SIEMENS

Referenz

Maximale Mobilität

IWLAN für Kommunikationssicherheit in energietechnischen Anlagen

Für den Betrieb von energietechnischen Anlagen gelten besonders hohe Sicherheitsstandards zum Schutz von Mensch und Umwelt. Die regelmäßigen Überprüfungen der im Außenbereich installierten Anlagenkomponenten sind mit IWLAN-Infrastruktur und Tablets betriebs- und kommunikationssicher möglich.

Die Bedienung, Prüfung und Wartung explosionsgefährdeter Bereiche gastechnischer Anlagen direkt aus dem Feld heraus bedeutet für die Betreiber einen erheblichen zeitlichen und personellen Aufwand. Schließlich müssen die meisten dafür erforderlichen Arbeitsschritte im Ex-Bereich durchgeführt und im Prozessleitsystem bestätigt werden. Bislang erfordern diese Arbeiten mehrere Personen und fahrbare Bedienterminals, die zwar einen direkten Zugriff auf das Prozessleitsystem aus dem Feld ermöglichen, aber aufgrund langer LAN-Leitungen nur eingeschränkt mobil sind.

Der Flensburger Systemspezialist Bilfinger GreyLogix hat eine kosteneffiziente Lösung entwickelt, mit der diese Arbeit deutlich vereinfacht und die speziellen Sicherheitsanforderungen im Energiesektor erfüllt werden. Der Siemens Solution Partner plant, projektiert und realisiert kundenindividuelle Lösungen für den Anlagenbetrieb.

Außer der Prozess- und Leittechnik deckt das Unternehmen die Bereiche Engineering und Anlagen-Consulting ab. Kern des neuen Konzepts ist der Aufbau einer Infrastruktur für ein Industrial Wireless LAN (IWLAN) im Ex-Bereich sowie der Einsatz von handelsüblichen Tablets als Thin-Clients zur Anlagenbedienung via Remote Desktop Sharing.

Für Anlagen, in denen bei der Herstellung, Verarbeitung und Lagerung von brennbaren Stoffen Gase, Dämpfe oder Nebel entstehen, die entweichen können, gelten strenge Sicherheitsauflagen. Denn es muss verhindert werden, dass in Verbindung mit Luftsauerstoff eine Atmosphäre entsteht, die bei Entzündung zur Explosion führt. Explosionsgefährdete Anlagenbereiche sind deshalb durch Verordnungen in Zonen eingeteilt.

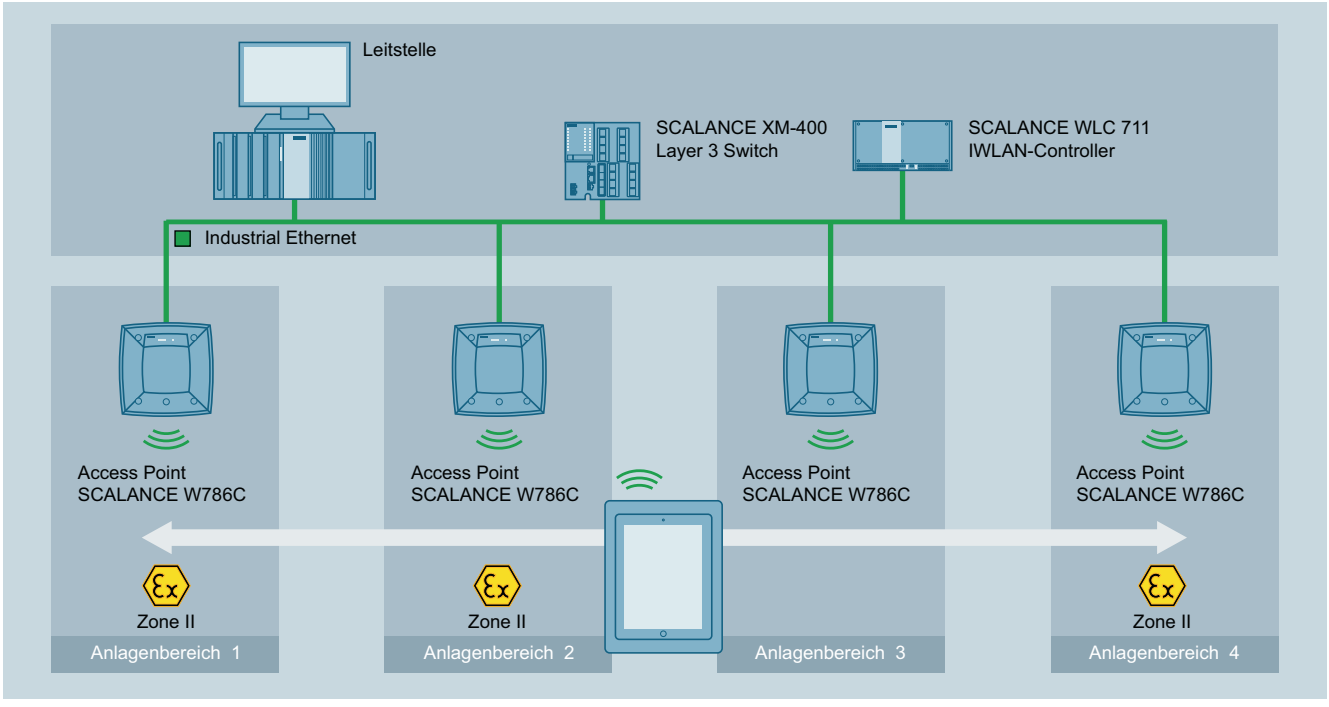
Im Einsatz sind die für die Außenmontage zugelassenen Access Points mit internen Antennen SCALANCE W786C-2IA RJ45

Voller Zugriff auf alle Funktionen des Prozessleitsystems

In der gastechnischen Anlage, deren Kommunikationsinfrastruktur GreyLogix in Zusammenarbeit mit Siemens-Spezialisten geplant und umgesetzt hat, steuert ein SIMATIC PCS 7-Prozessleitsystem den Anlagenbetrieb. Von zentraler Bedeutung ist für den Betreiber die Einhaltung höchster Sicherheitsstandards für die Prozessabläufe und für die Kommunikationsinfrastruktur. Für den Aufbau des IWLAN im explosionsgefährdeten Bereich wählte er deshalb Komponenten der SCALANCE-Produktfamilie, die für die jeweiligen ATEX-Zonen ausgeführt sind.

Bei der Frage, wie der Zugriff auf das Prozessleitsystem SIMATIC PCS 7 per Tablet erfolgen soll, entschied sich das Projektteam für eine Version der Fernzugriffs-Lösung RealVNC. „Das Prozessleitsystem steht in der Leitwarte, und wir haben mit den mobilen Clients aus dem Feld vollen Zugriff auf alle Funktionen. Hinzu kommt, dass auf den Tablets keine Informationen gespeichert sind“, erläutert Carsten Schöling, Projektverantwortlicher bei GreyLogix. Das Netzwerk kann so ausgelegt sein, dass die Tablets nur auf einen extra dafür bereitgestellten Rechner in der Leitwarte zugreifen. Der Vorteil: Während des Zugriffs über das Tool für Remote Desktop Sharing wird kein Arbeitsplatz blockiert und die Zugriffsrechte der Clients auf SIMATIC PCS 7 lassen sich exakt regeln.

Herz der Kommunikationsinfrastruktur ist ein IWLAN-Controller SCALANCE WLC711, der bis zu 48 Access Points (96 im Redundanzbetrieb) vom Typ SCALANCE W700 verwaltet und koordiniert. Im Fall der im Jahr 2014 in Betrieb genommenen Anlage sind es acht für die Außenmontage zugelassene Access Points mit internen Antennen vom Typ SCALANCE W786C-2IA RJ45. Sie sind in der Anlage so positioniert, dass sie den gesamten Ex-Bereich sicher abdecken. Sämtliche Konfigurations-, Management- und Diagnose- Aufgaben sind über den Controller realisiert. Access Points sind wegen innen liegender Stecker und Antennen ohne Umgehäuse in der ATEX-Zone 2 einsetzbar. Eine nachträgliche Integration weiterer Geräte – etwa bei einer Anlagenerweiterung – ist jederzeit mit geringem Aufwand möglich.



Für den Aufbau des IWLAN im explosionsgefährdeten Bereich kommen Komponenten der SCALANCE-Produktfamilie zum Einsatz, die für die jeweiligen ATEX-Zonen ausgeführt sind.

Mehrstufiges Sicherheitskonzept

Damit keine unbefugten Personen Zugriff auf sensible Daten haben, verfügt die Netzwerkinfrastruktur über eine ganze Reihe von Sicherheitsmaßnahmen. „Das fängt an bei der physikalischen Trennung des IWLAN-Netzes vom Terminalbus, geht über die Möglichkeit, das gesamte Netz über die SPS nur zu bestimmten Zeiten zu aktivieren und reicht bis zur Verschlüsselung der Kommunikation“, berichtet der Projektleiter. Alle Clients, die Zugriff auf das Netzwerk erhalten wollen, müssen sich über eine verschlüsselte Verbindung entweder mit einem regelmäßig wechselnden WPA2-Schlüssel anmelden oder mittels Zertifikaten über einen Radius-Server (Radius: Remote Authentication Dial-in User Service) authentifizieren. Zudem akzeptiert der IWLAN-Controller ausschließlich Access Points, deren Seriennummern zuvor manuell freigeschaltet wurden. Und schließlich läuft die Kommunikation zwischen Access Points und WLAN-Controller über verschlüsselte Tunnel, um kabelbasierten Angriffen vorzubeugen.

Der administrative Zugang zum IWLAN-Controller erfolgt ausschließlich per kabelgebundenem Gerät im entsprechenden Management-VLAN, also nur direkt am Controller im geschützten Bereich der Anlage. Sollte es einem Angreifer gelingen, einen aktiven Access Point trotz innen liegender Stecker zu demontieren, könnte er keine Konfigurations- und Verbindungsdaten auslesen. Die Daten befinden sich in einem flüchtigen Speicher, der bei Wegfall der Versorgungsspannung automatisch gelöscht wird.

Aufbau der IWLAN-Infrastruktur gemäß Standortanalyse

Im Vorfeld der Anlagenrealisierung führten die Flensburger Systemspezialisten gemeinsam mit Siemens-Beratern eine Standortanalyse durch. Diese Experten erfassten vor Ort alle notwendigen Werte, die für eine reibungslose Installation notwendig sind. Nach der Besichtigung wurden die aufgenommenen Daten analysiert und in einem Report dokumentiert. Die Analyse lieferte beispielsweise für jeden Access Point Angaben zum Aufbau der IWLAN-Infrastruktur. Die Umgebungsbedingungen wurden untersucht sowie potenzielle Sendestandorte, Reichweiten und Abdeckungen der Systeme ausgelotet. Basierend auf diesen Ergebnissen erfolgten das Design der Netzwerktopologie, die Auswahl der geeigneten Komponenten und die Erarbeitung des Lösungsvorschlags für den Kunden.

Fazit

Rund zwölf Monate nach der Inbetriebnahme der Pilotanlage lässt sich sagen, dass der Einsatz von Thin-Clients in puncto Benutzerfreundlichkeit und Effizienz einen Riesensprung im Vergleich zu fahrbaren Bedienterminals darstellt. Anlagenfahrer und Wartungspersonal schätzen vor allem die enorm gestiegene Bewegungsfreiheit, die schnellere Verbindung zum Prozessleitsystem und die intuitive Bedienung. Während des Projektablaufs hat der Anlagenbetreiber die Fachkompetenz der GreyLogix-Experten kennen und schätzen gelernt. Von der Planung bis zur Inbetriebnahme wurden die kommunikationstechnischen Aufgaben zusammen mit den Siemens-Spezialisten optimal und kompetent unter Berücksichtigung der hohen Sicherheitsstandards ausgeführt. Darüber hinaus trugen Praxisnähe und detaillierte Prozesskenntnis aller Teammitarbeiter maßgeblich zum erfolgreichen Projektabschluss bei.

Security-Hinweise

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts. Weitergehende Informationen über Industrial Security finden Sie unter
www.siemens.com/industrialsecurity

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

PDF
Referenz
FAV-399-2016-PD-PA
BR 0916 De
Produced in Germany

siemens.de/iwlan