLTN	VLTN	IoT deployment architectures/Cloud	BE
7.	Information Sharing Company	ICS	IoT Security	IT
8.	Trenitalia	TRIT	Railway systems engineering/safety	IT
9.	CLMS	CLMS	Systems integration	GR
10.	ASPISEC	ASP	Cybersecurity	IT
11.	TELCOSERV	TCS	IoT Gateway provider	GR

CHARIOT – Overall Vision & Focus

- **The CHARIOT Vision:**

*"To enable **next generation cognitive IoT platforms** that can support:*

1. *Create **intelligent IoT applications** with intelligent shielding and supervision of privacy,*
2. *Safeguard against **cyber-security and safety threats**,*
3. ***Complement existing IoT systems** in non-intrusive ways and*
4. *Help **guarantee robust security** "by placing devices and hardware as the root of trust"*

The CHARIOT Project Objectives

CHARIOT – Overall Vision & Focus

- CHARIOT’s central focus is **Safety Critical Systems (SCS)**
- SCSs are systems whose **failure or malfunction can result in harm, injury or death, loss or damage to property, or impact to the environment**
- SCSs comprise H/W, S/W, infrastructure, networks and human **aspects needed to perform safety functions**, where failure would cause a significant increase in the safety risk for the people or environment
- **Securing data, objects, networks, infrastructure, systems & people in IoT** will have a prominent role in the research and standardization activities over the next several years
- CHARIOT also recognises that **security threats are broad, and have the potential to compromise IoT systems or alter their intended operation**

CHARIOT – Objectives

Objective 1: Specify a **Methodological Framework for the Design and Operation of Secure and Safe IoT Applications** addressing System Safety as a cross cutting concern.

Objective 2: Develop an **Open Cognitive IoT Architecture and Platform (**CHARIOT Platform), **intelligent safety behaviour** in the diverse and complex ways in which the safety critical system and the IoT system will interact in a secure manner

Objective 3: Develop a **runtime IoT Privacy, Security and Safety Supervision Engine** (IPSE)

- Privacy Engine based on PKI and Blockchain technologies
- Firmware Security integrity checking
- IoT Safety Supervision Engine (ISSE)
- Analytics Prediction and Dashboard

Objective 4: **Test and validate Industrial IoT safety in three Living Labs** (LLs) addressing different industrial areas in IoT safety

- Trenitalia (Italy)
- IBM Ireland Campus (Ireland)
- Athens International Airport (Greece)

Objective 5: **Scale up** through wide dissemination, exploitation, capacity building activities

23

The CHARIOT Project Expected Results & Impact

The CHARIOT Expected Results

- A Privacy and security protection method building on state of the art **Public Key Infrastructure (PKI)**
- A **Blockchain ledger** in which categories of IoT physical, operational and functional changes are recorded, invalidating any and all changes be they malicious or otherwise
- A fog-based decentralized infrastructure for **Firmware Security integrity checking** to enhance physical, operational and functional security of IoT systems
- An **IoT Safety Supervision Engine** as novel solution for securing IoT data, devices and functionality in new and existing industry-specific safety critical systems
- A **Cognitive System and Method with accompanying supervision, analytics and prediction models** enabling high security and integrity of Industrials IoT
- New methods and tools for **static code analysis of IoT devices**, resulting in more efficient secure and safer IoT software development and validation/verification

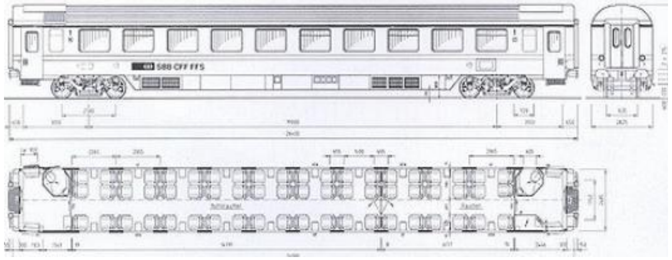
The CHARIOT Expected Impact

- Evolution of platform technologies and contribution to scientific progress **enabling novel**, **advanced semiautonomous IoT applications**
- Increase of IoT usability and user acceptance, notably through strengthened security and user control
- Contribution to emerging or future standards and pre-normative activities
- **Promote the adoption of EU platforms** in European and international context
- Support emergence of an open market of services and innovative businesses

Living Labs in H2020 CHARIOT Project

H2020 CHARIOT PROJECT LIVING LABS

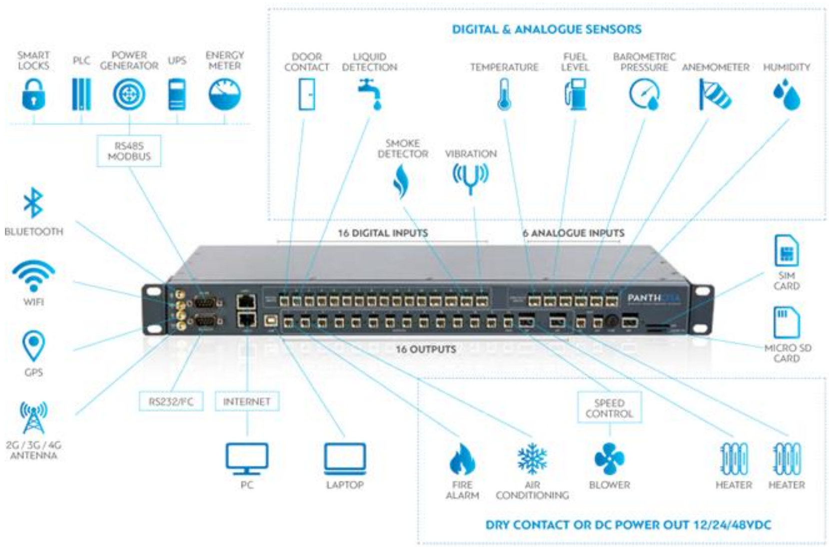
TRAIN



SMART CAMPUS

AIRPORT

PANTHORA IoT Gateway

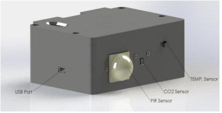


TELCOSERV Contribution in H2020 CHARIOT Project

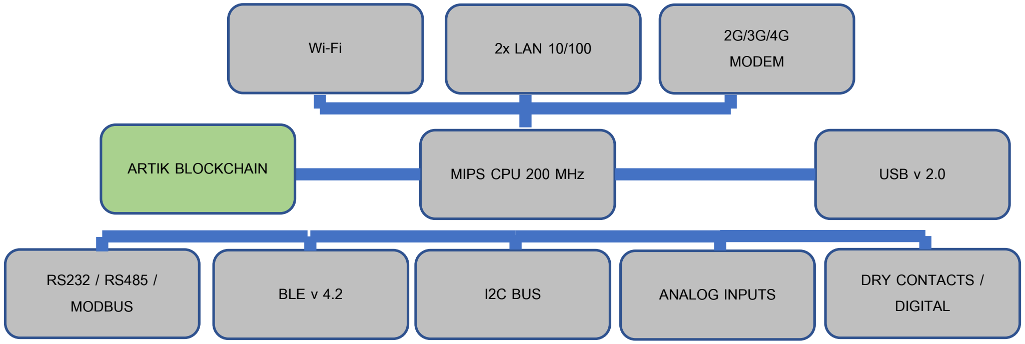
Work Performed and Key-Achievements

- Development of the **Blockchain PKI integration** into the sensor node firmware
- Development of **PANTHORA Gateway Firmware** to **support MQTT protocol** for secure communication to the CHARIOT Dispatcher or third party MQTT brokers
- Development of the **Firmware Upgrade** via FTP for PANTHORA Gateway
- New **BLE sensor hardware node** + **Firmware** enabling integration with Blockchain for exchanging public keys
- Implementation of SFTP server in PANTHORA Gateway for **firmware upgrade OTA** from trusted sources
- Design and Implementation of new **WiFi sensor hardware node + Firmware**
- Final implementations and improvements of three Living Labs (IBM, TRIT, AIA) with complete set of wireless sensors, Gateways and CHARIOT Dispatcher integration

USB Port
PIR Sensor
CO2 Sensor
TEMP. Sensor



Work Performed and Key-Achievements



Wi-Fi

2x LAN 10/100

2G/3G/4G MODEM

ARTIK BLOCKCHAIN

MIPS CPU 200 MHz

USB v 2.0

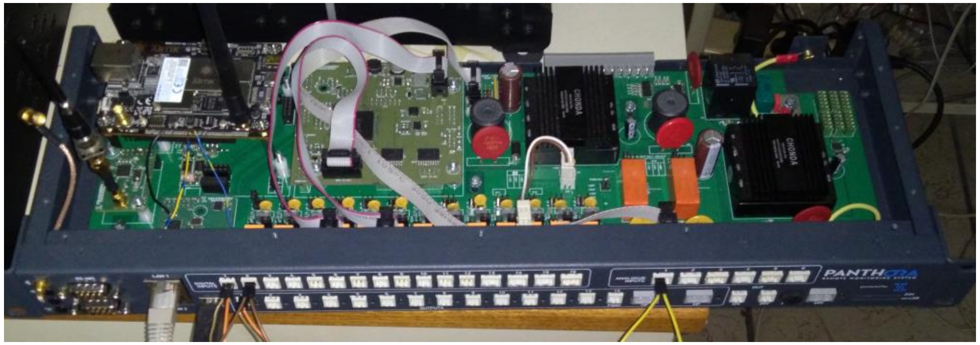
RS232 / RS485 / MODBUS

BLE v 4.2

I2C BUS

ANALOG INPUTS

DRY CONTACTS / DIGITAL



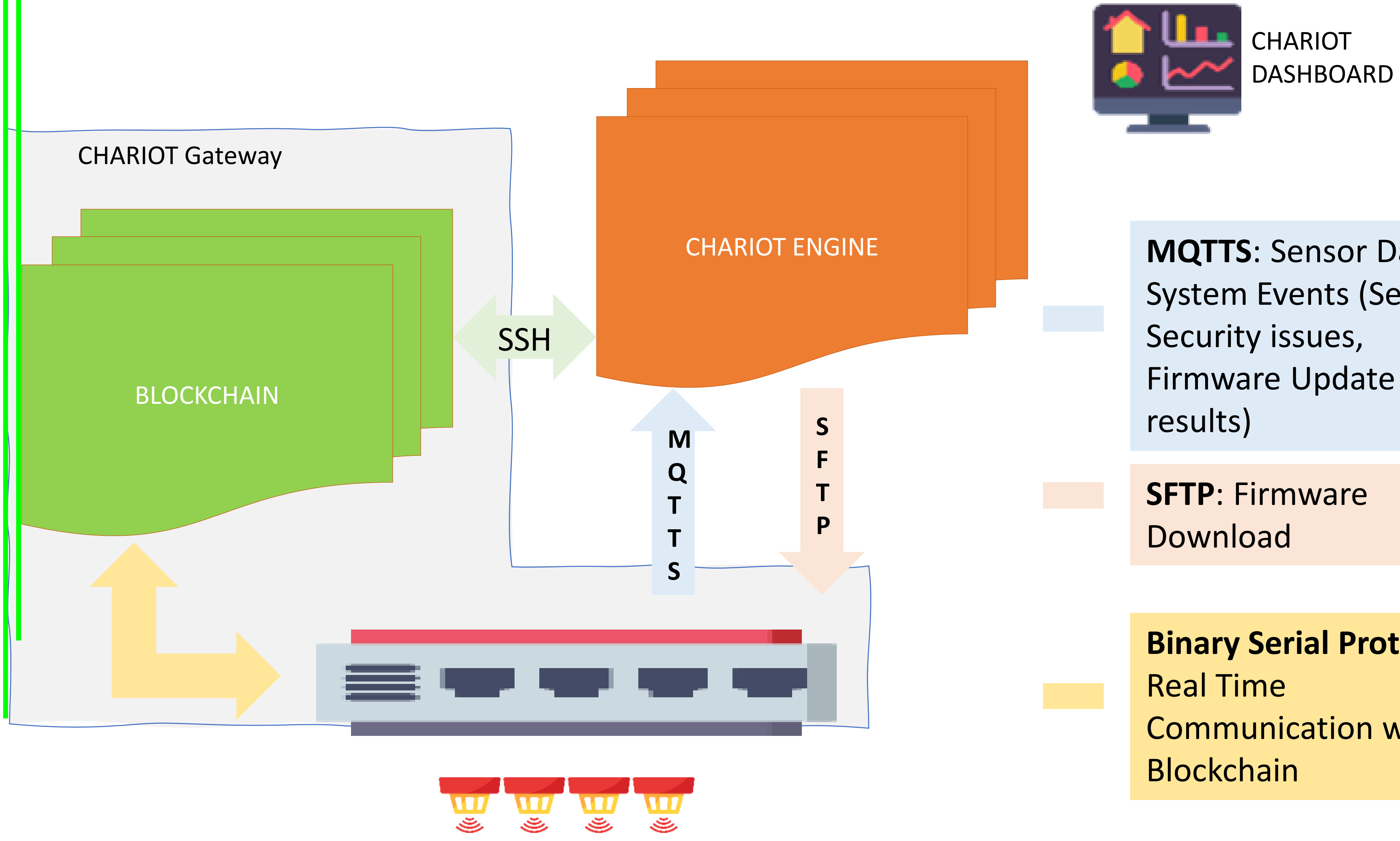
HARDWARE ADD-ON

- Add Blockchain functionality

FIMWARE ADD-ON

- Blockchain enabled
- MQTTS protocol
- Sensor Authentication
- Sensor data Encryption
- SFTP protocol
- Firmware update

Gateway’s Northbound Interface

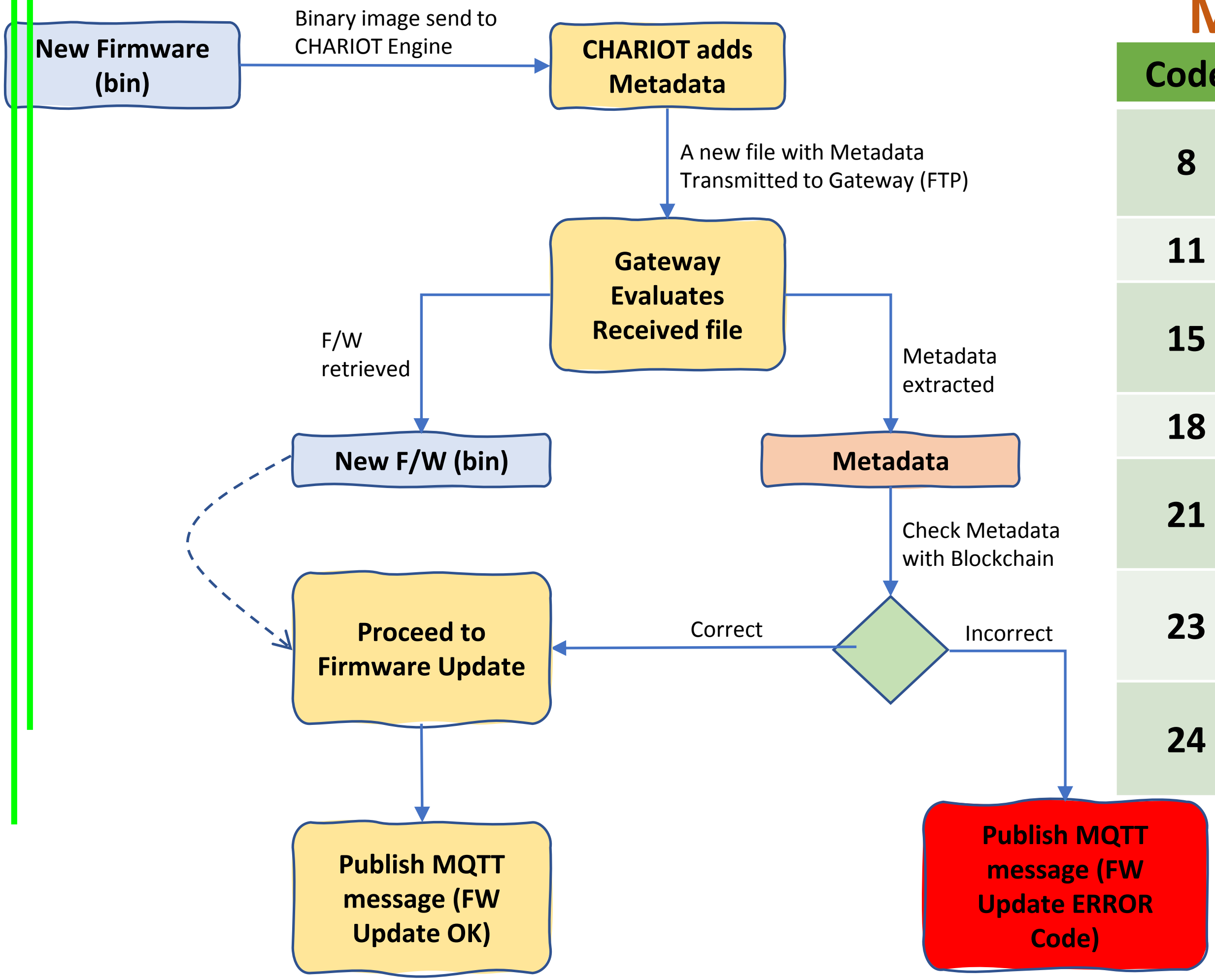


🟦 **MQTTS**: Sensor Data & System Events (Sensor Security issues, Firmware Update results)

🟧 **SFTP**: Firmware Download

🟨 **Binary Serial Protocol**: Real Time Communication with Blockchain

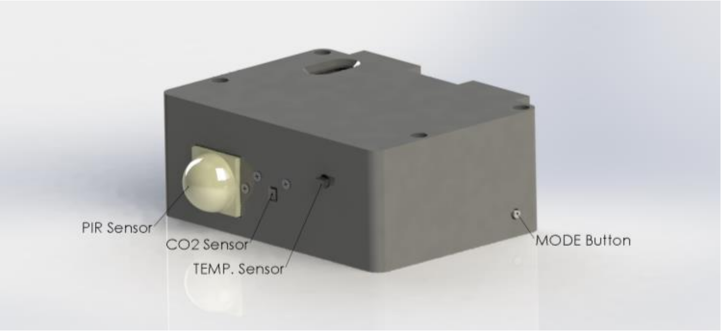
Firmware Update Algorithm @ Gateway

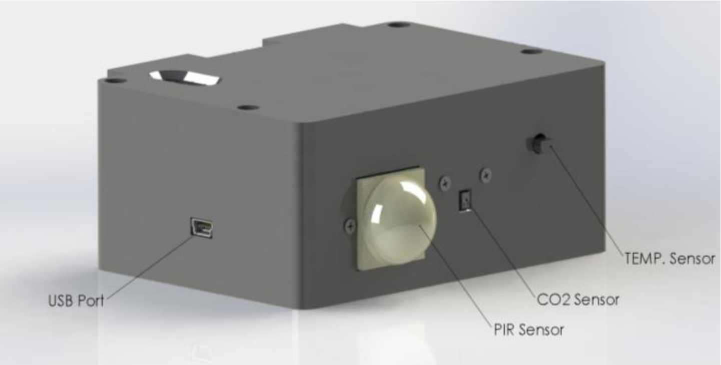

New Firmware (bin)
Binary image send to CHARIOT Engine
CHARIOT adds Metadata
A new file with Metadata Transmitted to Gateway (FTP)
Gateway Evaluates Received file
F/W retrieved
Metadata extracted
New F/W (bin)
Metadata
Check Metadata with Blockchain
Correct
Incorrect
Proceed to Firmware Update
Publish MQTT message (FW Update OK)
Publish MQTT message (FW Update ERROR Code)

FW UPDATE MQTT ERROR MESSAGES

Code	Description
8	Metadata does not start with valid string.
11	Metadata does not start with ‘:’
15	Metadata field has invalid header length.
18	Software_ID field is too long.
21	Metadata, field (hash or/and Software_ID) not found
23	Blockchain rejects firmware’s extracted Metadata
24	Blockchain did not respond within 15 seconds

CHARIOT IBM LL BLE Sensors





FEATURES

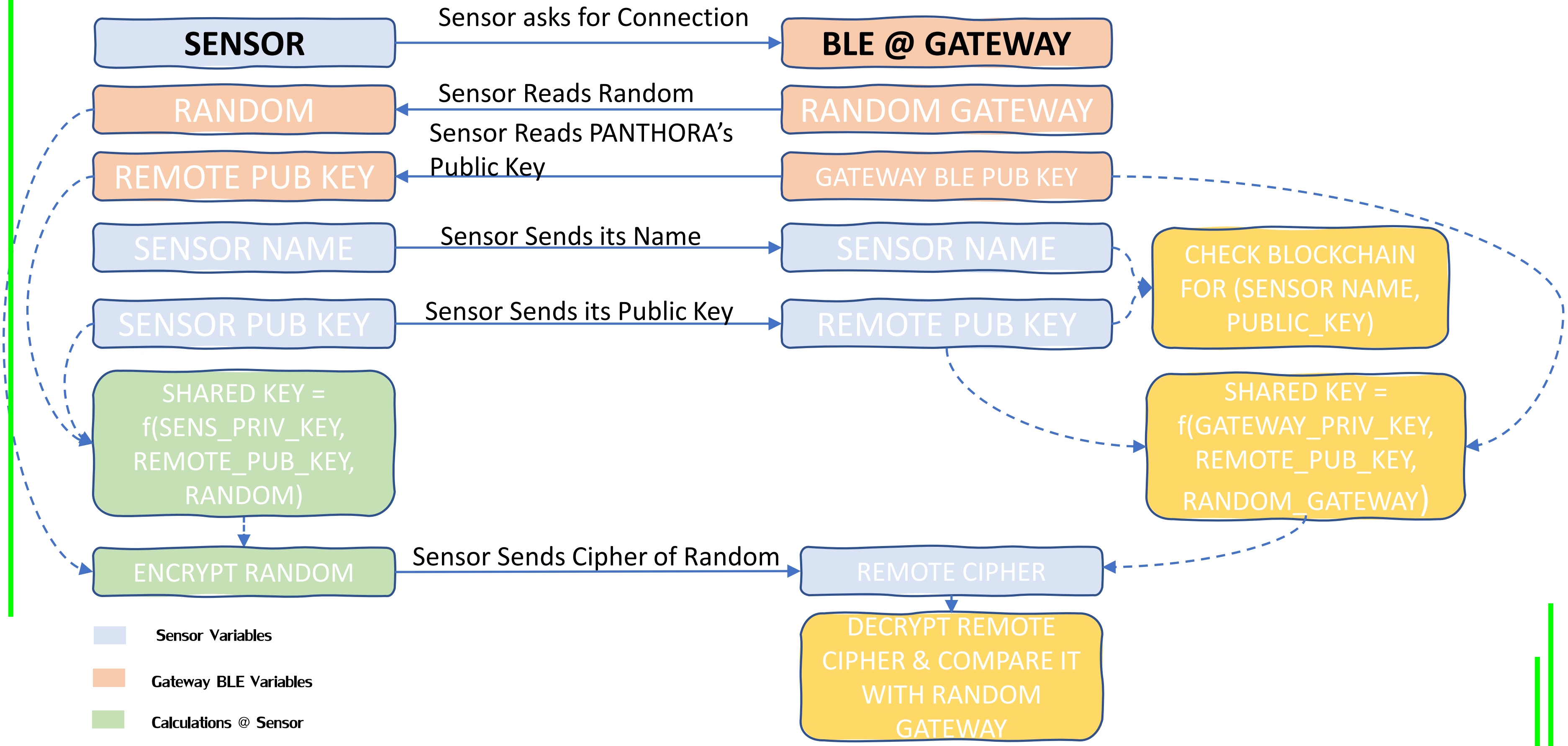
- BLE enabled
- Encryption / Authentication (Diffie-Hellman Elliptic Curve)
- BLE Provisioning ready

MEASUREMENTS

- Ambient Temperature
- Presence (Infrared / PIR)
- CO_2

3rd FITCE Technology Forum 2019

Authentication / Encryption Algorithm



SENSOR

BLE @ GATEWAY

Sensor asks for Connection

RANDOM

RANDOM GATEWAY

Sensor Reads Random

REMOTE PUB KEY

GATEWAY BLE PUB KEY

Sensor Reads PANTHORA’s Public Key

SENSOR NAME

SENSOR NAME

Sensor Sends its Name

CHECK BLOCKCHAIN FOR (SENSOR NAME, PUBLIC_KEY)

SENSOR PUB KEY

REMOTE PUB KEY

Sensor Sends its Public Key

SHARED KEY = f(SENS_PRIV_KEY, REMOTE_PUB_KEY, RANDOM)

SHARED KEY = f(GATEWAY_PRIV_KEY, REMOTE_PUB_KEY, RANDOM_GATEWAY)

ENCRYPT RANDOM

REMOTE CIPHER

Sensor Sends Cipher of Random

DECRYPT REMOTE CIPHER & COMPARE IT WITH RANDOM GATEWAY

🟦 Sensor Variables

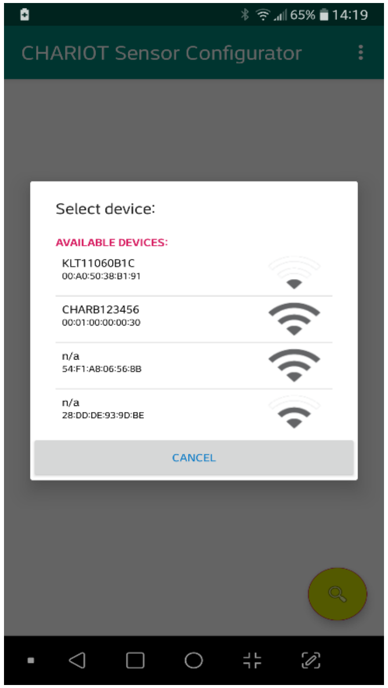
🟧 Gateway BLE Variables

🟩 Calculations @ Sensor

🟨 Calculations @ Gateway

28/12/2019

Android App for BLE sensor Configuration



Select device:

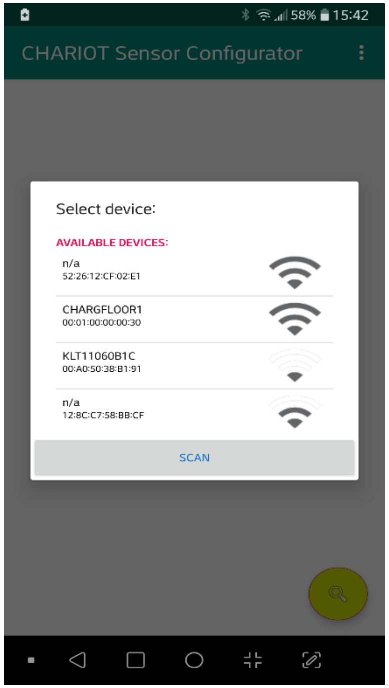
AVAILABLE DEVICES:

KLT11060B1C
00:A0:50:38:B1:91

CHARB123456
00:01:00:00:00:30

n/a
54:F1:A8:06:56:8B

n/a
28:DD:DE:93:9D:BE



Select device:

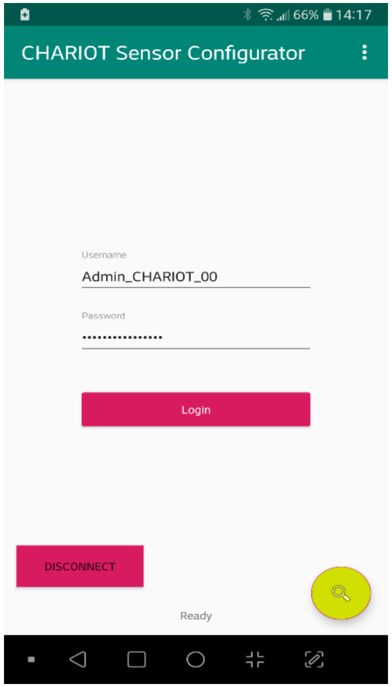
AVAILABLE DEVICES:

n/a
52:26:12:CF:02:E1

CHARGFLOOR1
00:01:00:00:00:30

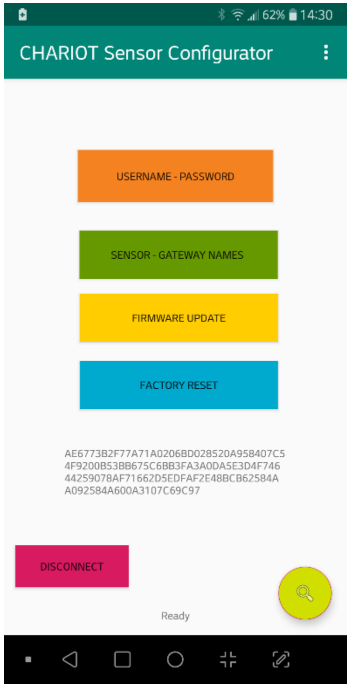
KLT11060B1C
00:A0:50:38:B1:91

n/a
12:8C:C7:58:BB:CF



Username
Admin_CHARIOT_00

Password
•••••••••••••••••



AE6773B2F77A71A0206BD028520A958407C5
4F9200B53BB675C6BB3FA3A0DA5E3D4F746
44259078AF71662D5EDFAF2E48BCB62584A
A092584A600A3107C69C97

- Configures Sensors & Gateway BLE module
- Encryption / Authentication (Diffie-Hellman Elliptic Curve)
- Key Pair generation on every factory reset
- Protected with Credentials

Thank you!