SIEMENS

Referenz

Fertigungsnetzwerk transparent und sicher

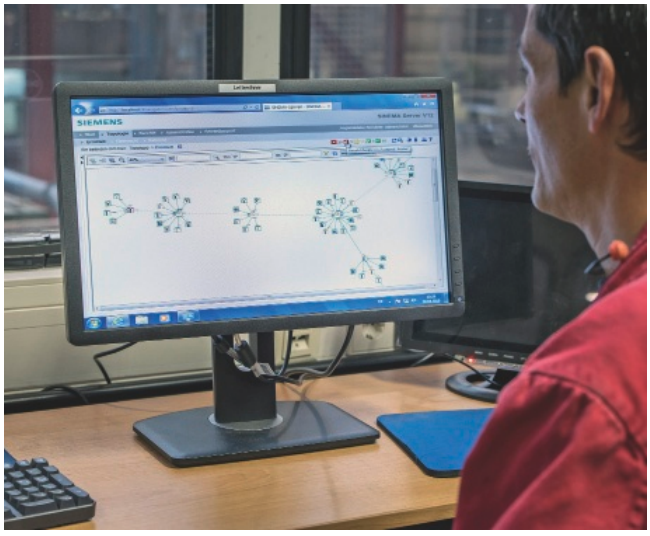
Skalierbare Netzwerktechnik für transparente, zugriffs- und fehlersichere Produktion von Alu-Profilen

Mit industriell zertifizierter, skalierbarer Netzwerktechnik aus einer Hand realisiert ein Hersteller von Aluminiumprofilen einen performanten, horizontal und vertikal durchgängigen Datenfluss und damit hohe Transparenz in seiner Produktion. Darauf abgestimmte IT-Security-Baugruppen bieten wirksamen Schutz vor unautorisierten Zugriffen von innen und außen. Wichtig war und ist die einfache, flexible Integration unterschiedlichster Kommunikationsebenen und -medien.

Seit 1958 werden in Rackwitz bei Leipzig Strangpressprofile (Halbzeuge) aus Aluminium hergestellt, veredelt und weiterbearbeitet. Das traditionsreiche Presswerk ist heute eines der leistungsstärksten der weltweit agierenden Sapa Group, einem Joint-Venture der Marktführer Sapa und Hydro Extruded Products. Am Standort Rackwitz produziert die Sapa Extrusion Deutschland GmbH auf zwei vollautomatisierten Presslinien (8 Zoll und 10 Zoll) hochwertige Aluprofile für unterschiedlichste Anwendungen.

Schon zu Beginn setzte Sapa auf Technik von Siemens: Die SCALANCE Industrial Wireless LAN (IWLAN)-Geräte sorgen dafür, dass die bisher störanfällige optische Kommunikation im Werk entlang der Profilziehstrecken bei der Aluminium-Verarbeitung nun hoch verfügbar und fehlersicher ist. Neue Anforderungen bezüglich Echtzeitkommunikation und PROFINET-Anbindung im Produktionsumfeld, um die Produktivität weiter zu steigern, machten eine Erneuerung der Netzwerk-Infrastruktur notwendig.

Auf zwei Strangpressen fertigt Sapa Extrusion Deutschland im Werk Rackwitz hochwertige Aluminiumprofile für unterschiedlichste Anwendungen, veredelt und bearbeitet diese.



Mit der Netzwerk-Management- und Diagnose-Software SINEMA Server behält der Profilhersteller künftig immer den Überblick über sein Produktionsnetzwerk.

Im Rahmen der CE-Zertifizierung seiner Erzeugnisse hat Sapa bestimmte Produktionsbedingungen im Werk überprüft. Dabei wurde gemeinsam mit den Fachberatern von Siemens, dem langjährigen Ausrüster des Herstellers für Elektro- und Automatisierungstechnik, auch ein sogenannter Security Quick-Check durchgeführt. Generell sollte damit die Verfügbarkeit des gesamten Netzwerkes untersucht werden, um das Risiko potenzieller Systemausfälle zum Beispiel durch Cyber-Attacken auf die Produktionssysteme beurteilen zu können. Die Security-Analyse hat dann ergeben, dass die Industrietauglichkeit einzelner Netzwerkkomponenten sowie der Zugriffsschutz auf Switches, PCs, Steuerungen und Kommunikationsprozessoren im Feld optimiert werden kann. Ebenso verhält es sich im Bereich der fehlersicheren Kommunikation beim Betrieb dreier Laufkatzen für den Transport von Presswerkzeugen und Schrott. Daraufhin wurden konkrete Maßnahmen abgeleitet, zusammen mit dem Ausrüster praktikable Lösungen erarbeitet und teilweise schon umgesetzt.

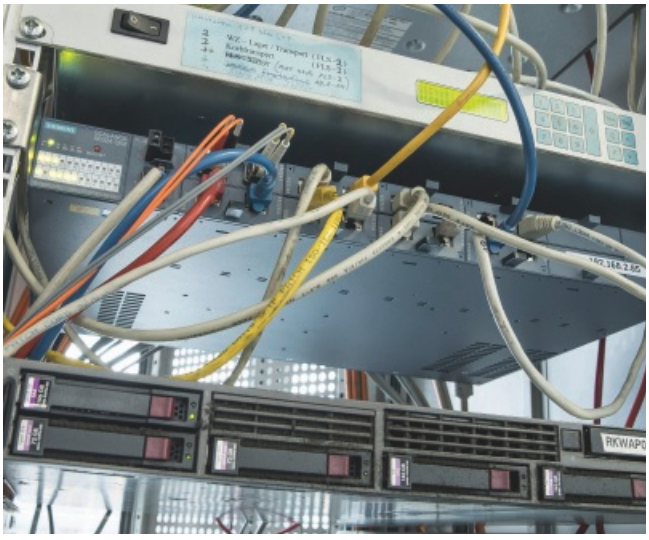
Sicherheit wird transparent –
Security Quick-Check zeigt Schwachstellen

Ergebnis des Security Quick-Checks von Siemens ist unter anderem eine Bestandsaufnahmen zu wesentlichen Verfügbarkeits- und Sicherheits-Anforderungen, die einen schnellen Überblick über den Stand der Dinge auf verschiedenen sicherheitsrelevanten Gebieten und potenzielle Risiken aufzeigt. Diese können bewertet und gezielt Lösungsmöglichkeiten erarbeitet werden.

Netzwerk-Management mit System

Eine der ersten Maßnahmen war der Einsatz des Netzwerk-Management- und Diagnosesystems SINEMA Server von Siemens. Mit dieser Software konnte sich der Betreiber schnell und komfortabel einen Überblick über das „gewachsene" Produktionsnetzwerk verschaffen sowie es permanent überwachen. Das einfach per Webbrowser nutzbare System erkennt automatisch klassische und industrielle Netzwerkkomponenten, visualisiert (in der aktuellen Version V13) automatisch doppelt vergebene IP-Adressen im Netzwerk und beugt damit zuverlässig Konflikten vor. Es zeigt aktuelle Zustände beliebig filterbarer Netzwerkteilnehmer übersichtlich an und ermöglicht individuelle Reports und Analysen. Die Ergebnisse können über Web-Mechanismen auf HMI-Systemen visualisiert, Reports beispielsweise per E-Mail automatisch an ausgewählte Empfänger versendet und Störungen per SMS gemeldet werden.

Das Programm überwacht eine einmal erfasste Infrastruktur und meldet jede Änderung daran. Mit diesen Mitteln konnte das Netzwerk den Bedürfnissen sowohl der Produktion als auch der IT-Spezialisten im Unternehmen entsprechend umgestaltet werden.



Neun vollmodulare managed Industrial Ethernet Switches SCALANCE XR324-12M von Siemens bilden einen performanten und zuverlässigen Backbone in der Profilproduktion.

Zum Teil sind die Netzwerkteilnehmer über unterlagerte managed Switches SCALANCE X-200 in den Schaltschränken an den Backbone angebunden.

Zuverlässiger Produktions-Backbones mit SCALANCE X-300

Als Ergebnis des Netzwerk-Monitorings mit SINEMA Server wurde ein industriegerechter, das heißt hoch performanter, robuster und zuverlässiger Produktions-Backbone basierend auf vollmodularen managed Industrial Ethernet Switches SCALANCE XR324-12M eingerichtet. Für erweiterte IT-Funktionen sorgen die robusten SCALANCE XR-300 Industrial Ethernet Switches von Siemens. Nach einem kurzen Testbetrieb mit einem dieser Switches wurden vorhandene, nicht explizit für den industriellen Einsatz konzipierte Geräte anderer Hersteller ersetzt, so dass inzwischen neun XR-300-Switches einen stabilen, einfach erweiterbaren Produktions-Backbone bilden. Dieser ist derzeit noch nicht zu einem redundanten Ring geschlossen, was sich aber jederzeit nachträglich einrichten lässt. Die Verfügbarkeit kann damit weiter erhöht werden. Ebenso ist die Anbindung an überlagerte Systeme auf der Unternehmensebene möglich.

„Für die Rack-Switches haben wir uns entschieden, weil diese in die vorhandenen 19"-Schränke passten und weil sich damit Teilnehmer über unterschiedlichste Medientypen, optisch oder elektrisch, einfach ins Netzwerk integrieren ließen und lassen", sagt Andreas Steinberg, der bei Sapa im Produktionsumfeld Verantwortliche für Instandhaltung und Automatisierungstechnik. Die Geräte sind mit zwölf Ports für (in diesem Fall frontseitig) steckbare Medienmodule mit jeweils zwei Ports ausgestattet. Damit sind auch zukünftige Erweiterungen einfach möglich, da die vorhandene Infrastruktur einfach ergänzt werden kann.

Die aktuell rund 200 relevanten Teilnehmer im Feld sind zum Teil direkt, zum Teil über unterlagerte managed Industrial Ethernet Switches der Baureihe SCALANCE X-200 in dezentralen Schaltschränken an den Backbone angebunden. So ist produktionsweit horizontal und vertikal durchgängig robuste und zuverlässige Kommunikation gewährleistet.

Die eingesetzten Switches von Siemens haben zudem einen Steckplatz für einen sogenannten C-PLUG, ein Speichermedium, auf dem die jeweils aktuelle Gerätekonfiguration gesichert ist. Dieses lässt sich durch einfaches Umstecken schnell auf ein Austauschgerät übertragen. Bei Siemens könne man zudem sicher sein, auch noch nach Jahren Ersatzteile für alle Komponenten zu bekommen, so die Verantwortlichen im Presswerk.

Zugriffsschutz von innen und außen

An den Schnittstellen zur Bürowelt sorgen spezielle Security Module der Familie SCALANCE S mit integrierter Firewall für eine Trennung der Produktionssysteme, insbesondere vom World Wide Web. So haben nur autorisierte interne und externe Nutzer Zugriff auf die Netzwerkkomponenten in der Produktion. Damit ist ein sicherer, aber auch komfortabler Geschäftsbetrieb gewährleistet. Auch die Fernwartung von Systemen externer Zulieferer ist möglich, was für die Verfügbarkeit entscheidend sein kann. Standard ist zudem ein geschützter Zugang des Wartungspersonals „remote" über VPN-(Virtual Private Network)-Tunnel, um bei Störungen schnell eingreifen zu können.

Ohne diese Trennung von Unternehmens- und Produktionsnetz sei es durchaus denkbar, dass sich beim Ausfall eines Teilnehmers im Unternehmensnetz das RST-(Rapid Spanning Tree)-Protokoll automatisch eine neue Route über das Produktionsnetz sucht, was unter ungünstigen Umständen die Netzwerklast derart erhöht, dass dort die Funktionalität nicht mehr gewährleistet werden kann. Auch das Missbrauchsrisiko sei ohne die Trennung höher. „Deshalb sind nur bestimmte Kommunikationsprotokolle und Teilnehmer zugelassen und auch Zugriffsrechte auf ein notwendiges, sicheres Maß reduziert, was mit der Siemens-Netzwerktechnik umzusetzen war", erklärt Karsten Konschak, der IT-Verantwortliche bei Sapa am Standort. Zudem sorgt die Echtzeitfähigkeit des Netzwerkes unter anderem für eine fehlersichere Kommunikation.

Das RCoax Cable von Siemens ist funkendes Antennenkabel, das entlang der Schienenwege verlegt wurde und ein WLAN-Feld über die Verfahrstrecke sicherstellt.

RCoax als einfache Lösung

Einfach in das große Ganze integrieren ließen sich auch zuvor beziehungsweise parallel modernisierte Teillösungen am mechanischen Rückgrat der Produktion, dem Einschienenhängebahnsystem für den Transport der Presswerkzeuge vom zentralen Hochregallager zu den Vorwärmöfen und Pressen, sowie von Schrott. Das ursprüngliche optische Kommunikationssystem war immer störungsanfälliger geworden und erfüllte auch nicht mehr die Anforderungen an die funktionale Sicherheit beim Verfahren von drei Laufkatzen in bestimmten, von Werkern zugänglichen Zonen. Die ebenfalls gemeinsam und mit SCALANCE IWLAN-Komponenten von Siemens umgesetzte Lösung ermöglicht störungsfreie fehlersichere, priorisierte Kommunikation via PROFINET/PROFIsafe und damit sicheres Arbeiten unter allen Umständen.

Dazu sind entlang des Schienenwegs bis zu 130 m lange, sogenannte RCoax-Kabel (Leckwellenleiter) von Siemens angebracht. Diese RCoax Cable von Siemens sind IWLAN-Antennen, die entlang der Verfahrstrecke verlegt wurden und ein homogenes WLAN-Feld über den gesamten Schienenweg sicherstellen. Sie übertragen fehlersicher über ein exakt definiertes Funkfeld die Signale der IWLAN-Clients im Verband der mitfahrenden SIMATIC-Steuerungen auf den Katzen zum zugehörigen IWLAN Access Point und umgekehrt.

Leistungsfähige Netzwerktechnik unabdingbar

Anders als in der Bürowelt stellt Netzwerktechnik für die Produktion deutlich höhere Anforderungen hinsichtlich Performance, Zuverlässigkeit und auch Verfügbarkeit. „Die Zuverlässigkeit der Kommunikation ist heute wichtiger denn je, da wir durch die konsequent auftragsorientierte Fertigung kleinere Losgrößen und somit häufigere Produktionswechsel und damit auch umfangreicheren Datenaustausch haben. Ebenso zum nachfolgenden Warenkorb-Transportsystem und zum überlagerten Leitrechner“, so Steinberg. Die fortschreitende Ablösung von PROFIBUS- durch PROFINET-Komponenten wird die Zahl der Netzwerkteilnehmer im Werk zwangsläufig weiter steigen lassen. Dadurch wird ein leistungsfähiges Netzwerk-Management unabdingbar sein, will man mit angemessenem Aufwand den Überblick behalten.

Mit den bisher realisierten Schritten und den Komponenten von Siemens sehen sich die Verantwortlichen bei Sapa in Rackwitz diesbezüglich auf einem guten Weg. Der Mehrwert dieses Gesamtpakets, bestehend aus Netzwerktechnik von IWLAN-Geräten über Switches bis hin zum Monitoring-System SINEMA Server, und der neuen Netzwerk-Infrastruktur, auf Basis der Ergebnisse des Security-Checks, zeichnet sich aus: Das Produktionsnetz ist damit hoch performant, hochverfügbar und transparent geworden. Weitere Modernisierungs- sowie Integrationsprojekte sind bereits angelaufen.

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-193-2016-PD-PA
BR 082016 De
Produced in Germany

siemens.de/scalance