DINUY

Brighten up your day

CRA Workshop
Case study: BLE Time switches

Cybersecurity Requirements for Products with Digital Elements: “Default class”

23th September 2025

CRA Workshop – Time switches

Outline

1. **Product context: what a time switch is, intended environment**
2. **Understand the product configuration process**
3. **Time switch, mobile app, and cloud architectural diagram**
4. **Third-party elements**
5. **Risk assessment and adaptation of the development process to the CRA**
6. **Risk assessment matrix and elements**
7. **For time switch, mobile app, and cloud:**

   a) Risk assessment: assets, threats, vulnerabilities, mitigation measures

   b) Link these elements with the CRA essential cybersecurity requirements in Annex I

   c) Relationship between decisions made according to the risk assessment and the essential requirements

   d) Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed (according to CRA)
8. **Annex II: Information and instructions for the user**
9. **Conclusions and highlights from the manufacturer's perspective**
10. **Q&A**
11. **Workshop scenarios**

Meet DINUY

About DINUY

DINUY S.A., founded in 1947, is a **family business** dedicated to the manufacture of electrical and **electronic** equipment located in Irún, with **50 employees** and **4,000 m2** of production facilities (SME).

With **its own R&D&I team** and the commitment to new technologies, the company has explored multiple technologies to offer cutting-edge products, **including light regulators, constant light control systems, motion and presence detectors, time switches, timers, twilight switches, remote control systems, and building automation devices based on the KNX standard** and **DALI**. We develop smart devices to offer maximum **energy efficiency** in building automation systems.

Our **objective and motivation** for participating in this project is to analyze how **CRA will affect our products with digital elements.**

About Eva Susperregui

I am a **Telecommunications Engineer** with **25 years of experience in research and development**. Throughout my career, I have been involved in **the design and development of both hardware and software products**, focusing on delivering reliable and innovative solutions for electronic sectors.

Currently, I am part of the **R&D team at DINUY**, where I contribute to the development of advanced technologies aligned with market and regulatory needs, ensuring our products remain at the forefront of the industry.

CRA Workshop – Time switches

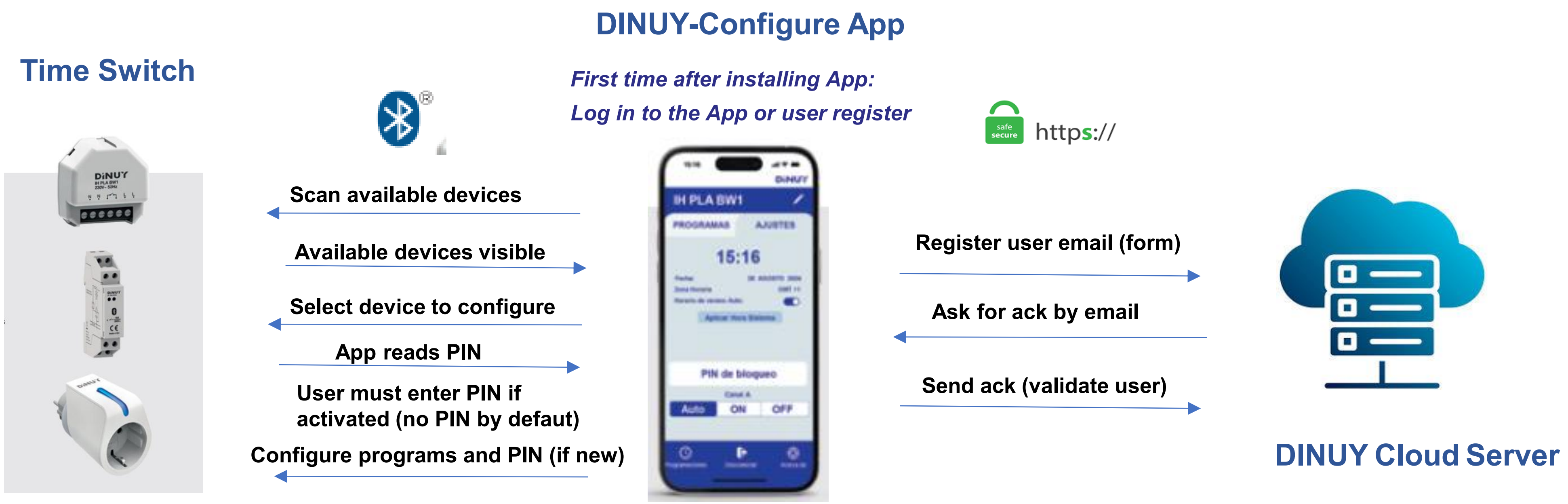
Product context: intended enviroment

A **time switch** is a device that **switches** a relay according to a **schedule**. It can be used in all types of venues and facilities, both outdoor and indoor, where **comfort and energy savings are required through automatic time-based activation** with weekly, annual, or astronomical repetition:

Use Case	Time switch use to	What happens if relay does not switch (cyberattack scenario)
Sports field lighting	Ensure **lighting only during sports activities** and save energy during the day.	Lights stay on all day, high energy costs do not turn on at night, making the field unusable.
Swimming pools	Operate **pumps and heaters** only during required hours for energy efficiency and water quality.	Pumps/heating may run continuously (high energy use) not run at all (stagnant water, hygiene issues).
	Turn lights on at dusk and off at dawn automatically for safety and efficiency.	Lights stay on all day, high energy costs do not turn on at night, making the swimming pool unusable or unsafe
Greenhouses and farms	Control artificial **lighting and heating schedules** for optimal crop growth and animal comfort.	Lights or heating stay always on or off, affecting crop growth or animal welfare.
School sirens	Automatically signal **school schedule** (entry, breaks, exit) without manual operation.	Sirens do not sound for schedule signaling, causing organizational chaos in the school.
Shop window lighting	**Illuminate shop windows** only at night to attract customers while saving energy during the day.	Lights stay on during the day (wasted energy) do not turn on at night (affects store visibility and sales).
Climate control in offices	Operate **HVAC systems only during working hours** to maintain comfort while reducing energy waste.	HVAC may overheat or overcool the office, causing discomfort and unnecessary energy consumption. It may cause issues in processes where temperature is important.
Outdoor lighting	**Turn lights on at dusk and off at dawn** automatically for safety and efficiency.	Lights do not turn on at dusk, leaving areas dark and unsafe stay on during the day wasting energy.
Ornamental lighting	Control decorative lights **during specific hours or seasons**, reducing energy costs.	Ornamental lights stay on unnecessarily (wasted energy) do not turn on, losing aesthetic/tourism value.
Time-based operation (irrigation pumps, etc.)	**Automate irrigation or other processes**, ensuring proper timing while avoiding manual activation.	Pumps may not activate (no irrigation for crops) may not stop (wasting water, potential flooding).
Charging EV at scheduled times	**Automate EV charging during off-peak hours** to save energy costs and ensure vehicles are ready when needed.	Charging does not start, causing fleet unavailability does not stop, leading to energy waste and potential overloading.

CRA Workshop – Time switches

Product configuration process



DINUY-Configure App

First time after installing App:

Log in to the App or user register

Time Switch

Scan available devices

Available devices visible

Select device to configure

App reads PIN

User must enter PIN if activated (no PIN by defaut)

Configure programs and PIN (if new)

https://

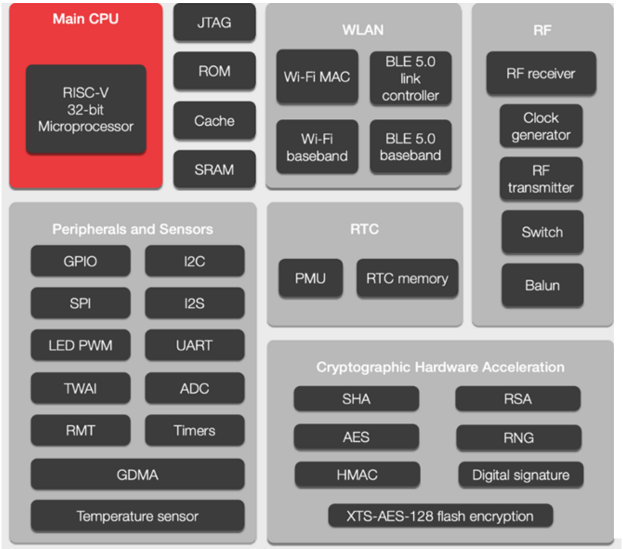
Register user email (form)

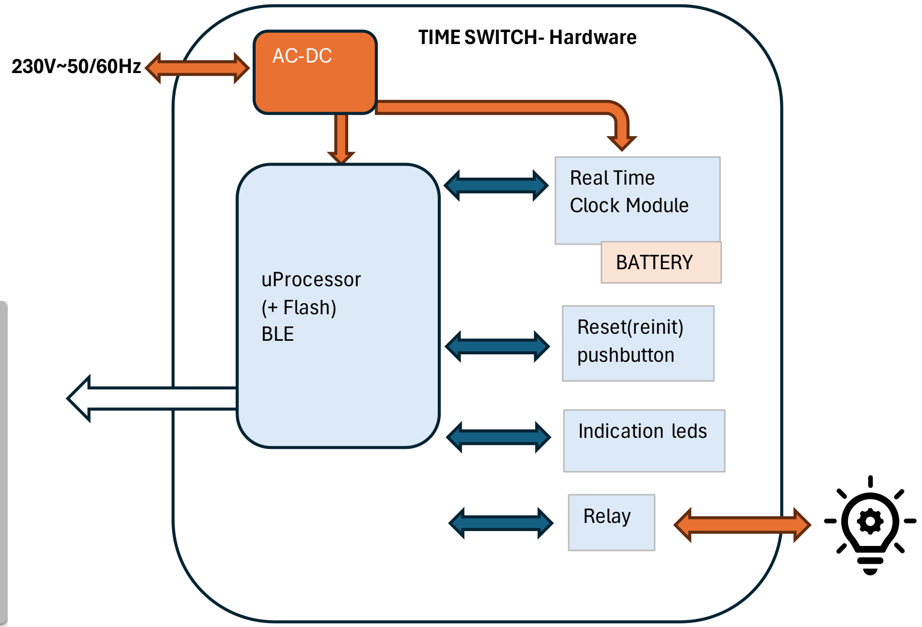
Ask for ack by email

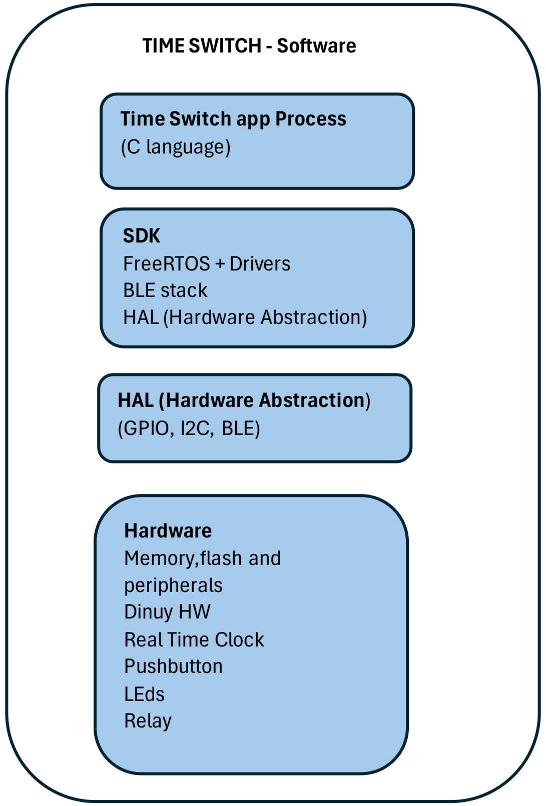
Send ack (validate user)

DINUY Cloud Server

Time Switch Architectural Diagram

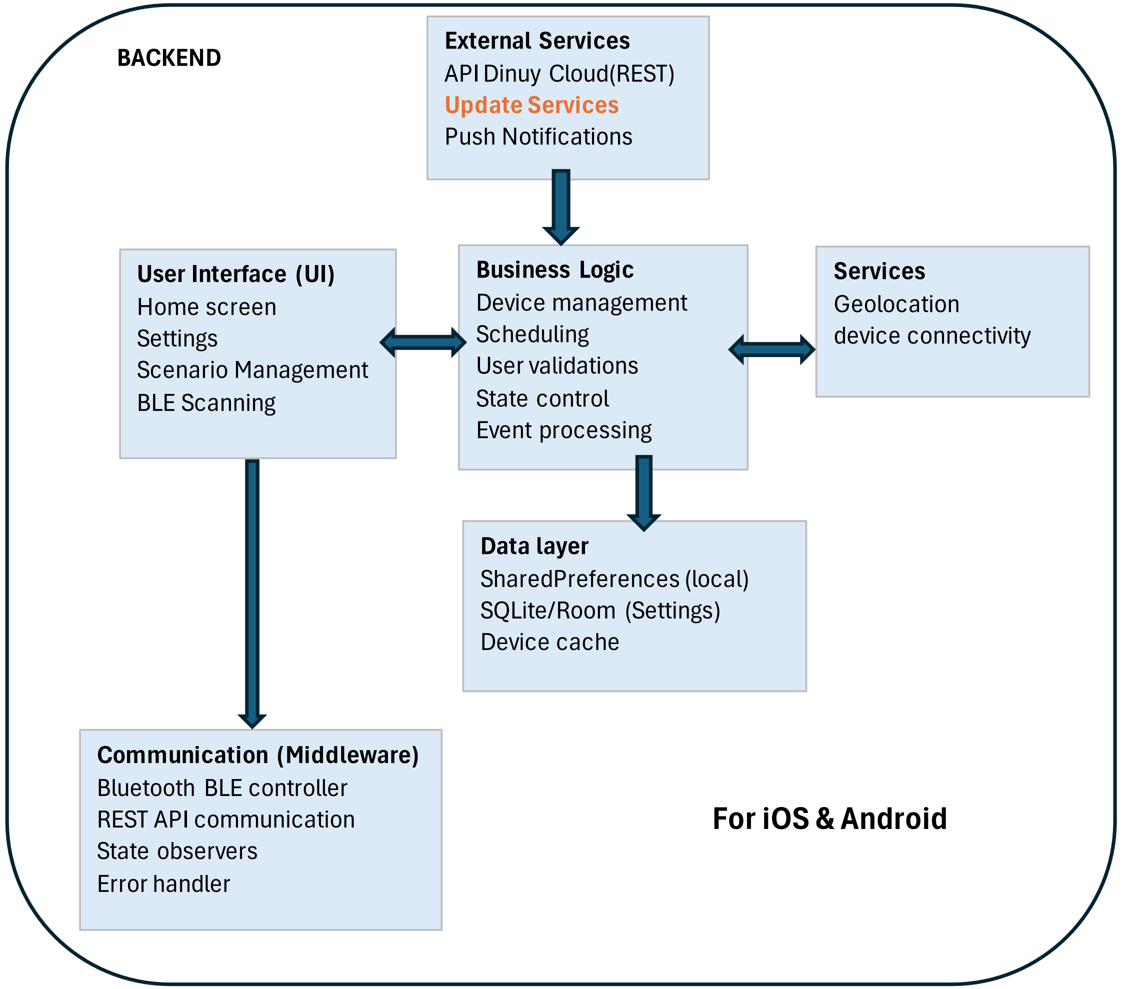






CRA Workshop – Time switches

Mobile App Diagram (Third party)



BACKEND

External Services
API Dinuy Cloud(REST)
Update Services
Push Notifications

User Interface (UI)
Home screen
Settings
Scenario Management
BLE Scanning

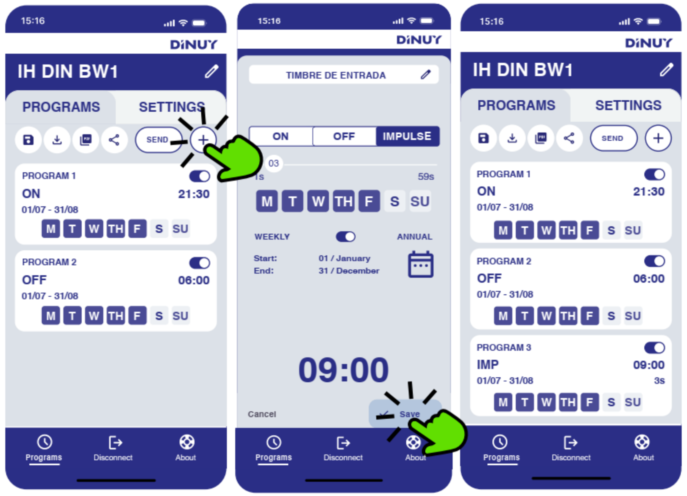
Business Logic
Device management
Scheduling
User validations
State control
Event processing

Services
Geolocation
device connectivity

Data layer
SharedPreferences (local)
SQLite/Room (Settings)
Device cache

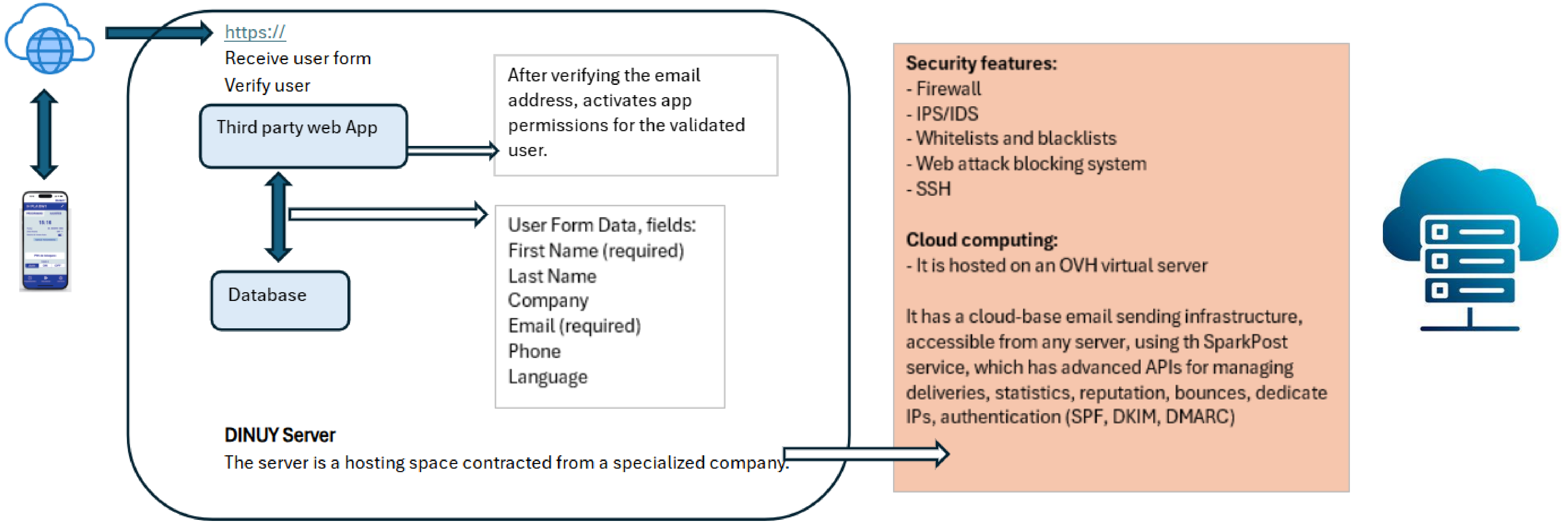
Communication (Middleware)
Bluetooth BLE controller
REST API communication
State observers
Error handler

For iOS & Android



CRA Workshop – Time switches

Cloud Server Diagram (Third party)



https://

Receive user form

Verify user

Third party web App

After verifying the email address, activates app permissions for the validated user.

Database

User Form Data, fields:
First Name (required)
Last Name
Company
Email (required)
Phone
Language

DINUY Server

The server is a hosting space contracted from a specialized company.

Security features:
- Firewall
- IPS/IDS
- Whitelists and blacklists
- Web attack blocking system
- SSH

Cloud computing:
- It is hosted on an OVH virtual server

It has a cloud-base email sending infrastructure, accessible from any server, using th SparkPost service, which has advanced APIs for managing deliveries, statistics, reputation, bounces, dedicate IPs, authentication (SPF, DKIM, DMARC)

IPS: Intrusion Prevention System
IDS: Intrusion Detection System

Subcontracting: components sourced from third parties

If components are subcontracted to a **third party**, as **manufacturer** you **have the final responsibility** of the components that are accompanying your product. We must ensure that the components of our supply chain incorporated into our designs are compliant with the CRA:

Article13 - 5. manufacturers shall exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements, including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.

Our third party elements:

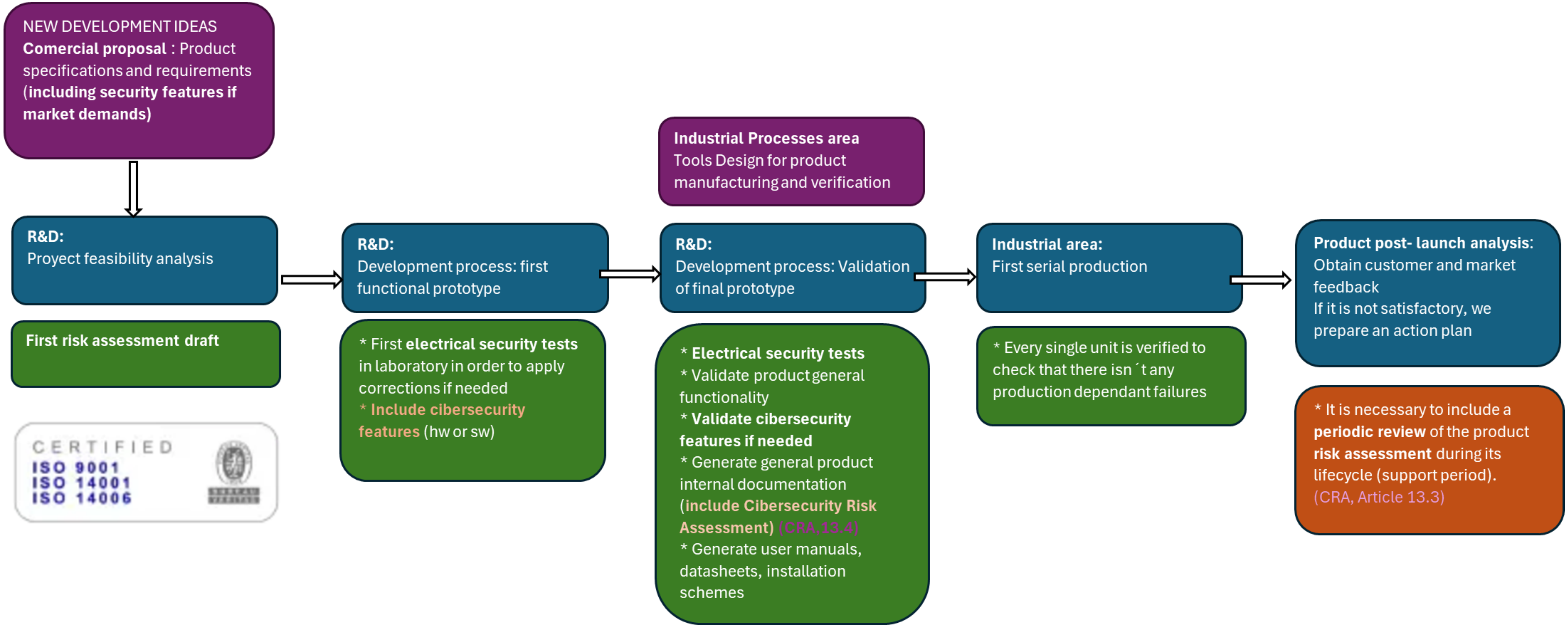
- **Mobile app**
- **Services in Cloud Server**
- Within the software component associated with the microprocessor SDK, we currently have **FreeRTOS** and the **BLE stack**.

We must have **procedures** to:

- Definition of **Software Bill of Materials** (manufacturer name, component name, component version)
- **Monitor** that the components in the SBOM don´t contain **known vulnerabilities**.
- Ensure **security updates** throughout the product’s **lifecycle**.
- Verify that **third-party software and hardware** complies with the necessary **security** measures.

CRA Workshop – Time switches

Annex I requirements based on Risk Assessment: product development process



NEW DEVELOPMENT IDEAS
Comercial proposal : Product specifications and requirements (**including security features if market demands)**

R&D:
Proyect feasibility analysis

First risk assessment draft

CERTIFIED
ISO 9001
ISO 14001
ISO 14006

R&D:
Development process: first functional prototype

* First **electrical security tests** in laboratory in order to apply corrections if needed
*** Include cibersecurity features** (hw or sw)

Industrial Processes area
Tools Design for product manufacturing and verification

R&D:
Development process: Validation of final prototype

*** Electrical security tests**
* Validate product general functionality
*** Validate cibersecurity features if needed**
* Generate general product internal documentation (**include Cibersecurity Risk Assessment)** (CRA,13.4)
* Generate user manuals, datasheets, installation schemes

Industrial area:
First serial production

* Every single unit is verified to check that there isn´t any production dependant failures

Product post- launch analysis:
Obtain customer and market feedback
If it is not satisfactory, we prepare an action plan

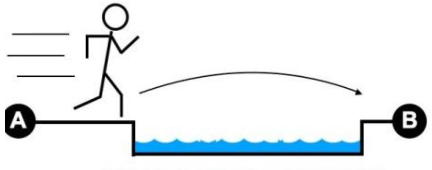
* It is necessary to include a **periodic review** of the product **risk assessment** during its lifecycle (support period). (CRA, Article 13.3)

CRA Workshop – Time switches

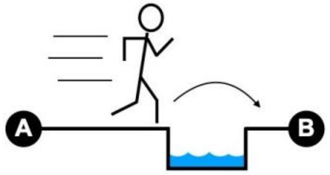
Risk Matrix: Probability / Impact

Probability: measures the likelihood or chance that a specific risk event will occur.

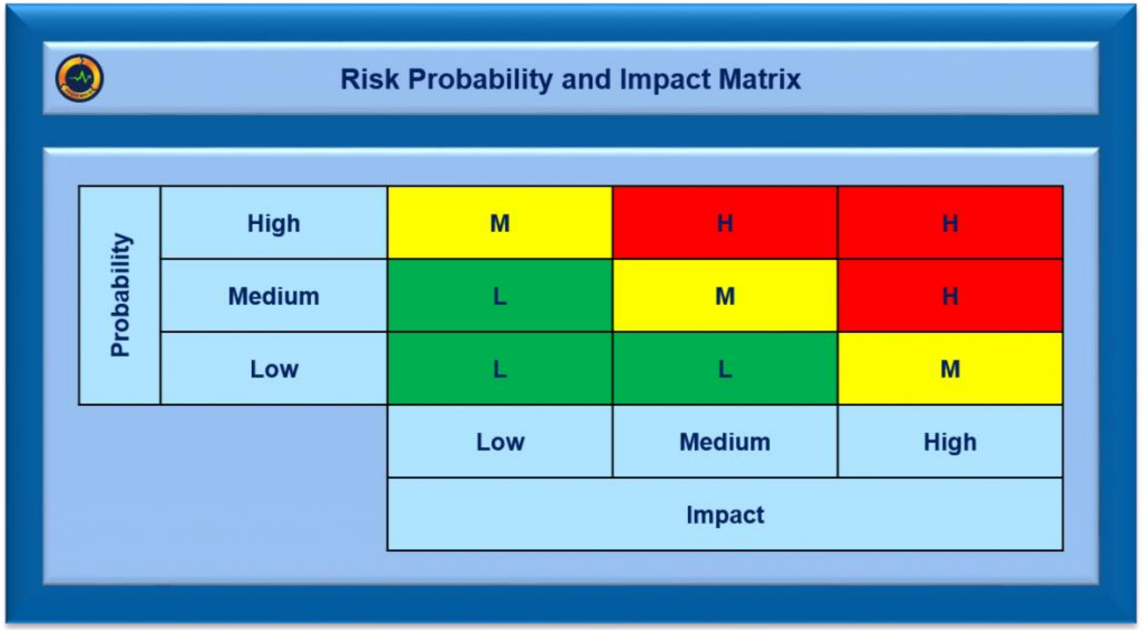
Impact: measures the severity of the consequences or effects if the risk event will occur.



High Probability, Low Impact Risk

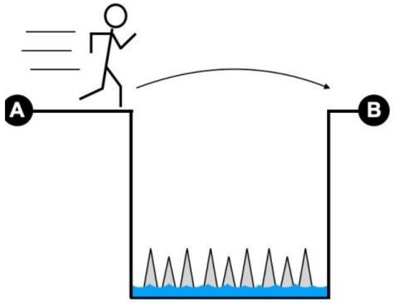


Low Probability, Low Impact Risk

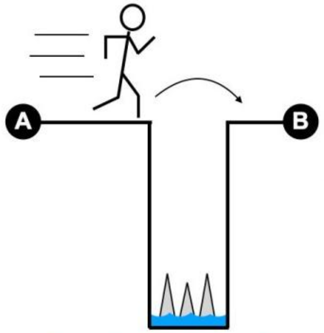


Risk Probability and Impact Matrix

Probability				
	High	M	H	H
	Medium	L	M	H
	Low	L	L	M
		Low	Medium	High
		Impact		



High Probability, High Impact Risk



Low Probability, High Impact Risk

CRA Workshop – Time switches

Time switch: Risk Assessment elements

ID	Asset	Threat	Vulnerability	Impact	Probability	Risk Level	Mitigation Measures	Comments	CRA Annex I Part I
RT1	**Scheduling function**	Bluetooth communication interception (MITM)	Unencrypted communication	Low	Low	Low		data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission.	(b), (e): secure by default, confidentiality
RT2	**On/Off control**	Unauthorized access	Weak/No pairing keys	Medium	Low	Low	PIN control in App	We consider that in the intended environment, a PIN will not be necessary in most cases, and to ensure user comfort and ease of use, we have not enabled it by default.	(b),(d), (j): secure by default, protection from unauthorised access, limit attack surfaces
RT3	**PIN configuration code**	Brute force attack	Weak PIN length	Medium	Low	Low	App lockout after 6 attempts	PIN is limited to 6 access attempts; if exceeded, access is blocked and it must be unlocked using a Master PIN.	(d), (j), (k): protection from unauthorised access, limit attack surfaces, reduce impact of incidents
RT4	**Master PIN code**	Social engineering	Spoofed call to the factory	Medium	Low	Low	No static Master PIN code	To obtain this Master PIN, the user must call the manufacturer, who will provide a code generated at that moment, which is valid only for that day.	(d), (j): protection from unauthorised access, limit attack surfaces
RT5	**Device firmware**	Malicious firmware installation	No integrity validation	High	Low	Medium	FW update with encryption, firmware signature validation and secure keys if applied	With the mitigation measures adopted, the risk of the device is low; therefore, we have not considered it necessary for it to require security updates upon installation	(a), (c) (e), (f), (h): available without known exploitable vulnerabilities, updates,confidentiality, integrity, availability of essential functions
RT6	**BLE network identifiers (name, UUID, MAC)**	Tracking and targeting	Publicly visible identifiers	Low	Low	Low		We consider them non-critical identifiers.	(e): confidentiality
RT7	**Pairing data**	Key sniffing	Plaintext key storage	Low	Low	Low	secure storage if applied	Not applied because of low risk	(e), (f): confidentiality, integrity
RT8	**Configuration app**	Social engineering	Lack of app access control	Low	Low	Low	Option to limit Time switch access control with PIN	We consider that mobile phones has its own access control	(d), (j): protection from unauthorised access, limit attack surfaces

CRA Workshop – Time switches

Time switch: Annex I - Essential Cybersecurity Requirements (I)

	Requirement Summary	Relationship between decisions made accoding to the risk assessment and the essential requirements.	Examples intended enviroment	Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed
(a)	Be made available on the market **without known exploitable vulnerabilities**	Included some **mitigation measures** (the items referenced in the risk assessment column) FreeRTOS and BLE stack **libraries updated**		
(b)	Be made available with **secure by default configuration,** including reset possibility	**Time Switch + Mobile App:** We consider that in the intended environment, a PIN will not be necessary in most cases, and to ensure user comfort and ease of use, we have not enabled it by default.	**PIN not required:** sports field lighting, private swimming pools, greenhouses and farms, shop window lighting, private houses outdoor lighting, ornamental lighting, time-based irrigation. **PIN required:** school sirens, public swimming pools, climate control in offices, EV fleet charging	**Time Switch:** PIN enabled by default with mandatory change on first use.
(c)	Ensure vulnerabilities can be addressed **through security updates, including automatic updates within an appropriate timeframe**	**Time Switch**: With the mitigation measures adopted, the risk of the device is low; therefore, we have not considered it necessary for it to require security updates upon installation. If a security update were necessary, it would be implemented at the factory.		**Time Switch:** The hardware and software resources of the device would allow us to develop the option of secure firmware updates in the field, using App and BLE for this purpose.
(d)	Ensure **protection from unauthorised access by appropriate control mechanisms**	**Time Switch + Mobile App:** We have considered it sufficient to be able to use a PIN in environments where it is needed. PIN is limited to 6 access attempts; if exceeded, access is blocked and it must be unlocked using a Master PIN. To obtain this Master PIN, the user must call the manufacturer, who will provide a code generated at that moment, which is valid only for that day.	**Environments with a higher likelihood of multiple incorrect PIN attempts:** School sirens: Students may attempt to change the siren schedule out of curiosity or mischief Climate control in offices:Individuals may attempt to change settings without authorization for personal comfort.	**Time Switch + Mobile App:** use secure pairing , limit number of boundings, temporal activation of BLE availability. Enforce password complexity Use physical pushbutton enable BLE temporal availability

CRA Workshop – Time switches

Time switch: Annex I - Essential Cybersecurity Requirements (II)

		Requirement Summary	Relationship between decisions made accoding to the risk assessment and the essential requirements.	Examples intended enviroment	Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed
(e)	🗂️🔐	Protect **confidentiality of stored, transmitted or otherwise processed data**	**Time Switch + Mobile App:** for device configuration, the Bluetooth "Services" and "Characteristics" properties are used, but with a custom definition for the Dinuy application. Therefore, the data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission.	A MITM (Man-in-the-Middle) situation could occur in the communication over Bluetooth with the time switch.	**TimeSwitch + Mobile App:** **Pairing:** process through which two BLE devices authenticate and generate link keys. The goal is to securily generate shared keys that can be used to enable encryption for the connection . **Bonding:** proccess of storing these keys for future-connections. We can limit number of bondings. Once paired, encryption is enabled to encrypt the data packets exchanged between the two devices.
(f)	🧩✅	Protect **integrity of stored, transmitted or otherwise processed data,** and report on corruptions	**TIme Switch + Mobile App:** PIN is required to access to stored data or change stored data (where required). PIN is required to set a new PIN		**Time Switch:** Use physical pushbutton to enable PIN change
(g)	📉📦	Process only adequate, relevant and limited data **(data minimisation**)	**TIme Switch + Mobile App:** only the necessary data is transmitted and stored		
(h)	💡🛡️	**Protect availability of essential and basic functions**, including after incidents	**TIme Switch:** We placed the manual on/off switch button in the Schuko format because the other formats are installed in locations that are harder to access.	If the time switch becomes inaccessible via BLE, for example due to a PIN lockout, and it is necessary to toggle the relay, the physical pushbutton can be used to manually change the relay state.	**Time Switch:** Enable an option to manually turn the switch on or off using the pushbutton in all device formats

Time switch: Annex I - Essential Cybersecurity Requirements (III)

		Requirement Summary	Relationship between decisions made accoding to the risk assessment and the essential requirements.	Examples intended enviroment	Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed
(i)	📶 ⚡	**Minimise negative impact** on availability of services provided by other devices or networks	We have considered it not applicable.		
(j)	🚪 🔒	Be designed to **limit attack surfaces**, including external interfaces	**TIme Switch:** only the necessary data is transmitted and stored, only configurable via BLE		**Time Switch**: temporal activation of BLE availability.
(k)	🛠️ 🛡️	Be designed to **reduce the impact of incidents** using mitigation techniques	We have considered it not applicable.		
(l)	📋 👁️	Provide security-related information by **recording and monitoring relevant internal activity**	We have considered it not applicable.		
(m)	🗑️ 🔒	**Provide the possibility to users to securely and easily remove all data and settings** permanently	**TIme Switch:** The PIN can be removed using the app.		

CRA Workshop – Time switches

Mobile App: Risk Assessment elements

ID	Asset	Threat	Vulnerability	Impact	Probability	Risk Level	Mitigation Measures	Comments	CRA Annex I Part I
RM1	**Mobile application code & configurations**	Reverse engineering of app	Insufficient app hardening	Medium	Low	Low	The Flutter app is compiled (Dart AOT). App is converted to native machine code before it runs	This makes the app faster and harder to reverse-engineer than if it were running interpreted code.	(a), (e), (f): without known exploitable vulnerabilities, confidentiality, integrity
RM2		Known flutter libraries threats	Outdated libraries	Medium	Low	low	Flutter libraries updated with identified critical vulnerabilities		(a), (c), (e), (f): without known exploitable vulnerabilities, updates,confidentiality, integrity
RM3	**Bluetooth communication channel**	Unauthorized Bluetooth access	Lack of authentication and secure pairing	Low	Low	Low	PIN control in App	data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission.	(d), (j): protection from unauthorised access, limit attack surfaces
RM4		MITM over Bluetooth	Lack of secure pairing	Low	Low	Low			(e), (f), (j): confidentiality, integrity, limit attack surfaces
RM5	**User data handled by the app**	Data interception in transmission	Absence of TLS Lack of cert validation	Low	Low	Low	Use of TLS for https	The user's email is sent the first time the app is used after installation, it is stored on a secure server	(e), (f): confidentiality, integrity
RM6		Unauthorized data access from storage	Unencrypted local data storage	Low	Low	Low	PIN control in App	It has been determined that the stored data is not sensitive personal data	(c), (e), (f): protection from unauthorised access, confidentiality, integrity
RM7	**Cloud server and API endpoints**	Data interception in transmission	Absence of TLS Lack of cert validation	Low	Low	Low	Use of TLS for https		(e), (f): confidentiality, integrity
RM8		Unauthorized API access	Insecure API design Inadequate input validation	Low	Low	Low		We have not considered it necessary to further enhance authentication security, as we consider the risk to be low.	(d), (j): protection from unauthorised access, limit attack surfaces
RM9	**Authentication credentials**	Credential theft/misuse	Unencrypted storage Outdated libraries	Medium	Low	Low	Flutter_secure_storage (or a native equivalent) is currently being used.		(a), (c), (e), (f): without known exploitable vulnerabilities, updates,confidentiality, integrity
RM10	**Firmware/Software Update Mechanism of the App**	Malicious firmware/software update	Lack of update signing and verification	High	Low	Medium	The app can be updated through the stores (Google Play/App Store). Use only official stores, secure developer accounts (double authentication + build certificate)	It is a third party component, In this case, we have included security updates, since it is a device with much broader connectivity and an internet connection. It also lets us add new features over time.	(a), (c), (f), (h): without known exploitable vulnerabilities, updates,integrity, availability of essential functions
RM11	**Logging & Monitoring**	Lack of detection	No logging implemented	Low	Low	Low	Local logs on the server		(l): recording and monitoring relevant internal activity
RM12	**Data management**	Excess data collection	No minimization controls	Low	Low	Low		Only strictly necessary data is processed.	(g): data minimisation

Brighten up your day

Mobile App: Annex I - Essential Cybersecurity Requirements (I)

	Requirement Summary	Relationship between decisions made accoding to the risk assessment and the essential requirements.	Examples intended enviroment	Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed
(a) 🛡️ ✅	Be made available on the market **without known exploitable vulnerabilities**	Included some **mitigation measures** (the items referenced in the risk assessment column) Flutter **libraries updated** with identified critical vulnerabilities		
(b) ⚙️ 🔒	Be made available with **secure by default configuration,** including reset possibility	**Time Switch + Mobile App:** We consider that in the intended environment, a PIN will not be necessary in most cases, and to ensure user comfort and ease of use, we have not enabled it by default. **Mobile App + Server**: Use of TLS for https.	**PIN not required:** sports field lighting, private swimming pools, greenhouses and farms, shop window lighting, private houses outdoor lighting, ornamental lighting, time-based irrigation. **PIN required:** school sirens, public swimming pools, climate control in offices, EV fleet charging **TLS**: Prevents interception of user-related form data when it is sent to the server	**Time Switch:** PIN enabled by default with mandatory change on first use. **Mobile App + Server:** TLS 1.3, cert pinning in App
(c) 🔄 🛡️	Ensure vulnerabilities can be addressed **through security updates, including automatic updates within an appropriate timeframe**	**Mobile App:** In this case, we have included security updates, since it is a device with much broader connectivity and an internet connection. It also lets us add new features over time. Use only official stores, secure developer accounts (double authentication + build certificate)	user can download updates from the official stores when required	**Mobile App:** Mandatory digital signature for all updates (App firmware). Binary verification before execution (integrity check)
(d) 🚫 👤	Ensure **protection from unauthorised access by appropriate control mechanisms**	**Time Switch + Mobile App:** We have considered it sufficient to be able to use a PIN in environments where it is needed. PIN is limited to 6 access attempts; if exceeded, access is blocked and it must be unlocked using a Master PIN. To obtain this Master PIN, the user must call the manufacturer, who will provide a code generated at that moment, which is valid only for that day. **Mobile app + Server**: TLS use **Dinuy Server:** includes security features: firewall, blacklists and whitelists, intrusion prevention and detection systems, web attack blocking system	**Environments with a higher likelihood of multiple incorrect PIN attempts:** School sirens: Students may attempt to change the siren schedule out of curiosity or mischief Climate control in offices:Individuals may attempt to change settings without authorization for personal comfort.	**Time Switch + Mobile App:** use secure pairing , limit number of boundings, temporal activation of BLE availability. Enforce password complexity Use physical pushbutton enable BLE temporal availability **Mobile App + Server**: TLS 1.3, cert pinning- OAuth 2.0, input validation, authorization for API REST (application layer)

Mobile App: Annex I - Essential Cybersecurity Requirements (II)

		Requirement Summary	Relationship between decisions made accoding to the risk assessment and the essential requirements.	Examples intended enviroment	Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed
(e)	📁🔒	Protect **confidentiality of stored, transmitted or otherwise processed data**	**Time Switch + Mobile App:** for device configuration, the Bluetooth "Services" and "Characteristics" properties are used, but with a custom definition for the Dinuy application. Therefore, the data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission. **Mobile App + Dinuy server:** use of TLS (Transport Layer Security) protocol.	A MITM (Man-in-the-Middle) situation could occur during the form exchange with the server or in the communication over Bluetooth with the time switch.	**TimeSwitch + Mobile App:** **Pairing:** process through which two BLE devices authenticate and generate link keys. The goal is to securily generate shared keys that can be used to enable encryption for the connection . **Bonding:** proccess of storing these keys for future-connections. We can limit number of bondings. Once paired, encryption is enabled to encrypt the data packets exchanged between the two devices. **Mobile App + Server:** Enforce TLS 1.3, implement certificate validation and pinning
(f)	🧩✅	Protect **integrity of stored, transmitted or otherwise processed data,** and report on corruptions	**TIme Switch + Mobile App:** PIN is required to access to stored data or change stored data (where required). PIN is required to set a new PIN **Mobile App**: Flutter_secure_storage. The Flutter app is compiled (Dart AOT). App is converted to native machine code before it runs. This makes the app faster and harder to reverse-engineer than if it were running interpreted code. **Dinuy Server:** use of OVH service provider, aligned with data protection	The integrity of the app could be compromised during the update process	**Mobile App**: Implement **secure storage** using the Android Keystore and the iOS Keychain via flutter_secure_storage. **Anti-tampering** protects the integrity of the software (programs, commands, configuration) against unauthorized modifications. Mandatory **digital signature for all updates** (App and firmware). Binary verification before execution (**integrity check**).
(g)	📉📦	Process only adequate, relevant and limited data **(data minimisation**)	**TIme Switch + Mobile App:** only the necessary data is transmitted and stored **Mobile App + Server:** only the necessary data is transmitted and stored		

CRA Workshop – Time switches

Mobile App: Annex I - Essential Cybersecurity Requirements (III)

		Requirement Summary	Relationship between decisions made accoding to the risk assessment and the essential requirements.	Examples intended enviroment	Measures not implemented at this stage according to the level of risk, but could be considered for future implementation if needed
(h)	💡🛡️	**Protect availability of essential and basic functions**, including after incidents	**Mobile App:** the application can be reinstalled		
(i)	📶⚡	**Minimise negative impact** on availability of services provided by other devices or networks	We have considered it not applicable.		
(j)	🚪🔒	Be designed to **limit attack surfaces**, including external interfaces	**Mobile App:** only the necessary interfaces are active The Flutter app is compiled (Dart AOT). App is converted to native machine code before it runs. This makes the app faster and harder to reverse-engineer than if it were running interpreted code.		**Mobile App**: Code obfuscation, anti-tampering, secure coding practices
(k)	🛠️🛡️	Be designed to **reduce the impact of incidents** using mitigation techniques	We have considered it not applicable.		
(l)	📋👁️	Provide security-related information by **recording and monitoring relevant internal activity**	**Server:** Local logs on the server		**Server**: Centralized logging system + SIEM with incident monitoring and alerts
(m)	🗑️🔒	**Provide the possibility to users to securely and easily remove all data and settings** permanently	**TIme Switch + Mobile App:** The PIN can be removed using the app.		

Cloud Server: implemented Security Measures (I)

iptables

iptables is the default firewall in many Linux systems. It operates at the kernel level using the netfilter framework and allows creating precise rules to filter, redirect, or block network traffic based on multiple criteria (source/destination IP, ports, protocols, connection state, etc.). Although very powerful, its manual configuration requires a deep understanding of the Linux networking system and the logic of tables and chains.

APF (Advanced Policy Firewall)

APF is a high-level firewall system based on iptables, designed to provide an advanced abstraction layer. While its purpose is to simplify common tasks (such as whitelisting and blacklisting, scan detection, or blocking IP ranges), it requires manual configuration of multiple files in /etc/apf/ and a good understanding of network policies. It is aimed at experienced administrators, as it allows defining complex custom rules tailored to specific environments.

ModSecurity for Apache

ModSecurity is a web application firewall (**WAF**) integrated as a module in Apache. It intercepts, analyzes, and filters HTTP requests in real-time. Its main function is to detect and block attacks against web applications, such as SQL injections, XSS, or fuzzing. It operates through a set of rules (such as OWASP CRS) that must be kept updated and well-tuned.

Fail2ban

Fail2ban is a brute-force attack protection tool that monitors log files (such as /var/log/auth.log or /var/log/apache2/error.log) to detect repeated failed login attempts. When a suspicious pattern is detected, it temporarily applies blocking rules using iptables. Although it has templates, its full potential is leveraged when creating custom filters and specific actions per service, making it a flexible solution that requires advanced configuration and understanding of regular expressions and system logs.

Linux Malware Detect (LMD)

LMD is a malware detection system designed specifically for shared Linux environments like web servers. It uses its own signatures and those from ClamAV, along with heuristics, to identify malicious or altered files in the filesystem. It can run on demand or as a background daemon and is capable of sending alerts, quarantining files, or automatically deleting them based on configuration.

rsyslog

rsyslog is one of the most widely used logging systems on Linux. It collects, filters, and redirects system and application messages to log files, databases, or remote systems. It supports templates, advanced rules, and encrypted forwarding via TCP or UDP, making it suitable for integration with centralized monitoring or auditing systems.

Logwatch

Logwatch is a log analysis and summary tool that generates daily reports on system status. It processes log files and presents consolidated information by services (such as SSH, Apache, Dovecot, etc.), allowing detection of anomalies or events of interest without manually examining raw logs. It is useful for maintaining an automated overview of what is happening on the server.

Cloud Server: implemented Security Measures (II)

rkhunter (Rootkit Hunter)

Rootkit Hunter scans the system for known rootkits, suspicious changes in system binaries, irregular permissions, and dangerous configurations. It compares checksums of critical files with reference databases and alerts about possible alterations. Although it does not provide active protection, it is an effective tool for auditing and detecting malicious persistence.

OpenSSL

OpenSSL is the most widely used general-purpose cryptography library in Unix systems. It provides tools and APIs for managing X.509 certificates, TLS/SSL connections, RSA/ECDSA keys, and digital signatures. It is a fundamental component for security in web services, mail, and VPNs, ensuring compatibility with modern cryptographic protocols.

SpamAssassin

SpamAssassin is a rule-based, scoring, and Bayesian analysis email filtering system. It evaluates incoming messages and assigns a spam score based on multiple heuristics and external blacklists. It can integrate with mail servers like Postfix or Exim to classify or reject emails before they reach users, improving mail system hygiene.

SSH Configuration

SSH access is configured with PermitRootLogin=no, which prevents direct root user access, and PasswordAuthentication=yes, meaning password authentication is still allowed (instead of enforcing public key only). This configuration balances basic security and accessibility, although it can be strengthened by completely disabling password authentication.

TCP Wrappers

The TCP Wrappers system is active, with a rule in hosts.deny and none in hosts.allow. This allows implementing access restrictions to traditional network services (like SSH, SMTP, etc.) at the application layer, although its use has become obsolete compared to modern firewalls like iptables or nftables.

Kernel Hardening

The kernel configuration shows basic hardening settings. The parameter icmp_echo_ignore_all=0 indicates the system responds to pings, useful for diagnostics but which could be limited to prevent scanning. Enabling tcp_syncookies=1 protects against SYN flood attacks, enhancing resistance against TCP-level denial-of-service attempts.

PAM Security

The PAM (Pluggable Authentication Modules) system is configured, allowing flexible access control policies, lockout after failed attempts, and password complexity requirements. Proper configuration is key to strengthening login security and privileged command use.

Sudo Security

The sudo privilege system is active and configured, although entries with the NOPASSWD option were detected, allowing commands to be executed without prompting for a password. While useful for automation, this practice should be used cautiously and only in controlled contexts. Additionally, a specific configuration file inside /etc/sudoers.d has been identified, indicating administrator customization.

Supports templates, advanced rules, encrypted forwarding via TCP/UDP

Ideal for centralized monitoring and auditing

Cloud Server Security Concepts Summary

Security concepts usage

Network Security:

Use iptables, APF, ModSecurity, and Fail2ban to **filter traffic, block brute-force attempts**, and **mitigate DoS attacks**.

Communication Security:

Enforce **TLS 1.3** via OpenSSL and implement **certificate pinning** in the application.

Use **SPF**, **DKIM**, and **DMARC** with your SMTP provider to ensure email authenticity.

Access Control & System Hardening:

Apply **RBAC** (Role-Based Access Control).

Perform **database hardening** and ensure **encryption at rest**.

Regularly update the OS and services; apply **kernel hardening**.

Intrusion Detection & Malware Protection:

Run regular scans with tools like **LMD** (Linux Malware Detect) and **rkhunter**.

Email & Spam Protection:

Use **SpamAssassin** and **SMTP rate limiting** to reduce spam and abuse.

Monitoring & Logging:

Enable centralized logging with **rsyslog** and perform daily analysis with **Logwatch**.

Monitor delivery systems, implement **retry logic**, and use **SMS fallback** for critical alerts.

Backup & Recovery:

Implement **regular backups** and routinely **test recovery** procedures.

Data Disposal:

Enforce **secure data wiping** practices.

Concepts used in risk assessment mitigation measures column

TLS 1.3 – Transport Layer Security version 1.3

A cryptographic protocol for secure communications over networks.

Certificate Pinning – Cert Pinning

A technique that binds an app to a specific certificate to prevent man-in-the-middle (MITM) attacks.

SPF – Sender Policy Framework

A system to prevent spoofing of sender email addresses.

DKIM – DomainKeys Identified Mail

A method that uses cryptographic signatures to verify email integrity.

DMARC – Domain-based Message Authentication, Reporting and Conformance

A policy that tells email receivers how to handle messages that fail SPF or DKIM checks.

RBAC – Role-Based Access Control

An access control model based on user roles within an organization.

Encryption at Rest

The encryption of stored data to protect it from unauthorized access.

Kernel Hardening

The process of securing the operating system kernel to reduce vulnerabilities.

LMD – Linux Malware Detect

A tool used to detect malware on Linux systems.

rkhunter – Rootkit Hunter

A scanner that checks for rootkits and other exploits on Unix/Linux systems.

SpamAssassin

A rule-based email spam filter.

SMTP – Simple Mail Transfer Protocol

The protocol used for sending email messages.

rsyslog

An advanced logging and log forwarding system for Linux.

Logwatch

A tool that analyzes and summarizes system log files on a daily basis.

Secure Wipe

A data erasure method that ensures deleted data cannot be recovered.

CRA Workshop – Time switches

Cloud Server: Risk Assessment elements

ID	Asset	Threat	Vulnerability	Impact	Probability	Risk Level	Mitigation Measures	CRA Annex I Part I
RC1	**User Form Data** (Name, Email, etc.)	Data interception during submission	No TLS, invalid certificates	Medium	Low	Low	**OpenSSL**: Enforce TLS 1.3	(e), (f): confidentiality, integrity
RC2		Unauthorized access to stored data	Misconfigured DB, weak permissions	Medium	Low	Low	**iptables, APF:** limit access **RBAC, DB hardening, encryption at rest**	(d), (e), (f): confindentiality, integrity, protection from unauthorised access
RC3	**API endpoints (form submission, verification)**	Unauthorized access attempts	Weak authentication, lack of filtering	Medium	Low	Low	**iptables, APF, ModSecurity, Fail2ban:** filter traffic and block brute force	(d), (j), (k): protection from unauthorised access, limit attack surfaces, reduce impact of incidents
RC4		Denial of Service	No rate limiting, no WAF	Medium	Low	Low	**ModSecurity (WAF), Fail2ban, iptables:** mitigate DoS	(h), (i), (j): availability of essential functions, minimise negative impact, limit attack surfaces
RC5	**Email verification process**	Spoofing of verification emails	Improper SPF/DKIM/DMARC setup	Medium	Low	Low	Use **SPF, DKIM, DMARC** with SMTP provider	(d), (e), (f): confindentiality, integrity, protection from unauthorised access
RC6		User does not receive email	Delivery issues	Medium	Low	Low	Monitor delivery, retry logic	
RC7	**Database storing user form data**	Data loss or corruption	No backups, no redundancy	Low	Low	Low	Implement **regular backups, test recovery**	(h), (i), (k):availability of essential functions, minimise negative impact, , reduce impact of incidents
RC8	**Cloud Server**	Compromise via outdated software	Unpatched services	Medium	Low	Low	Regular OS and service updates, kernel hardening	(a), (c): available without known exploitable vulnerabilities, updates
RC9		Rootkit or malware persistence	Lack of detection tools	Medium	Low	Low	**LMD, rkhunter:** periodic scans	(d), (k): protection from unauthorised access, reduce impact of incidents
RC10		Spam from server	Uncontrolled mail flow	Medium	Low	Low	**SpamAssassin, SMTP rate limiting**	(l): monitoring relevant internal activity
RC11	**Logging and Monitoring**	Lack of incident detection	No log analysis or monitoring	Low	Low	Low	**rsyslog, Logwatch:** enable log collection and daily analysis	(l): monitoring relevant internal activity
RC12	**Decommissioning user data**	Residual data post-deletion	No secure deletion policy	Low	Low	Low	Implement secure wipe procedures	(m); possibility to users to remove all data

CRA Workshop – Time switches

DINUY
Brighten up your day

Annex II: Information and instructions to the user

Requirement	How It Is Provided
1 **Manufacturer identity and contact details** (name, registered trade name/trademark, postal address, email or digital contact, website)	Datasheet, user manual, and website (CRA Art. 13.16)
2 **Contact for reporting vulnerabilities and CVD (**Coordinated Vulnerability Disclosure) **policy**	Technical support section on website (CRA Art. 13.17) PCVD pending (CRA Art. 13.8)
3 **Product unique identification (name, type, additional info)**	Laser marking: product reference, production order, date, HW & SW version, BLE MAC address readable in the app
4 **Intended purpose, security environment, essential functionalities, information about the security properties**	User manual (Dinuy App - Configure, PIN management)
5 **Known/foreseeable circumstance which may lead to significant cybersecurity risks**	User manual (Dinuy App - Configure, illustrated)
6 **EU Declaration of Conformity internet address**	Website (CRA Art. 13.20)
7 **Technical security support type and support period for vulnerabilities and updates**	Pending: relevant information that was taken into account to determine the support period (Annex VII- technical doc content 4.)
8 **Measures during initial commissioning and lifetime to ensure secure use**	Datasheet, user manual (Dinuy App - Configure)
9 **Where to access software bill of materials if available**	Not available

Conclusions and highlights

- Every **decision** regarding which **security measures to implement** in the product is based on the **risk assessment** carried out by the manufacturer, identifying the assets to be protected, threats, and vulnerabilities, while taking into account the **context** in which the product will be used. **Vulnerability ≠ Risk.**

- A **balance** must be struck between the **implemented security measures** — to ensure the product is sufficiently secure in its intended context — and the **development effort,** as well as the **hardware and software resources** allocated to it.

- The **risk assessment** must be taken into account throughout the entire product **development process**, its manufacturing, and during the entire product´s lifecycle; it is a **living document**, manufacturers must monitor the product once it is placed on the market.

- If components are subcontracted to a **third party**, as manufacturer you have the final responsibility of the components that are accompanying your product.

- The manufacturer is responsible **for informing the user** on how to configure the product to ensure it is secure.

- A manufacturer shall **notify any actively exploited vulnerability** and ensure that vulnerabilities can be addressed through **security updates.**

- Manufacturers shall determine the **support period**, and document relevant information that was taken into account to determine the support period pursuant to Article 13(8).

- Technical documentation (annex VII) must contain necessary information and specifications of the **vulnerability handling processes,** including the **software bill of materials**, the **coordinated vulnerability disclosure policy**, evidence of the provision of a **contact address for the reporting of the vulnerabilities** and a description of the **technical solutions chosen for the secure distribution of updates**.

- Products placed on the market **before the application date of the CRA** are not subject to the regulation, except for the **reporting** obligation on **actively exploitable vulnerabilities**. In case of a **substantial modification** after placing on the market, the modified product is considered a new product under CRA and must comply with its requirements.

- If you place the **same product but another batch the future individual products should comply with CRA as per date of application**. **CRA apply to each individual product** with digital elements when placed on the market, irrespective of whether the product with digital elements is manufactured as an individual unit or in series.

CRA Workshop – Time switches

Q&A

CRA Workshop – Time switches

Workshop Scenarios

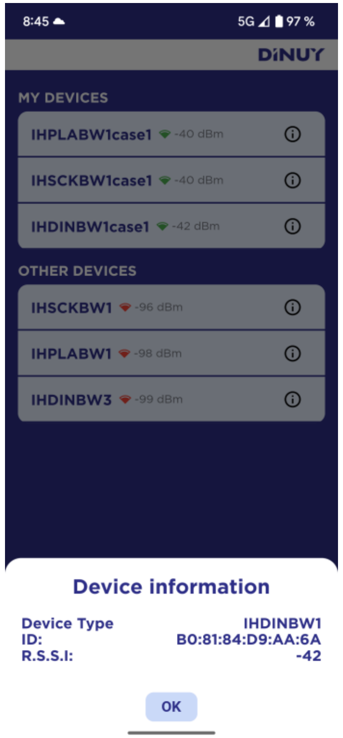
SCENARIO - CURRENT PRODUCT INTENDED ENVIROMENT
A **time switch** installed in office buildings is used to **control heating or air conditioning systems** based on programmed schedules to optimize energy consumption and comfort.

OBJECTIVE
Consider what activities a company like Dinuy (SME) needs to do in order to ensure that the time switch shall be designed, developed, produced, maintained, and disposed of in such a way that they ensure an appropriate level of cybersecurity based on the risks across the entire lifecycle of the product.

Consider at least the following:
- Risk assessment and treatment
- Essential Cybersecurity Requirements
- Communication with relevant stakeholders
- Updates - lifecycle
- Documentation

CRA Workshop – Time switches

QR: App Dinuy-Configure



8:45 5G 97 %

DINUY

MY DEVICES

- IHPLABW1case1 -40 dBm ⓘ
- IHSCKBW1case1 -40 dBm ⓘ
- IHDINBW1case1 -42 dBm ⓘ

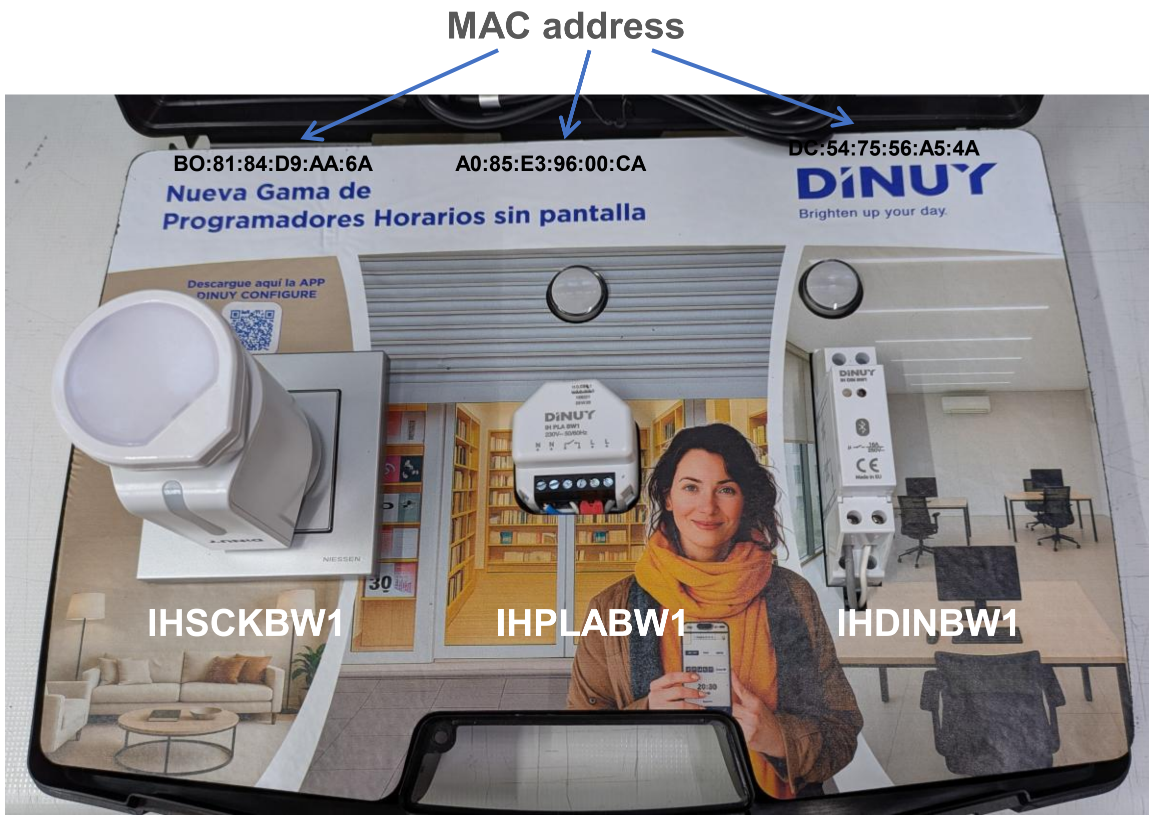
OTHER DEVICES

- IHSCKBW1 -96 dBm ⓘ
- IHPLABW1 -98 dBm ⓘ
- IHDINBW3 -99 dBm ⓘ

Device information

Device Type	IHDINBW1
ID:	B0:81:84:D9:AA:6A
R.S.S.I:	-42

OK



DINUY

Brighten up your day

Thank you!