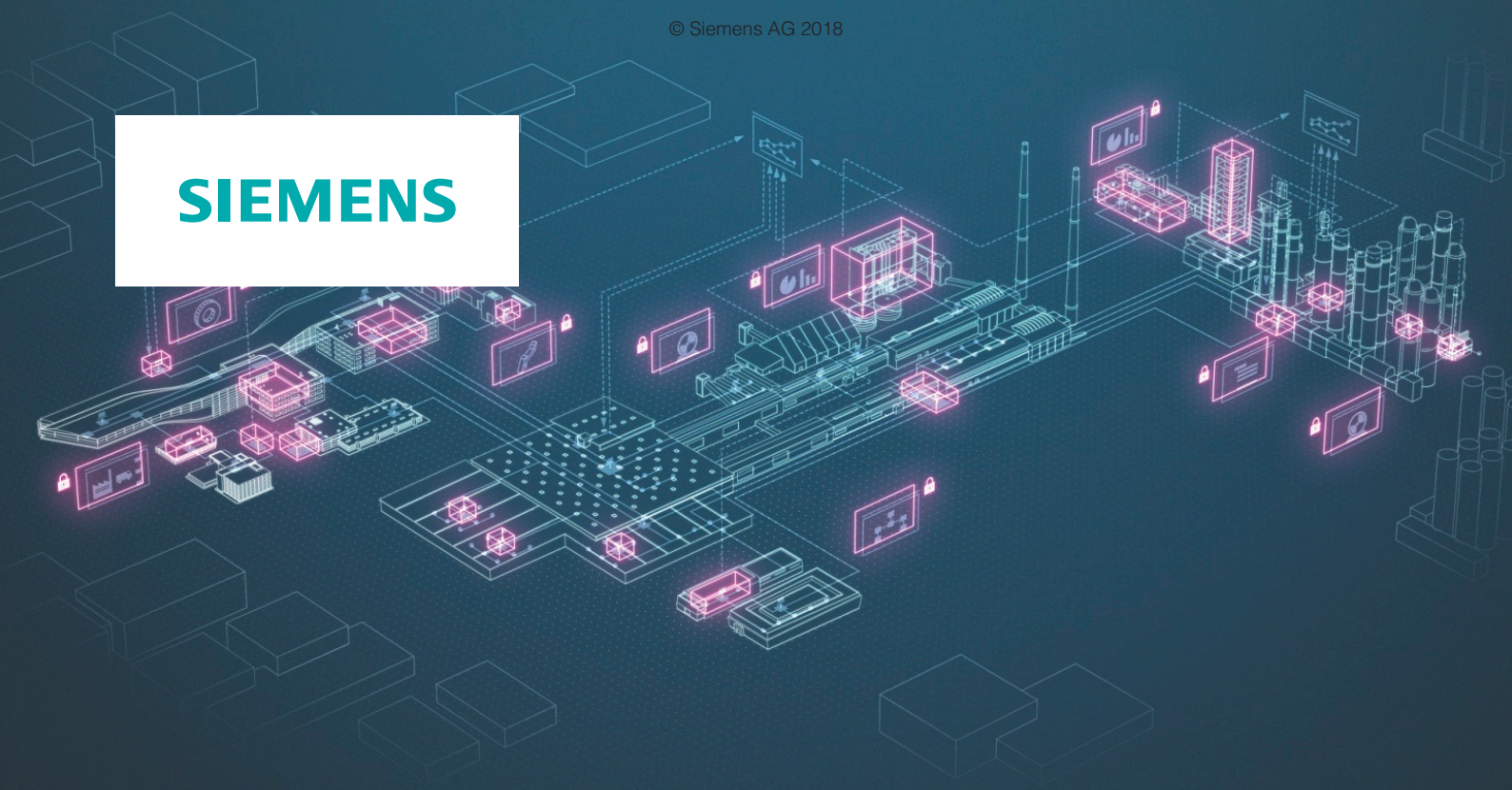
SIEMENS



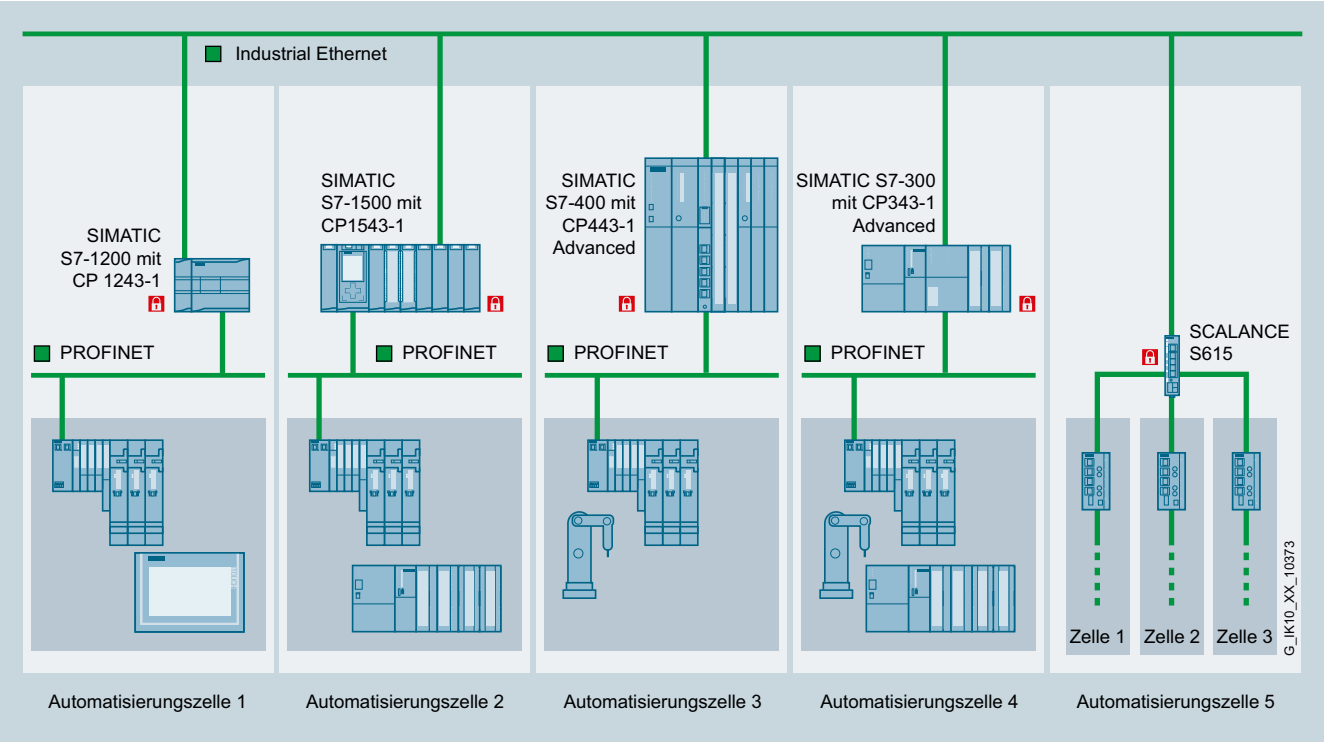
Fachartikel

Security Anforderungen von Industrie 4.0 meistern

Die Fabrik- und Prozessautomatisierung erreicht neue Integrationsebenen, die weit über die Automatisierung hinausgehen. Dies öffnet nicht nur den Weg für einen deutlich höheren Grad an Effizienz, Prozesskontrolle und Flexibilität, sondern verlangt auch erhöhte Sicherheit, um die gesamte Fabrik vor Malware und unbefugtem Zugang zu schützen.

Digitalisierung, Industrie 4.0 und ähnliche Initiativen sind nicht nur Schlagworte. Sie stehen für nicht weniger als die nächste Dimension der Effizienz in industriellen Produktionssystemen und Prozessanlagen. Automatisierungssysteme und Informationstechnologie verschmelzen, während Fernzugriff, Prozessüberwachung, Steuerung und Wartung ein neues Maß erreichen. Big Data gewährt neue Einblicke und hilft, Prozesse effizient zu steuern und die Anlagenverfügbarkeit zu steigern. Mit mehr und mehr vernetzten Geräten im industriellen Internet der Dinge (IIoT) werden Automatisierungsinseln verschwinden – daher sind zuverlässige, sichere und zukunftsfähige industrielle Kommunikationsnetzwerke so wichtig.

Allerdings sind viele Anlagenbetreiber der Meinung, dass Industrie 4.0 neue Herausforderungen schafft, wenn es darum geht, Automatisierungssysteme vor Malware, unbefugtem Zugang und Sicherheitslücken zu schützen – sowohl vorsätzliche als auch unbeabsichtigte. Anlagenbetreiber sind frühere, medienwirksame Vorfälle wohl bekannt, und zögern deshalb oft, innovative Technologien einzuführen – aus Angst, diese könnten ihr System neuen Schwachstellen und Angriffsmöglichkeiten aussetzen.



Für die Implementierung von Zellschutzkonzepten verfügt Siemens über Komponenten mit integrierter Sicherheit – diese Komponenten bieten nicht nur integrierte Kommunikationsfunktionen, sondern auch spezielle Sicherheitsfunktionen wie Firewalls und VPNs.

Offenheit als Schlüssel zum Erfolg

Siemens weiß aus eigener Erfahrung, dass Cyber-Angriffe nicht zu unterschätzen sind. Als Global Player im Bereich Automatisierung und Betreiber vieler Fabriken weltweit hat Siemens daher eine Philosophie angenommen, die dieses Thema tatkräftig adressiert – mit Einbindung von Security Belangen in das Produktdesign, die Systementwicklung und die Dienstleistungen. Komponenten mit integrierter Sicherheit sind ein Paradebeispiel dafür – sie verfügen nicht nur über integrierte Kommunikationsfunktionen, sondern auch über spezielle Sicherheitsfunktionen wie Firewalls und VPNs. Darüber hinaus arbeitet Siemens eng mit Kunden zusammen, um jede Schwachstelle offen anzugehen und effektiv auf Systemeinbrüche zu reagieren.

Vorteile von Erfahrungen aus erster Hand

Für Anbieter von Automatisierungssystemen ebenso wie Anlagenbetreiber ist die Systemverwundbarkeit ein heikles Thema. Technologiepartner sollten aber in der Lage sein, dieses Thema in einem Umfeld gegenseitigen Vertrauens und offener Kommunikation zu behandeln. Als Global Player sowohl in der diskreten Fertigung als auch in Prozessindustrien, können Siemens-Experten und ihre Lösungsanbieter auf enormes Know-how von unzähligen Installationen rund um den Globus zurückgreifen – und sind daher mit den besonderen Herausforderungen unterschiedlichster Branchen und Kunden vertraut.

In vielen Teilen der Welt betreibt Siemens auch eigene Fertigungsstätten, wo Siemens seine Produkte und Komponenten mit integrierter Sicherheit wirksam in ganzheitlichen Sicherheitskonzepten zum Schutz von Fabriken und Automatisierungssystemen einsetzt. Dies ermöglicht es Siemens seinen Kunden führende Lösungen anzubieten, die auf Komponenten und Systemen basieren, die sich in den eigenen Anlagen bewährt haben.

Ganzheitliche Sicherheitskonzepte (Holistic Security Concepts) werden bereits in Siemens-Fabriken eingesetzt.

Neben dem entscheidenden Aspekt der Sicherheit, ist ein weiteres wichtiges Produktattribut die Möglichkeit Inbetriebnahme- und Wartungsarbeiten ohne technische Fachkenntnisse vor Ort ausführen zu können. Erreicht wird dies, indem alle Hardwarekonfigurationen entweder in die Engineering-Software oder intelligente Plug-Ins integriert werden – so dass keine manuelle Konfiguration vor Ort notwendig ist. Servicetechniker müssen lediglich die defekte Komponente abtrennen, austauschen und wieder anschließen, ohne sich um Konfigurationseinstellungen und mögliche Fehler Sorgen zu machen.

Ganzheitlicher Ansatz für industrielle Sicherheit

Security geht weit über eine effektive Firewall hinaus. Angesichts der allgegenwärtigen Gefahr von Cyber-Angriffen ist ein ganzheitlicher Ansatz erforderlich, der vom physischen Anlagenschutz auf Basis eines effektiven Zugangskontrollsystems bis zur Behebung von Softwareproblemen, z. B. über Sicherheits-Patches und Updates, reicht.

Aus diesem Grund hat Siemens einen Hard- und Software-Entwicklungsprozess (Secure-by-Design) eingeführt, der alle relevanten Sicherheitsaspekte von Anfang an aktiv integriert. In allen Entwicklungsprojekten arbeitet der verantwortliche Projektmanager zusammen mit einem fest zugeordneten Sicherheitsexperten. Dieser Experte ist für eine umfassende Sicherheitsüberprüfung der angeforderten Eigenschafften und des Designs verantwortlich, und führt auch Sicherheitstests vor Markteinführung eines Produkts durch. Der Sicherheitsexperte ist ermächtigt, die Freigabe eines Projekts im Falle von schwerwiegenden Sicherheitslücken zu stoppen.

Die neuen Industrial Security Appliances SCALANCE SC-600 – Secure-by-Design nach IEC 62443-4-1 in Verbindung mit Bedrohungs- und Risikoanalysen und Penetrationstests

Der Sicherheitsprozess muss alle Bedrohungen und Risiken für das industrielle Umfeld, in dem die Produkte eingesetzt werden, detailliert beurteilen und bewerten. In diesem Zusammenhang ist anzumerken, dass Siemens Mitglied der ISA 99 – der Normungsorganisation für die führende internationale Industriesicherheitsnorm IEC 62443 – ist, mit der klaren Zielsetzung, die etablierten Industrienormen vollständig zu erfüllen. Siemens treibt auch die Entwicklung solcher Normen tatkräftig voran – unter Berücksichtigung von Kundenanforderungen hinsichtlich der Integration von Zuverlässigkeits- und Sicherheitsaspekten, die für ihre Fabrik- und Prozessautomatisierungssystemumgebungen von entscheidender Bedeutung sind.

Sicherheit als Qualitätsstandard und offene, transparente Schwachstellenbehebung

Im Rahmen des Secure-by-Design-Entwicklungsprozesses werden alle neu entwickelten Hardware- und Softwarekomponenten von einem Team von Sicherheitsexperten analysiert. Diese Experten suchen nach Problemen, die die Komponente anfällig für Angriffe von außen machen, und somit die Sicherheit des gesamten Automatisierungssystems beeinträchtigen. Diese Überwachung wird fortgesetzt, selbst nachdem das Produkt auf den Markt gebracht worden ist.

Deshalb arbeiten Sicherheitsexperten von Siemens eng mit namhaften Sicherheitsforschern an Universitäten, Sicherheitsdienstleistern und CERT-Organisationen auf der ganzen Welt zusammen. Dadurch hat Siemens Zugriff auf die neuesten sicherheitsrelevanten Informationen. Jede identifizierte Schwachstelle wird in kürzester Zeit von einer speziell für diesen Zweck gebildeten Arbeitsgruppe beseitigt. Produkt-Updates werden entwickelt und verifiziert – und Sicherheits-Patches werden allen Kunden, die betroffen sein könnten, zur Verfügung gestellt.

So reflektieren diese Hardware- und Softwareprodukte einen Qualitätsstandard, bei dem der Produktsicherheit eine höhere Priorität eingeräumt wird, wie z.B. möglichst schneller Markteinführungszeiten. Mit dem Ziel sich als vertrauenswürdiger langfristiger Partner bei seinen Kunden zu etablieren, legt Siemens – basierend auf dem Secure-by-Design-Entwicklungsprozess – weitaus größeren Wert darauf, ein sicheres Produkt auf den Markt zu bringen, als zuerst eine neue Technologie einzuführen.

Mit der tiefengestaffelten Verteidigung (Defense-in-Depth) liefert Siemens ein vielseitiges Konzept, das Anlagen und Systeme rundum und tiefgreifend schützt. Das Konzept basiert auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität – in Übereinstimmung mit den Empfehlungen der IEC 62443.

Security als wesentlicher Faktor zur Senkung der Gesamtbetriebskosten

Cyber-Angriffe können ganze Prozessanlagen oder Fertigungssysteme zum Stillstand bringen. Daraus resultiert nicht nur ein erheblicher Kapitalverlust für das beteiligte Unternehmen, sondern es kann – je nach Branche – auch zu einem Reputationsschaden führen und das Unternehmen kostspieligen Haftungsansprüchen aussetzen. Güter können sogar auf die schwarze Liste gesetzt werden, wenn sie Teil einer öffentlichen Infrastruktur sind.

Als Folge dessen sind immer mehr Unternehmen bereit, in die Sicherheit ihrer Automatisierungssysteme zu investieren – durch Zusammenarbeit mit einem Partner wie Siemens, der Sicherheit als integralen Bestandteil seiner Geschäftsstrategie hervorhebt. Investitionen in gehärtete Produkte lohnen sich, denn sie tragen erheblich dazu bei, die Betriebskosten während des gesamten Lebenszyklus des Systems zu senken.

Lebenslange Sicherheitsdienstleistungen

„Die zunehmende Anzahl von Cyber-Angriffen ist eine Tatsache, die nicht übersehen werden kann. Aber das darf kein Grund sein, auf die Digitalisierung der industriellen Produktion zu verzichten. Stattdessen sollte Cyber-Sicherheit als Wettbewerbsvorteil und nicht als Kostenfaktor angesehen werden“, erklärt Helmuth Ludwig, Chief Information Officer bei Siemens.

Industrielle Sicherheit ist ein strategisches Sicherheitskonzept, das helfen soll, den Weg zum digitalen Unternehmen von morgen zu ebnen. Es basiert auf dem in der IEC 62443 vorgeschlagenen tiefengestaffelten Verteidigung (Defense-in-Depth).

Industrielle Sicherheit umfasst nicht nur sicherheitsrelevante Produkteigenschaften, sondern auch die Gestaltung von Automatisierungssystemen mit Hilfe vordefinierter und sicherheitsgeprüfter Softwarekomponenten. Darüber hinaus bietet es Kunden eine Reihe von sicherheitsrelevanten Dienstleistungen, die Automatisierungssysteme kontinuierlich überwachen, sowie die Entwicklung von präventiven Sicherheitsmaßnahmen.

Industrielle Cyber-Sicherheit ist eine Herausforderung, die jedoch durch gemeinsame Anstrengung, offene Kommunikation und dedizierte Dienstleistungen gemeistert werden kann. Die Dienstleistungen für Anlagensicherheit, Patch-Management und Schwachstellen-Management bieten genau die richtige Unterstützung, die hier benötigt wird.

Securityhinweise

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 **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Deutschland

PDF
Fachartikel
FAV-390-2017-PD-PA
BR 0318 / 4 De
Produced in Germany

siemens.de/industrialsecurity