




SIEMENS



Fachartikel



Kranhafen-Netzwerk professionell geplant und remote in Betrieb genommen

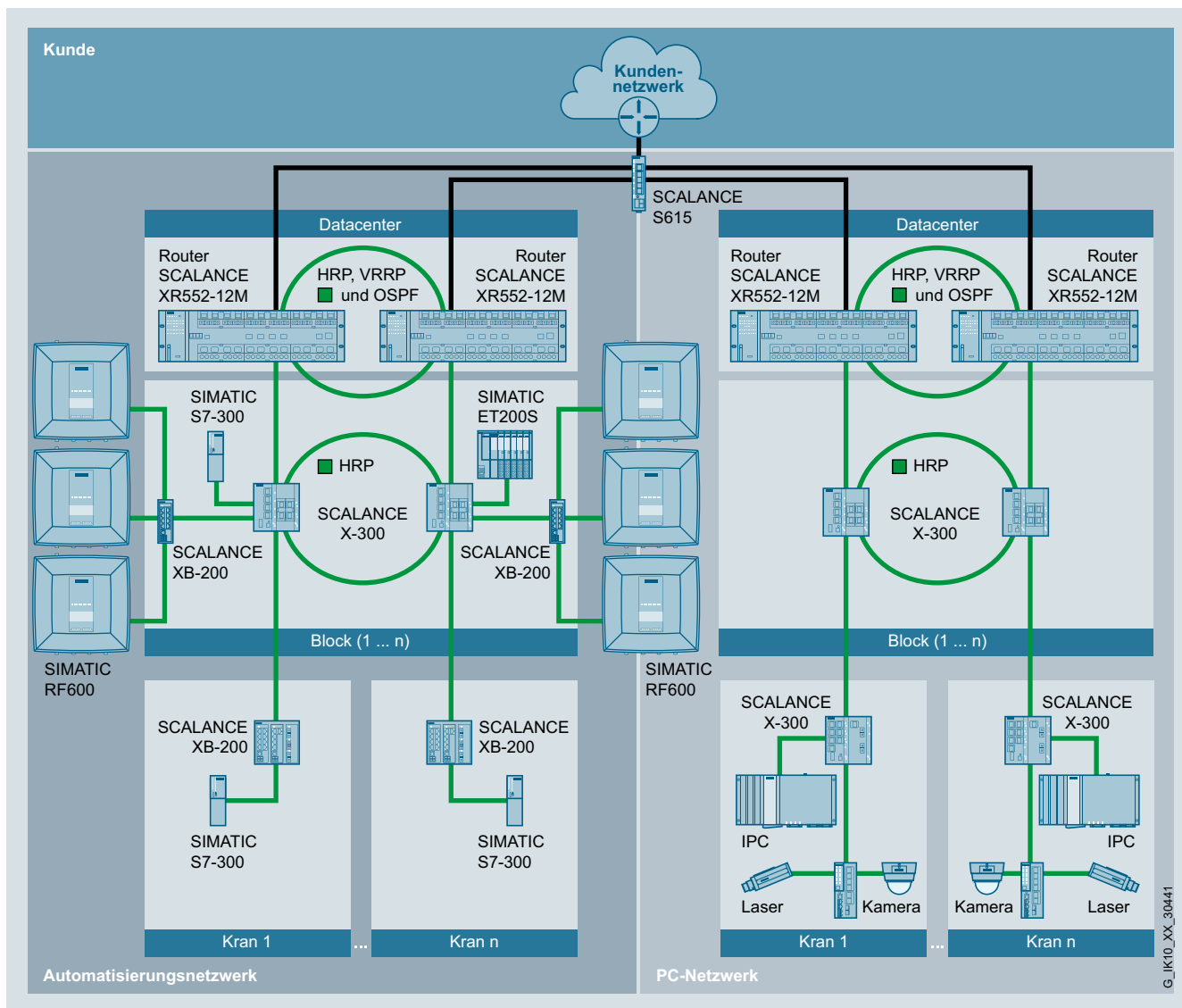
Das Netzwerk für eine Vielzahl automatischer Container-Stapelkrane haben Spezialisten von Siemens Professional Services im Detail geplant und abgesichert, Geräte vorkonfiguriert, sukzessive in Betrieb genommen und die Abläufe optimiert. Das weitgehend redundante, geroutete Netzwerk mit eindeutiger IP-Adressierung von über 1.000 Teilnehmern und strikter Trennung der Automatisierungs- und PC-Systeme ist hoch verfügbar. Es trägt damit maßgeblich zur Leistung des Container-Terminals bei.

Über 70 Prozent der weltweit gehandelten Stückgüter werden aktuell in ISO-Containern per Schiff, Bahn und Lkw transportiert. Zentren für einen effizienten Warenumsatz sind dabei Container-Terminals, die es in jedem größeren Hafen gibt. Entscheidend für performante Prozesse darin sind Stapelkrane, die die Container zum vorgesehenen Lagerplatz bringen und von dort für den Weitertransport wieder abholen. Aus Kosten- und Sicherheitsgründen geschieht dies immer häufiger vollautomatisch.

Für zeit- und wegoptimierte, kollisionsfreie Abläufe braucht es neben einem performanten Lagerverwaltungssystem und robuster Kran-Automatisierung auch ein auf die spezifischen Belange ausgerichtetes, zuverlässiges Kran-Netzwerk. Eines,

das Fahraufträge schnell, störungsfrei und manipulationssicher zum jeweiligen Kran überträgt. Die Qualität der Automatisierung wie der Vernetzung ist entscheidend für die Verfügbarkeit der Gesamtanlage. Fällt nur ein Teil davon aus, können Fahrbefehle nicht mehr übermittelt und schlimmstenfalls nicht mehr ausgeführt werden.

Um diesbezüglich auf Nummer sicher zu gehen, setzt(e) ein renommierter Anbieter von Container-Handling-Lösungen beim Aufbau eines neuen Hafen-Terminals auf performante Kran-, Automatisierungs- und Netzwerktechnik von Siemens. Verteilt auf mehrere Lagersegmente mit jeweils mehreren Lagerblöcken, werden im Endausbau eine Vielzahl Stapelkrane vollautomatisch agieren. Bindeglied zwischen Ship-to-Shore-Kranen und



G_IK10_XX_30441

Kernkomponenten der mit Siemens Professional Services realisierten Netzwerklösung sind über 300 Switches der Baureihen SCALANCE X-500, X-300 und X-200 für die strukturierte, weitgehend redundante Kommunikation unter mehr als 1.000 Teilnehmern.

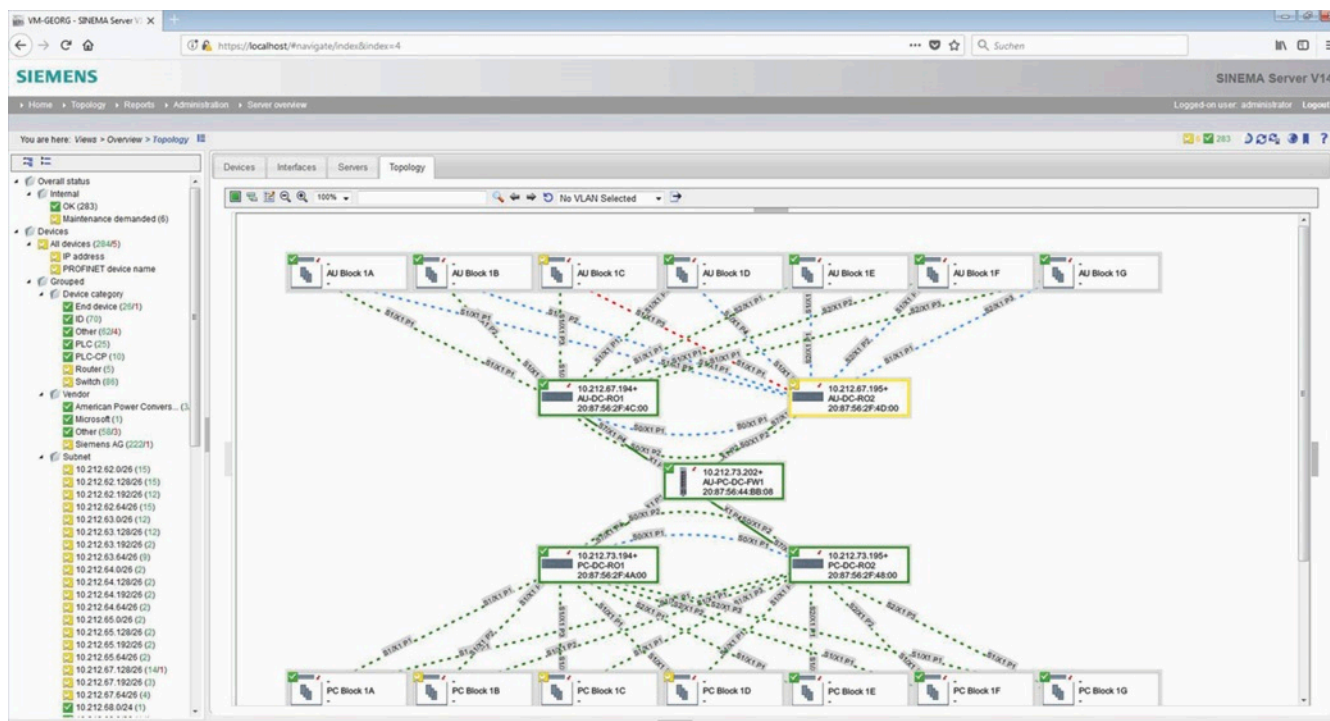
Lager sind bemannte Portalhubwagen, die die Container übernehmen und zum vorgegebenen Übergabepplatz transportieren. Dabei spielt auch RFID-(Radio Frequency Identification)-Technologie von Siemens eine wichtige Rolle.

Mit vereinten Kompetenzen zur hoch verfügbaren Lösung

Mit der Automatisierung und Vernetzung der Krane und der Anbindung an das Lagerverwaltungssystem betraut wurde das Siemens Expert House in Bremen, das sich für den Bereich Netzwerktechnik Spezialisten aus dem konzern-eigenen Team Industrial Networks Professional Services ins Boot geholt hat. Dabei wurde eine auf die Anforderungen der Anwendung maßgeschneiderte, individuell strukturierte und segmentierte, über weite Strecken redundante Lösung erarbeitet, die höchste Verfügbarkeit und Ausfallsicherheit bietet. Dabei wurden auch bewusst zwei separate, vom Datacenter bis zur Kranebene physikalisch getrennte Netz-

werke für Automations- und PC-Anwendungen eingerichtet. So beeinträchtigt beispielsweise die datenintensive Kameraüberwachung keine der anderen Anwendungen und Gewerke. Ein Ausfall einer Netzwerkkomponente oder Leitung in einem Subnetz wirkt sich ebenfalls nur begrenzt auf den dazugehörigen Block aus. Redundante Ringstrukturen und Redundanzmechanismen wie High Speed Redundancy Protocol (HRP) und Standby-Kopplung, Virtual Router Redundancy Protocol (VRRP) und das Routing-Protokoll Open Shortest Path First (OSPF) realisieren kürzeste Rekonfigurationszeiten im Fehlerfall – und damit höchste Verfügbarkeit des gesamten Kran-Netzwerks.

Dreh- und Angelpunkt der in drei Ebenen gegliederten Netzwerklösung sind jeweils zwei zu einem redundanten Ring verbundene Layer-3-Router SCALANCE XR552-12M im Datacenter des Betreibers. Ein Paar für die Vernetzung der Automationskomponenten wie Steuerungen, Peripheriebaugruppen und Antriebe, ein weiteres für PC-basierte Anwendungen wie Serversysteme für die Kransteuerung,



Über die Managementplattform für Remote Networks SINEMA Remote Connect konnten die Netzwerkgeräte sukzessive aus der Ferne in Betrieb genommen werden. Mit der Netzwerkmonitoring und -diagnosesoftware SINEMA Server (im Bild) lässt sich die gesamte Netzwerklösung komfortabel aus der Ferne überwachen.

Kameraüberwachungs- und Lasersensoriksysteme. Alle vier Router sind über eine Industrial Security Appliance SCALANCE S615 angebunden an den überlagerten Backbone des BetreiberNetzwerks. So sind alle Gewerke des Kran-Netzwerks zuverlässig geschützt vor unautorisierten Zugriffen auch aus dem Internet heraus. Über Single-Mode-Glasfaserleitungen kommunizieren die Router mit der unterlagerten, ebenfalls ringredundant aufgebauten Blockebene, bestehend aus jeweils zwei Layer-2-Switches der Baureihe SCALANCE X-300 pro Block in eigenen VLAN-Segmenten. In diesen interagieren nur die logisch zusammengehörenden Teilnehmer eines Blocks, alle anderen werden nicht beeinträchtigt. Mit weiteren vier Switches der Baureihen X-300 und X-200 für jeden Kran erhöht sich die Zahl der verbauten SCALANCE-Geräte auf über 300 und die der Netzwerkteilnehmer auf deutlich über 1.000. Um sämtliche Teilnehmer schnell identifizieren und ansprechen zu können, wurde jedem eine eindeutige IP-Adresse zugeordnet.

Getestet und vorkonfiguriert auf die Baustelle

Um möglichst früh hohe Funktionssicherheit zu erlangen, hat das Expert House die vorgesehene Vernetzung mit allen Geräten für den Betrieb eines Kranpaars in Bremen aufgebaut und sämtliche Abläufe intensiv getestet. Die optimierten Konfigurationen konnten gesichert und mit angepassten IP-Adressen einfach auf weitere Geräte übertragen werden. Die Spezialisten der Professional Services haben schon in dieser frühen Phase die Managementplattform für Remote Networks SINEMA Remote Connect und die Software für Netzwerkmonitoring und -diagnose, SINEMA Server genutzt, was sich im weiteren Projektverlauf als äußerst nützlich erweisen sollte.

Sukzessive Inbetriebnahme und Optimierung aus der Ferne

Über die SCALANCE Firewall und eine abgesicherte VPN-(Virtual Private Network)-Verbindung konnten die Geräte auf der Baustelle via SINEMA Remote Connect in Betrieb genommen werden, und zwar immer genau dann, wenn wieder ein Kran aufgebaut und dafür bereit war. Dadurch hat sich die ursprünglich vorgesehene, zeitlich vom Kranbau abhängige und somit schwer planbare Unterstützung vor Ort erübrigt. Unterstützt durch SINEMA Server konnten Siemens Netzwerkspezialisten während der schrittweisen Inbetriebnahme auftretende Fehler und Problemstellungen diagnostizieren und erkennen, um eine rechtzeitige Behebung zu ermöglichen.

Vom Einsatz der Siemens Software profitier(t)en letztendlich alle Beteiligten. Per SINEMA Remote Connect kann das Siemens Expert House seine Automatisierungssysteme von Bremen aus im TIA Portal projektieren und programmieren, auch Firmware-Updates lassen sich auf diesem Weg einfach einspielen. SINEMA Server bietet umfassende Möglichkeiten für Netzwerkmonitoring, -diagnose und -wartung. Das komfortable Handling lässt auch den Terminal-Betreiber überlegen, die Siemens-Lösung zusätzlich zu bereits vorhandenen Tools einzusetzen. Durch die Arbeit mit SINEMA Server konnten wertvolle Erkenntnisse zur Weiterentwicklung der Software gewonnen werden.

Professional Services: Umfassende Unterstützung in allen Belangen industrieller Kommunikationsnetzwerke

Gemeinsam mit branchen- und IT-erfahrenen Siemens-Solution-Partnern bietet Siemens aufeinander abgestimmte Industrial Networks Professional Services für bestehende wie neue industrielle Kommunikationsnetzwerke. Das Team wurde eigens dafür etabliert, Hersteller wie Betreiber von Maschinen und Anlagen mit Netzwerktechnik von Siemens und anderen Ausrüstern in jeder Lebenszyklusphase zu unterstützen, von der Planung bis zum Service. Auf Wunsch beraten erfahrene Spezialisten bei der Auslegung industriegerechter LAN- sowie WLAN-Netzwerkinfrastrukturen und -mechanismen und übernehmen auch die Inbetriebnahme sowie die Optimierung vor Ort. Darüber hinaus vermitteln verschiedene Standard- und kundenindividuelle Schulungen fundiertes Produkt- und Netzwerkfachwissen.

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 <https://www.siemens.com/industrialsecurity>

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
Fachartikel
DI-PA-18/19-7
BR 0619 4 De
Produced in Germany
© Siemens 2019

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Erzeugnisbezeichnungen können Marken oder Erzeugnisnamen der Siemens AG oder anderer, zuliefernder Unternehmen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

www.siemens.de/industrial-networks-services