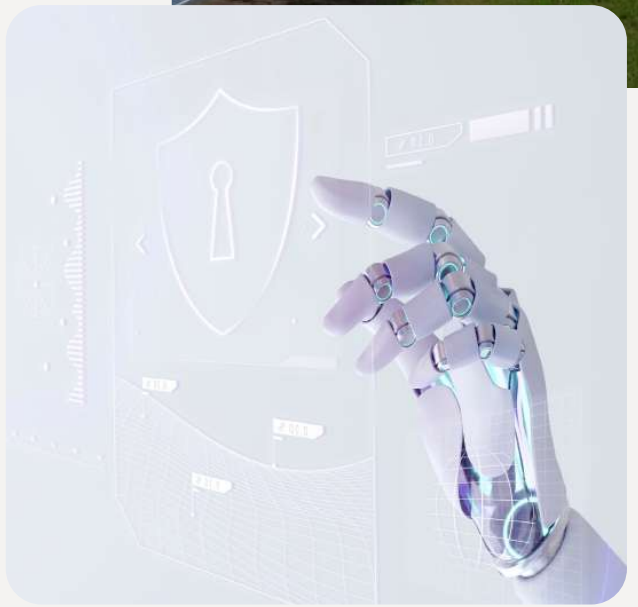
WEBINAR

Cybersecurity in Solar PV sites



suntrack

Company Overview

We are the largest worldwide **solar tracking control systems** vendor

suntrack

We **scale up PV projects** maximizing solar energy production with the most advanced **products & services ecosystem**

Powering a **Sustainable** Future.

+20 YEARS

providing industry-scale solutions for Solar PV

34 product variants of our TCU

The most avanced product & services ecosystem

Global Design Manufacturing & Services capabilities

3 Production Plants,
6 Service Centers
1 R&D Center

+40 GW

of installed capacity

+800k devices
+1.700 solar sites

Since 1999

We have specialized in the engineering and manufacturing of electronic products and systems for high demand industries **since 1999**.

The mix between innovation and knowledge and leveraging P4Q's extensive experience on in HW and SW development, gave birth to our **Suntrack** product line: the most flexible and reliable single axis tracker controller in the world.

With a robust design and validation process, Suntrack products also benefit from a 100% controlled production using the latest manufacturing technologies.

Suntrack **Ecosystem**

Suntrack provides an open and adaptive system designed to achieve a +99% tracking uptime and obtain a low LCOE.

Our ecosystem consists on an extensive product and service portfolio ready to be customized to your utility-scale PV project and designed to help obtaining a cybersecure net.

TCU/DCU

MOBILE APP FOR EASY INSTALLATION

RSU

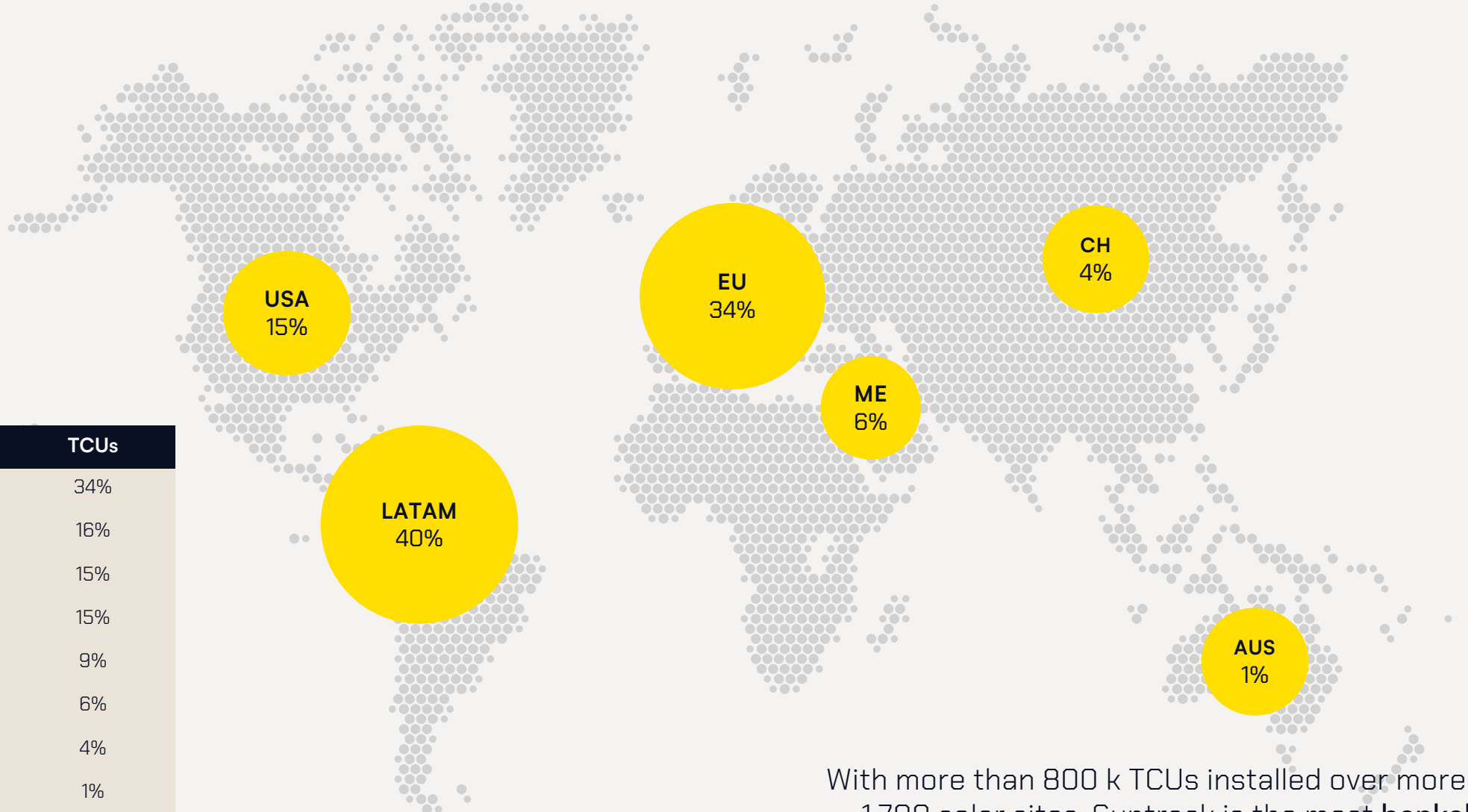
NCU WITH WEB SERVER

CUSTOMER SERVICE PORTAL ADVANCED ALGORITHMS & SMART MONITORING

DISCOVER OUR END-TO-END ECOSYSTEM ON SUNTRACK.P4Q.COM

Deployed TCUs by Suntrack

>800k TCU (*), > 1,700 solar sites



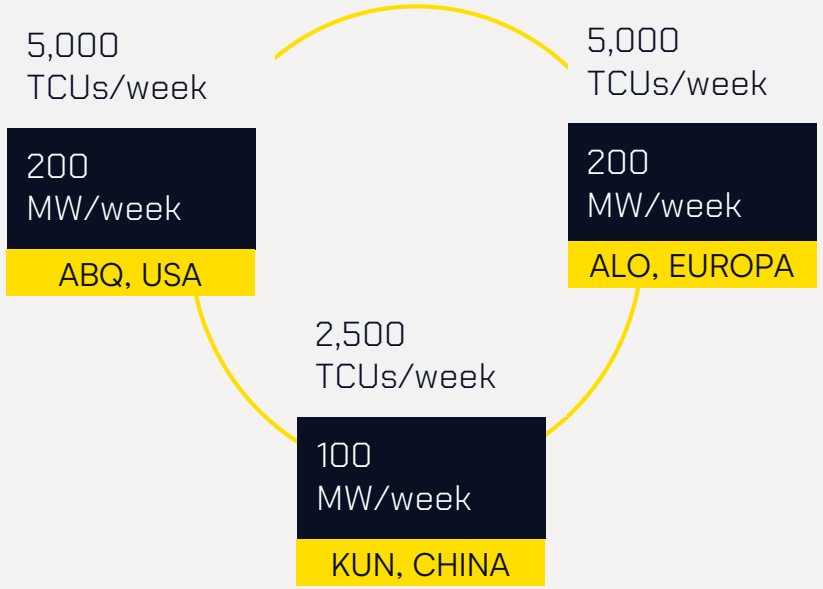
TOP COUNTRIES	TCUs
EUROPE	34%
BRAZIL	16%
MEXICO	15%
UNITED STATES	15%
CHILE	9%
EGYPT	6%
CHINA	4%
AUSTRALIA	1%

(*) 2016 & 2020 TCU only (updated nov'23) > 75k TCU more of legacy models not shown

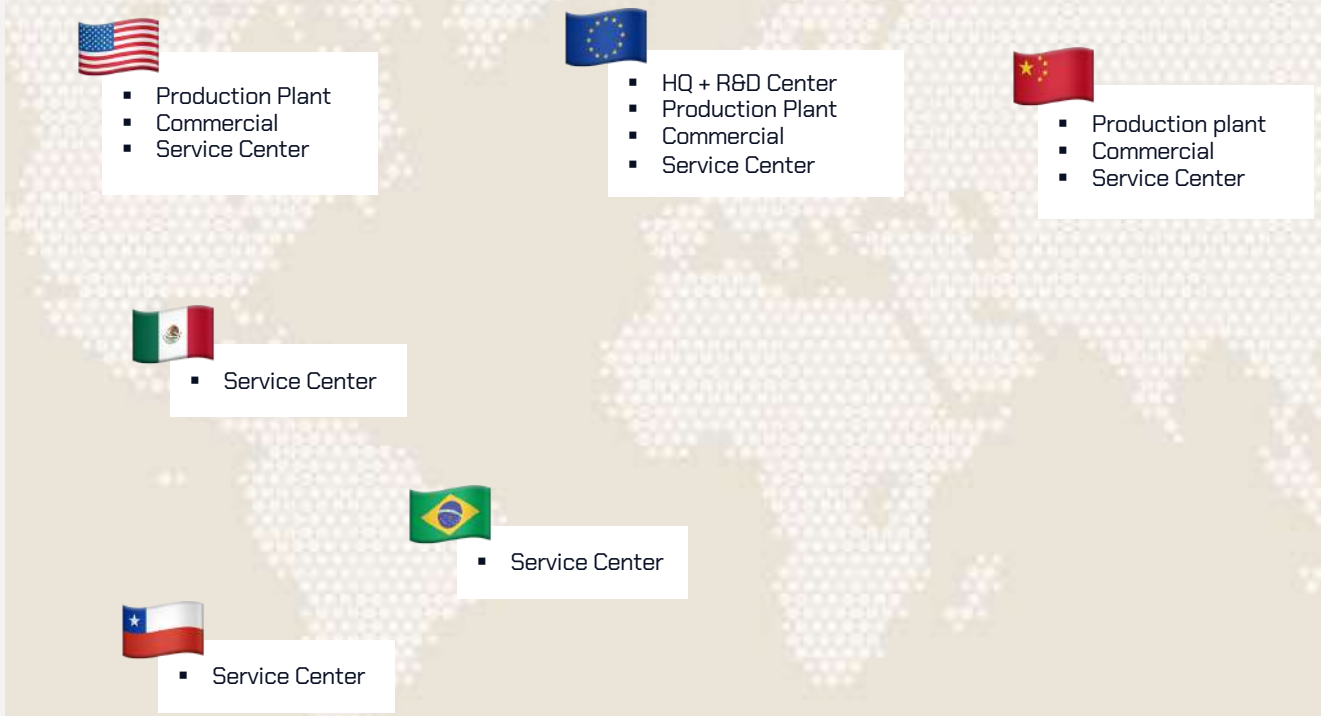
With more than 800 k TCUs installed over more than 1,700 solar sites, Suntrack is the most **bankable & reliable** solution for utility scale projects worldwide

An extensive total production capacity of 500 MW/week

(Average of 25 TCU/MW)



We are a trusted partner for global leaders´ internationalization strategy supporting the operations from its **3 production plants (Spain, USA and China)**, and **6 Service Centers** to guarantee a close service to the solar plants.



1,000,000

In 2024 we will achieve one million delivered TCUs

SECUREIT by LKS Next

100% Spanish company created in 2009 by **expert lawyers in ICT law**, **engineers** and **experts in information security**.

Mission: to help companies **reduce the risks** to which they are exposed due to the management of their information.

Trofeos de la Seguridad TIC

Mejor Empresa de Seguridad TIC

Leaders in auditing and implementation of advanced **cybersecurity and compliance management models.**

Two Advanced-SOC security centers for 24x7x365 control and supervision

Madrid – Vitoria

ISO27001 / ISO9001 / CERT / ENS

360º Security for your company's information:

- Corporate Processes
- IT Security
- Industrial Cybersecurity
- Regulatory Compliance

LKS Next

MONDRAGON

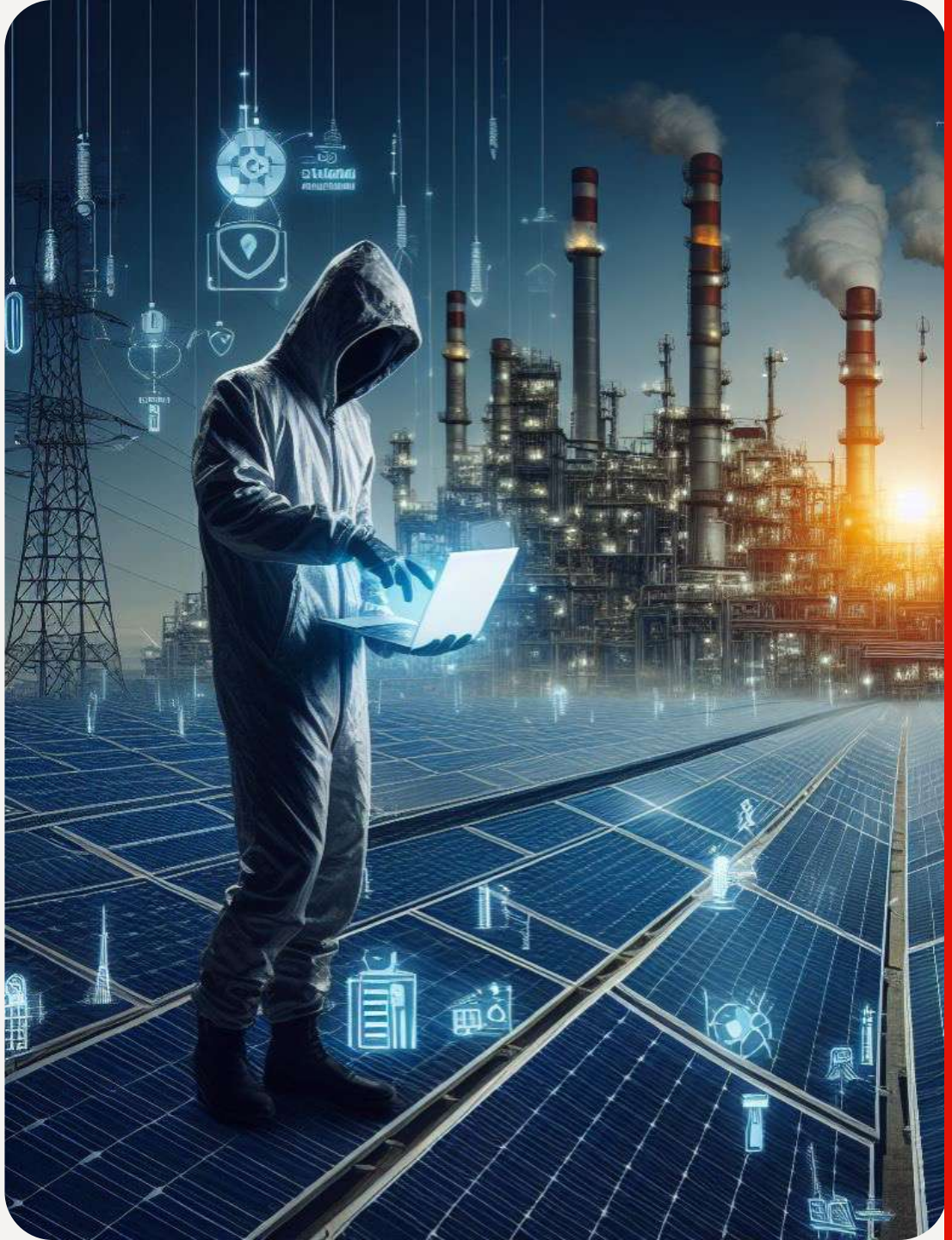
Part of **LKS Next**, a service consulting firm of the **Mondragon Cooperative Group.**

Some definitions...

- **Vulnerabilities** are weaknesses in information and **operational** systems, system **procedures**, controls, or **implementations** that can be exploited by a threat source.
- **Understanding** the source of vulnerabilities and predisposing conditions can help identify optimal mitigation strategies.
- Three main groups:
  - **System**
  - **Communication channels**
  - **Policy and Procedures.**
- A vulnerability can be a potential risk that a Threat Source could exploit by a defined Attack Vector.
- **Consequence** is not **Impact.**
- **Consequence = Operational**
- **Impact = Money**

Incidents

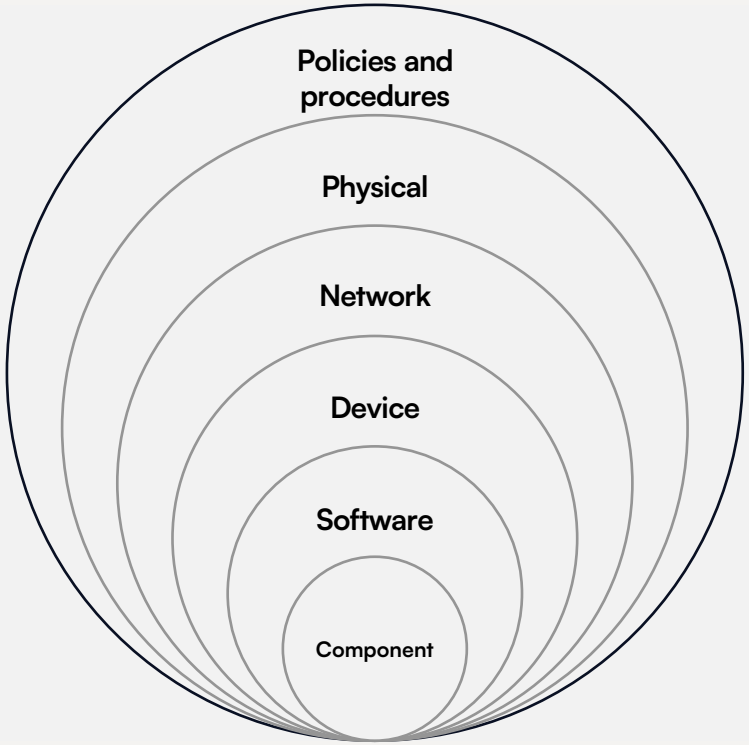
- Physical damage
- Loss visibility
- Loss of control
- Manipulation of variables or parameters
- Stop operations
- Denial of Service, DoS
- Electric outages
- Tailored malware for Electric grid operations

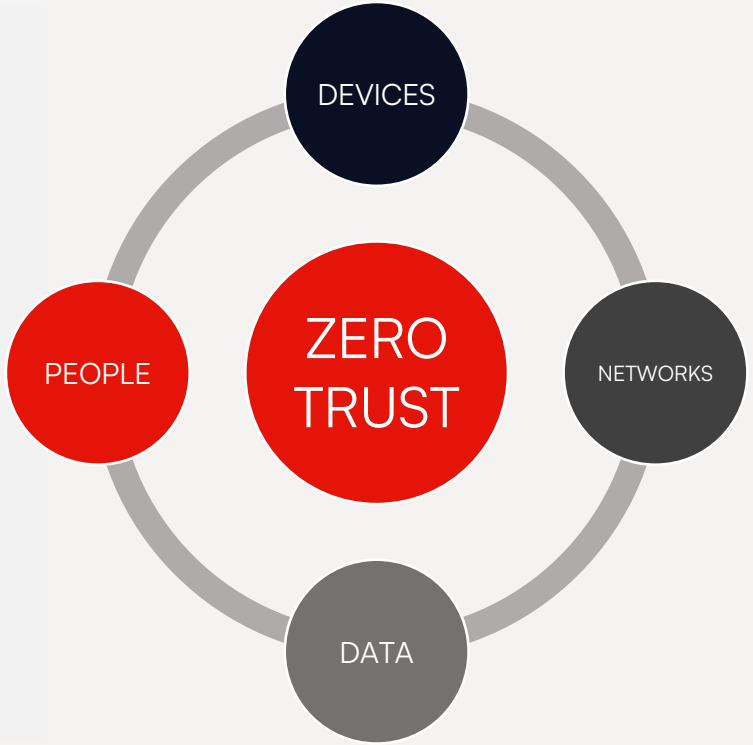


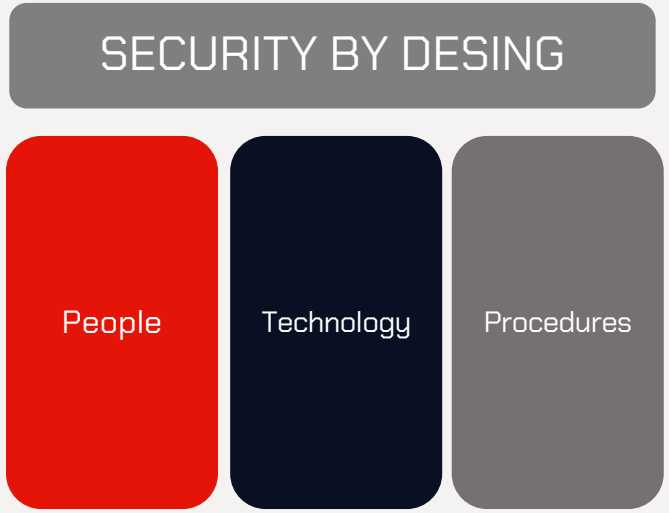
Technology

- Solar inverters
- Metheo stations
- Power Plant Controllers
- Managed Network Devices
- Local SCADA Servers
- Time Servers
- Real Time Automation Controllers
- Protection and control equipment

Strategies

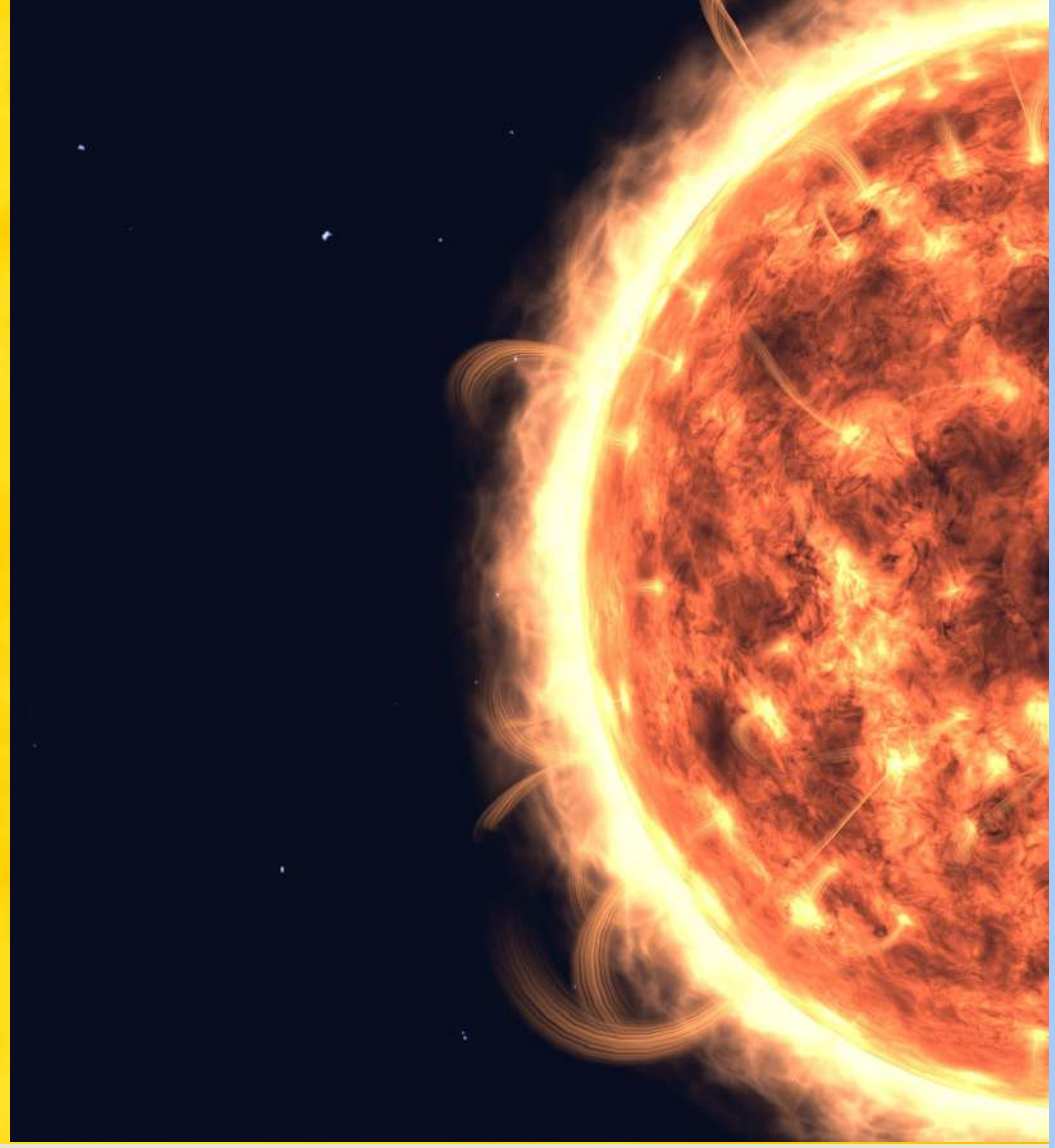






CYBERSECURITY MANAGEMENT SYSTEM, CSMS

Devices focused on Solar Sites Cybersecurity



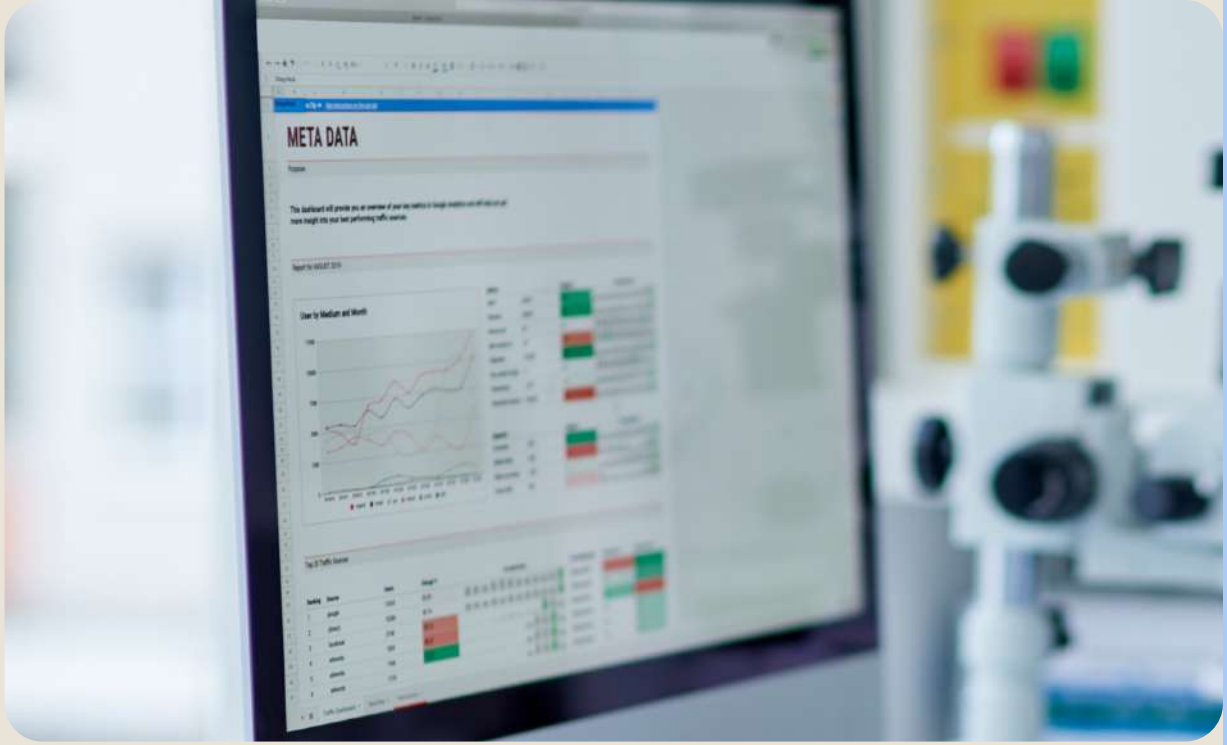
SUNTRACK© BY P4Q

WHERE THE SUN MEETS TECH

IT Device

(Information Technology Device)

/ Physical device or piece of equipment that is used in information technology environments.



Devices typically designed to:

- Facilitate information processing
- Communication
- Data management

Purpose:

- Information Management
- Communication
- Computational Tasks

OT Device

(Operational Technology Device)

/ Physical device or piece of equipment that is used in operational technology environments.

Devices typically designed to:

- Monitor
- Control
- Automate physical processes

Purpose:

- Operational Control
- Industrial Application
- Connectivity

Why we need **both systems** to be **communicating?**

OT

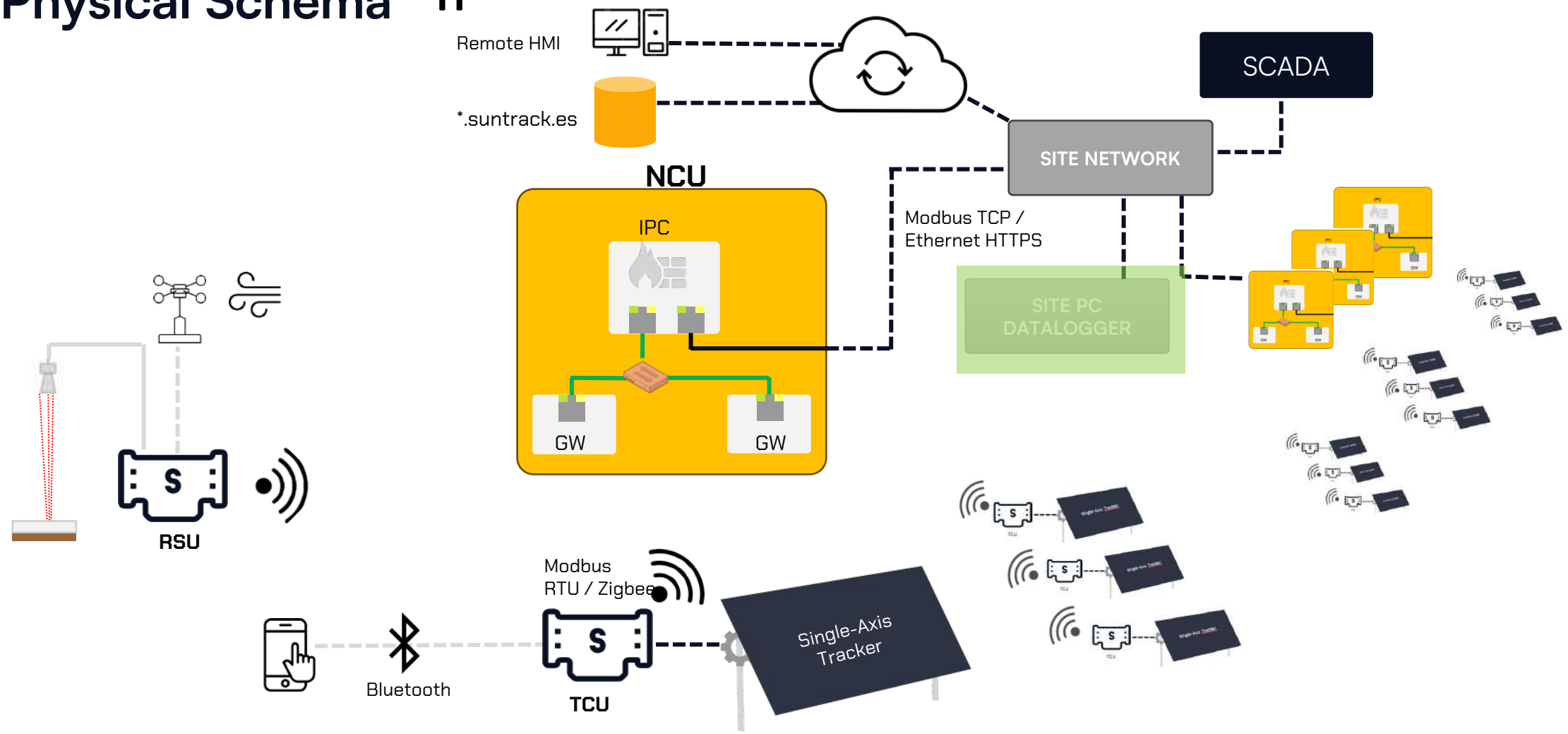
Control and monitoring of physical processes

IT

Primarily used for information processing & communication

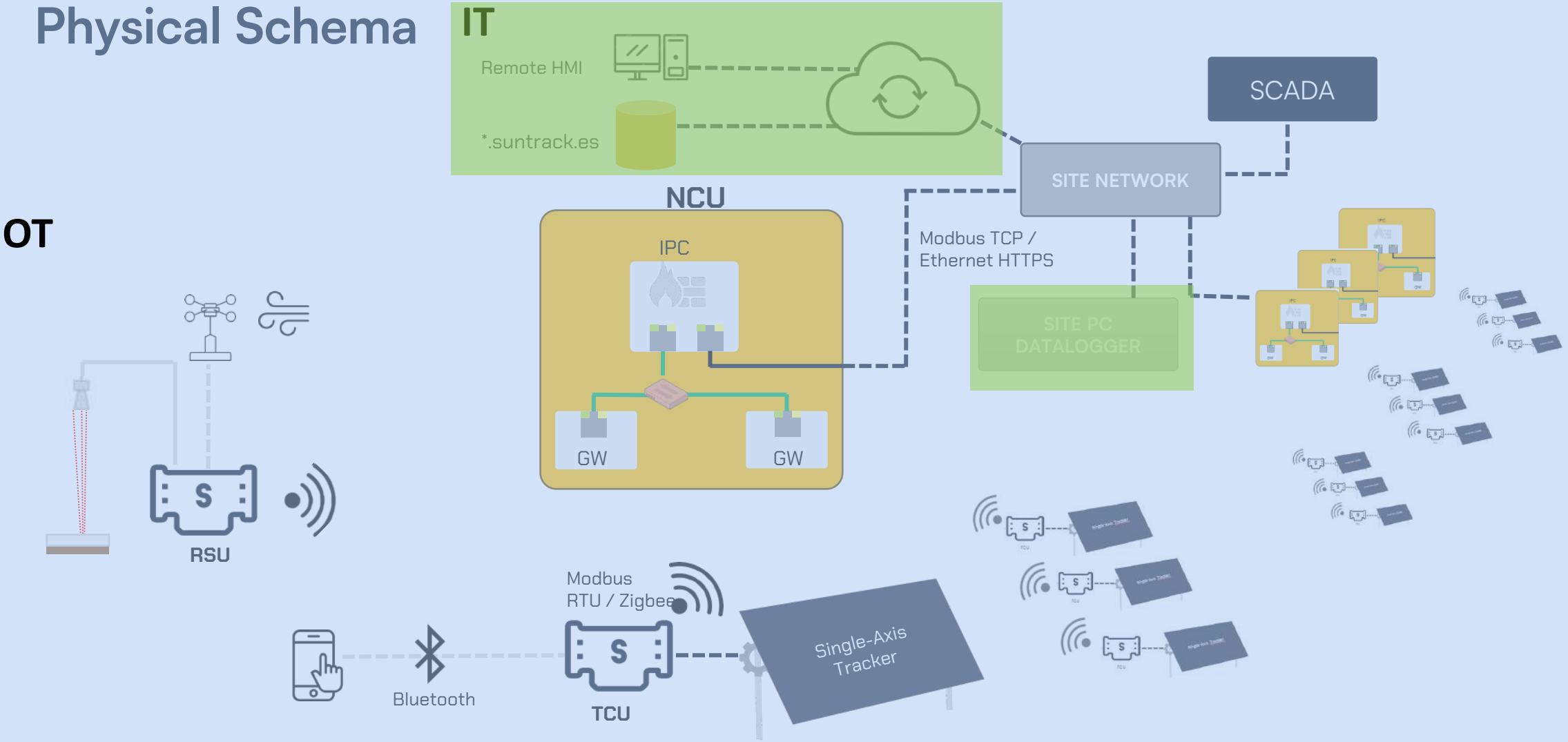
With the increasing integration of OT and IT systems, there may be instances where devices serve dual purposes or bridge the gap between these two domains.

Physical Schema



IT and OT devices

Physical Schema



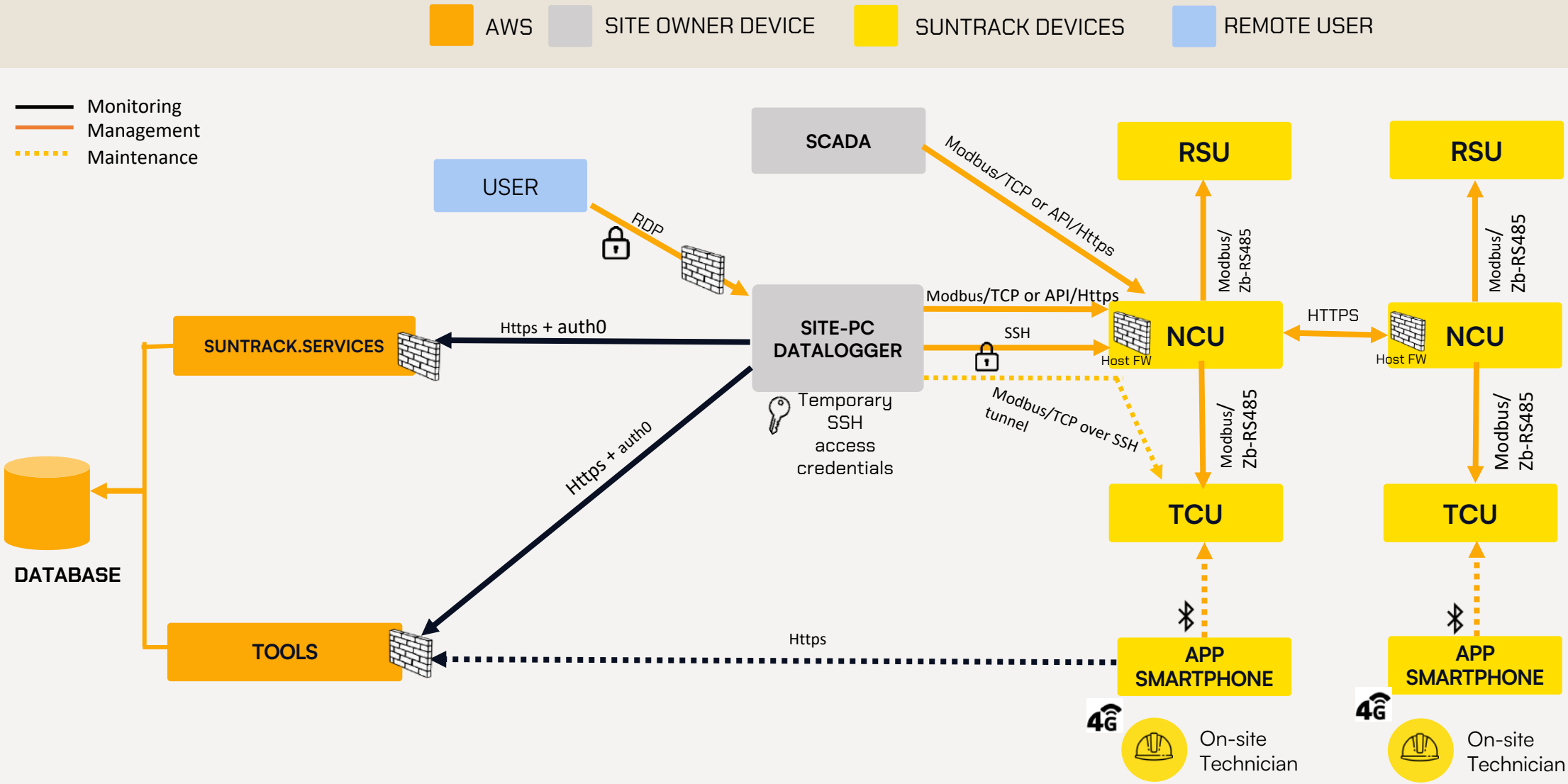
TRACKER CONTROL UNIT (**TCU**) · NETWORK CONTROL UNIT (**NCU**) · REMOTE SENSOR UNIT (**RSU**)

Main changes,
Hardened NCU

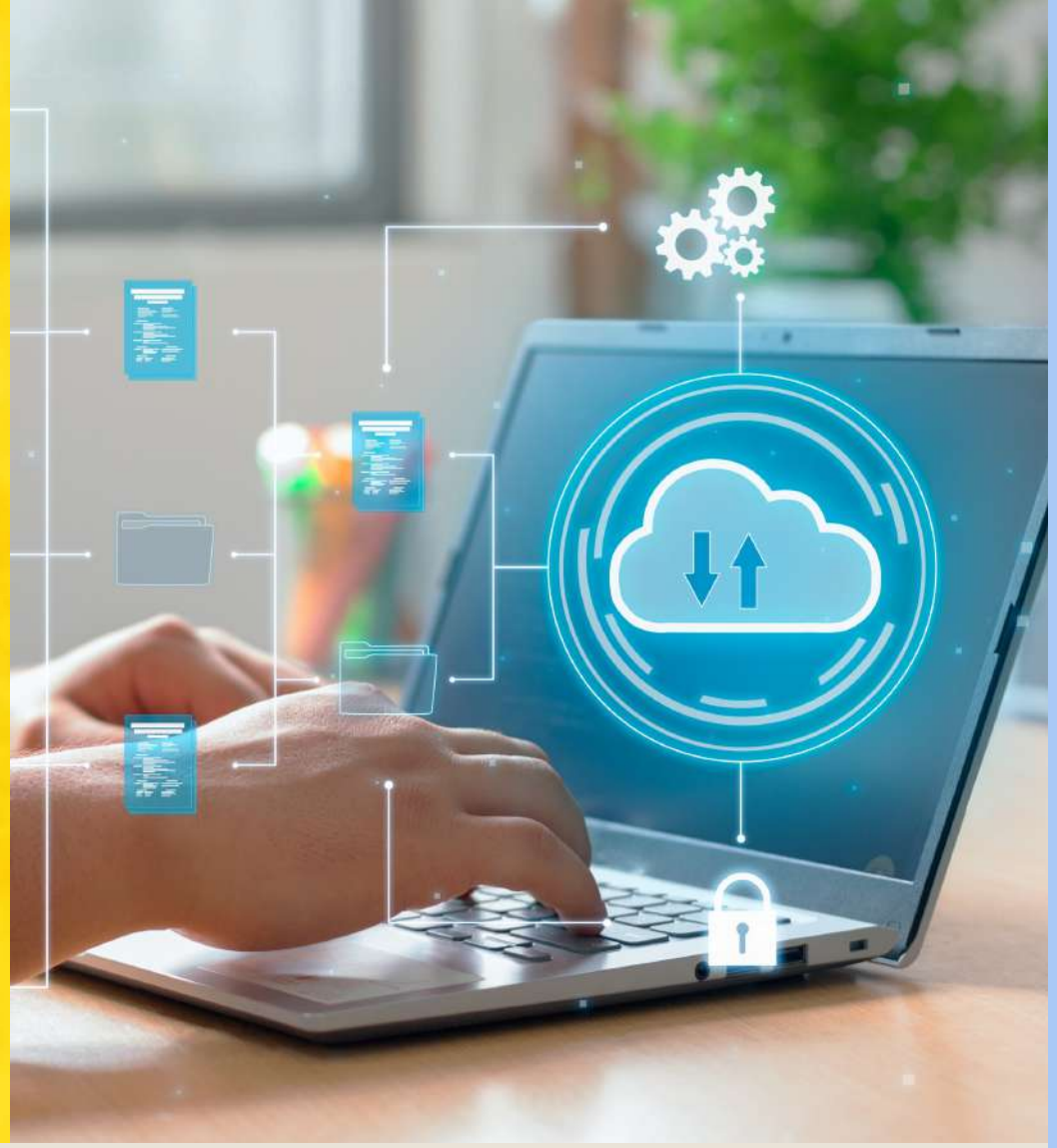
An additional device into sites network

- Encrypted Zigbee
- Only one IPC port exposes to the outer network
- NCU IPC
  - Secure boot
  - OTP
  - Disk encryption
  - Fw configuration
  - SSH Certificates, CAs
- HTTPS connection
- Suntrack Password policy:
  - Robust passwords
  - Password Rst
  - Restric Psw reuse
  - MFA
  - Restric authentication

Secure Access Schema



Our
On Cloud Systems



Suntrack Services
IIoT in Solar PV Trackers

Universal Login

- *Secure Authentication:* Universal login offers robust, multi-factor security.
- *Encrypted Data:* Passwords and sensitive data are encrypted at rest.
- *Compliance with Standards:* It employs OpenID Connect and OAuth 2.0 security protocols.
- *Brute Force Protection:* Shields against brute force and dictionary attacks.
- *Audit Trails:* Provides comprehensive audit logging for incident response.Token
- *Management:* Ensures effective access token control.
- *Regulatory Compliance:* Assists in adhering to GDPR, CCPA, and other regulations.

Suntrack.Services Data Lake & Data Encryption

- *Encryption at Rest:* Safeguards data at rest within the Data Lake.
- *Encryption in Transit:* Ensures data is encrypted during transmission.
- *Data Loss Protection:* Offers robust data replication.
- *Access Control:* Provides granular access controls for data protection.
- *Regulatory Compliance:* Aids in meeting GDPR, CCPA, and other regulations.
- *Physical Security:* Ensures the security of physical data center facilities.
- *Monitoring & Alerts:* Incorporates real-time monitoring and alerting systems.
- *DDoS Protection:* Offers protection against Distributed Denial-of-Service attacks.
- *Data Segregation:* Facilitates secure data segregation and organization.

suntrack

QUICK VIEW OF

IEC 62443 & NERC-CIP

IEC 62443

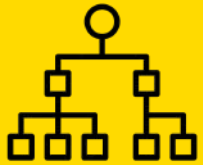
*IEC 62443 is a series of international standards for **Industrial Automation and Control Systems (IACS)** security.*

Developed by the **International Electrotechnical Commission (IEC)** to address the growing concerns around cyber threats in critical infrastructure. Aimed at providing a systematic approach to protect IACS from cyberattacks, ensuring the reliability and safety of industrial processes.

- IEC 62443-4-1 - Secure product development lifecycle requirements
- IEC 62443 3 3 - System security requirements and security levels

Defense in depth

PLANT SECURITY



NETWORK SECURITY

SYSTEM INTEGRITY

What Is NERC-CIP?

North American Electric Reliability Corporation — Critical Infrastructure Protection.

A non-profit **international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid**. The NERC has authority over the continental United States, Canada, and the northern area of Baja California, Mexico.

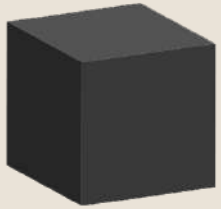
The **CIP standards establish a baseline set of requirements and best practices** that are the basis for maintaining the reliability of the **North American Bulk Electric System (BES)** and protecting it from cyber-attack.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

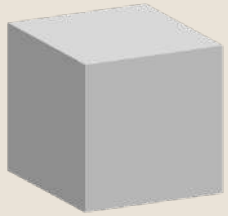
Standard	Topic
NERC CIP-002	BES Cyber System Categorization
NERC CIP-003	Security Management Controls
NERC CIP-004	Personnel and Training
NERC CIP-005	Electronic Security Perimeter(s)
NERC CIP-006	Physical Security of BES Cyber Systems
NERC CIP-007	Systems Security Management
NERC CIP-008	Incident Reporting and Response Planning
NERC CIP-009	Recovery Plans for BES Cyber Systems
NERC CIP-010	Configuration Change Management and Vulnerability Assessments
NERC CIP-011	Information Protection
NERC CIP-013	Supply Chain Risk Management
NERC CIP-014	Physical Security

Ethical Hacking Audit

Suntrack System Pentesting



BLACK BOX
Zero
knowledge



GREY BOX
Some
knowledge

VULNERABILITY CLASSIFICATION	DESCRIPTION
CRITICAL	Requires immediate attention and prioritization to prevent significant security breaches and protect system integrity, as their exploitation can allow attackers to gain full control over web application and server.
HIGH	Should be assessed and corrected whenever possible. If these vulnerabilities are exploited valuable information about the system is accessible and can be the door to other weaknesses.
MEDIUM	Minimal risk to data security but can serve as attack vector that might create new point of entry.
INFORMATIONAL	Information with preventive nature to continuously enhance security practices.

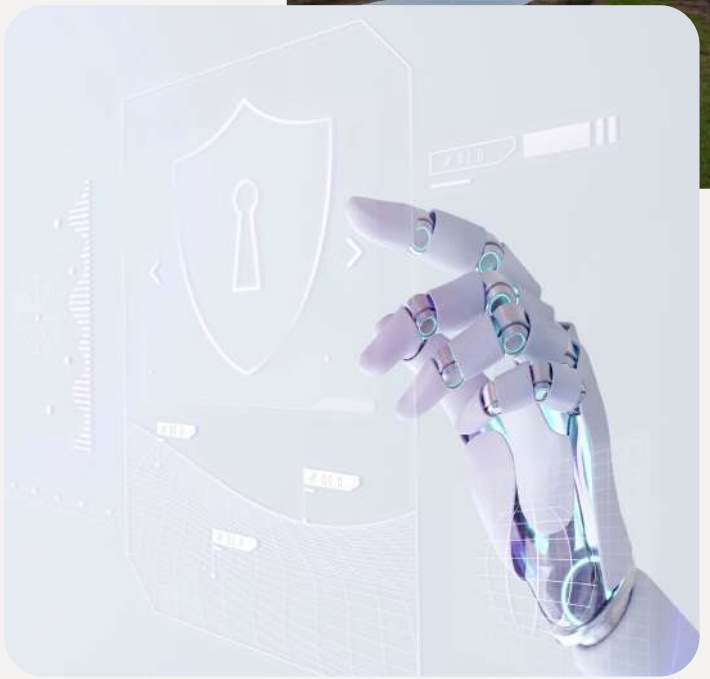
Suntrack System Pentesting

THE RESULTS OF THE PENTESTING

- **No vulnerabilities** in the **Zigbee communication**.
- **No vulnerabilities** in any access to the **IPC**.

- All vulnerabilities detected classified as **MEDIUM severity has not impact in Suntrack system** and all of them require **physical access** to be exploited.

Thank you!



suntrack

Follow us
on Linkedin!