ARCADIAN-IoT

AUTONOMOUS TRUST, SECURITY AND PRIVACY MANAGEMENT FRAMEWORK FOR IOT

Sérgio Figueiredo (IPN)

“Identity, trust and privacy in an intelligent, smart IoT World: Challenges and Outcomes” Workshop

23/6/2022

CONTENT

ARCADIAN-IoT

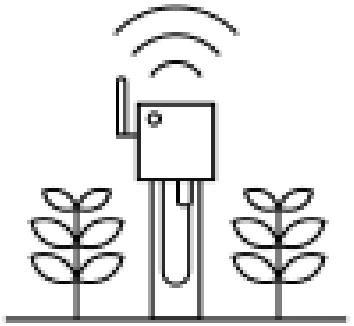
1. Background & Challenges
2. Project Overview
3. Project Status & Results
4. Conclusions

1 - BACKGROUND & CHALLENGES

BACKGROUND & MOTIVATION

ARCADIAN-IoT

- Significant IoT penetration and impact across most sectors
  - **IDC: Driving markets** include Consumer, Transportation, Manufacturing, Grid & Utilities, Retail, Healthcare



By 2025: - 27 billion active IoT connections
iot-analytics.com (State of IoT - Spring 2022 report)

BACKGROUND & MOTIVATION

ARCADIAN-IoT

- Increase in IoT threats, risks and high-profile incidents

BACKGROUND & MOTIVATION

ARCADIAN-IoT

- Increase in IoT threats, risks and high-profile incidents

CONTROL | NEWS | SECURITY

MARCH 30, 2020

Report: 57% of IoT Devices Vulnerable to Severe Attack

A recent uptick in cybersecurity attacks are linked directly to Internet-of-Things devices such as intercom systems and security cameras. Here's how to keep customers safe.

Amy Rock

BACKGROUND & MOTIVATION

ARCADIAN-IoT

- Increase in IoT threats, risks and high-profile incidents

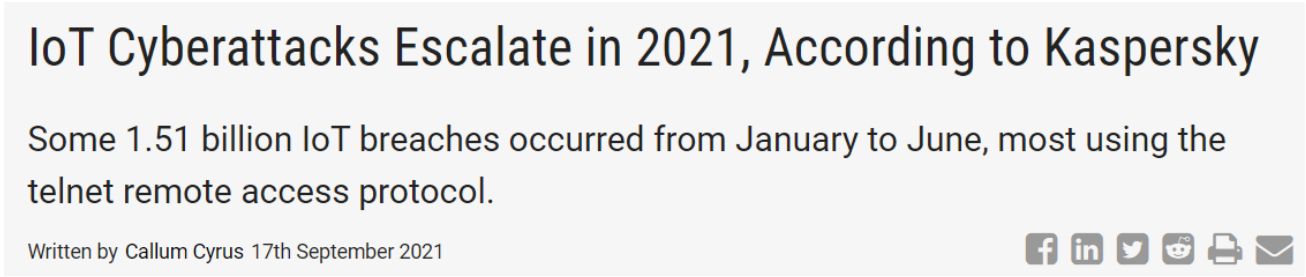
CONTROL | NEWS | SECURITY

MARCH 30, 2020

Report: 57% of IoT Devices Vulnerable to Severe Attack

A recent uptick in cybersecurity attacks are linked directly to Internet-of-Things devices such as intercom systems and security cameras. Here's how to keep customers safe.

Amy Rock



IoT Cyberattacks Escalate in 2021, According to Kaspersky

Some 1.51 billion IoT breaches occurred from January to June, most using the telnet remote access protocol.

Written by Callum Cyrus 17th September 2021

BACKGROUND & MOTIVATION

ARCADIAN-IoT

- Increase in IoT threats, risks and high-profile incidents

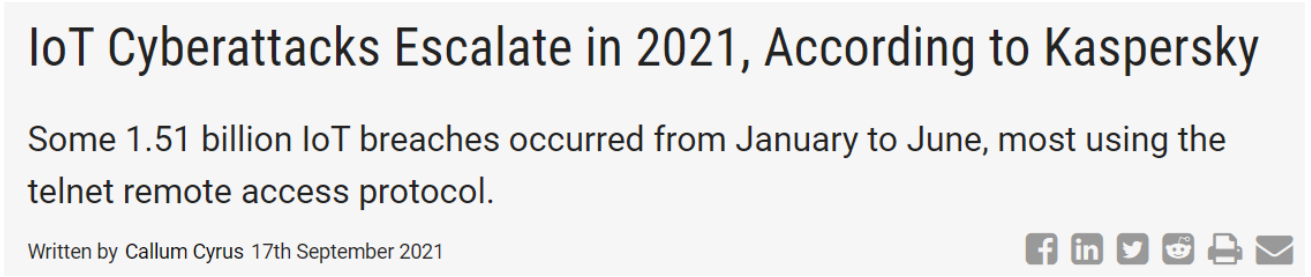
CONTROL | NEWS | SECURITY

MARCH 30, 2020

Report: 57% of IoT Devices Vulnerable to Severe Attack

A recent uptick in cybersecurity attacks are linked directly to Internet-of-Things devices such as intercom systems and security cameras. Here's how to keep customers safe.

Amy Rock



IoT Cyberattacks Escalate in 2021, According to Kaspersky

Some 1.51 billion IoT breaches occurred from January to June, most using the telnet remote access protocol.

Written by Callum Cyrus 17th September 2021

Report: More than 1B IoT attacks in 2021

VB Staff

April 25, 2022 2:20 PM

BACKGROUND & MOTIVATION

ARCADIAN-IoT

- Security and privacy represent a major barrier to wider IoT adoption

85% of 170 IoT industry leaders believe that security concerns remain a major barrier to IoT adoption
Omdia (2020)

KEY TECHNICAL CHALLENGES

- **Security and privacy** are managed in a fragmented way

KEY TECHNICAL CHALLENGES

- **Security and privacy** are managed in a fragmented way
- **Strong human factor** in security monitoring, forecasting and updates

KEY TECHNICAL CHALLENGES

- **Security and privacy** are managed in a fragmented way
- **Strong human factor in security** monitoring, forecasting and updates
- Dispersed **threat intelligence** communication and sharing

KEY TECHNICAL CHALLENGES

ARCADIAN-IoT

- **Security and privacy** are managed in a fragmented way
- **Strong human factor in security** monitoring, forecasting and updates
- Dispersed **threat intelligence** communication and sharing
- Broader **attack surface** and **risk of propagation** with advances in IoT, AI, 5G, …

KEY TECHNICAL CHALLENGES

ARCADIAN-IoT

- **Security and privacy** are managed in a fragmented way
- **Strong human factor in security** monitoring, forecasting and updates
- Dispersed **threat intelligence** communication and sharing
- Broader **attack surface** and **risk of propagation** with advances in **IoT, AI, 5G, …**
- **Dependency on trusted 3rd parties** to coordinate transactions across interconnected places

KEY TECHNICAL CHALLENGES

ARCADIAN-IoT

- **Security and privacy** are managed in a fragmented way
- **Strong human factor in security** monitoring, forecasting and updates
- Dispersed **threat intelligence** communication and sharing
- Broader **attack surface** and **risk of propagation** with advances in **IoT, AI, 5G, …**
- **Dependency on trusted 3rd parties** to coordinate transactions across interconnected places
- Mostly **centralized and static trust management and recovery** approaches

KEY TECHNICAL CHALLENGES

ARCADIAN-IoT

- **Security and privacy** are managed in a fragmented way
- **Strong human factor in security** monitoring, forecasting and updates
- Dispersed **threat intelligence** communication and sharing
- Broader **attack surface** and **risk of propagation** with advances in **IoT, AI, 5G, …**
- **Dependency on trusted 3rd parties** to coordinate transactions across interconnected places
- Mostly **centralized and static trust management and recovery** approaches
- Lack of trustworthy methods for **persons and/or objects identity management**

2 – PROJECT OVERVIEW

KEY DETAILS

ARCADIAN-IoT

CONSORTIUM

IPN INSTITUTO PEDRO NUNES

RI.SE Research Institutes of Sweden

load

BOX2M industry 4.0

IRGB medical devices

MARTEL innovate

Atos

e-lex STUDIO LEGALE

Use case leaders

Clínica Universidad de Navarra

UNIVERSITY OF THE WEST of SCOTLAND UWS

TRUPHONE

XLAB

DURATION

May 2021 – April 2024

OBJECTIVES & APPROACH

ARCADIAN-IoT

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

OBJECTIVES & APPROACH

ARCADIAN-IoT

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

1 • Decentralized framework for IoT systems

- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes

OBJECTIVES

APPROACH

OBJECTIVES & APPROACH

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

	OBJECTIVES	APPROACH
1	• Decentralized framework for IoT systems	- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes
2	• Secure and trustworthy management of objects' identification	- Root of Trust HW, Chained identification (DIDs + VCs)

OBJECTIVES & APPROACH

ARCADIAN-IoT

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

OBJECTIVES	APPROACH
1 • Decentralized framework for IoT systems	- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes
2 • Secure and trustworthy management of objects' identification	- Root of Trust HW, Chained identification (DIDs + VCs)
3 • Distributed security and trust in persons' identification management	- SSI approach; Novel Multifactor authentication methods

OBJECTIVES & APPROACH

ARCADIAN-IoT

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

	OBJECTIVES	APPROACH
1	• Decentralized framework for IoT systems	- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes
2	• Secure and trustworthy management of objects' identification	- Root of Trust HW, Chained identification (DIDs + VCs)
3	• Distributed security and trust in persons' identification management	- SSI approach; Novel Multifactor authentication methods
4	• Distributed and autonomous models for trust, security and privacy, enabling a Chain of Trust	- Trust/reputation system supported by Blockchain; Federated AI for anomaly detection & CTI, Remote Attestation w/ HW-based RoT

OBJECTIVES & APPROACH

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

	OBJECTIVES	APPROACH
1	• Decentralized framework for IoT systems	- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes
2	• Secure and trustworthy management of objects' identification	- Root of Trust HW, Chained identification (DIDs + VCs)
3	• Distributed security and trust in persons' identification management	- SSI approach; Novel Multifactor authentication methods
4	• Distributed and autonomous models for trust, security and privacy, enabling a Chain of Trust	- Trust/reputation system supported by Blockchain; Federated AI for anomaly detection & CTI
5	• Hardened encryption with recovery ability	- Combine Functional Encryption with Root of Trust HW

OBJECTIVES & APPROACH

ARCADIAN-IoT

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

	OBJECTIVES	APPROACH
1	• Decentralized framework for IoT systems	- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes
2	• Secure and trustworthy management of objects' identification	- Root of Trust HW, Chained identification (DIDs + VCs)
3	• Distributed security and trust in persons' identification management	- SSI approach; Novel Multifactor authentication methods
4	• Distributed and autonomous models for trust, security and privacy, enabling a Chain of Trust	- Trust/reputation system supported by Blockchain; Federated AI for anomaly detection & CTI
5	• Hardened encryption with recovery ability	- Combine Functional Encryption with Root of Trust HW
6	• Self and coordinated healing with reduced human intervention	- IoT network anomaly detection and mitigation for known and unknown threats

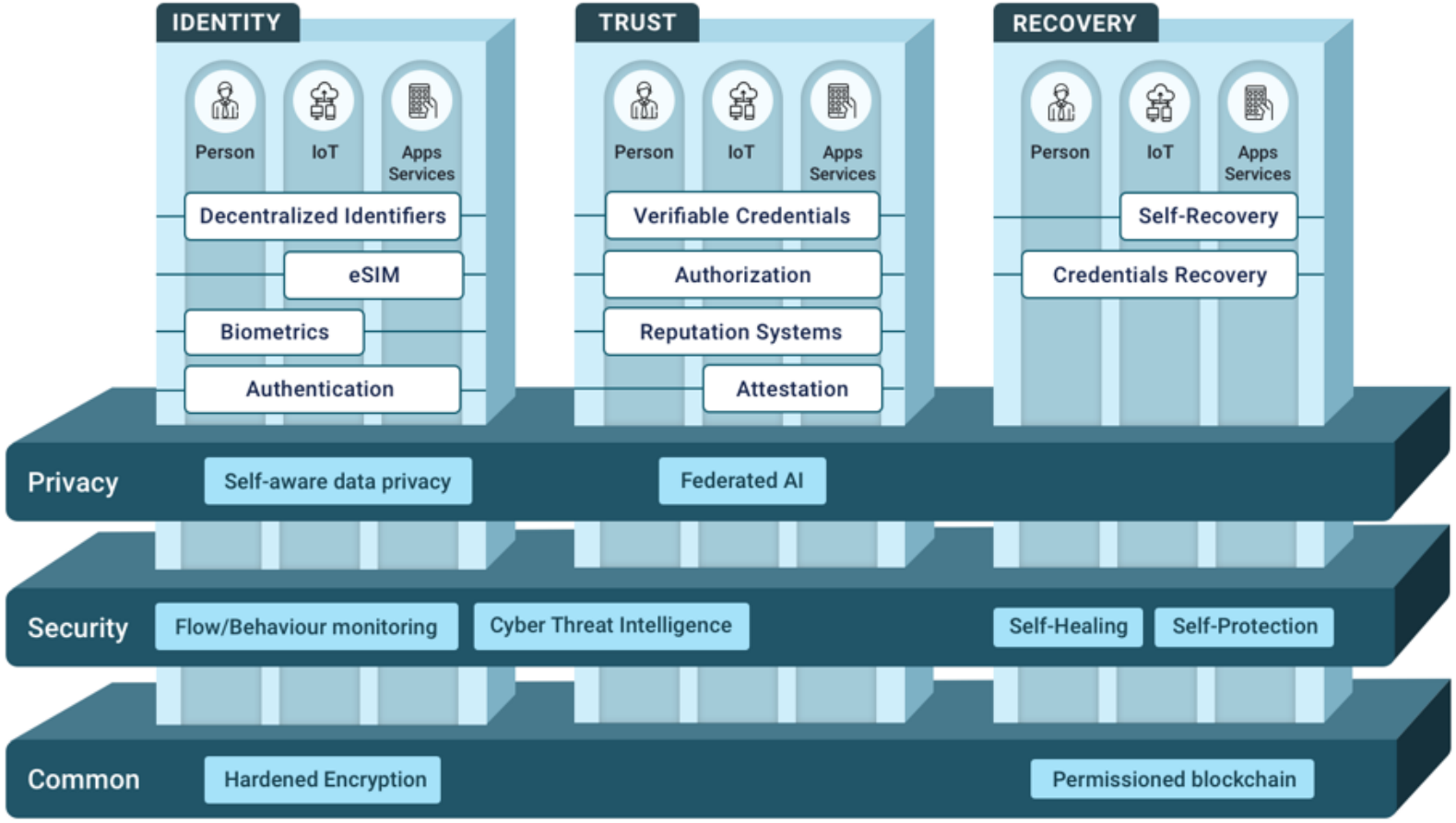
OBJECTIVES & APPROACH

ARCADIAN-IoT

- The overall goal of ARCADIAN-IoT is to develop and make available an innovative and solid framework for **trust, security and privacy management for IoT systems**, accelerating the development of **IoT systems towards decentralized, transparent and user controllable privacy**.

OBJECTIVES	APPROACH
1 • Decentralized framework for IoT systems	- 3 vertical (Identity, Trust, Recovery) + 3 horizontal (Security, Privacy, common) planes
2 • Secure and trustworthy management of objects' identification	- Root of Trust HW, Chained identification (DIDs + VCs)
3 • Distributed security and trust in persons' identification management	- SSI approach; Novel Multifactor authentication methods
4 • Distributed and autonomous models for trust, security and privacy, enabling a Chain of Trust	- Trust/reputation system supported by Blockchain; Federated AI for anomaly detection & CTI
5 • Hardened encryption with recovery ability	- Combine Functional Encryption with Root of Trust HW
6 • Self and coordinated healing with reduced human intervention	- IoT network anomaly detection and mitigation for known and unknown threats
7 • Proactive information sharing for trustable Cyber Threat Intelligence and IoT Security Observatory	- IoT-specific Cyber Threat Intelligence → MISP4IoT

HIGH LEVEL ARCHITECTURE



Domains

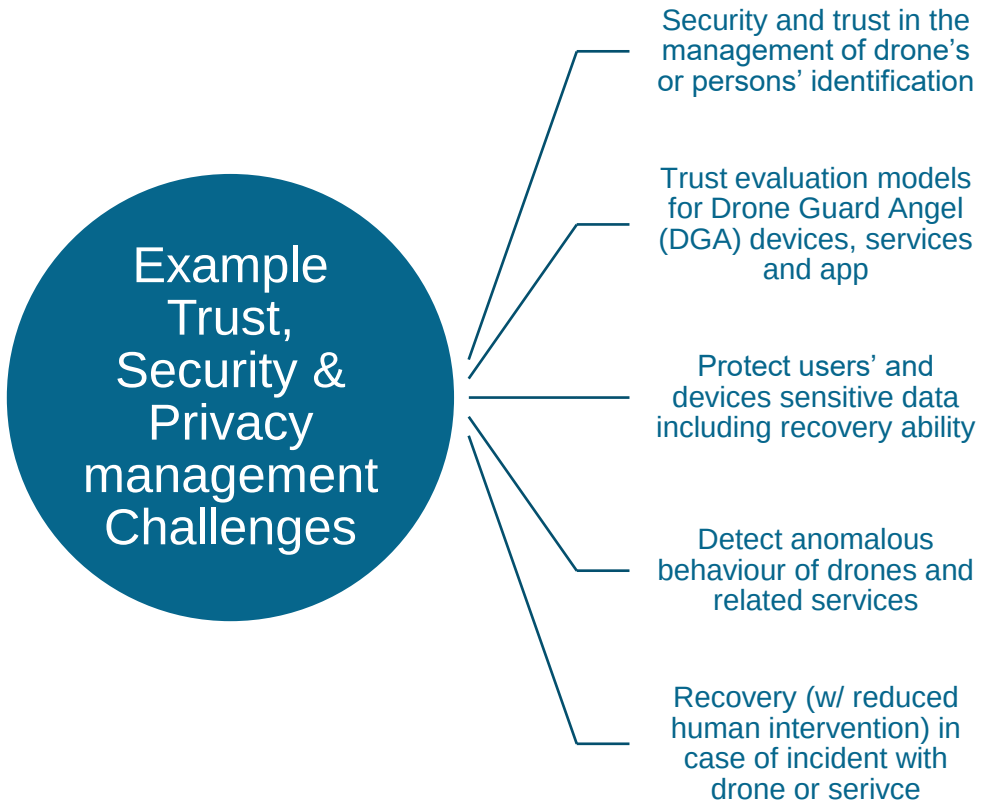
#Domain A	#Domain B	#Domain C
Emergency and Vigilance	Grid Infrastructure Monitoring	Medical IoT

3 – PROJECT STATUS & RESULTS

DOMAIN A – EMERGENCY AND VIGILANCE USING DRONES AND IOT

ARCADIAN-IoT

- Drone Guard Angel (DGA) service intends to provide a citizen-centric urban vigilance service easily accessible via a smartphone.

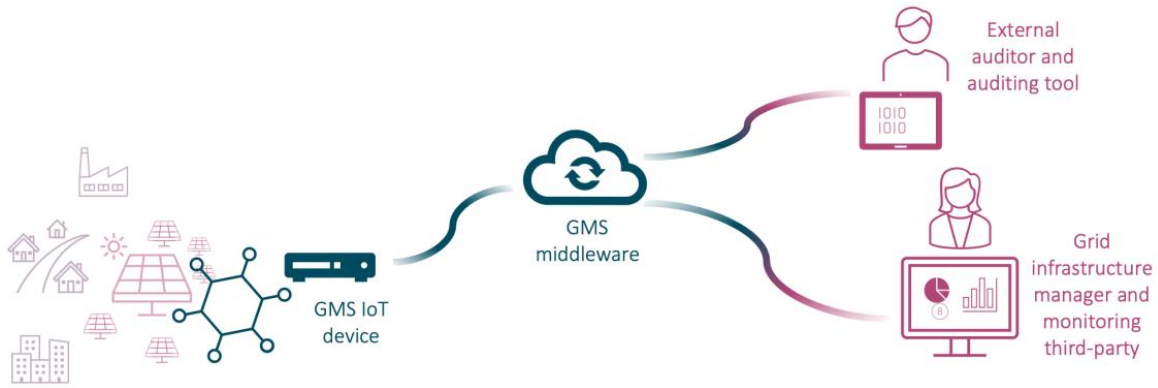


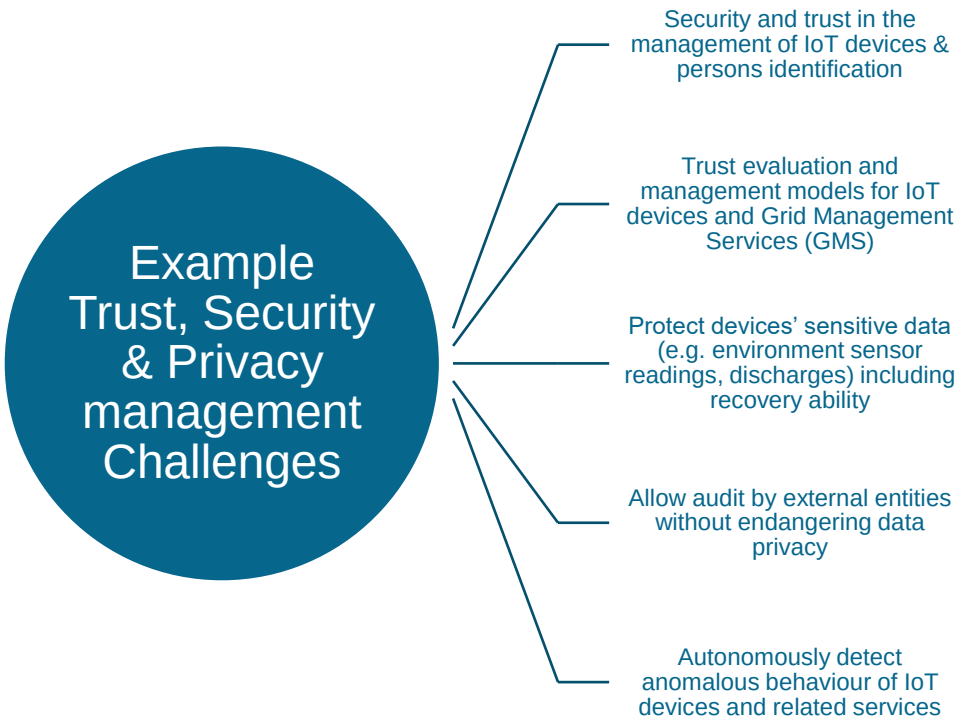
ARCADIAN-IoT, "D2.1: Use case specification", December 2021

DOMAIN B – SECURED EARLY MONITORING OF SMART GRID INFRASTRUCTURES

ARCADIAN-IoT

- Grid Management Service (GMS) is a solution for monitoring grid infrastructures, i.e. collecting and aggregating sensor data via a IoT GW.
  - **(more details on the demo later on)**

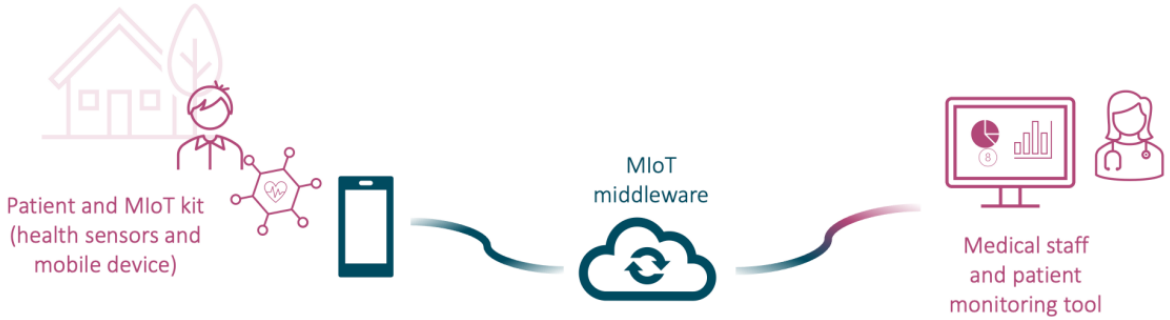




ARCADIAN-IoT, "D2.1: Use case specification", December 2021

DOMAIN C – MEDICAL IOT

- Medical IoT service to improve the conditions of monitoring and follow-up of cancer patients at home, in the active treatment process where patients complement the sensorial data with their perceived well-being



Example Trust, Security & Privacy management Challenges

- Security and trust in the management of devices & patients or medical staff identification
- Detect anomalous behaviour of IoT devices and related services
- Self-recovery of data and system functionalities with reduced human intervention
- Automated and privacy preserving CTI approach for IoT threat information management

ARCADIAN-IoT, "D2.1: Use case specification", December 2021

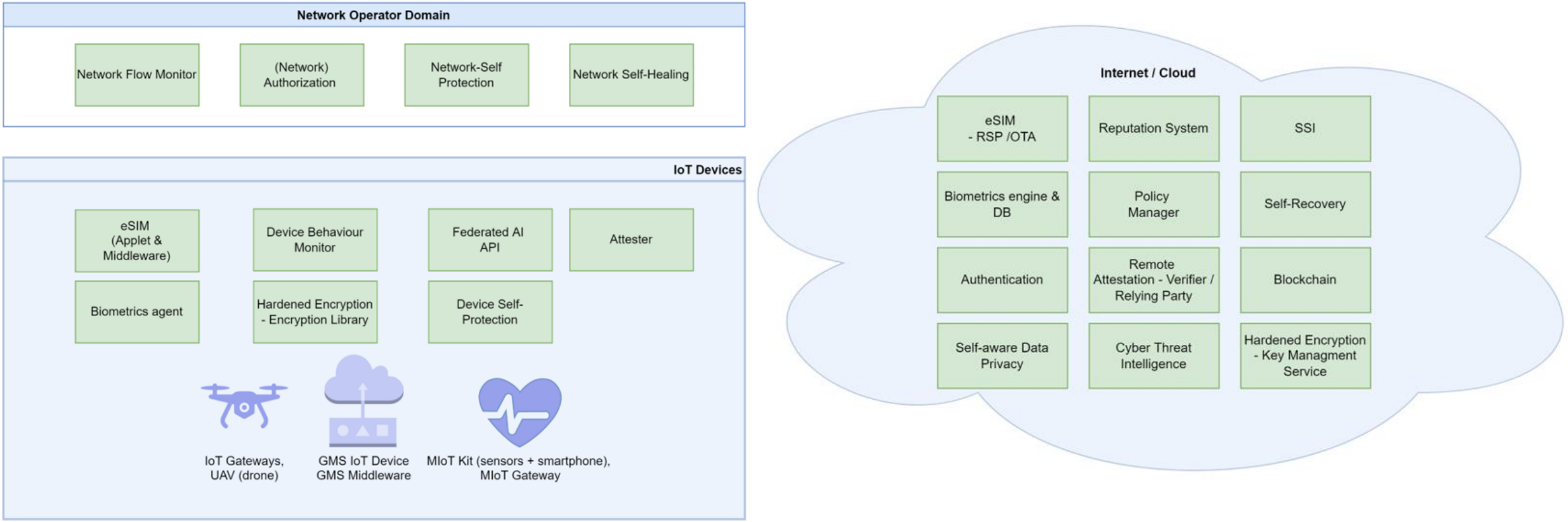
ARCADIAN-IOT REQUIREMENTS

- **52** technical requirements relating to the framework's 20 components and spread across the 6 planes
- **8** regulatory / legal requirements linking to:
  - Blockchain, Biometrics, Anonymisation / pseudoanonymisation, Drones
- **77** KPIs defined and quantified
  - Under revision / improvement for planning evaluation & validation stage

ARCADIAN-IoT, "D2.3: ARCADIAN-IoT requirements", April 2022

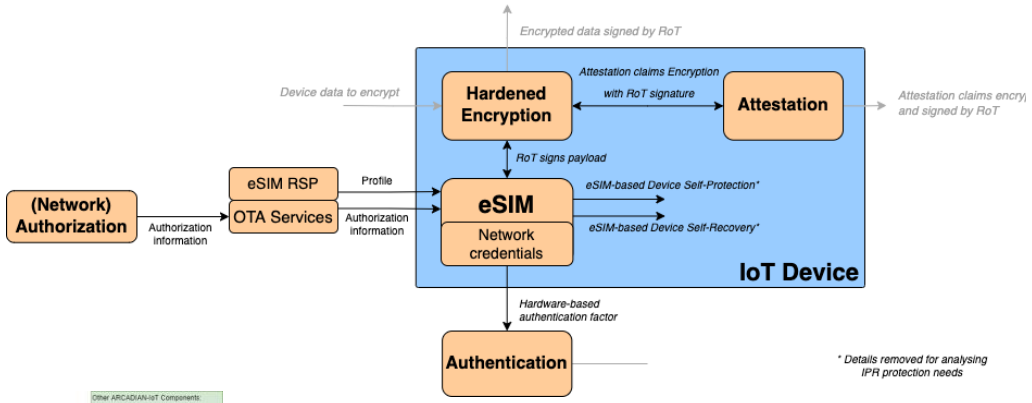
ARCADIAN-IOT ARCHITECTURE

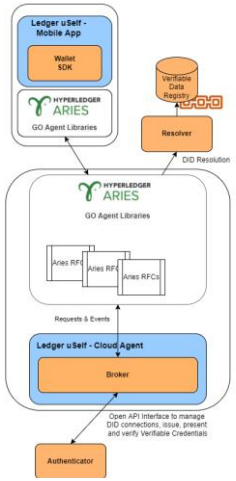
- Simplified deployment view

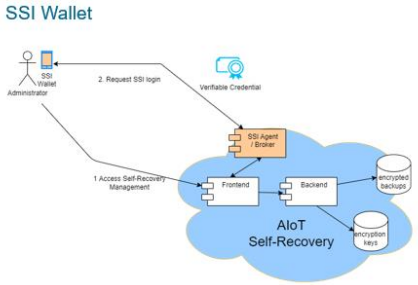


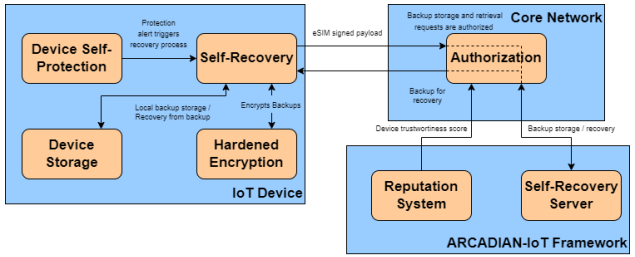
ARCADIAN-IoT, "D2.5: ARCADIAN-IoT architecture", April 2022

SOME OUTCOMES FROM SPECIFICATION WORK

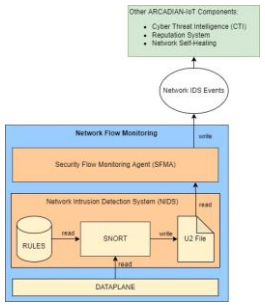


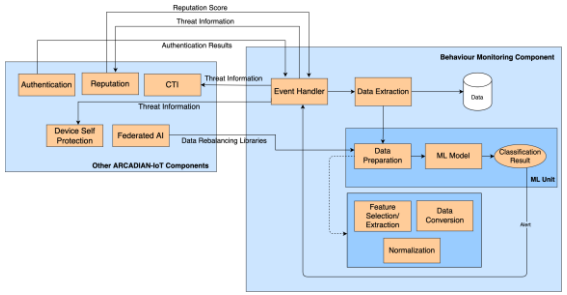


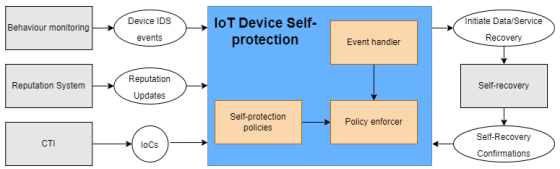


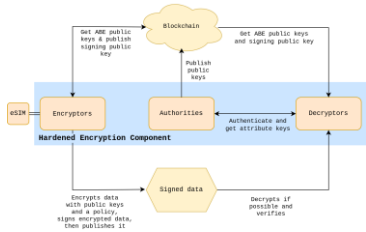


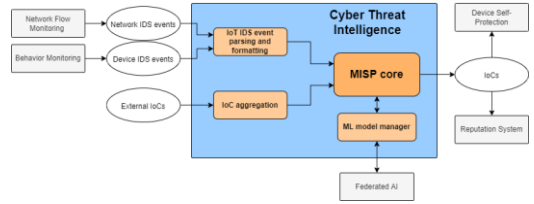
* Details removed for analysing IPR protection needs

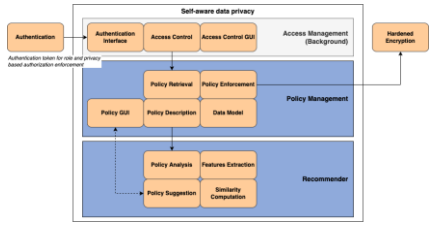


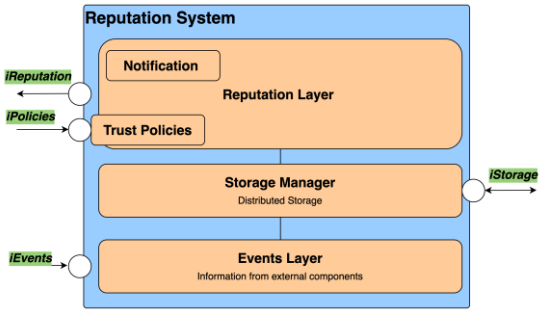


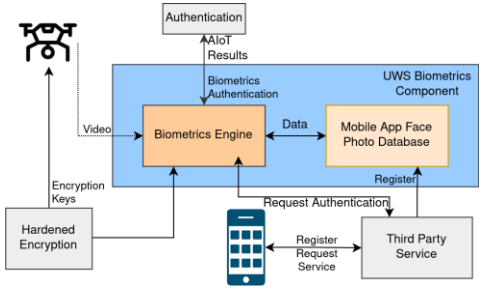


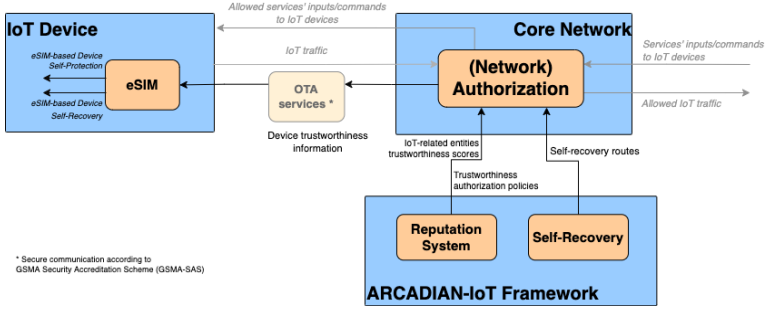


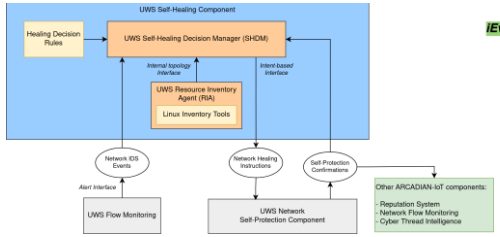












ARCADIAN-IoT, "D2.5: ARCADIAN-IoT architecture", April 2022

PROJECT STATUS

Task	Y1												Y2												Y3											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
WP1 Project Management																																				MS6
WP2 Use Cases Definition, Requirements and Architecture								MS1				MS2																								
WP3 Horizontal Planes of ARCADIAN-IoT Framework																																				
WP4 Verticals Planes of ARCADIAN-IoT Framework																																				
WP5 Use Case Implementation, Integration and Validation																		MS3												MS4						MS5
WP6 Dissemination, Communication and Exploitation																																				
WP7 Ethics requirements																																				

- **MS1** – Baseline with legal, functional analysis of **use cases**
- **MS2** – Design of the ARCADIAN-IoT framework **architecture**
- **MS3** – First **Prototype**
- **MS4** – Final **Prototype**
- **MS5** – Security and privacy awareness **training**

4 – CONCLUSIONS

CONCLUSIONS & WRAP-UP

- ARCADIAN-IoT intends to ultimately lead to:
  - Reduced **number and impact of cybersecurity** incidents → E.g. Monitoring, protection & self-healing of IoT infrastructure, Federated AI for IoT device incident detection and CTI

CONCLUSIONS & WRAP-UP

- ARCADIAN-IoT intends to ultimately lead to:
  - Reduced **number and impact of cybersecurity** incidents → E.g. Monitoring, protection & self-healing of IoT infrastructure, Federated AI for IoT device incident detection and CTI
  - Timely and effective cooperation and information sharing as well as **novel tools for** CERTS & CSIRTS → E.g. IoT-specific CTI for information sharing through MISP4IoT

CONCLUSIONS & WRAP-UP

ARCADIAN-IoT

- ARCADIAN-IoT intends to ultimately lead to:
  - Reduced **number and impact of cybersecurity** incidents → E.g. Monitoring, protection & self-healing of IoT infrastructure, Federated AI for IoT device incident detection and CTI
  - Timely and effective cooperation and information sharing as well as **novel tools for** CERTS & CSIRTS → E.g. IoT-specific CTI for information sharing through MISP4IoT
  - Widespread adoption of **distributed, enhanced trust management schemes** → E.g. Trust management supported by distributed immutable storage with Permissioned Blockchain

CONCLUSIONS & WRAP-UP

ARCADIAN-IoT

- ARCADIAN-IoT intends to ultimately lead to:
  - Reduced **number and impact of cybersecurity** incidents → E.g. Monitoring, protection & self-healing of IoT infrastructure, Federated AI for IoT device incident detection and CTI
  - Timely and effective cooperation and information sharing as well as **novel tools for** CERTS & CSIRTS → E.g. IoT-specific CTI for information sharing through MISP4IoT
  - Widespread adoption of **distributed, enhanced trust management schemes** → E.g. Trust management supported by distributed immutable storage with Permissioned Blockchain
  - **User-friendly and trustworthy** on-line products, services and business → E.g. Validation of the 3 SME-led domains, Trust modeling of services reputation, standards contributions (GSMA, IETF)

CONCLUSIONS & WRAP-UP

ARCADIAN-IoT

- ARCADIAN-IoT intends to ultimately lead to:
  - Reduced **number and impact of cybersecurity** incidents → E.g. Monitoring, protection & self-healing of IoT infrastructure, Federated AI for IoT device incident detection and CTI
  - Timely and effective cooperation and information sharing as well as **novel tools for** CERTS & CSIRTS → E.g. IoT-specific CTI for information sharing through MISP4IoT
  - Widespread adoption of **distributed, enhanced trust management schemes** → E.g. Trust management supported by distributed immutable storage with Permissioned Blockchain
  - **User-friendly and trustworthy** on-line products, services and business → E.g. Validation of the 3 SME-led domains, Trust modeling of services reputation, standards contributions (GSMA, IETF)
  - A stronger, more innovative and more competitive **EU cybersecurity industry** → E.g. Distributed trust/reputation information enabled via Blockchain, IoT-specific CTI, contribution to standards (e.g. GSMA, IETF)

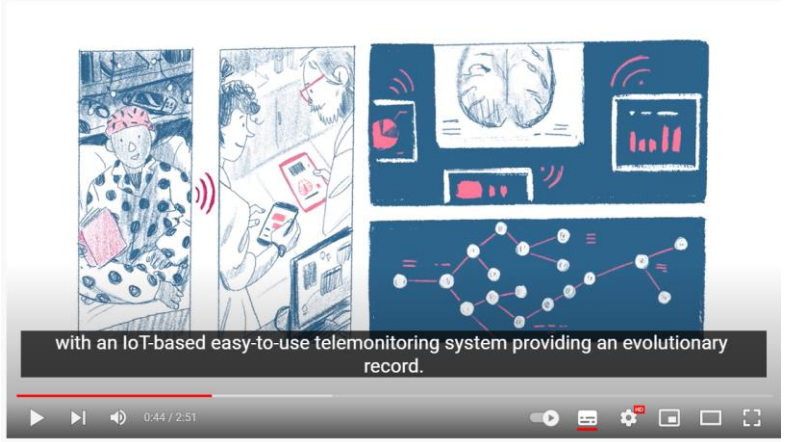
JOIN US

arcadian-iot.eu

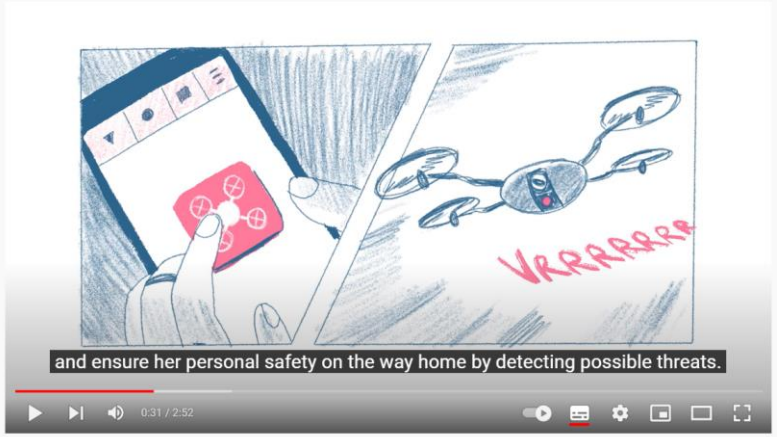
@ARCADIANIoT

@ARCADIAN-IoT

SEE OUR VIDEOS ON YOUTUBE



ARCADIAN IoT - Medical IoT



ARCADIAN IoT - Emergency and vigilance using drones and IoT

ARCADIAN-IoT

THANK YOU FOR YOUR ATTENTION

arcadian-iot.eu

ARCADIAN-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020259

THIS PROJECT IS PART OF THE NEXT GENERATION IoT

www.ngiot.eu