Process Control Network Security

Motivation

Durch die steigende Vernetzung der sehr heterogenen Komponenten im industriellen Umfeld entstehen immer höhere Anforderungen an Verfügbarkeit, Integrität und Anlagensicherheit. Im geplanten Projekt liegt der Fokus auf Prozess-Kontroll-Netzwerken (engl.: Process Control Networks, PCN). Eine besonders große Herausforderung ist dabei die Tatsache, dass die einzelnen Endgeräte aus unterschiedlichen Hardwarekomponenten und Betriebssystemstrukturen bestehen. Dies ist auch auf die hohe Lebensdauer (ca. 20 Jahre) und den steigenden Vernetzungsgrad der verwendeten Industrial Control Systems (ICS) zurückzuführen. Die eingesetzten Automatisierungs- bzw. Prozesssteuerungs- und leitsysteme waren bis vor einigen Jahren isolierte Geräte bzw. Netzwerke. Deswegen lag der Fokus vor allem auf funktionaler Sicherheit (engl.: safety). Heutzutage sind diese immer stärker, sowohl untereinander als auch mit dem restlichen Firmennetzwerk, vernetzt. Dies dient z.B. dem Auslesen des aktuellen Produktionsstatus. Dass dadurch wesentlich höhere Angriffspotential wird allmählich von den Herstellern, Integratoren sowie Anwendern gleichermaßen erkannt. So findet seit dem Auftauchen von Stuxnet, Duqu und Flame ein kontinuierliches Umdenken statt. Und auch aktuellere Vorfälle sowie die Tatsache, dass hunderte Industrieanlagen ungesichert im Internet auffindbar sind führen die Brisanz der Lage vor Augen und verdeutlichen den akuten Handlungsbedarf. Ein systemischer Ansatz zur Erkennung von Anomalien und die Umsetzung entsprechender Sicherheitsmaßnahmen speziell in Prozessnetzen fehlen bis dato komplett. Weiter werden in den vorhandenen Netzwerken sicherheits- und vertrauensrelevante Aspekte oftmals als sekundär erachtet und nur rudimentär umgesetzt. Gründe hierfür sind das fehlende Bewusstsein für die aktuell bestehenden Bedrohungen für ICS und die Kosten, die entsprechende Schutzmaßnahmen mit sich bringen würden. Das Ergebnis sind erheblich anfälligere IT-Infrastrukturen und insgesamt substanziell höhere Gesamtkosten (Total Cost of Ownership, TCO) für PCN, z.B. durch den Ausfall einer Produktionsanlage oder den Imageverlust bei einem erfolgreichen Angriff.

Vorgehen

Im geplanten Vorhaben sollen intelligente Sensoren entwickelt werden, die Anomalien in PCN erkennen und gegebenenfalls eindämmen können. Wesentliche Faktoren dabei sind die Wirtschaftlichkeit und die Benutzerfreundlichkeit der angestrebten Lösung.

Um dies zu garantieren werden folgende Teilziele definiert:

1. Spezifikation der Anwendungsfälle Die angestrebten Sicherheitsmechanismen sollen in diversen Anwendungsbereichen eingesetzt werden können, z.B. Fertigungs- und Prozessindustrie oder auch kritische Infrastrukturen, wie beispielweise der Energieversorgung. Dafür ist es notwendig die Problemstellungen und den Bedarf der einzelnen Branchen zu kennen und dementsprechend zu berücksichtigen. Dies soll durch die beteiligten Industriepartner gewährleistet werden. So sollen einerseits ihre Problemstellungen sowie auch die Bedürfnisse ihrer Kunden in einen Demonstrator, der die Anforderungen der einzelnen Anwendungsfälle widerspiegelt, einfließen.

2. Konzipierung der Messsensoren Ausgehend von den analysierten Anwendungsfällen werden die intelligenten Sensoren, die für eine Vorverarbeitung der Daten vorgesehen sind, entwickelt. Hier liegt das Hauptaugenmerk auf der Ressourceneffizienz, um das Produktionsnetzwerk nicht zu stark zu belasten und die Schutzziele zu bewahren. Sie sollen ein skalierbares und benutzerfreundliches Sicherheitsmanagement vernetzter Industriesteuerungen und Produktionsanlagen ermöglichen ohne dabei die Verfügbarkeit der Anlage zu gefährden. So darf beispielweise keine Beeinträchtigung des Echtzeitverhaltens erfolgen.

3. Auswertung der Messdaten Die von den Sensoren vorverarbeiteten Daten werden im nächsten Schritt ausgewertet. Hier ist darauf zu achten, dass möglichst wenige Fehlmeldungen ausgelöst werden und auf Vorfälle angemessen reagiert werden kann. Ein Ziel ist es die Daten so aufzubereiten, dass bereits eine Vorauswahl an Möglichkeiten zur Verfügung gestellt wird und so ein hohes Maß an Benutzerfreundlichkeit ermöglicht werden kann. Durch eine verteilte Datenvorverarbeitung und eine Reaktionsunterstützung zur Anomalieeindämmung soll eine hohe Verfügbarkeit und Funktionssicherheit sowohl bei gezielten IT-basierten Angriffen als auch Eingriffen durch Fahrlässigkeit oder Fehlbedienung gewährleistet werden.

4. Erstellen eines Implementierungskonzeptes Zusammen mit den Industriepartnern soll ein Implementierungskonzept erstellt werden. Ein wesentliches Ziel ist dabei die Wirtschaftlichkeit. Denn nur kostengünstige, leicht zu bedienende Lösungen werden auf positive Resonanz und schließlich Akzeptanz stoßen. Ein wichtiger Eckpunkt, um die Akzeptanz zu steigern ist das Bestreben die Erkenntnis (engl.: Awareness) der Notwendigkeit von Sicherheitsmaßnahmen in Process Control Networks zu etablieren. Gemeinsam mit den Industriepartnern sollen hierfür geeignete Strategien entwickelt werden.

Eckdaten

Kurztitel

PCN-Sec

Forschungsschwerpunkt

Digital Technologies

Laufzeit

01.07.2015 - 30.06.2019

Fördergeber

Bundesministerium für Bildung und Forschung

Projektleitung

Prof. Dr.-Ing. Peter Fröhlich