Fachbeitrag

SAFETY NONSTOP HIMA

Safetylösungen erfordern auch Security

Anlagen zuverlässig vor Cyber-Attacken schützen

(Brühl, Januar 2013)

Während die Netzwerke der Büro-IT und der industriellen Automation immer mehr zusammenwachsen, nimmt gleichzeitig das Risiko für Cyber-Attacken auf Anlagen über diese Netzwerke zu. Der Bedarf Security-Barrieren in der Automation zu erhöhen wächst dadurch kontinuierlich. In diesem Beitrag wird erläutert, welche Maßnahmen zur Cyber Security beitragen und welche Vorteile autarke Sicherheitssteuerungen dabei bieten.

Safety dient dem Schutz von Mensch, Anlage und Umwelt. Die Anlage darf also keinen Schaden anrichten. Bei Security hingegen ist die Anlage selbst vor Schaden zu schützen. Es ist sicherzustellen, dass Informationen und Daten – und damit auch Programme – ausschließlich für den bestimmungsgemäßen Gebrauch verwendet werden können und dass ein möglicher Schaden durch Verfälschung vermieden wird.

Sowohl für Safety als auch für Security gilt, dass es einen Zustand „sicher“ oder „dauerhaft sicher“ nicht gibt. Man kann nur die Barrieren u. a. gegen Angriffe erhöhen oder Fehler vermeiden, um das Risiko zu reduzieren. So sind bei Safety sowohl zufällige, nicht reproduzierbare Fehler als auch systematische, reproduzierbare Fehler zu betrachten. Dagegen ist bei Security ausschließlich von systematischen Fehlern auszugehen; hier steht die gezielte Manipulation im Vordergrund.

Security ist ein Prozess, der durch organisatorische und technische Maßnahmen unterstützt werden muss. Im Folgenden wird erläutert, was Hersteller- und Anwender dabei berücksichtigen sollten.

Sinnvolle Dokumentation

Safety kann durch die hohen Qualitätsanforderungen einiges zur Security beitragen. Grundvoraussetzung ist, dass die Eigenschaften richtig dokumentiert sind. Als Hersteller sicherheitsgerichteter Steuerungen dokumentiert HIMA so für jede Phase des Lifecycles sämtliche

sicherheitsrelevanten Informationen zu den Produkten wie z. B. Passwortvergabe, Ports und Protokolle für die Hard- und Software. Integratoren sind beispielsweise für die Dokumentation von Netzwerkstruktur und Back-ups verantwortlich. Anwender sollten z. B. stets den tatsächlichen Zugriffsschutz und Updates verwalten und dokumentieren.

Unsicherheitsfaktor Mensch

Im Fall der Cyber Security spielt der unberechenbare Faktor Mensch eine entscheidende Rolle. Awareness und Ausbildung sind hier wichtige Elemente des Schutzes. Denn werden Mitarbeiter über mögliche Gefahren für die Anlagensicherheit aufgeklärt und in den Security-Prozess einbezogen, können sie wertvolle Hilfe zu deren Verbesserung liefern. Die internationale Normreihe ISO 2700X oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) geben wertvolle Hinweise, z.B. wie man Netzpläne erstellt, Recovery-Strategien erarbeitet, mit Passwörtern umgeht, Mitarbeiter schult und Reviews organisiert.

Autarke Sicherheitssysteme bringen Vorteile

Neben organisatorischen Maßnahmen sind geeignete technische Maßnahmen für die Security zu treffen. Safety und Security nutzen oft ähnliche Konzepte. So rät die Norm Safety-Norm IEC 61511 zur Verwendung von Schutzebenen (Layers of Protection). Des Weiteren wird eine Trennung von Betriebs- und Schutzeinrichtung zur Reduzierung von common-code-Fehlern gefordert. In der Betriebseinrichtung sind häufig Änderungen durchzuführen, die Schutzeinrichtung hingegen ist statischer und obliegt sehr wenigen Änderungen.
Auch der Entwurf der Security-Norm IEC 62443 empfiehlt, Teilsysteme zu trennen. Dieses Prinzip wird „Defence in the Depth“ genannt.
Danach bildet die sichere Steuerung die letzte Verteidigungslinie gegen Cyber-Attacken.

Autarke Sicherheitssysteme bieten klare Vorteile, da sie systematische Fehler deutlich reduzieren. Die getrennten Verantwortungsbereiche und die Zuständigkeiten für das Sicherheitssystem werden „automatisch“ geregelt, was die Anzahl gleichartiger Engineering-Fehler minimiert.

Sicherheitsfokussierter Entwicklungsprozess

Security beginnt bereits in den Entwicklungsabteilungen der Hersteller. So bezieht HIMA von Anfang an Maßnahmen zur Cyber Security in die Produktentwicklung mit ein. Dazu zählt das „Achilles“-Testverfahren von Wurldtech, das international im Bereich Öl&Gas für die Überprüfung industrieller Cyber Security anerkannt ist und eine Online-Simulation von Cyber-Angriffen beinhaltet. Das Prozessormodul X-CPU 01 und das Kommunikationsmodul X-COM 01 des HIMA-Sicherheitssystems HIMax haben bei diesen Tests ihre Widerstandsfähigkeit gegen Cyber-Angriffe bewiesen und das Achilles Level I-Zertifikat erhalten.

Des Weiteren lässt HIMA kontinuierlich alle wichtigen Faktoren zum Thema Security in die Sicherheitshandbücher der Produkte einfließen.

Ein sicherheitsfokussierter Entwicklungsprozess gewährleistet einen hohen Qualitätsstandard der Produkte. Ein wichtiger Aspekt ist hier das Vier-Augen-Prinzip. Es wird nur das entwickelt, was spezifiziert wurde. Dadurch wird verhindert, dass nicht geplante Eigenschaften in die Steuerungen einfließen können. Bei der Entwicklung des Sicherheitssystems HIMax wurde zum Beispiel darauf geachtet, dass das System Telegramme, deren Inhalt nicht der Protokollspezifikation oder der Erwartung entsprechen, verworfen und nicht beantwortet werden. So werden u. a. nicht benutzte Ports, ähnlich wie bei einer Firewall, gesperrt.

Sicherheitssteuerung bietet Security-Vorteile
Speziell für die Funktionale Sicherheit konzipierte SIL 3-Sicherheitssteuerungen wie HIMax beinhalten Eigenschaften, die auch für die Cyber Security enorm hilfreich sind.

Durch die physikalische Trennung von CPU und Kommunikationsmodul kann die Kommunikation von der X-CPU zu X-COM nicht erzwungen werden. Die funktionale Sicherheit ist dadurch selbst dann gewährleistet, wenn der Kommunikationsprozessor attackiert wird. Eine weitere Security-Maßnahme ist die Port-Deaktivierung, mit der nicht genutzte physikalische Ports auf der CPU bzw. dem Kommunikationsmodul deaktiviert werden können.

Durch die Verwendung von sogenannten Systemvariablen können Steuerungszugriffe auf ein HIMax System blockiert werden. Damit ist es z.B. möglich durch einen vor-Ort Schlüsselschalter oder über ein anderes Freigabesignal den Zugriff auf das System zu erlauben oder zu sperren.
So können über Variablen im Anwenderprogramm das „Forcen“ deaktiviert, im laufenden Betrieb ein reiner „Nur lesen“-Zugriff ermöglicht und die Möglichkeit der Online Änderung (Reload) deaktiviert werden. Zusätzliche Security bietet auf dieser Ebene der CRC-Schutz. Prüfsummen (CRC) des Projekts und der einzelnen Programme werden hierbei in Variablen angeboten und können im SCADA bzw. Prozessleitsystem angezeigt und überprüft werden. Zusätzlich kann jedes Laden mittels Systemvariablen erkannt und alarmiert werden. Das HIMax-System bietet durch diese integrierten Sicherheitsmaßnahmen die Möglichkeit, ein Anlagensystem ganz nach den jeweiligen Bedürfnissen vor externen Einflüssen abzuschotten.

Engineeringtool unterstützt Security
Auf der Engineeringebene schützt das Programmiertool SILworX vor Manipulationen und Bedienfehlern. Über ein zweistufiges Benutzermanagement können unabhängig Zugriffsrechte für Projektdaten

(PADT-Benutzerverwaltung) und einzelne Steuerungen (PES-Benutzerverwaltung) vergeben werden. Dabei werden die Benutzer auf Projektebene den Benutzergruppen zugeordnet und nur die Benutzergruppen auf der Steuerung hinterlegt. Damit ist es möglich personalisierte Benutzerrechte zu verwenden ohne bei jeder Änderung der Personen oder deren Passworte die Steuerung anpassen zu müssen.

SILworX kann sich mittels CRC-Schutz zusätzlich selbst schützen, indem alle relevanten Dateien anhand ihrer Prüfsummen kontrolliert werden – bei falscher Prüfsumme wird die Codegenerierung konsequent verweigert.

Über HIMA

HIMA ist der weltweit führende Spezialist für sicherheitsgerichtete Automatisierungslösungen. HIMA-Lösungen bieten maximale Sicherheit, maximale Verfügbarkeit und sie lassen sich in jedes Automatisierungsumfeld integrieren. Über 30.000 HIMA-Systeme wurden in mehr als 40 Jahren in über 80 Ländern installiert und schützen die Anlagen der weltweit größten Unternehmen der Öl- und Gas-, der chemischen, pharmazeutischen und der energieerzeugenden Industrie. In den Bereichen Schienenverkehr, Logistik und Maschinensicherheit zeigen HIMA-Lösungen neue Wege zu mehr Sicherheit und Profitabilität auf. Mit dem Konzept der HIMA LIFECYCLE SERVICES gewinnen HIMA-Kunden den Überblick über alle Anforderungen der „Funktionalen Sicherheit“ und treffen stets zum richtigen Zeitpunkt die richtige Entscheidung. Mehr Informationen über HIMA finden Sie hier: www.hima.de

Autor:

Stefan Ditting, Produktmanager bei HIMA Paul Hildebrandt GmbH + Co KG

Pressekontakt:

HIMA Paul Hildebrandt GmbH + Co KG
Nicole Pringal
Albert-Bassermann-Straße 28
68782 Brühl
Tel.: +49 6202 709-405
Fax: +49 6202 709-123
E-Mail: n.pringal@hima.com
Internet: www.hima.de

BILDER

Die Bilder stehen auf unserer Homepage zum Download bereit oder werden auf Wunsch per E-Mail zugesandt.
Link: http://www.hima.de/Presse/default.php

Bild 1
Schmuckbild

Bild 2
Quelle: HIMA Paul Hildebrandt GmbH + Co KG
BU: Die SIL 3-Sicherheitssteuerung HIMax bietet Eigenschaften, die zur Cyber Security beitragen.

Bild 3
Quelle: HIMA Paul Hildebrandt GmbH + Co KG
BU: Auf der Engineeringebene schützt das Programmiertool SILworX vor Manipulationen und Bedienfehlern.

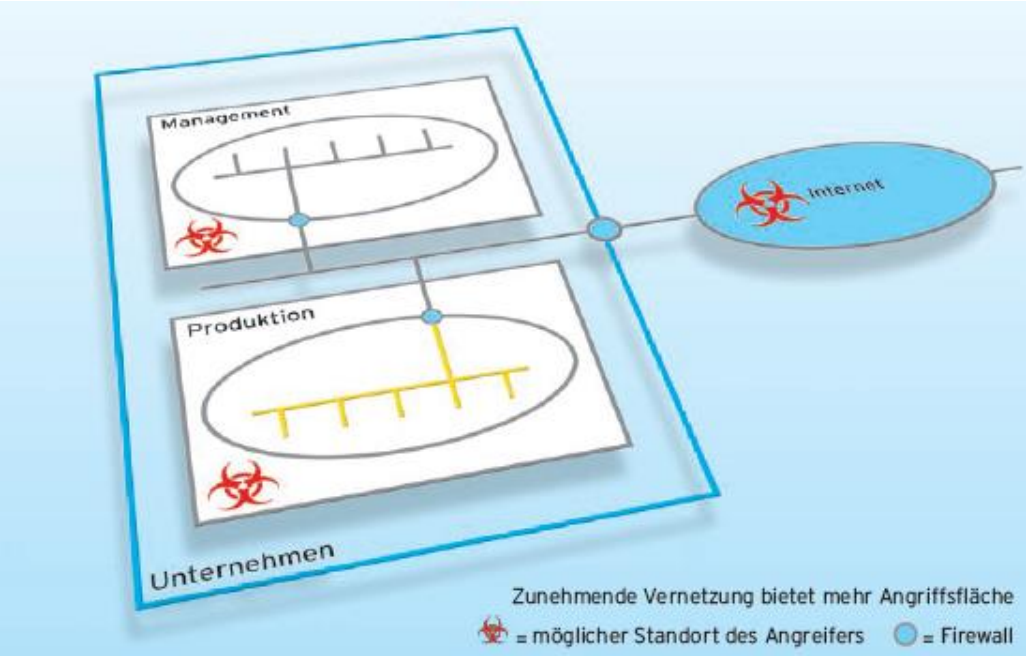

Bild 4
Quelle: HIMA Paul Hildebrandt GmbH + Co KG