© tom - Fotolia.com

MASCHINEN- UND ANLAGENSICHERHEIT

Hacker ohne Chance

Powerlink: Ein sicheres industrielles Datenkommunikationsnetzwerk

Industrie 4.0 ist die breit angekündigte, nächste industrielle Revolution, die auf dem „Internet der Dinge" basiert. Viele Produzenten zögern, ihre Produktionsmittel an externe Leitungen anzuschließen, von cloudbasierten Angeboten ganz zu schweigen. Sie haben Angst davor, dass Hackerangriffe oder Schadsoftware die Produktion lähmen könnten. Tatsächlich existiert jedoch ein industrielles Datenkommunikationsnetzwerk, das hohe Geschwindigkeit und kompromisslose Offenheit bietet und dessen Architektur ein Eindringen sicher verhindert, und zwar ohne externe Sicherheitsmaßnahmen ergreifen zu müssen.

Vor 30 Jahren galt ein Virus als mikroskopisch kleiner, krank machender Organismus, das Trojanische Pferd war ein Geschenk aus der griechischen Mythologie und das Wort „Schadsoftware" war noch nicht erfunden worden. Mittlerweile ist die Internet-Sicherheit für viele Unternehmen weltweit zu einer wesentlichen Sorge geworden. Zudem beschränkt sich die Angst vor Hackern nicht mehr auf die Büro-Umgebung, wo diese seit Jahren Chaos verbreiten und enormen Schaden anrichten.

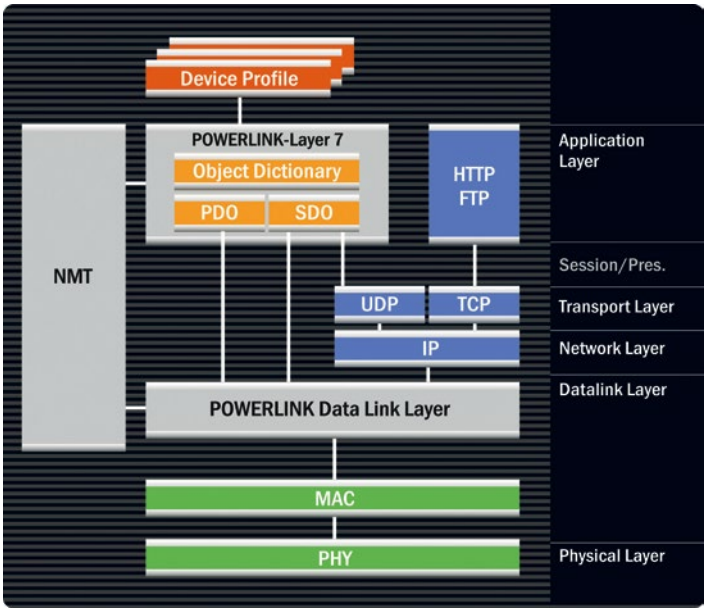
Trotz offensichtlicher Effizienzgewinne zögern viele Unternehmen, die PC-basierte Automatisierungshardware ihrer Maschinen und Anlagen für Betrieb, Diagnose, Wartung, Aktualisierung und andere Dienste von entfernten Standorten aus an das Internet anzuschließen. „Das ist verständlich, denn jedweder Stillstand einer Produktionsmaschine verursacht Verluste", sagt Stefan Schönegger, Geschäftsführer der Ethernet Powerlink Standardization Group (EPSG). „Produzenten, die im harten Wettbewerb stehen, können auch dem Gedanken wenig abgewinnen, dass sich vertrauliche Produktionsdaten in fremden Händen befinden."

Eine Frage des Protokolls

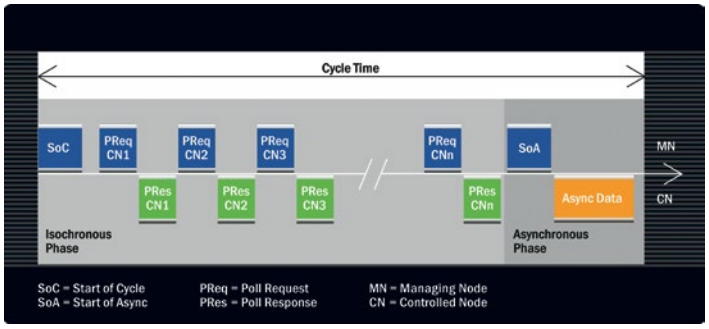
Die Sicherheit industrieller Steuerungs- und SCADA-Systeme ist seit mehr als einem Jahrzehnt ein ernstes Thema. Auf dieses wird seit der Entdeckung des Stuxnet-Virus im Jahr 2010, des Duqu-Virus 2011 und des Shamoon-Virus 2012, die alle spezifisch industrielle Steuerungssysteme angegriffen hatten, ein besonderes Augenmerk gelegt. Im Oktober 2013 veröffentlichte das Repository for Industrial Security Incidents (RISI) seinen Jahresbericht über die Internet-Sicherheitsvorfälle und Trends, die industrielle Steuerungssysteme betreffen. Dieser Bericht enthält eine tiefgreifende Analyse von 240 Vorfällen, die zwischen 2001 und 2012 in der RISI-Datenbank verzeichnet wurden, sowie detaillierte Ergebnisse und Analysen der jährlichen RISI-Sicherheitsuntersuchung für Steuerungssysteme. Demnach sind 33 Prozent aller Sicherheitsvorfälle in Steuerungen mittels Fernzugriff erfolgt. Die Anzahl der gemeldeten Internet-Sicherheitsvorfälle hat sich in den vergangenen Jahren deutlich erhöht, in einzelnen Branchen um über 150 Prozent.

Hacker und Programmierer von Schadsoftware verschaffen sich über das Internet Zugriff zu einzelnen Computern über deren eindeutige IP-Adressen. Da dieses Adressierungsverfahren von den Protokollen TCP und UDP – den meist verwendeten Protokollen auch in LANs – verwendet wird, werden Angreifer in internen Netzwerken direkt zu individueller Hardware geleitet, selbst wenn diese selbst nicht direkt mit der Außenwelt verbunden ist.

Um die maximale Leistungsfähigkeit zu erreichen, basiert das Powerlink-Protokoll direkt auf dem IEEE 802.3 Ethernet MAC Standard. Der TCP/IP-Stack liegt über der Datenverbindungsschicht von Powerlink. Das bietet den Echtzeit-Kommunikationsschichten einen inhärenten Schutz ▶



Am Ende folgt die asynchrone Phase, in der Anwenderdaten und TCP/IP-Pakete durch das Netzwerk gesendet werden. Eingebaute Router trennen sicher und transparent Echtzeitinformationen und asynchrone Daten; das nicht zu tun, würde ein Risiko für das Echtzeitverhalten des gesamten Systems darstellen. Schadsoftware bliebe deshalb komplett isoliert, selbst wenn sie direkt in das System geschleust wird ▼



Die Hardware in Produktionsmaschinen ist über Feldbus oder immer öfter über eine der gegenwärtig verfügbaren Implementierungen von Industrial Ethernet verbunden. Die verschiedenen Standards unterscheiden sich wesentlich durch die Art, in der Netzwerkknoten adressiert und Daten übertragen werden. Manche davon nutzen weiterhin unverändert das TCP/IP-Protokoll. Daher begegnen Hersteller von Automatisierungssystemen und Anbieter industrieller IT-Hardware, die diese Standards unterstützen, diesem Problem, indem sie zum Schutz ethernetbasierter Netzwerke in der Maschinenhalle Sicherheitskonzepte mit industrietauglicher Firewall-Hardware anbieten.

Eingebaute Firewall

Andere Industrial-Ethernet-Protokolle, besonders solche, die harte Echtzeitanforderungen abdecken, nutzen für den Großteil der Datenübertragung Master-Slave-Kommunikationsmechanismen und greifen nur zum Durchschleusen der regulären Ethernet-Kommunikation durch das System auf TCP/IP-Kommunikationsschichten zurück. Einige dieser Modelle bedienen sich keinem Standard entsprechender Schichten und können so zukünftig Kompatibilitätsprobleme nach sich ziehen. Es gibt jedoch Netzwerkprotokolle für Industrial Ethernet, die nicht nur auf unveränderten, zertifizierten Ethernet-Layers nach IEEE 802.3 aufsetzen, sondern auch deterministische Kommunikationsschichten für die Echtzeitkommunikation nutzen.

Eine Technologie, die eine solche Architektur aufweist, ist Powerlink. Es kombiniert Zeitschlitz- und Polling-Verfahren für die isochrone Datenübertragung. Wie der Master-Knoten die von ihm kontrollierten Knoten adressiert, können Softwareentwickler mittels entsprechender Entwicklungswerkzeuge einstellen. Das ist jedoch anderen Einheiten im Netzwerk nicht transparent. „Da für Anwender keinerlei Möglichkeit besteht, während der Laufzeit auf diese Konfigurationsdetails zuzugreifen, besteht kein Bedarf für besonderen Schutz vor bösartigen Manipulationen im System selbst", sagt Schönegger.

Allgemeine Daten vollständig isoliert

Jeder Powerlink-Kommunikationszyklus besteht aus drei Phasen. In der Initialisierungsphase sendet der Master-Knoten als Vorbereitung für den in der zweiten, zyklischen Periode erfolgenden isochronen Datenaustausch eine Synchronisierungsnachricht an alle von ihm kontrollierten Knoten. Am Ende folgt die asynchrone Phase, in der Anwenderdaten und TCP/IP-Pakete durch das Netzwerk gesendet werden. Eingebaute Router trennen sicher und transparent Echtzeitinformationen und asynchrone Daten; das nicht zu tun, würde ein Risiko für das Echtzeitverhalten des gesamten Systems darstellen. Schadsoftware bliebe deshalb komplett isoliert, selbst wenn sie direkt in das System geschleust wird.

Von außen eindringende Hacker oder Schadsoftware haben zudem keine Chance, ein Powerlink-Netzwerk zu gefährden. Sie würden nur auf die andere Seite des als steuernder Netzwerkknoten fungierenden Rechners gelangen. Da Angriffe auch davon abgehalten werden sollten, über die TCP/IP-Kommunikationsschichten durch das Industrie-Netzwerk zu reisen, ist es sinnvoll, auf der Nicht-Powerlink-Seite der Router alle externen Leitungen mit einer passenden Firewall zu schützen. Die Echtzeit-Kommunikationsschichten von Powerlink sind jedoch auch ohne derartige Vorsichtsmaßnahmen inhärent geschützt.

Hohe Geschwindigkeit, Verfügbarkeit und Sicherheit

Powerlink verdankt viel von seinem Sicherheitsniveau der Tatsache, dass es sich um Open-Source-Software handelt. Der Quellcode des Stacks und alle Abwandlungen davon sind häufigen Überprüfungen durch die Gemeinschaft ausgesetzt. Das verhindert nicht nur Sicherheitsprobleme – diese werden entdeckt und eliminiert, lang bevor sie Schaden anrichten können – sondern bietet auch wirksamen Schutz vor verborgenen Backdoor-Angriffen.

„Da die frühen Phasen von Industrie 4.0 zur Realisierung hoher und nachhaltiger Effizienz auf das ‚Internet der Dinge' setzen, benötigen Anlagen industrielle Kommunikationsmechanismen, die nicht nur schnell und offen sind, sondern zugleich hoch verfügbar", sagt Schönegger. „Powerlink erfüllt alle nötigen Kriterien: hohe Geschwindigkeit unabhängig von der Größe des Netzwerks, völlige Offenheit, eine große Unempfindlichkeit gegenüber elektrischer Störungen, Leitungs- und Masternode-Redundanz sowie inhärente Sicherheit, an der sich Angreifer die Köpfe anrennen." ■

KONTAKT

Ethernet Powerlink Standardization Group
Tel.: +49 33439 539 270
info@ethernet-powerlink.org
www.ethernet-powerlink.org