

Über die Verwundbarkeit industrieller Anlagen

Wartungs- und Servicezugang sichern



Halle 9,
Stand 141

In der Investitionsgüterindustrie wird der Service immer wichtiger. Er wird zur lukrativen Ertragsquelle und zum wichtigen Kundenbindungsinstrument. Aktuell besteht allerdings noch großer Handlungsbedarf: bei der Effizienz der Serviceorganisation, der Nutzung neuer technischer Möglichkeiten und der Verbesserung des Sicherheitsstandards vernetzter Anlagen.

Service ist der Erfolgsträger der Zukunft. Die häufig sehr lange Lebensdauer von Investitionsgütern sorgt in Verbindung mit der zunehmenden Komplexität der Anlagen und Systeme für einen steigenden Servicebedarf und höhere Ertragspotenziale. Der durchschnittliche Serviceanteil am Gesamtumsatz im Maschinen- und Anlagenbau, der Elektro- und ITK-Branche wird von aktuell 27% nach Schätzung des Consultingunternehmens Impuls bis zum Jahr 2015 auf bis zu 40% steigen. Mit Nettoerträgen von bis zu 30% Prozent ist der Service die „Erfolgssperle“ der Investitionsgüterindustrie, so schreibt die Studie „Exzellenz im internationalen Service-Controlling“ des VDMA. Gleichzeitig verweist die Studie darauf, dass 65% der Kunden den Lieferanten wechseln, weil sie mit dem Service unzufrieden sind.

Mechanik, Elektronik, Software Komplexität steigt

Verbindliche Service Levels, immer kürzere Reaktionszeiten und schnelle Fehlerdiagnosen für weltweit installierte Systeme und Anlagen sind inzwischen ohne Fernwartung beziehungsweise Teleservice kaum noch denkbar. Führende Werkzeugmaschinenhersteller stellen ihre Produkte je nach Komplexität bereits zu 60% bis 90% mit Funktionen wie Teleservice oder Selbstüberwachung aus. Die Komplexität aus der Verknüpfung von Mechanik, Elektronik und Software wird aus Sicht des Verbands deutscher Werkzeugmaschinenhersteller (VDW) weiter steigen. Gleichzeitig wird die Software nach Schätzungen des VDW künftig für 90% der Maschinenstillstände verantwortlich sein. Um dieser Komplexität bei

Wartungs- und Servicezugriffen aus der Ferne noch gerecht werden zu können, steigen die technischen Anforderungen der Servicezentralen sprunghaft an. Der Ruf nach mehr Bandbreite für Software-Updates, für Anwendungen wie Telefonie über Voice over IP oder zur Live-Übertragung von Kamerabildern ist inzwischen erhört worden, denn DSL ist weltweit preisgünstig verfügbar. Besorgte Anlagenbetreiber fragen allerdings: Wie sicher sind Produktionsanlagen gegen unerwünschte Zugriffe über DSL und Internet geschützt?

Vernetzte Industrieanlagen werden zum Security-Risiko

Bekannte Sicherheitsprobleme aus der Office-Welt halten Einzug in die mit Industrial Ethernet zunehmend vernetzte Fabrik. Un-



terschiedlichste Anwendungsbereiche werden jetzt miteinander vernetzt: von SAP-gestützten ERP- und PC-Anwendungen über die Prozesssteuerung bis zur Feldebene. Durch diese Vernetzung ergeben sich beim Zugriff auf die Feldebene komfortable Möglichkeiten der Fernwartung und -diagnose. Die Kehrseite der Vernetzung: Die Sicherheitsrisiken steigen im gleichen Umfang wie die Vernetzung selbst. Die PA Consulting Group sieht eine steigende Anzahl vorsätzlicher Attacken auf industrielle Kontrollsysteme und die Prozessautomatisierung verstärkt im Blickfeld von Hackern. Das Problem: Die Erkenntnis über die Verwundbarkeit industrieller Anlagen ist zwar gestiegen, die tatsächlichen Maßnahmen bleiben dahinter allerdings zurück.

Sichere technische Lösungen für weltweiten Teleservice

Technische Lösungen für den weltweiten Servicetrend und die Sicherheit vernetzter Fertigungsanlagen sind verfügbar. Für Produktionsumgebungen sind allerdings besondere Sicherheitslösungen gefordert, die Rücksicht auf teilweise extreme Umgebungsbedingungen nehmen, die komplexen und sensiblen Prozesse und das höhere Schadensrisiko. Für den Teleservice empfiehlt der Security-Spezialist Innominate Security Technologies AG die Nutzung von preiswerten und breitbandigen Internet-Zugängen, wenn für ausreichende Sicherheit

gesorgt wird. Die noch überwiegend genutzten Wählverbindungen über Modems erweisen sich zunehmend als unwirtschaftlich, für die IT-Sicherheit als problematisch und bezüglich Stabilität und Bandbreite als ungenügend.

Quality of Service für kritische Anwendungen

Fehlfunktionen oder gezielte Netzwerk-attacken haben in der Vergangenheit durch eine Überlastung des Netzwerks die Kommunikation im internen Netz oder zur entfernten Anlage oftmals komplett lahmgelegt. Die Quality of Service (QoS)-Funktionalität, eine Applikation zur Sicherung kritischer Anwendungen von Innominate, sorgt für deren Sicherheit, indem die Anzahl von Datenpaketen beziehungsweise das Datenvolumen pro Zeiteinheit (Bandbreite), die durch das Netzwerk fließen, gezielt reglementiert werden. Wenn das zentrale Service Center in Deutschland über eine ADSL-Leitung auf eine Maschine bei einem Kunden in Brasilien zugreift, um ein Anwendungsbeispiel aus dem Bereich Teleservice zu nennen, ist die Verbindung real auf 192 kbit/s beschränkt. Wird jetzt ein großer File-Transfer zum Software-Update gestartet, sind weitere Zugriffe des Servicetechnikers praktisch unmöglich. Unzureichende Sprachqualität für ein VoIP-Telefonat beziehungsweise schlechte Antwortzeiten des Fernwartungs-Tools sind nur zwei mögliche Folgen. Mit dem Leistungsmerkmal QoS wird das Fernwartungs-VPN-Interface mit einer Maximalbandbreite von 192 kbit/s aktiviert. Den Anwendungen VoIP und Desktop Sharing werden garantierte Bandbreiten mit jeweils 64 kbit/s zugeordnet. Jetzt kann der Servicetechniker optimal arbeiten, obwohl im Hintergrund der File-Transfer stattfindet. Auch für externe Wählverbindungen über Modem oder ISDN ist die QoS-Funktionalität ein hilfreicher Ansatz, denn so lässt sich die schmale Bandbreite deutlich effektiver ausnutzen. Um das Ausfallrisiko einer Ethernet-basierten indust-

riellen Steuerung zu minimieren, dies als Anwendungsbeispiel für ein Produktionsnetz, sollen die Kommunikationsströme abgesichert werden. Die Steuerung kommuniziert vorrangig mit einer zweiten Steuerung außerhalb der eigenen Zelle, zum Beispiel per Modbus/TCP-Feldbus-Protokoll über Port 502, und soll von dieser mindestens 500 Pakete und maximal 2.000 Pakete pro Sekunde empfangen können. Mit der QoS-Funktion wird von der externen zur internen Steuerung durch Filter-Regeln und -Funktionen der gewünschte Mindest-Durchsatz sowie eine Queue für das Feldbus-Protokoll garantiert und die Steuerung vor Überlastung geschützt. Die Funktion kann auch genutzt werden, um für die Kommunikation zum Leitstand Mindestbandbreiten zu garantieren. So ist die Überwachung der Security Appliances und gegebenenfalls Einleitung von Gegenmaßnahmen bei Angriffen und Störungen auch bei Netzwerküberlast sichergestellt. ■

Autor Torsten Rössel ist Director Business Development bei Innominate in Berlin.

www.innominate.de