Anomalieerkennung und eingebettete Sicherheit in industriellen Informationssystemen

Motivation

Industrielle Steuerungen und Computersysteme sind wesentlich weiter verbreitet als dem Normalbürger bewusst ist. Während ca. 200 Mio PCs pro Jahr produziert werden, entstehen gleichzeitig ca. 2 Mrd. Geräte mit eingebetteten Rechner-Kernen. Während in vielen Einsatzbereichen vor Jahren noch isolierte Einzelsysteme vorherrschten, ist mittlerweile eine enge und mehrdimensional vermaschte Struktur vieler Teilsysteme die Regel. Die Anbindung an das Internet und die Unterstützung von Funktionen wie Fernsteuerung, Fernwartung und Fernmanagement sind mittlerweile eine Notwendigkeit. Die Sicherheit inhomogener Computer- und Netzstrukturen wird zwar von Fachleuten aus Industrie und Forschung seit langem als Problem angesehen, sie wird aber mangels verfügbarer einfacher Standardlösungen meist als erstes von der Anforderungsliste gestrichen. Seit dem Bekanntwerden des Stuxnet-Virus setzt in der Branche ein Umdenken ein. Nach Ansicht der meisten Experten kann von einer drastischen Zunahme solcher Angriffe ausgegangen werden. Neben diesen bekannten Bedrohungen gibt es auch eine zunehmende Gefährdung durch systemimmanente Fehler. Durch die schiere Komplexität moderner Software und Hardware verbleibt ein zunehmendes Risiko von unerkannten Entwurfs- und Implementierungsfehlern.

Vorgehen

Aufgrund dieser Bedrohungen zielt das Verbundprojekt zielt auf die Entwicklung resistenter, integrierter Sicherheitstechnologien, welche gleichzeitig Anomalie-Erkennung, integrierte Schutz- und Sicherheitsmaßnahmen und eine Begrenzung des Schadenspotentials (z.B. durch Kompartmentisierung) beinhalten. Die schon lange diskutierten Schutzphilosophien wie „Operation under Attack“ und „ Attack Countermeasurement“ die davon ausgehen, dass solche Angriffe nicht zu verhindern sind und sich ein System selbst schützen muss, werden zunehmend ein Muss. Integrierbare Vertrauens- und Sicherheitsfunktionen wie auch Mechanismen zur sicheren und vertrauenswürdigen Kommunikation, die soweit wie möglich Angriffe eindämmen, den Betrieb komplexer Systeme auch unter Angriffen ermöglichen und die Eindämmung der Reichweite bzw. die Begrenzung von Schäden realisieren sind das Ziel dieses Vorhabens.

Konsortium

Seitens der Industrie wird das Forschungsprojekt durch die Infineon Technologies AG, Hirschmann Automation and Control GmbH, EADS und die Kontron GmbH unterstützt. Dabei beleuchten diese Partner unterschiedliche Ebenen von integrierten Sicherheitsbausteinen, über individuelle eingebettete Systeme bis hin zu Netzwerkkomponenten und komplett vermaschten industriellen Netzwerken. Auf diese Weise können flexible Methoden gefunden und entwickelt werden. Die akademischen Partner bieten durch den unterschiedlichen Blickwinkel eine perfekte Ergänzung für das Vorhaben. Das Fraunhofer-Institut für Sichere Informationstechnik zählt zu den Experten auf dem Gebiet der IT-Sicherheit. Die Technische Universität München als auch die Technische Hochschule Deggendorf unterstützen die Industriepartner bei der Bearbeitung wissenschaftlicher Fragestellungen.

Eckdaten

Kurztitel

ANSII

Forschungsschwerpunkt

Digital Technologies and their Applications

Laufzeit

01.03.2012 - 28.02.2014

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

EADS DEFENCE & SECURITY

Fraunhofer SIT

HIRSCHMANN A BELDEN BRAND

Infineon technologies

kontron

Technische Universität München

Fördergeber

Bundesministerium für Bildung und Forschung

Projektleitung

Prof. Dr.-Ing. Andreas Grzemba