Der Gefahr trotzen

Erweiterte Sicherheit für industrielle Anlagen

Dipl.-Ing. Jana Krimmling, M. Sc. Alexander Sänn
IHP – Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder)

Im Automatisierungsbereich finden wir verschiedenartige Strukturen und eine Vielzahl unterschiedlicher Feldbus- und Kommunikationsprotokolle vor. Doch wie gestaltet man unter diesen Umständen einen besseren IT-Schutz im Feldbusbereich, den sich Hersteller, Integratoren und Anwender der Automatisierungstechnik wünschen? Verteilte Sicherheitskonzepte können zukünftig einen wirksamen Beitrag zur IT-Sicherheit leisten und die Herausforderungen hinsichtlich des Übergangs zur Industrie 4.0 und des „Internets der Dinge“ bewältigen.

Die Automatisierungstechnik steht heute vor einem Punkt, an dem sie sich nur bedingt dem steigenden Grad der Vernetzung entziehen kann. Smart-Factory- oder Smart-City-Anwendungen sind hier nur zwei Schlagwörter des aktuellen Trends. Vor allem hinsichtlich des Übergangs zur Industrie 4.0 treten neue Herausforderungen im Bereich der IT-Sicherheit für Automatisierungsanlagen auf und damit ist die IT-Sicherheit ein allgegenwärtiges Thema geworden. IT-Sicherheit dient dem Schutz von Daten, Anlagen und deren Verfügbarkeit und stellt mögliche Lösungen bereit, um den aktuellen und zukünftigen Gefahren trotzen zu können. Eine solche Lösung können verteilte Sicherheitskonzepte wie die hier vorgestellte verteilte Einbruchserkennung (Intrusion Detection) für industrielle Anlagen [1] bieten.

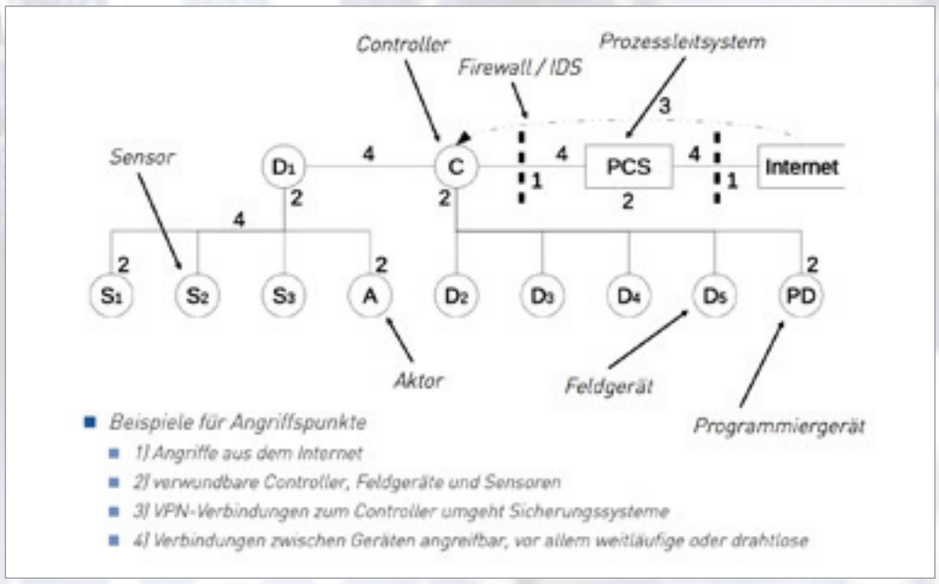

Abb. 1 Hot Topic IT-Security

Jana Krimmling hat Informationstechnologie an der Universität Magdeburg studiert. Sie arbeitet seit 2009 als wissenschaftliche Mitarbeiterin im IHP – Leibniz-Institut für innovative Mikroelektronik in Frankfurt (Oder). Ihre Forschungsgebiete sind eingebettete Systeme, Design und Implementierung von drahtlosen Sensornetzwerken und deren Integration in industrielle Umgebungen, IT-Security und Privacy sowie der Schutz kritischer Infrastrukturen.

Alexander Sänn studierte an der Brandenburgischen Technischen Universität Cottbus eBusiness mit Abschluss M.Sc. Seit 2008 war er für die Fraunhofer-Gesellschaft tätig und wechselte 2009 an das IHP – Leibniz-Institut für innovative Mikroelektronik. Seit 2013 geht er der Promotion an der BTU Cottbus-Senftenberg nach. Seine Forschungsgebiete sind Innovation Management, IT-Sicherheit und die Marktorientierte Produktgestaltung.

Sicherheitsaspekte

Typische Schwachstellen üblicher Installationen zeigen sich auch in Automatisierungssystemen mit den nach IEC-62443 empfohlenen grundlegenden Sicherheitsmaßnahmen. Die am Markt verfügbaren Produkte zur IT-Sicherheit für die Automatisierungstechnik beruhen auf zentralen Ansätzen wie Firewalls und Intrusion- Detection-Systemen (IDS) an den Übergangspunkten vom Automatisierungsnetzwerk zu anderen internen oder externen Netzen. Diese Produkte stellen eine solide Basis zur IT-Sicherung dar. Dennoch treten an anderen neuralgischen Punkten wie an Firewalls selbst, den Feldgeräten, den VPN-Verbindungen zum System oder der drahtlosen Kommunikation zwischen den Teilsystemen des Netzwerkes weiterhin Schwachstellen auf [1]. Firewalls und Intrusion-Detection-Systeme (IDS) werden nach und nach zur Sicherung der Steuerungen in der Feldebene adaptiert, verschieben die Schwachstellen jedoch nur um eine Hierarchieebene in die Feldebene hinein. Die angeschlossenen Sensoren und Aktoren sind weiterhin ungeschützt, werden aber zunehmend komplexer, intelligenter und übernehmen mehr und mehr Aufgaben. Damit bieten sie zukünftiges Potenzial für ausgeklügelte Angriffe.

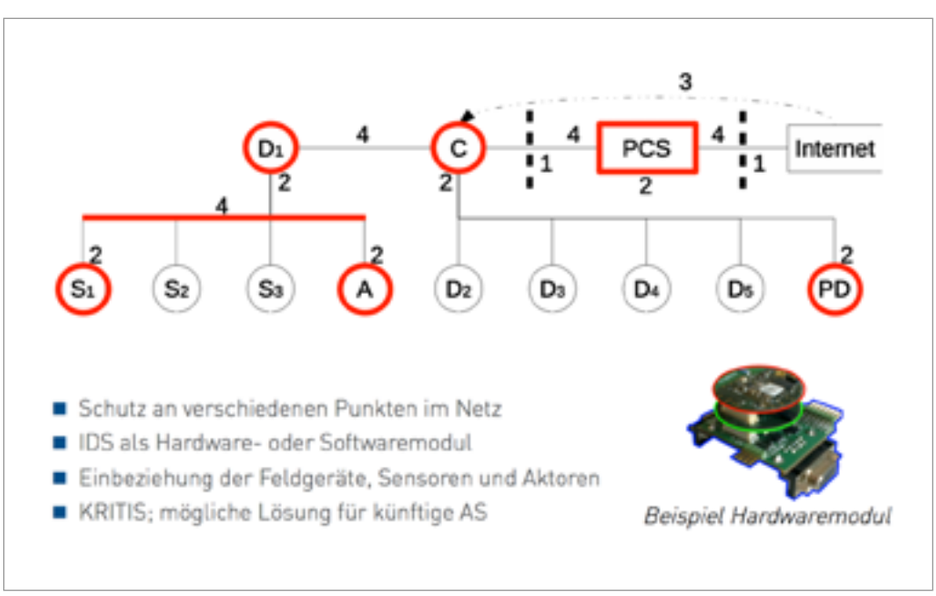

Abb. 2 Ansatz zur verteilten IT-Sicherheit (für industrielle Anlagen in KRITIS)

Sicherheitsprodukte im Focus

Einer Befragung [2] aus dem Jahr 2012/2013 zeigt, dass sich Hersteller, Integratoren und Anwender der Automatisierungstechnik einen deutlich besseren Schutz ihrer Netzwerke wünschen. Dabei ziehen die Befragten die protokollunabhängige Erzielung eines bestimmten Schutzziels vor. Hierzu muss das explizit gewählte Schutzziel, z. B. die Wahrung der Verfügbarkeit oder die Sicherung der Informationsvertraulichkeit, über alle Instanzen hinweg gesichert werden. Weiterhin fordern die Befragten den wirksamen Schutz vor spezifischen Angriffen, vor allem gegen Denial-of-Service (DoS)-Angriffe, Code Injection und Man-in-the-Middle-Attacken. Dies aber nur nachrangig.

Hierbei leistet ein verteiltes Intrusion-Detection-System [3] einen gewinnbringenden Beitrag durch die Einbeziehung der Feldgeräte, Sensoren und Aktoren in die IT-Sicherungsmaßnahmen [4]. Die Wahrung eines Schutzzieles über alle Instanzen hinweg wird möglich – auch gegen komplexe Angriffsmethoden. Wesentliche Herausforderungen, um dies in die Tat umzusetzen, stellen jedoch die enorme Ressourcenlast und der Implementierungsaufwand dar. Damit ist die Nutzung neuerer Ansätze aus der Forschung bisher noch nicht allumfassend möglich, doch zeigen erste Ergebnisse zur Anpassung der Ansätze an reale Gegebenheiten eines solchen SCADA-Systems schon Erfolge. Auch fehlende Vergleichsmöglichkeiten zur Evaluierung [5] werden gegenwärtig geschaffen.

Verteilte Sicherheit

Zwei Lösungsvarianten sind für verteilte Sicherheitssysteme zunächst denkbar. Zum einen können die Feldgeräte, Sensoren und Aktoren jeweils selbst durch ein lokal installiertes IDS-Softwaremodul geschützt werden. Zum anderen können mehrere dedizierte Monitoringgeräte mit IDS-Modul parallel zu vorhandenen Geräten im Feldbus installiert werden und überwachen so deren Kommunikation auf dem Bus.

Der triviale Ansatz für solche Lösungen sind regelbasierte verteilte IDS-Module. Diese beeinträchtigen bei einer überschaubaren Anzahl von Regeln kaum die Echtzeitfähigkeit und lassen sich relativ einfach implementieren sowie an das jeweilige Protokoll adaptieren. Dafür sind diese in ihrer Erkennungsfähigkeit eingeschränkt, da sich komplexe Verhaltensmuster im Netzwerk nur schwer anhand von Regeln beschreiben lassen. Mit Anomalieerkennungen oder Algorithmen aus dem Bereich maschinelles Lernen können sich hier anwendungsabhängig Verbesserungen ergeben.

Nach der Ausbringung der IDS-Module müssen bestimmte Regelsätze, Verhaltens- und Strukturmodelle, die für das Automatisierungssystem relevant sind, erstellt und mit den Modulen abgeglichen werden. Entsprechende Werkzeuge können den Anwender bei der Erstellung von Konfigurationen für verteilte Sicherheitssysteme unterstützen.

Die IDS-Module führen nun fortlaufend eine Sicherheitsanalyse und Bewertung des Systemverhaltens des Automatisierungssystems durch. Hierzu erfassen diese die Topologie und das Verhalten des Automatisierungssystems und vergleichen beides mit den zuvor erstellten Regelsätzen, Verhaltens- und Strukturmodellen. Mögliche Abweichungen vom Modellverhalten werden so identifiziert.

Ein solcher Ansatz ist in zukünftigen Automatisierungsstrukturen flexibel einsetzbar. Die verteilten Module können ihre Resultate bei Erkennung eines sicherheitsrelevanten Ereignisses an ihre unmittelbaren Nachbarn sowie an zentrale Überwachungsstellen bzw. PCS oder Leitsysteme weitergeben. In dieser Konstellation sind bei entsprechender Abstraktion protokollübergreifende IT-Sicherungssysteme denkbar.

krimmling@ihp-microelectronics.com
saenn@ihp-microelectronics.com

Literatur

[1] Krimmling, J., Lange, S., Sänn, A., „Erweiterte Einbruchserkennung mit Hilfe von Netzsensoren in industriellen Anlagen zur frühzeitigen Erfassung des IT-Sicherheitszustandes von Kritischen Infrastrukturen“, SPS/IPC/DRIVES 2014.

[2] Sänn, A. & Krimmling, J. (März 2014) „Neue Wege für die IT-Sicherheit“, Zeitschrift für Automation und Security (a+s), Nr. 1, 27–29, Ingelheim, SecuMedia Verlags-GmbH, ISSN 2193-8555.

[3] Krimmling, J. & Langendörfer, P. (2014) „Intrusion Detection Systems for (Wireless) Automation Systems“, Pathan, A. K. (ed.), The State of the Art in Intrusion Prevention and Detection, S. 431–448, USA, CRC Press.

[4] Sänn, A., Krimmling, J., Baier, D., M. Ni. (2013) „Lead User Intelligence for Complex Product Development – the Case of Industrial IT-Security Solutions“, International Journal of Technology Intelligence and Planning, 9 (3), 232–249.

[5] Krimmling, J. & Peter, S. (2014) „Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications“, 1st IEEE Workshop on Security and Privacy in Machine-to-Machine Communications (M2MSec'14), San Francisco, USA.

Bild: © istockphoto.com | MF3d

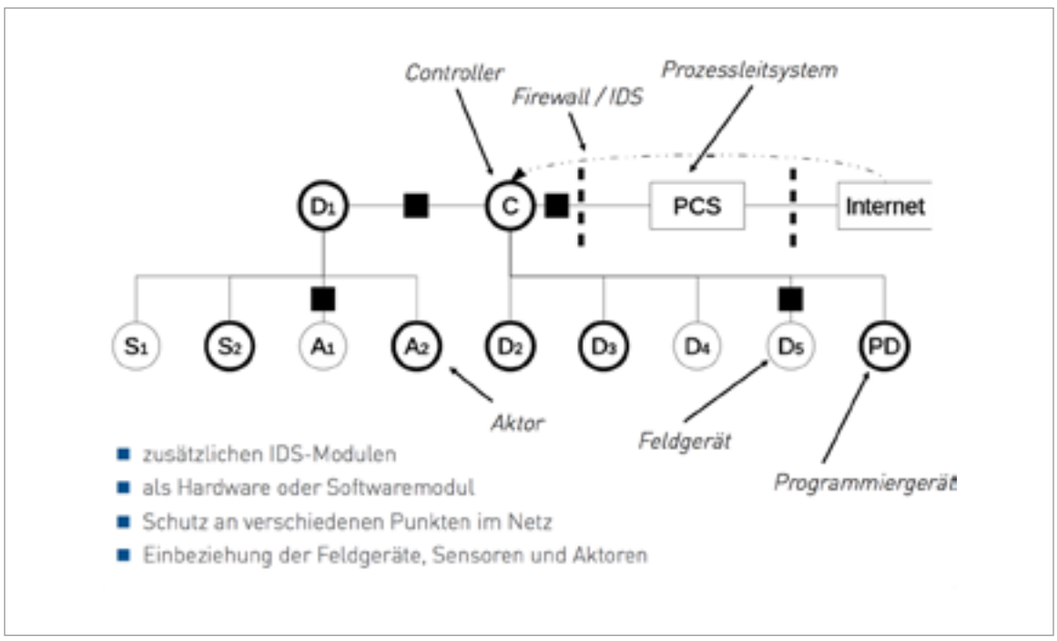

Abb. 3 Verteilte IT-Sicherheit–Einbringung von Netzsensoren