VDMA Benchmark Security

Technik im praktischen Vergleich

Am 8. November veranstaltete der VDMA-Fachverband Technische Automation in Frankfurt seinen dritten Technik Benchmark. Wieder waren Automatisierungsspezialisten gefordert, eine praxisnahe Aufgabe zu lösen. Es ging darum, eine bestehende Anlage zur Spanplattenfertigung unter den Gesichtspunkten der IT-Sicherheit zu erweitern.

▶ Die beispielhafte Automatisierungsaufgabe stellte die Dieffenbacher GmbH+Co. KG aus Eppingen. Deren Anlage zur Spanplattenfertigung soll erweitert werden. Dabei taucht natürlich eine Reihe von Fragen auf.

- ▶ Wie soll der Maschinenbauer bei Engineering, Wartung und Umbau mit 'seinem' Anlagennetzwerk umgehen?
- ▶ Welche Regeln sollte er zum Betrieb und zur Pflege aufstellen?
- ▶ Mit welchen Argumenten kann er die neuen Technologien seinem Endkunden verkaufen?

Zu dieser Aufgabe haben sechs Maschinenbau-Zulieferer jeweils einen Lösungsansatz entwickelt und stellten ihn zur Diskussion. Auf den folgenden Seiten können Sie Details der Aufgabenstellung und die Ergebnisse der Diskussionsrunde nachlesen. Weiterhin stellen wir die verschiedenen Lösungsansätze in abgespeckter Form vor. Detailliertere Informationen erhalten Sie über infoDIRECT unter www.iee-online.de.

Zahlreiche Maschinenbauer verfolgten die Ausführungen und Konzeptvorstellungen der Automatisierungsspezialisten auf dem dritten VDMA Technik Benchmark.

Die Aufgabenstellung

Unter dem Aspekt der IT-Sicherheit soll die Steuerungstechnik des ca. 300 x 400 m² großen Spanplattenwerkes erweitert werden. Die Anforderungen beschrieb Ulf Könekamp, Hauptabteilungsleiter Elektrik und Automatisierungstechnik im Geschäftsbereich Holz bei Dieffenbacher: „Wir beabsichtigen zum Schutz der Kommunikation und zur Erhöhung der Anlagenverfügbarkeit, die Netzwerk-Sicherheit schrittweise in ein zum Teil bestehendes und zum Teil neu zu errichtendes System zu integrieren." Bei der Wahl einer geeigneten Security-Strategie sind zwei komplexe Herausforderungen zu meistern. Erstens sind die physikalischen Rahmenbedingungen vor Ort sowie die vorhandene und die erweiterte Netztopologie zu berücksichtigen. Zweitens muss das Gesamtsystem mit einem praktikablen Bedienkonzept betreibbar gemacht werden. Ein Problem dabei ist, dass die bestehende Anlage, wie oft üblich, nicht komplett dokumentiert ist.

Zurzeit enthält die Anlage zwölf Steuerungen und sieben Schaltanlagen. Das Produktionsnetzwerk ist über eine VPN-Verbindung mit der Servicezentrale in Eppingen verbunden. Das von Dieffenbacher ausgelieferte und projektierte Equipment wird noch durch Geräte und Netzwerkteilnehmer von Unterlieferanten, dem Kunden selbst sowie Lieferanten des Kunden ergänzt. Zur Produktionssteigerung sind fünf Steuerungen und vier Schaltanlagen sowie verschiedene SPSen und Visualisierungen zu ergänzen. Im Zuge der Erweiterung sollen vor allem Fragestellungen in Bezug auf die IT-Security beachtet werden. Weiterhin ist die bestehende Netzwerkstruktur zu optimieren. Das Problem ist nämlich, dass sich durch die räumliche Ausdehnung des Netzwerkes sowie die verschiedenen Zulieferer praktisch nicht mehr kontrollieren lässt, was wo angeschlossen ist.

Aspekte der Lösungsansätze

Die vorgelegten IT-Konzepte unterschieden sich teilweise schon in der Herangehensweise an die Problematik. In einem waren sich jedoch alle Referenten einig: Die Aufgabe ist ein harter Brocken. Es gibt einige Stolperfallen und Untiefen, die die Lieferanten nur schwer umschiffen können. Das fängt schon bei der detaillierten Erfassung des Ist-Zustandes der Netzwerk-Infrastruktur an. Alle waren sich einig, dass dies mit den entsprechenden Randbedingungen (passenden Switches) machbar sein sollte. Einige Alt-Komponenten könnten jedoch Schwierigkeiten verursachen.

Um den Umbau möglichst ohne Beeinträchtigung der laufenden Produktion

„Im Zuge der Anlagenerweiterung steht für uns vor allem die Sicherstellung der IT-Security im Vordergrund.“

Ulf Könekamp, Dieffenbacher, Eppingen

durchzuführen, bietet sich eine modulare Vorgehensweise mit einer Segmentierung der Abteilungen an. Die Ferndiagnose lässt sich dabei allerdings nur per Telefon realisieren. Der Einsatz eines zweiten Netzwerkes für den Service würde Störungen minimieren.

Als große Störungsursache wurde die unterschiedliche Denkweise von ITlern und Automatisieren erkannt. Betriebselektriker sind nicht in der Lage, die IT-Systeme zu administrieren. Siemens und Rockwell bieten zwar Tools an, um diese Arbeit zu vereinfachen, allerdings ist deren Verträglichkeit mit heterogenen Umgebungen nicht sichergestellt. Generell scheint es vor allem in der Produktion noch eine Menge Weiterbildungsbedarf zum Thema Industrial-Ethernet zu geben.

Die Diskussion hat gezeigt, dass das Thema Wartung eine Menge Konfliktpotenzial birgt. Die Hersteller sehen diesbezüglich keinen Informations- beziehungsweise Handlungsbedarf, da sie anscheinend voraussetzen, dass der Anwender IT-Experte ist und sein Netzwerk selbst managed. Vielleicht wäre hier ein Betreibermodell für Netzwerke sinnvoll?

Aus technischer Sicht spricht heute kaum noch etwas für passive Netzwerkkomponenten. Vor allem im IT-Bereich findet man überwiegend aktiv gemanagte Switches. Das größte Hindernis für einen breiteren Einsatz ist der hohe Preis. Für sie spricht die Möglichkeit eines Netzwerk-Monitoring die Verfolgung von Trends und Lasten, sowie die Benachrichtigung bei Ereignissen. Außerdem erlauben sie den einfachen Austausch sowie die Identifikation von Geräten.

Meinung der Experten

Henry Stubert von der Insystems Automation GmbH, Berlin, gab in der anschließenden Diskussion zu bedenken, dass sich auch die schönste technische Lösung nicht durchsetzen kann, wenn sie dem Kunden nicht wertorientiert angeboten wird. Diesen Ansatz des Value Based Selling-Konzept vermisst er von den Komponentenlieferanten.„Ich möchte die vorgestellten technischen Lösungen aus diesem Technik-Benchmark auf die Erkennbarkeit dieser Win-Win-Situation hinterfragen. Schließlich interessiert mich auch, ob die Kosten für die dargestellten Lösungen einem erkennbaren Nutzen gegenüberstehen und sich ein Preis mit ausreichender Marge durchsetzen lässt“, betont der Automatisierungsspezialist.

Für Klaus-Peter Willems von der TMG – Technologie und Engineering GmbH in Karlsruhe ist das größte Problem, dass in der Produktion in der Regel das notwendige Spezialwissen für die Administration von umfangreichen Netzwerken nicht vorhanden ist. Andererseits verfügen die IT-Abteilungen nicht über das Wissen über die Automatisierungssysteme sowie die Echtzeitanforderungen und die Verfügbarkeit von Maschinen und Anlagen. Willems betont: „Die Experten der Bereiche sollten mehr miteinander sprechen und sich nicht abgrenzen. Schließlich müssen sie unter dem Gesichtspunkt unternehmensweiter durchgängiger Kommunikation zwangsläufig miteinander arbeiten.“ Die Administration von Netzwerken in der Produktion sollte deshalb so gestaltet sein, dass sie auch das für den Betrieb und die Wartung der Anlagen verantwortliche Personal durchführen kann, sich aber in die Security-Konzepte des gesamten Unternehmens einfügt.

infoDIRECT **776*iee*0108**

www.iee-online.de
- ▶ Langfassungen der einzelnen Beiträge
- ▶ pdf's der sechs IT-Konzepte
- ▶ Link zu den Unternehmen
- ▶ Link zum VDMA-Benchmark

Exklusiv VDMA Benchmark

Entflechtung von Kommunikationsbeziehungen

Nicht sammeln, sondern liefern

Maschinenbauer sind heute kaum noch in der Lage, die komplexer werdenden Netzwerkstrukturen nachzuvollziehen und anfallende Aufgaben zu erledigen. Deswegen sind intuitiv bedienbare Werkzeuge erforderlich. Werden die Prozessdaten, ohne das Steuerungsprogramm zu verändern, direkt in die Datenbank übertragen, ist die Administration des Anlagennetzes auch durch den Betriebstechniker möglich.

▶ Bei Anlagenerweiterungen ist die Erfassung des Ist-Zustandes unabdingbar. Dies gilt nicht nur für mechatronische, sondern auch für Netzwerk-Komponenten. So eine Netzwerkdiagnose kann aktiv oder passiv erfolgen. Bei der aktiven Diagnose wird mit einem Scan gezielt durch alle Topologien des Netzwerkes gesucht. Dazu gibt es frei am Markt frei verfügbar Tools. Der Nachteil ist, dass die aktive Suche das Netzwerk stark belastet und nur eine Aktivität anzeigt, aber nicht welche.

Passive Netzwerkanalyse

Inat entschied sich deswegen bei der Problemlösung für ein passives Diagnosetool, das die Teilnehmer und den Inhalt der Kommunikation aufzeichnet sowie einen grafischen Überblick des Netzwerkes erstellt. Mithilfe von Hardwareagenten in Form von Seriell-Ethernet-Konvertern ist die Diagnosefunktionalität auch in ältere gewachsene Netze integrierbar. Durch die Analyse der Kommunikationsbeziehungen lässt sich nicht nur die Verbindung, sondern auch der komplette funktionale Ablauf des Montage- oder Produktionsschrittes dokumentieren. Zusammen bildet das die Grundlage für ein Engineeringtool, das nicht nur in den Inbetriebnahmephasen, sondern auch während des kontinuierlichen Produktionsbetriebs wichtige Kenngrößen liefert.

„Um einen Zugriff von außen auf die Steuerungsebene zu verhindern, sind der Produktions- und der Administrations-Teil mittels Firewall zu trennen.“

Werner Krings, Inat GmbH, Nürnberg

Um die notwendigen Beziehungen während der Umbauphase aufrechtzuerhalten, würde Inat das Anlagennetz durch eine Firewall vom Büronetz trennen und in kleinere Netzwerksegmente aufteilen: Den Übergang zwischen zwei getrennten Netzsegmenten schützt die Zwischenschaltung einer Hard- oder Software, die das Eindringen in das jeweilige Anlagensegment verhindert. Gezielte und bewusste Bypässe ermöglichen die Aufrechterhaltung und die Sicherung des Produktionsablaufes während des Umbaus.

OPC sammelt die Prozessdaten

Über die OPC-Schnittstelle ist der Datenaustausch zwischen Automatisierungshardware und Anwendungssoftware auf einfache Weise möglich. Dank der DCOM-Technologie ist OPC auch netzwerkfähig. Da DCOM den Zugriff auf ‘fremde’ Rechner sowie von ‘fremden’ Rechnern zulässt, sind Sicherheitsmechanismen nötig, die den unerlaubten Zugriff auf Ressourcen verhindern. Die Konfiguration ist jedoch alles andere als trivial und kann sehr komplex und aufwändig werden.

Ein weiteres Problem, das DCOM mit sich bringt, ist die Tatsache, dass das Verbindungs-Timeout nicht konfigurierbar ist. Das kann dazu führen, dass der Client bei einer Unterbrechung der Netzwerkverbindung mehrere Minuten auf eine Antwort warten muss – auch wenn die Verbindung sofort wiederhergestellt wird. Des Weiteren funktioniert DCOM nicht, wenn Firewalls zwischengeschaltet sind. Hinzu kommt, dass DCOM 2002 von Microsoft abgekündigt wurde und seitdem nicht mehr supported wird. Windows Vista unterstützt DCOM überhaupt nicht mehr. Clients, die auf Rechnern mit Nicht-Windows-Betriebssystemen laufen, zum Beispiel ERP-Systeme, SAP usw., haben keine Möglichkeit auf OPC-Server zuzugreifen – denn diese Betriebssysteme kennen OPC nicht.

Das ERP-System bekommt die Prozessdaten geliefert

Die Lösung ist ein netzwerkfähiger, systemunabhängiger OPC-Kanal. Diese OPC-Pipe ‘tunnelt’ die Daten, die bei der Kommunikation zwischen Client und Server ausgetauscht werden, indem sie sie in eine TCP/IP-Kommunikation umwandelt. Dieses Prinzip funktioniert in beide Kommunikationsrichtungen, umgeht die diversen DCOM-Probleme und macht OPC auch für nicht-Windows-Systeme nutzbar.

Erfolgt die Prozessdatenerfassung über OPC, kommt man um das Projektieren von Verbindungen nicht herum. Anders sieht es aus, wenn dem ERP-System die Daten direkt zur Verfügung gestellt werden. Durch den Einsatz von echocollect reduziert sich der Programmieraufwand. Das Gerät sammelt die Prozessdaten und überträgt diese in eine Datenbankstruktur (SQL bzw. SAP). Es ist dabei völlig egal, um welches ERP es sich handelt. Der Datensammler stellt die Daten genau in dem Format zur Verfügung, in dem diese benötigt werden. Das mit zwei Ethernet-Schnittstellen ausgestattete Gerät fungiert zudem als Gateway und macht so die Trennung zwischen dem Büro- und dem Anlagennetz möglich. Die Zuordnung erfolgt über Tabellen, so dass es OPC-unabhängig arbeiten kann.

Sicherheit in industriellen Netzwerken

Abgestuftes Schutzkonzept

Exklusiv VDMA Benchmark

Die Durchgängigkeit der Informations- und Automatisierungstechnik erfordert eine neue Bewertung der Sicherheit von Automatisierungssystemen unter Beachtung der Echtzeitfähigkeit sowie der Security. Auf der Basis eines abgestuften Sicherheitskonzeptes sowie einer konsequenten Installation lässt sich jede Applikation mit sinnvollen und ausreichenden Security-Maßnahmen wirkungsvoll schützen.

▶ Der Versuch, typische Security-Strategien aus der Office-Welt in Produktionsanlagen anzuwenden, ist überwiegend zum Scheitern verurteilt. Um netzwerkbasierte Störungen und einen Produktionsausfall dennoch zu vermeiden, bieten Phoenix Contact und Innominate ein dreistufiges Konzept an. Es arbeitet mit mechanischem Zugriffsschutz, nutzt die Security-Möglichkeiten von Managed Switches bei höchster Performance und platziert spezielle Firewall/Router Appliances an geeigneten Knotenpunkten im Netzwerk. Dabei ist Phoenix Contact für die Visualisierung zuständig und Innominate übernimmt die Überwachung sowie die Absicherung.

Dreistufige Sicherheitsmaßnahmen

Der einfachste Schutz vor einem unberechtigten Zugriff auf das Produktionsnetzwerk, ist der Einsatz von mechanischen Verriegelungen. Offene RJ45-Ports werden mit einem Stopfen verschlossen, der sich ebenso wie gesteckte Patchkabel nur mithilfe eines speziellen Werkzeugs wieder entfernen lässt. Mithilfe solch simpler Maßnahmen wird ein großer Anteil der Schadhandlungen unterbunden, nämlich das Trennen wichtiger Verbindungen und das fehlerhafte bzw. unbefugte Verbinden von Teilnehmern ins Netz.

Die Konfigurationsmöglichkeiten eines Managed Switches der Produktlinie Factory Line bieten eine Reihe von Industrial Ethernet-konformen Security-Funktionen, die Zugriffe regeln, unerwünschten Datenverkehr unterbinden und das Abhören von Daten erschweren sowie die Betriebssicherheit und Verfügbarkeit der Anlage maßgeblich erhöhen. Zu diesen

„Ein ungesichertes Ethernet ist genauso sicher wie ein Feldbus."

Oliver Puls, Phoenix Contact GmbH, Blomberg

„Die Switch-Technologie bietet Features, die bisher nur selten genutzt werden."

Torsten Rössel, Innominate Security Technologies, Berlin

Funktionen gehören das Einrichten von VLANs, Access Control auf Basis von MAC-Adressen sowie die Beschränkung von Zugriffen über die Port Security. Für deren Parametrierung gibt es die Netzwerkmanagement-Software Factory Manager, SNMP oder Web-based Management. Darüber hinaus ist eine Multi-Device Configuration bei Infrastruktur-Komponenten möglich. Ein Tool wie Diag+ von Phoenix Contact ermöglicht eine sinnvolle Administration der Ethernet-Infrastruktur aus dem SPS Engineering-Werkzeug heraus.

Dezentraler Schutz

Der dezentrale Einsatz von Firewall/Router Appliances ermöglicht die individuelle Absicherung von verteilten Automatisierungssystemen. Die für den Einsatz im rauen Industrieumfeld konzipierten FL MGuard-Geräte werden als eigenständiges System in das Netzwerk integriert und schützen dort einen Teil des Anlagennetzes, eine komplette Produktionszelle oder eine einzelne Automatisierungskomponente – und das ohne Rückwirkung auf das abzusichernde System. Sie lassen sich in einem so genannten 'Stealth Mode' auch völlig transparent in flache Netze ohne Routing nachrüsten, mit minimaler Netzwerkunterbrechung und ohne Änderungen an der sonstigen Netzwerkkonfiguration.

Trotz ihrer dezentralen, physisch verteilten Anordnung im Netzwerk können die Geräte übrigens durch eine Device Management Software effizient zentral verwaltet und bei Bedarf bzgl. Konfiguration oder Firmware aktualisiert werden – ohne Eingriffe vor Ort. So verbinden sie die Vorzüge eines zentralen Systems mit flexibler Nachrüstbarkeit und völliger Freiheit im Netzwerk-Design ohne Zwang zu sternförmiger Verkabelung.

Mehrwert sichere Fernwartung

Sind aus Sicherheitsgründen erst einmal Security Appliances an fernzuwartenden Teilen einer Anlage vorhanden, lassen sich diese mit geringem Mehraufwand auch elegant für die VPN-basierte sichere Fernwartung über Internet nutzen. Erneut schützen Firewall-Regeln dabei die Beteiligten 'voreinander' und vor Übergriffen in weitere Netzwerksegmente.

Engineering der Netzwerk-Infrastruktur

Sicherheit durch Segmentierung

Exklusiv VDMA Benchmark

Für mehr Übersichtlichkeit und Verfügbarkeit sollte ein Produktionsnetzwerk in funktionale, logische oder datenbezogene Segmente unterteilt werden. Intelligente, managebare Switches, die in der SPS-Programmierumgebung integriert sind, machen dies möglich. Dadurch lassen sich die Übersichtlichkeit und die Verfügbarkeit steigern sowie der Zugriffsschutz und die Administration verbessern.

▶ Das Planen einer Netzwerk-Infrastruktur setzt die Erfassung des Ist-Zustandes voraus. Es muss ermittelt werden, welche Geräte sich bereits im Netz befinden, welche Kommunikationsbeziehungen für den laufenden Betrieb notwendig sind und wie das Netzwerk abgestuft bzw. skaliert werden kann. Außerdem ist das Beschaffen von Informationen zu den vorhandenen Netzwerkkomponenten in Bezug auf deren Kommunikationsleistung und Netzwerklast unerlässlich. Konventionell lassen sich alle Netzwerkteilnehmer nach Standort, Typ, Bussystem und Busadresse ermitteln, indem die Anlage durchlaufen wird. Das ist zwar sicher, aber sehr zeitaufwendig und fehlerbehaftet. Eine andere Möglichkeit stellt die Netzwerkkonfigurations- und Analyse-Software RSNetWorx dar. Sie erfasst alle Teilnehmer inklusive Feldbus und Busadresse, auch an physikalisch unterschiedlichen Netzwerken, automatisch.

Sicher trennen mit Switches

Um eine neue Linie autark in Betrieb nehmen zu können, sollte die Erweiterungslinie in ein eigenständiges Netzwerksegment unterteilt sowie die einzelnen Produktionszellen in der Erweiterungslinie segmentiert werden. Dies sorgt für eine höhere Verfügbarkeit und Betriebssicherheit, vereinfacht die Netzwerkadministration und erhöht den Zugriffsschutz. Allen-Bradley Managed Switches bieten sich für diese Aufgabe an. Sie eliminieren auch Risiken, die durch das Hinzufügen neuer Netzwerkteilnehmer in das bestehende Produktionsnetzwerk entstehen können, wie die doppelte Vergabe einer IP-Adresse, das Anschalten einer fehlerhaften Netzwerkkomponente oder eine fehlerhafte Konfiguration.

„Eine Netzwerksegmentierung ist ein wesentlicher Schritt zu mehr Verfügbarkeit, Leistungsfähigkeit, Übersichtlichkeit und Zugriffsschutz."

Frank Loew, Rockwell Automation, Haan

Das unerlaubte bzw. unkontrollierte Anbinden von externen Firmen an das Produktionsnetzwerk birgt ein hohes Risiko und kann zu unvorhersehbaren Problemen im Netzwerk führen. Um dieses Risiko zu eliminieren, verwenden Allen-Bradley Managed Switches Port Security. Diese Funktion begrenzt die Anzahl der MAC-Adressen, also der Programmiergeräte, die gleichzeitig mit dem Switch verbunden sein dürfen. Außerdem stellt Port Security sicher, dass alle nicht registrierten MAC-Adressen keinen Zugang zum Netzwerk erhalten.

Eine Sache der Diagnose

Eine maximale Anlagenverfügbarkeit erfordert aber auch eine Diagnose-Möglichkeit der Teilnehmer, was lokal oder zentral möglich ist. Unter lokal ist zu verstehen, wenn beispielsweise weder der Frequenzumrichter noch das Bedienpanel an das Kommunikationsnetz angebunden sind. Das lokale Bedienpanel ermöglicht die Steuerung sowie die Diagnose für den jeweils angebundenen Antrieb. Die lokale Diagnose reduziert die Netzwerklast. Allerdings ist dabei das Erkennen von Störungen sowie das Einstellen von Parametern nur vor Ort möglich.
Bei der zentralen Diagnose werden hingegen die Antriebe in das Netzwerk eingebunden und können von jeder beliebigen Stelle am Netzwerk angesprochen werden. Ihre Integration in die SPS-Programmiersoftware ermöglicht deren zentrale Diagnose und Parametrierung bei gleichzeitiger Gewährleistung der Minimierung der Netzwerklast.
Die Ferndiagnose der Steuerungstechnik einer Produktionsanlage ist sowohl während als auch nach dem Umbau eine wichtige Anforderung. Sie erfordert die Unterstützung von Funktionen wie die Erfassung des Soll- und des Ist-Zustandes eines Netzwerkes. Weiterhin ist das Erkennen sowie das Analysieren defekter Teilnehmer unerlässlich. Dafür muss der Einwahlpunkt, in der Regel ein Ethernet-Modem, die installierte Netzwerksicherheit unterstützen und gleiches nach außen zur Verfügung stellen. Das Rockwell Ethernet-Modem bietet dafür bis zu zehn Einwahl-Benutzerkonten, eine Fehlersuche mittels Port Mirror Ring und Port Diagnose sowie VLAN-Funktionalität und IGMP Snooping zur Reduzierung von Datenverkehr. Zur Sicherheit werden nur zuvor definierte Telefonnummern als Anrufer akzeptiert und es gibt ein Passwort mit Rückruffunktion.

Exklusiv VDMA Benchmark

Sicherheits-Architektur in Industrienetzen

Integrierte Konzepte

Als essenzielle Komponente ist die Produktion das Herz eines jeden Unternehmens in der verarbeitenden Industrie. Der Wichtigkeit entsprechend sind Sicherheitsfunktionen auf den verschiedensten Ebenen zu implementieren, um einen reibungslosen und zuverlässigen Ablauf zu sichern. Eine ganzheitliche Sicherheitsarchitektur hilft, diese neuen Anforderungen zu adressieren.

▶ Die Sicherung von Ethernet-basierten Industrienetzwerken sowie deren Einbindung in andere Unternehmensnetzwerke ist zum vordringlichen Problem für Unternehmen geworden. Als offene Kommunikationsplattform erleichtert das Ethernet zwar den Informationsaustausch von und zur Produktion, allerdings wird es immer wichtiger, mit geeigneten Security-Mechanismen nur die wirklich gewollte Kommunikation zu erlauben. Nicht autorisierte Zugriffe von außen oder von innen können dazu führen, dass Produktionsabläufe gestört oder gar unterbrochen werden.

In der Vergangenheit musste sich das Betriebspersonal kaum Gedanken über Sicherheitsaspekte in der Produktion und Logistik machen. Abgetrennte Industrienetze wurden als 'sicher' angesehen. Durch die Einbindung in globale Unternehmensanwendungen bzw. ins Intranet und somit zwangsläufig ins Internet, muss sich die Betriebsmannschaft mit einer neuen Art von Bedrohungen auseinandersetzen (z. B. Würmer, Viren und Hacker-Attacken).

„Ein sukzessiver Umstieg auf IP-basierte Technologien ist die Voraussetzung, um eine effektive Sicherheitsarchitektur umsetzen zu können."
Gerhard Koch, Cisco Systems, Stuttgart (links) und Dr. Arne Manthey, SAP, Walldorf

Kritische Komponenten einer Sicherheitsarchitektur

Es gibt drei grundsätzliche Aspekte und Überlegungen, um eine effiziente 'Security Policy' für den Produktionsprozess zu entwickeln:

- 'Trust and identity' – Zugriffsrechte und Privilegien von überprüfbaren Nutzern
- 'Thread Defense/Mitigation' – Schutz von Netzwerkkomponenten und Endpunkten (PCs, Server, PDAs, usw.)
- 'Secure Communication/Management' – Sicherer Transport von Daten und sichere Kommunikation

Eine Sicherheitsstrategie in einer Produktionsumgebung sollte analog zu einer Sicherheitsstrategie in einer Bank erfolgen. Zuerst ist sicherzustellen, dass ungewollte Personen keinen Zugriff zum Netz bekommen. Beim Zugriff wird die Identität überprüft und dann basierend auf dieser bestimmte Zugriffsbereiche freigeschaltet. Bei Sicherheitsverletzungen sollte ein entsprechendes Alarming erfolgen und reported werden. Weiterhin ist der Produktionsbereich als solcher vom restlichen Unternehmensnetz mit einer sogenannten DMZ (entmilitarisierte Zone) zu entkoppeln. In dieser kann eine Firewall einen unberechtigten Zugriff von außen verhindern. Auch die Überprüfung von Nutzern und gegebenenfalls ein System, um den Netzwerkverkehr als solchen auf Anomalien zu untersuchen, (Intrusion Prevention) ist hier angesiedelt. Zum Management der ganzen Security-Funktionen bietet sich ein eigenes System an, das sich ebenfalls innerhalb der DMZ befinden sollte.

Ein wichtiger Aspekt eines gut abgestimmten Sicherheitssystems ist die integrierte Zusammenarbeit der einzelnen Sicherheitselemente, wie Firewall, Intrusion Prevention, Überprüfung und Zulassung. Jedes Element teilt seinen Status den anderen über das Sicherheitsmanagement mit, was ein proaktiv agierendes Sicherheitssystem erst ermöglicht.

Entwickeln einer Security Policy

Eine der wichtigsten Aufgaben überhaupt, um Sicherheit in Produktionsnetzwerken zu erhöhen, ist die konsequente Ausarbeitung von Sicherheitsregeln. Bevor diese definiert werden können, sind folgende Fragen zu beantworten:

- Wer hat Zugang zur Fabrik?
- Auf welche Anwendungen muss in der Produktion zugegriffen werden?
- Wer hat Fernzugang zu den Systemen und welche Änderungen sind erlaubt?
- Welches 'intellectual property' muss geschützt werden?
- Was gibt es für Auswirkungen, wenn die Geschäftsabläufe unterbrochen werden?
- Wie oft ist ein Ausfall zu verkraften?
- Wie werden Software Updates vollzogen?

Beim Entwickeln der Security Policy muss man berücksichtigen, dass es Unterschiede zwischen der traditionellen IT und den Produktionsbereichen gibt. Einer der Hauptunterschiede ist, dass 'nicht berechtigtes Personal' in der Lage sein soll, unterbrochene Prozesse wieder in Gang setzen zu können. Weiterhin gibt es Unterschiede im Bereich Intrusion Detection. Werden Anomalien im Netzwerkverkehr festgestellt, führt diese in der Regel zum Herunterfahren der betroffenen Netzwerkports, um eine Ausbreitung zu verhindern. Dies ist natürlich im Produktionsumfeld so nicht akzeptierbar. Dementsprechende Änderungen sind deshalb in der Policy zu verankern.

IT-Sicherheit im Maschinenbau

Gehärtete Steuerungen

Exklusiv VDMA Benchmark

Die IT-Infrastruktur der Fertigung sowie die Steuerungen von Holzbearbeitungsmaschinen müssen heutzutage gegen die unterschiedlichen Angriffe gewappnet sein. Schließlich sind die Kosten und logistischen Auswirkungen eines durch bösartige Software verursachten Produktionsausfalls sehr hoch und besonders schmerzlich – ganz abgesehen vom Imageverlust. Deswegen ist ein dreistufiger Schutz wichtig.

▶ Ein optimaler Schutz umfasst eine durchgängige IT-Security-Policy, eine IT-Security als integralen Bestandteil der Steuerung sowie ein sicheres Zellenkonzept der Automatisierung. Deswegen härtet Siemens seine Steuerungen gegen IT-Störungen. Sein auf Automatisierungssysteme abgestimmtes IT-Security-Konzept mit den Security-Modulen Scalance S ermöglicht darüber hinaus den sicheren Betrieb von vernetzten Automatisierungslösungen mit Industrial Ethernet und Profinet.

Zugriff von außen

Die weltweite Interneteinwahl per DSL zur Störungsdiagnose gehört bei vielen Maschinen zu den Standardwerkzeugen der Serviceabteilungen. Ebenso zur Norm geworden ist der Fernzugriff auf aktuelle Produktionsdaten, Stückzahlen, Standzeiten oder Werkzeugverschleißdaten direkt in der Produktion. Für akzeptable Sicherheit vor verbreiteten IT-Risiken sorgen in der Produktion bisher physikalisch abgeschottete Netzwerke mit teilweise 'exotischen' Protokollen. Diese Abschottung – und die so erreichte Sicherheit – erodiert, je weiter offene Netzwerkstandards und -Protokolle (Ethernet/Internet), Remote-Access-Lösungen und die Einbindung in unternehmensweite Netze in das Fertigungsumfeld vordringen.

Security von Anfang an

Bereits bei der Entwicklung der CNC Sinumerik 840D sl und deren Bedienkomponenten – häufig Bedienfelder mit integriertem Industrie-PC und einem Windows-Betriebssystem – berücksichtigte man entsprechende IT-Security-Belange. Siemens überprüft kontinuierlich Maßnahmen zur Härtung der Sinumerik PCU

„Sicherheit im Anlagennetzwerk erfordert gehärtete Produkte sowie eine Trennung durch Firewalls."

Harald Mayer, Siemens AG, Erlangen

50/70 und testet regelmäßig führende Virenscanner-Fabrikate auf Verträglichkeit. Härten bedeutet, die Betriebssysteme so zu konfigurieren, dass Angriffspunkte, beispielsweise über Ports oder nicht benötigte Dienste, minimiert werden. Die PCUs werden als Hochsicherheits-Desktops mit aktiver Windows-XP-Firewall ausgeliefert, gemäß 'Windows XP Security Guide' von Microsoft. Somit sind nur die Ports geöffnet, die von systembekannten Applikationen benötigt werden.

In vergleichbarer Weise schützt Siemens die auf Linux basierenden CNC-Steuerungen, die nur mit aktiver Linux-Paketfilter-Firewall ausgeliefert werden. Auch dabei gilt: Nur Ports, die von den eigenen Applikationen benötigt werden, sind geöffnet. Das verwendete Linux zeichnet sich durch besonders sichere Software, zum Beispiel gehärtete TCP/IP-Stacks, aus. Der so genannte Nessus-Test der Ethernet-Schnittstellen gehört zum Standard-Repertoire, um mögliche Gefahren und Schwachstellen zu erkennen und zu beseitigen.

Up-to-date bleiben

Die IT-Sicherheit, die eine CNC mit gehärtetem Betriebssystem mitbringt, ist auf die Bedrohungen zugeschnitten, die bei der Auslieferung des Systems bekannt sind. Auf lange Sicht kann diese Schutzwirkung nachlassen. Dies betrifft insbesondere Betriebssysteme, die zwar noch angewendet, aber nicht mehr unterstützt werden, wie Windows NT4.0. Die Firma Solidcore bietet eine gegenüber herkömmlichen Virenscannern optimierte Security-Software an, die einen stets aktuellen Schutz vor IT-Bedrohungen gewährt, ohne auf häufige Updates angewiesen zu sein. Sie ist auch für NT4.0-basierte CNCs verfügbar.

Befinden sich in einem Fertigungsverbund Steuerungen oder andere intelligente Geräte, deren Eigenschutz weder durch Konfiguration noch durch Updates oder Zusatzsoftware auf den Stand der Technik gebracht werden kann, ist für diese Geräte eine abgesicherte Netzwerkumgebung zu schaffen. Dies ist am einfachsten mit darauf spezialisierten Routern oder Gateways zu leisten. Sie stellen IT-Sicherheit durch integrierte Firewalls in Industriequalität her und sind selbst durch ihre für Malware unempfindliche Firmware geschützt.

Für die Integrität der transferierten Daten sorgt eine VPN-Funktionalität mit Verschlüsselungs- und Authentifizierungsalgorithmen. Mit dieser Security-orientierten Infrastruktur wird unüberwachte Datenübertragung ausgeschlossen, so dass das Eindringen schädigender Malware in die geschützte Netzwerkzelle verhindert werden kann.

Exklusiv
VDMA Benchmark

Informationssysteme für Produktionsunternehmen

Sicherheit durch Prävention

Da moderne Systeme heute Informationen austauschen und Remote-Zugriffe zulassen müssen, sind sie nicht mehr physikalisch getrennt. Dadurch ergeben sich Sicherheitsrisiken mit ganz neuen Anforderungen. Nur wer flexible und erweiterbare Lösungen zur IT-Sicherheit einsetzt, kann über den gesamten Lebenszyklus das Sicherheitsrisiko minimieren.

▶ Aufgrund von verschiedenen Anforderungen an Betriebssysteme, besonders in Bezug auf Verfügbarkeit und Performance, ist es fast unmöglich, diese zu verbinden oder gar zu integrieren. Die Systeme sind nicht nur komplex und teuer, sie sind auch nur schwer auszutauschen, wenn sie einmal etabliert sind. Dazu kommt ein unterschiedliches Verständnis für 'Zeit' in Abläufen zwischen Produktions- und IT-Ebene. So entstehen auch verschiedene Ansprüche an Security in Bezug auf die Anwendung.

Intelligente Softwaretechnologien wie ArchestrA ermöglichen es bereits am Objekt, die Security zu definieren und somit Benutzerfehler im Ansatz zu minimieren. Der auf der ArchestrA-Technologie basierende Wonderware Application-Server enthält ein Security Model auf Objektbasis mit voller Rückverfolgbarkeit der Runtime-Änderungen. Er bietet auch eine Unabhängigkeit von Hardware Clients. Seine Security lässt sich bis auf Objektlevel herunter definieren und konfigurieren. Jedes der Attribute eines Objektes kann einzeln in Bezug auf Zugriffs- und Benutzerberechtigung definiert werden. Somit ist es möglich, den Benutzern verschiedene Rollen zuzuweisen.

Zugriffssicherheit

Die Technologie setzt im Vorfeld auf die Verhinderung von nicht autorisierten Eingaben oder Zugriffen, sodass Daten und Produktionsprozesse weitgehend vor unberechtigter Manipulation geschützt sind. Somit kann das intelligente Softwaretool bereits bei der Erstellung einer Applikation aktiv zur Sicherheit beitragen – natürlich unter dem Aspekt der Wiederverwertbarkeit und Kostenreduzierung.

Projekte, welche mittels Wonderware-Lösungen und ArchestrA-Technologie realisiert werden, ermöglichen es, Bedienoberflächen auf Zugriffsberechtigungen zu gruppieren und Rollen zu vergeben. Ein wesentlicher Baustein beim Realisieren eines ArchestrA-Projektes ist das Security Model, welches es ermöglicht, schon auf Objektebene aktiv in den Sicherheitsmechanismus einzugreifen. Es ist zu definieren, nachdem die Namen und Produktbereiche definiert und Vorlagen sowie Ableitungen geplant wurden. Das Model reguliert und dokumentiert die Zugriffe. Durch Deployment ist es möglich, Anlagenteile zu testen und dann zur Laufzeit zu implementieren.

„Statt die Steuerungssysteme von der Business Domain logisch zu trennen, kann man die Applikation auch auf einem virtuellen Laufwerk laufen lassen."

Markus Stadelhofer, Wonderware GmbH, München

Objektorientierte Applikation

Die Applikationsobjekte, wie I/O Definition, Logik and Scripting, History Configuration, Security and Access Controls, Alarm/Event Configuration, sind der grundlegende Bestandteil einer objektorientierten Lösung. Mit ihnen lassen sich direkt am Objekt Attribute erstellen und definieren. Somit können diese Objekte mitsamt ihren Attributen wiederverwendet und zentral verwaltet werden. Das spart Zeit und Kosten.

Einzelne Objekte und deren Attribute sind bezüglich der Berechtigung und Benutzerverwaltung auf die Zugriffsberechtigung individuell anpassbar, was Manipulationen und Fehlbedienungen durch nicht autorisierte Benutzer weitgehend ausschließt.

Upgrades als Risikofaktor

Die Erweiterung von Anlagen bringt meistens auch Unterschiede zwischen Software-Versionen der historischen und der neuen Anlagenteile. Durch Aufwärtskompatibilität werden hier die ursprünglichen Investitionen geschützt und neue Technologien sind einfach implementierbar. Wonderware bietet die Dienstleistung eines Upgrade-Scans, welcher mögliche Risiken durch Upgrades beschreibt.

In der sich schnell verändernden IT-Umgebung kann verlässliche Sicherheit und wirkungsvolle Risikoreduzierung nur durch eine Mischung aus vorbeugenden Sicherheitsmaßnahmen und Technologie-Einsatz erzielt werden. Ein wirksames Patch-Management ist ein wesentlicher und unerlässlicher Garant für Schutz vor Attacken. Wartungsverträge bieten hier proaktive Sicherheit. Dadurch entfallen wichtige Fragen wie: wann und wo finde ich den aktuellen Patch, was muss getestet werden und in welchem Umfang.

Letztendlich bleibt immer ein Restrisiko, denn 100 % Sicherheit ist nicht möglich. Die Kosten steigen aber überproportional im Verhältnis zur Security. Durch eine Risikoanalyse und die daraus resultierenden Ergebnisse können Unternehmen plausible Maßnahmen ergreifen. Diese Analysen sind auch die Basis zur Ermittlung von Aufwand und Nutzen.