PRAMAC STORAGE SYSTEMS

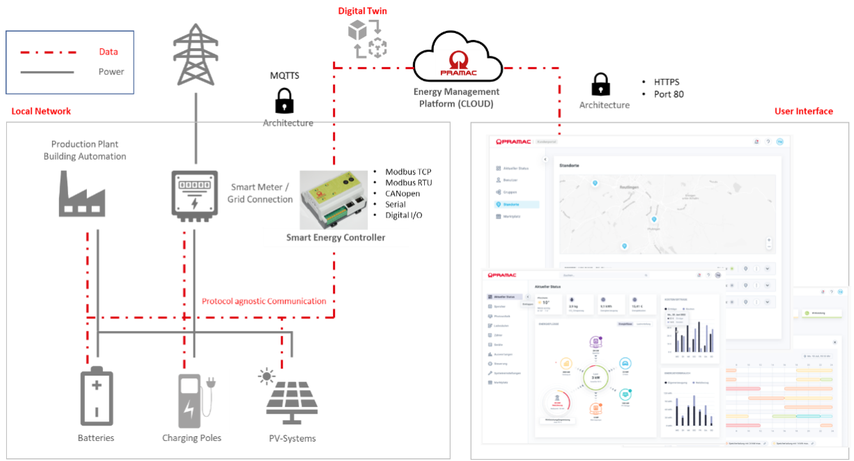
Cybersecurity in Energy Management Systems: Application of ISO 27001 and IEC 62443 within Pramac Smart Energy Controller (PSEC) and Platform

ISO 27001

- International standard for Information Security Management Systems (ISMS).
- Managing sensitive information to ensure confidentiality, integrity, and availability.
- Systematic approach for establishing, implementing, maintaining, and improving ISMS.
- Managing information security risks effectively.
- Enhancing trust with customers, partners and stakeholders

IEC 62443

- International standard for Industrial Automation and Control Systems (IACS) security.
- Safeguarding industrial networks and control systems against cyber threats.
- Guidelines and best practices for cybersecurity in industrial environments.
- Enforcing risk assessment, security policies, access control, network segmentation and incident response.
- Enhancing the resilience and reliability of industrial processes.



Pramac Smart Energy Platform - Architectural design and core concepts

Implementation of core concepts

Risk Assessment: Extensive risk assessment conducted on development environment (DEV) to identify and assess security risks related to the energy management platform. Identified severe security vulnerabilities successfully remediated in the development of the first productional release. Additional risk assessment for productional platform (PROD) planned.

Security Policies: PSEC equipped with TPM 2.0 module chip for best in class data security and transport encryption

Access Control: Access control implemented by a multi-tier user and user group rights management using *Keycloak* ensuring only authorized personnel have access to the energy management platform and data. „MQTTS only“ communication between edge controller and cloud platform and thus neither open ports nor access from outside the platform

Network Segmentation: PSEC with dedicated LAN ports for separation of internal operational (OT) and external network (IT). Communication of internal devices (e.g. inverter, BMS, grid meter) separated from customer network. Limitation of network communication between internal and external network via *Gatekeeper*.

Security Monitoring and Incident Response: Notification service within smart energy platform already implemented. Alerting service as immediate response mechanism in progress. Onboard UPS for safe shutdown and restart in case of security incidents and power failure.

Lifecycle Management: Secure deployment, configuration management, and regular rollout of incremental over-the-air (OTA) updates and patches on edge devices via *Mender*

Vendor Management: Extensive security and safety analysis of interfaces (e.g. Modbus RTU/TCP protocols, REST APIS) conducted prior to the integration of external hardware and software into both local controller and cloud platform

Continuous Improvement: Continuously improving information security processes and standards using a three-tier development process, from internal testing phase on simulated hardware and rollout on internal test hardware at the company site in Pfullingen (Germany) until final production release.

Creator: Jan Seidemann (MD) Date: 03.05.2024

PRAMAC Storage Systems GmbH
Marktstraße 185
D-72793 Pfullingen
Tel.: +49 (0) 7121-159-77-0
www.pramac-storage-systems.com