SIEMENS

Reference

Maximum mobility

IWLAN for secure communication in power plants

The operation of power plants is subject to especially high security standards in order to protect people and the environment. Regular tests of the plant components installed in the outdoor area together with the IWLAN infrastructure and tablets make the operation and communication secure.

Operating, testing and maintaining hazardous areas of gas plants directly from the field saves the operator a substantial amount of time and labor costs. After all, most of the steps required to do this have to be performed in the hazardous area and confirmed in the process control system. Until now, several people and mobile operator terminals have been required to do this work. These terminals facilitate direct access to the process control system from the field, but have only limited mobility because of long LAN lines.

Bilfinger GreyLogix, a system specialist from Flensburg, has developed a cost-effective solution, which considerably simplifies this work, and fulfills the specific security requirements in the energy sector. This Siemens Solution Partner plans, configures and implements customized solutions for plant operation. Apart from process and control systems, the company also covers the engineering and plant consulting fields. The core of the new concept is the installation of an infrastructure for an industrial wireless LAN (IWLAN) in the hazardous area, and the use of conventional tablets as Thin Clients for operating the plant via remote desktop sharing.

Strict safety regulations apply to plants in which gases, vapors or mists could escape during the production, processing and storage of flammable materials. An atmosphere containing oxygen that explodes when ignited must be prevented from developing. Hazardous areas of the plant are therefore divided into zones in accordance with regulations.

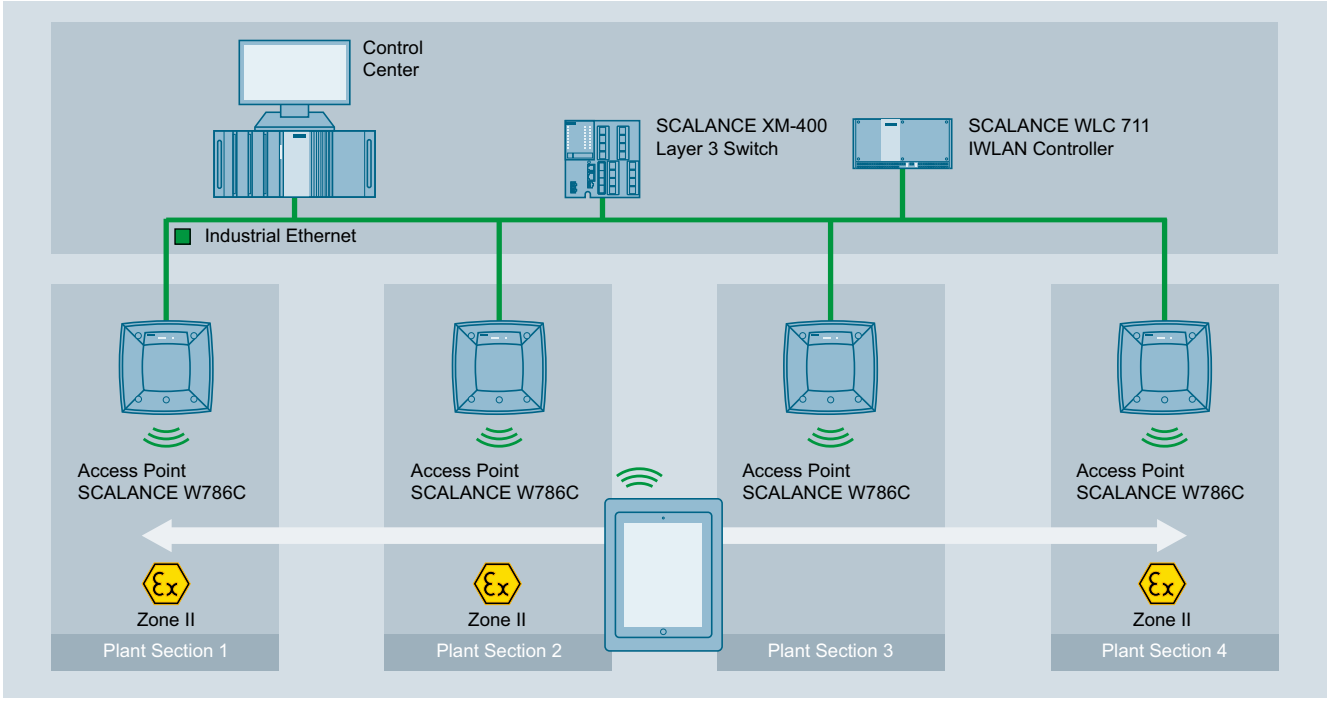
Access points with internal SCALANCE W786C-2IA RJ45 antennas permitted for outdoor installation are in use

Full access to all functions of the process control system

Siemens specialists worked with GreyLogix to plan and implement a communication infrastructure in the gas plant, which is controlled by a SIMATIC PCS 7 process control system. The maintenance of the highest security and safety standards in the process operations and communication infrastructure is of crucial importance to the operator. Components of the SCALANCE product family designed for the particular ATEX zones were therefore selected to construct an IWLAN in the hazardous area.

The project team chose a version of the RealVNC remote access solution to access the SIMATIC PCS 7 process control system from a tablet.. Carsten Schöling, project manager at GreyLogix, explained, "The process control system is located in the control room, and the mobile clients give us full access from the field to all functions. Furthermore, no information is stored on the tablets." The network can be designed so that the tablets access only a single extra computer, which is provided for that purpose in the control room. The advantages are that a work station is not blocked during access via the remote desktop sharing tool, and the access rights of the clients to SIMATIC PCS 7 can be precisely defined.

The heart of the communication infrastructure is a SCALANCE WLC711 IWLAN controller, that manages and coordinates up to 48 SCALANCE W700 access points (or 96 in redundant mode). The plant was brought into operation in the fall of 2014. Eight access points with SCALANCE W786C-2IA RJ45 internal antennas are permitted for outdoor installation. They are positioned round the plant so that they reliably cover the entire hazardous area. All configuration, management and diagnostic tasks are performed through the controller. Access points can be used in ATEX zone 2 without an enclosure because they have internal connectors and antennas. Additional devices can be retrofitted – for example if the plant is enlarged – at any time with little effort.



Components of the SCALANCE product family designed for the particular ATEX zones were used to install an IWLAN in the hazardous area

Multilevel security policy

The network infrastructure has a whole range of security measures to prevent unauthorized persons accessing sensitive data. The project manager added, "This starts with the physical separation of the IWLAN from the terminal bus, continues with the option of activating the entire network via the PLC at specific times only, through to encrypting the communication." All clients wanting access to the network must either log on via an encrypted connection with a regularly changing WPA2 key, or authenticate themselves by means of certificates from a radius server (Radius: Remote Authentication Dial-in User Service). Furthermore, the IWLAN controller only accepts access points with serial numbers that have previously been manually enabled. And finally, the communication between access points and WLAN controllers runs through encrypted tunnels to prevent cable-based attacks.

The administrative access to the IWLAN controller runs exclusively through a cable-connected device in the corresponding management VLAN, that is exclusively and directly to the controller in the protected part of the plant. Even if, despite the internal connectors, an attacker succeeds in dismounting an active access point, he cannot read out any configuration or connection data. The data is stored in a volatile memory, which means that it is automatically deleted if the supply voltage fails.

GreyLogix experts have exploited the possibilities of restricting rights to protect tablets and minimize the consequences of any loss. All devices can only be used for their previously defined purposes. They are password-protected and must be logged on to the RealVNC client. In turn, the process control system can only be accessed through a password-protected logon with automatic log out. If a device were to be lost, no relevant data could be found on it.

Installation of the IWLAN infrastructure in accordance with the site analysis

The system specialists from Flensburg analyzed the site together with Siemens consultants before the system was implemented. These experts determined on site all the values required for trouble-free installation. After the on-site inspection, the recorded data were analyzed and documented in a report. The analysis provided, for example, information about each access point for the installation of the IWLAN infrastructure. The investigation looked into not only the ambient conditions, but also the potential transmission locations, ranges and coverage of the systems. On the basis of these results, the network topology was designed, the suitable components were selected, and the suggested solution was worked out for the customer.

Summary

Round about twelve months after the commissioning of the pilot plant it can now be said that the Thin Clients are much more user-friendly and efficient than the mobile operator terminals. Plant drivers and maintenance personnel value above all the enormously increased freedom of movement, the faster connection to the process control system and the intuitive operation. During the course of the project, the plant operator got to know and value the technical competence of the GreyLogix experts. Together with the Siemens specialists, they performed the technical communication tasks optimally and competently in compliance with the high security standards from the planning through to commissioning. The practical and detailed knowledge of the process possessed by all team members also made a big contribution to the successful completion of the project.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit **www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Deutschland

PDF
Reference
FAV-399-2016-PD-PA
BR 0916 En
Produced in Germany

siemens.com/iwlan