Hardening the Energy Edge:

Smart Ethernet Switches Infrastructure for Resilient Solar Operations

Region: Spain

Moxa Products

Smart Ethernet Switches SDS-3006 Series

- Supports RSTP/STP, and MRP for network redundancy to ensure high network availability
- Supports EtherNet/IP, PROFINET, and Modbus TCP industrial protocols
- Supports MXstudio for easy, visualized industrial network management

Industrial Computers UC-1200A Series

- Armv8 Cortex-A53 dual-core 1 GHz processor
- 2 LAN, 2 RS-232/422/485, and 1 USB ports
- Rich set of programmable LEDs and a programmable button for easy installation and maintenance
- Moxa Industrial Linux with 10-year superior long-term support
- Compliance with IEC 62443-4-2 Security Level 2 requirements

Ethernet Remote I/Os ioLogik E1200 Series

- Supports RESTful API for IIoT applications
- Saves time and wiring costs with peer-to-peer communications
- Simplifies I/O management with MXIO library for Windows or Linux
- Wide operating temperature models available for -40 to 75°C (-40 to 167°F) environments

Background

In utility-scale solar energy, profitability is a game of precision. Solar trackers are used to dynamically tilting panels to capture every possible photon thereby maximizing the internal rate of return (IRR). At the center of this operation is the network control unit (NCU)—the brain that processes environmental data and executes tracking algorithms to optimize operations for maximum output.

However, as dispersed solar assets are increasingly brought online, they have moved to the frontline of a new, digital battlefield. For a leading global provider of solar tracker solutions, this threat became a reality when one of their major projects fell victim to a targeted cyberattack. By exploiting vulnerabilities at the edge, hackers were able to disrupt communications, causing widespread downtime. Beyond the immediate loss of revenue, the breach left expensive mechanical assets unable to enter stow mode exposing them to severe physical damage during high-wind events.

This incident was a wake-up call on the importance of cybersecurity in modern solar operations. Cybersecurity is not an auxiliary requirement; it is a prerequisite for operational continuity. To protect the power grid and their clients' investments, the solution provider realized they needed a platform where security and ruggedness were built into the solution, not added on as an afterthought.

Project Requirements

To support rapid scaling and consistent global deployments of energy assets, the project demanded a solution that addressed both technical and commercial complexities:

- **Immutable System Integrity:** A Secure Boot mechanism inspects the system before startup to ensure only trusted code is loaded during startup preventing unauthorized access by malware. Unused ports can be disabled and the system can run antivirus software for enhanced protection.
- **Regulatory Readiness:** Products that are built according to IEC 62443-4-1, EN 18031-1 and Cyber Resilience Act (CRA) requirements to satisfy stringent global mandates for critical infrastructure.
- **Compact Size and Industrial-Grade Reliability:** Compact hardware designed to fit into tight, outdoor-rated enclosures mounted on tracker pylons.
- **Long-term Asset Life Cycle Management:** 10-year maintenance to protect against security vulnerabilities throughout the power plant's life cycle

Why Moxa

- **Defense-in dept From the Beginning:** Moxa's IEC 62443-4-2 SL2 complaint UC-1200A establishes a hardware-based Root of Trust using the Secure Boot, which verifies digital signature of the software at startup, ensuring that the core of the system is untampered. Even if an attacker gained access to the network, they will not be able to compromise the core control logic because the threat is neutralizing before it reaches the application layer.
- **Streamlining Grid Compliance and Market Entry:** Moxa eliminates the trade-off between "Secure" and "Rugged." By providing components that are both secure-by-design and built for extreme environment, Moxa allowed the provider to bypass the cost and time of third-party hardening. This "ready-to-deploy" rugged and secure solution as platform accelerated their time-to-market for grid-critical projects.
- **A Decade of Resilience as a Standard:** In the energy sector, an asset is only as secure as its last security upgrade/patch. Through Moxa Industrial Linux (MIL), Moxa provides a 10-year security update window. This long-term commitment ensures that as cyber threats evolve, the system defenses evolve with them—significantly lowering the total cost of ownership (TCO) and safeguarding the long-term yield of the solar farm.

System Diagram

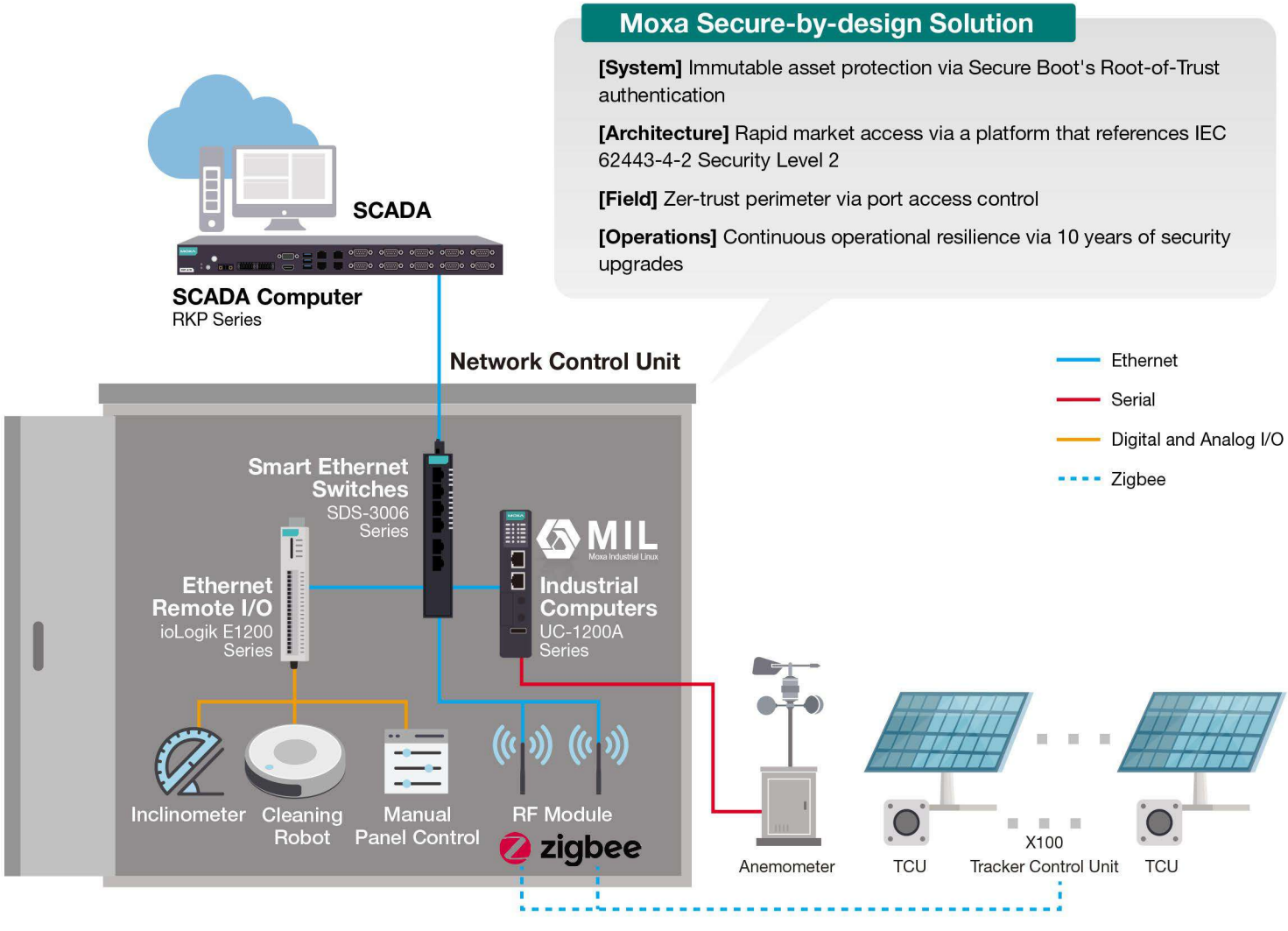
Moxa Secure-by-design Solution

[System] Immutable asset protection via Secure Boot's Root-of-Trust authentication

[Architecture] Rapid market access via a platform that references IEC 62443-4-2 Security Level 2

[Field] Zer-trust perimeter via port access control

[Operations] Continuous operational resilience via 10 years of security upgrades



ExcelNex Integrated Sdn Bhd (KL) +603-5636 0306 (KL) +6012-371 6198 sales@excelnex.com