PROTELION

Use Cases

Highly Secure Communication for Critical Infrastructure

Recent research has shown that the utility sector is increasingly vulnerable to cyber attacks. Steps toward digitalization and the use of cloud services have revealed vulnerabilities in industrial control systems and sensors, which are used extensively in both energy and water utilities. Exciting new technologies and business models being deployed in the utility sector to improve customer service, reduce waste and enable efficiencies are creating a multitude of new vulnerabilities and attack surfaces. The potential consequences of a successful attack on automated or robotic systems could be catastrophic, including disruption of service, loss of sensitive data, degradation of service reliability and quality, not to mention the risks to public safety and health.

Duties and As-Is Situation for the Utility Sector

Extensive use of operational technology which was not designed to be connected to the Internet and lacks robust built-in security also for remote connectivity

Various utilities and power plants are connected together in highly dense and fragile energy transport grids, which are mostly unprotected and prone to cyber attacks

Wide use of unsafe ICS and SCADA systems, sensors as well as traditional networks and networks of other companies, including the ones of clients

Collecting system data from various sources, such as network traffic logs and endpoint devices (turbines, reactors, generators, water pumps etc.) which is transferred to a central computation center where it is processed and analyzed

Project Specification

Much of the data of critical infrastructures today is stored and deployed on cloud servers or data centers. This requires secure point-to-point connections with the respective servers and special monitoring of cloud-based operations

Nowadays, utilities urge to protect ICS and SCADA infrastructure, including IoT industrial systems, machine-to-machine interaction (M2M) and the more traditional legacy systems

Today, executives and field workers still use open, unsecured cell phones and tablets. Field diagnostic readouts and video inspection images of critical assets by drones are often transmitted over open communication channels that are highly vulnerable and need to be secured and protected

Project Implementation

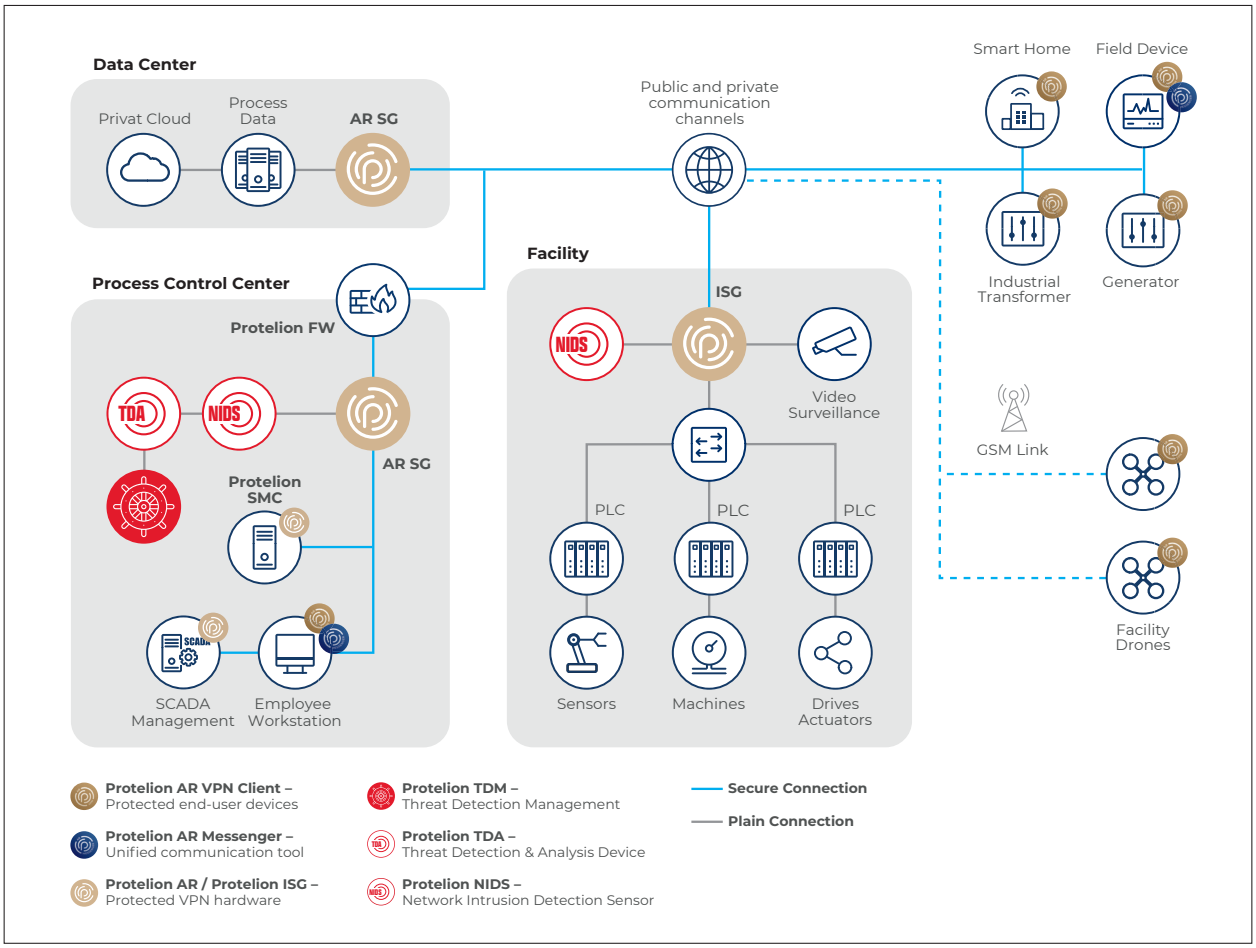
1 The Protelion Security Solutions provide secure and controlled access to the facility's video surveillance cameras and patrolling drones by protecting the transmission and exchange of their critical data and image information through Protelion's encryption algorithm

2 Protelion VPN Technology protects the utility production facilities and IT networks from unauthorized access to sensitive data, process control mechanism and critical assets when accessing via remote connections

3 Protelion Security Solutions protect endpoint devices, sensors, valves and SCADA networks against a multitude of cyber threats and therefore secure power production, distribution infrastructures industrial systems and machine-to-machine (M2M) interactions

4 The implemented Protelion TDR-System detects and analyzes malware activities in the network and provides fast real-time alerts to security officers. It can easily be integrated in an existing SIEM

Scheme for Critical Infrastructure



Protelion Features

Comprehensive Protection
Protelion Security Solutions offer comprehensive protection against a wide range of cyber threats, using advanced technologies and flexible, modular and cost-effective hardened platforms

Easy Use and Integration
Easy and seamless integration of Protelion Security Solutions within existing legacy networks, which still use old legacy devices in their systems

Certified AES Algorithm
The implemented, fast and efficient, certified military grade AES algorithm is particularly suitable for protecting industrial operations and processes that require low latency

Operational Availability
Protelion Security Solutions provide a protected utility production and distribution infrastructure as well as secure remote access to control and monitoring sensors. They also secure endpoint devices' firmware and sensitive update processes

PROTELION
Oberwallstrasse 24
D-10117 Berlin
+49 30 206 43 66-0
info@protelion.de
gov.protelion.com

GD – DKV23.1