# Herausforderungen bei der Sicherung von Automatisierungssystemen gegen netzwerkbasierte Angriffe

Martin Naedele
ABB Corporate Research
CH-5405 Baden-Dättwil, Schweiz

**Abstract:** Auf Grund anwachsender Vernetzung wird Informationssystem (IS)- und Netzwerksicherheit immer stärker auch zu einem wichtigen Thema für Automatisierungs- und Prozessleitsysteme, wie sie z. B. in Fabriken oder zur Steuerung von Infrastruktureinrichtungen wie Gas-/Wasser-/Strom-Netzen verwendet werden.

Dieses Paper präsentiert und erläutert eine Reihe von Problemen und Herausforderungen, die sich beim Entwurf von Sicherheitsmechanismen und -architekturen speziell für Automatisierungssysteme ergeben.

Ziel dieses Papers ist es, als Anregung für industrierelevante Forschungsarbeiten im Bereich Informatik/IS Sicherheit zu dienen.

## 1 Einführung

In den letzten Jahren werden Automatisierungssysteme, auf Grund von Anforderungen des Marktes und auch der Verfügbarkeit entsprechender neuer Technologien, zunehmend miteinander vernetzt, um Reaktionszeiten zu verringern, Entscheidungen zu optimieren, und die Zusammenarbeit und Koordination zwischen Fertigungsstandorten, Unternehmen und Industriebranchen zu verbessern. Anfänglich basierten derartige Vernetzungen auf spezialisierten, kaum öffentlich dokumentierten, proprietären Protokollen. Heutzutage wird zunehmend Internet-Technologie zu diesem Zweck verwendet, weshalb Informationssystem- und Netzwerksicherheit nun auch für die Automatisierungstechnik relevant sind.

Dieses Paper erläutert einige der Schwierigkeiten - und damit Forschungsprobleme, die sich bei Sicherheitsmechanismen und -architekturen speziell für den Einsatz in Automatisierungssystemen ergeben.

Die aufgeführten Sicherheitsprobleme sind nicht systematisch abgeleitet, sondern haben sich im Laufe unserer Beratungstätigkeit und Diskussion mit Kunden ergeben. Die Reihenfolge in diesem Paper drückt keine Wichtung aus.

## 2 Firewalls für Web-Service-Protokolle

Firewalls haben heute einen festen Platz in jeder Netzwerksicherheitsarchitektur.

Die Effektivität von Firewalls beruht implizit darauf, dass hinter jedem TCP/UDP Port, den der Firewall freigibt, nur genau eine Anwendung verfügbar ist. Diese Grundannahme ist immer weniger gültig, je mehr Protokolle gemultiplext und getunnelt werden (z. B. für ein Virtual Private Network (VPN)). Besonders relevant ist dies für neue Protokolle, die auf Web Services (Simple Objekt Access Protocol, SOAP) beruhen, und einen ganzen neuen Protokollstack einschliesslich Routing mit sich bringen. Web Services über HTTP durch Port 80 (u.ä.), der auf den meisten Firewalls offen ist, hebeln die Filterregeln von Firewalls basierend auf Nachrichtenquelle, -ziel, und -empfängeranwendung völlig aus.

Auch in der Automatisierungsindustrie haben Kommunikationsprotokolle basierend auf Web Services inzwischen Einzug gehalten, z. B. OPC-XML [OP].

Die beschriebene Problematik besteht in gleicher Weise sowohl für Büro- als auch für Automatisierungsnetzwerke. Allerdings sind neuartige, darauf spezialisierte Sicherheitsprodukte gegen diese Gefahren, so genannte Web Service Firewalls, in Bezug auf Preis und Leistung auf den Schutz von grossen Unternehmensnetzwerken ausgelegt, und für typische Automatisierungssysteme nicht wirtschaftlich einsetzbar.

## 3 Intrusion Detection Systeme mit niedriger Fehlerrate und Alarmen für Nichtexperten

Da mit heutiger Technik kein realistisches System mit Sicherheit gegen jede Art von elektronischen Angriffen geschützt werden kann, muss eine Sicherheitsarchitektur neben abwehrend-verzögernden Mechanismen auch Angriffserkennungs- und Reaktionskomponenten beinhalten.

Die Erkennungskomponente sind heute typischerweise Intrusion Detection Systeme (IDS). Heutige Intrusion Detection Systeme leiden unter zwei Problemen:

Zum einen erzeugen sie eine grosse Anzahl von Fehlalarmen, wie zum Beispiel aus den Papern in [VJK03] hervorgeht. Die personellen Ressourcen, die notwendig sind, um IDS-Alarme zeitnah auszuwerten, sind bei Betreibern von Automatisierungsanlagen im Normalfall nicht vorhanden. Man kann jedoch vermuten, dass der Netzwerkverkehr in Automatisierungsanlagen, der weder Email, noch freien Web Zugriff, noch Instant Messaging (IM) beinhaltet, sehr viel weniger Varianz aufweist als in Büronetzwerken, und dass man IDS-Algorithmen und Regeln entwerfen kann, die für diese Anwendung massgeschneidert sind und signifikant weniger Fehlalarme erzeugen.

Zum anderen sind die Meldungen, die IDSs ausgeben, für den Benutzer im Automatisierungssystem, den Prozessbediener, nicht verständlich. Hier wäre es nützlich, das IDS so in das Prozessleitsystem zu integrieren, dass die Ausgabe den Paradigmen entspricht, die der Benutzer gewohnt ist, z. B. Zeitreihenanzeigen für sicherheitsrelevant Parameter wie Netzwerkauslastung oder Zugriffe auf bestimmte Ports. Der Benutzer kann dann daraus Anomalien, beispielsweise einen Wurm-Angriff, ableiten [NB04].

## 4 Gewährleistung der Sicherheit während langer Systemlebensdauer

Automatisierungssysteme haben eine Lebensdauer von 20 bis 30 Jahren, und zwar in der ursprünglich installierten Form. Solange die Anlage zur Steuerung des Prozesses ausreichend ist, möchte der Betreiber weder Geld noch Zeit in den Austausch einzelner Komponenten investieren. In Bezug auf IS Sicherheit schafft dies mehrere Probleme: Diese Haltung steht im Gegensatz zur gängigen IT Praxis des häufigen Einspielens von Betriebssystem-Aenderungen, um auf die neusten Angriffe zu reagieren. Sogar wenn das akzeptabel und praktikabel wäre, ist die nächste Hürde, dass kommerzielle Betriebssysteme wie Microsoft Windows überhaupt nur noch für fünf bis zehn Jahre vom Hersteller unterstützt werden, d. h. nach diesem Zeitraum werden keine Sicherheits-Patches mehr bereitgestellt. Eine Migration des Prozessleitsystems auf die Nachfolgeversion des Betriebssystems ist jedoch sowohl wegen der Kosten als auch wegen der möglichen Nebenwirkungen auf die Anlage selten eine Option. Ebenso sind auch andere Sicherheitsanwendungen betroffen, die einerseits eng mit dem Betriebssystem der Automatisierungsapplikation zusammenarbeiten müssen, also nicht auf einem separaten Rechner installiert werden können, und andererseits regelmässige Aktualisierung verlangen, z. B. Virenscanner.

Für Automatisierungssysteme müssen neue Konzepte und Mechanismen gefunden werden, die es erlauben, für ein Netzwerk mit minimalem Aufwand über Jahrzehnte einen sicheren Zustand aufrechtzuerhalten.

## 5 Updates über langsame Verbindungen

Viele Automatisierungssysteme, insbesondere eingebettete Steuerungen, sind nur über Verbindungen mit niedriger Bandbreite, e.g. GSM-Modem, zugänglich. Dies ist ausreichend für den normalen Betrieb ebenso wie für Angriffe. Es ist jedoch nicht realistisch, über diese Links Betriebssystem-Aenderungen der Grösse üblicher Microsoft Updates zu laden und zu installieren. Bei stark dezentralen Automatisierungsanlagen, z. B. bei Energieversorgern ist auch die Verteilung und manuelle Installation via Datenträger nicht wirtschaftlich. Hier ist die Entwicklung neuartiger, bandbreiteneffizienter Patchtechniken notwendig.

## 6 Virenscanner in Echtzeitsystemen

Virenscanner sind nicht nur wegen fehlenden Verfügbarkeit von Signaturupdates über die gesamte Systemlebensdauer ein Problem, sondern auch der Normalbetrieb ist nicht unkritisch:

Wie kann man sicherstellen, dass die im Hintergrund ablaufende Prüfung auf Viren nicht zu viel Prozessorkapazität beansprucht und Echtzeittasks des Automatisierungssystems behindert?

Was passiert, wenn tatsächlich ein Virus entdeckt wird? Soll die infizierte Datei auto-

matisch ”gereinigt”werden? Was könnten Nebenwirkungen sein? Wie kann man diese abschätzen? Wie kann man die Auswirkungen einer Virenreinigung auf ein Automatisierungssystem für beliebige Viren testen? Falls der Prozessbediener die Entscheidung über die Reaktion fällen muss, welche Entscheidungshilfen kann man ihm geben? Ist ein Virenscanner in einem Automatisierungssystem überhaupt ein angemessener Mechanismus, oder ist es bei der Entdeckung eines Virus eigentlich schon zu spät?

## 7 Zugriffskontrolle in Notfällen

Notfälle und sicherheitskritische Ereignisse in der Anlage stellen eine Herausforderung für die Auslegung der Zugriffskontrollmechanismen dar.

Einerseits kann es im Notfallbetrieb erforderlich sein, dass der Prozessbediener Aktionen ausführen darf, zu denen er unter Normalbedingungen nicht berechtigt ist.

Andererseits kann erforderlich sein, dass ein anderer Benutzer, z. B. mit höheren Privilegien den Arbeitsplatz des Normalbenutzers übernimmt. Die Notwendigkeit zur Eingabe von Passworten für das Aendern des Benutzers nimmt möglicherweise zuviel Zeit in Anspruch, insbesondere wenn aus Nervosität das Passwort falsch eingegeben wird, oder dies gar mehrfach passiert und der Benutzer ausgesperrt wird.

## 8 Risikountersuchung für industrielle Anlagen

Standards und Vorschriften für hinreichende Mechanismen für funktionelle Sicherheit, z. B. IEC 61508 [In98], basieren auf zu einem grossen Teil auf Ausfallhäufigkeitsdaten, die im Betrieb gesammelt wurden und aus denen zukünftige Ausfallswahrscheinlichkeiten hochgerechnet werden. Derartige Methoden sind in Bezug auf IS Sicherheit ungeeignet, da sich mit jeder neuen Softwareversion und mit jeder neu entdeckten sicherheitsrelevanten Schwachstelle in einer Anwendung die Basis für die Beurteilung ändert. Ein äquivalentes Werkzeug für IS Sicherheitsbetrachtungen wird sowohl für die Auslegung der Mechanismen als auch für die Rechtfertigung der Ausgaben (return on investment) dringend benötigt.

## 9 Bedrohungsanalyse

Die Analyse einer Anlage und ihrer Kommunikationsszenarien in Bezug auf Bedrohungen durch netzwerkbasierte Angriffe und die daraus resultierende Ableitung einer angemessenen und kosteneffizienten technischen und administrativen Sicherheitsarchitektur wird heutzutage intuitiv und ad hoc durchgeführt. Für den Bereich der SW-Entwicklung existieren einige Empfehlungen [HL03], aber für Gesamtsysteme und speziell Automatisierungssysteme besteht noch ein grosser Bedarf an einer Methodik zur systematischen Ableitung

von Sicherheitsmechanismen aus Schutzzielen und Bedrohungsannahmen.

## 10 Zusammenfassung

Dieses Paper skizziert im Rahmen des zur Verfügung stehenden Platzes einige der drängenden offenen Probleme in Bezug auf IS Sicherheit für Automatisierungs- und Prozessleitsysteme, die sich als Forschungsthemen für dieses noch sehr junge Untergebiet der IT-Sicherheitsforschung anbieten.

Ziel dieses Papers ist es nicht, schon Lösungsansätze anzubieten. Beschreibungen einiger Sicherheitslösungen, meist für andere als die hier aufgelisteten Sicherheitsprobleme industrieller Systeme, finden sich z. B. in [NDS01, vHC03, Na03a, Na03b, NB04, Na04].

## Literatur


[HL03] Howard, M. und LeBlanc, D.: *Writing secure code*. Microsoft Press. 2003.

[In98] International Electrotechnical commission (IEC). Functional safety of electrical/electronic/programmable electronic safety-related systems, part 1-7. Standard IEC 61508. Dec 1998.

[Na03a] Naedele, M.: IT Security for Automation Systems - Motivations and Mechanisms. *atp*. 45(5). May 2003.

[Na03b] Naedele, M.: Security log time synchronization for high-availability systems. In: *Proc. IEEE Int. Conf. on Industrial Informatics (INDIN'03)*. 2003.

[Na04] Naedele, M.: Innovative Lösungen für die Informationssicherheit in Automatisierungssystemen. In: *eingereicht für den VDE-Kongress 2004*. 2004.

[NB04] Naedele, M. und Biderbost, O.: Human-assisted intrusion detection for process control systems. In: *Technical Track Proceedings, 2nd Int. Conf. on Applied Cryptography and Network Security (ACNS'04)*. June 2004.

[NDS01] Naedele, M., Dzung, D., und Stanimirov, M.: Network security for substation automation systems. In: Voges, U. (Hrsg.), *Computer Safety, Reliability and Security (Proceedings Safecomp 2001)*. volume 2187 of *LNCS*. 2001.

[OP] OPC Foundation. OPC-XML-DA specification. http://www.opcfoundation.org/04_tech/04_spec_xml.asp.

[vHC03] von Hoff, T. und Crevatin, M.: Http digest authentication in embedded automation systems. In: *Proc. IEEE Int. Conf. on Emerging Technologies for Factory Automation (ETFA'03)*. 2003.

[VJK03] Vigna, G., Jonsson, E., und Kruegel, C. (Hrsg.): *Recent Advances in Intrusion Detection (Proceedings 6th Int. Symposium RAID 2003)*. Number 2820 in LNCS. Springer. 2003.