

Innovative Lösungen für die Informationssicherheit in Automatisierungssystemen

Dr. Martin Naedele, ABB Corporate Research, Baden, Schweiz

Kurzfassung

Informationssystem- und Netzwerksicherheit werden immer wichtigere Themen auch für industrielle Automatisierungssysteme. Diese Systeme haben gewisse sicherheitsrelevante Eigenschaften mit Bürokommunikations- und Informationstechnologie gemeinsam, aber sie weisen auch beträchtliche Unterschiede auf. Diese Unterschiede machen es einerseits schwieriger und andererseits einfacher, sie gegen Angriffe zu sichern. Dieser Beitrag beschreibt, wie Sicherheitsanforderungen und -lösungen unter Bezugnahme auf acht grundlegende Sicherheitsziele spezifiziert werden können. Ausserdem werden drei Beispiele für neuartige Schutzkonzepte und -mechanismen vorgestellt, die auf die besonderen Bedürfnisse und Eigenheiten von Automatisierungssystemen ausgerichtet sind.

1 Einführung

Automatisierungssysteme beeinflussen viele Aspekte unseres Alltags. In der Form von Fabrikautomatisierungs- und Prozesskontrollsystemen ermöglichen sie hohe Produktivität in der industriellen Fertigung, und in der Form von Systemen für Strom-, Gas-, und Wasserversorgungsunternehmen bilden sie das Rückgrat unserer technischen Zivilisation.

Heutzutage bestehen die meisten Automatisierungssysteme aus verschiedenen Teilen, die im LAN, WAN, oder sogar weltweit verteilt sind. Derartige Systeme haben entweder die Architektur von verteilten Kontrollsystemen (Distributed Control System/DCS) oder von Leitsystemen (Supervisory Control and Data Acquisition/SCADA)

Bis heute sind die meisten dieser gegenüber öffentlichen Netzen wie dem Internet isoliert. In den letzten Jahren jedoch 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.

Ursprünglich basierten derartige Vernetzungen auf spezialisierten, kaum öffentlich dokumentierten, proprietären Protokollen. Heutzutage wird zunehmend Internet-Technologie zu diesem Zweck verwendet, weshalb folglich Informations- und Netzwerksicherheit nun auch für die Automatisierungstechnik relevant werden.

In der IT-Sicherheits-Terminologie existiert ein Risiko dann, wenn eine Sicherheitslücke und eine Bedrohung zusammentreffen. Eine Sicherheitslücke

bezeichnet hier eine Gelegenheit, Schaden zu verursachen, und eine Bedrohung ist definiert als die Tatsache, dass es Personengruppen gibt, die Sicherheitslücken ausbeuten um jemanden zu schädigen.

Die Bedeutung von Automatisierungssystemen für das Funktionieren unserer Gesellschaft zusammen mit Wettbewerbsdruck auf der einen und weltpolitischen Spannungen auf der anderen Seite lassen die Existenz verschiedener Bedrohungsquellen plausibel, wenn nicht sogar wahrscheinlich erscheinen.

Die weite Verbreitung von Automatisierungssystemen und ihre weltweite Zugänglichkeit über Kommunikationsmittel deren Funktion und Sicherheitsprobleme allgemein wohlbekannt sind, schafft eine grosse Zahl relevanter Sicherheitslücken.

Das tatsächliche Auftreten sicherheitsrelevanter Ereignisse, z. B. im Verkehrswesen [1,6] und im Kontrollsystem eines Kernkraftwerks [5] zeigen auf, dass ein echtes Risiko besteht. Investitionen in die Erforschung von Massnahmen zur Verringerung der Sicherheitslücken industrieller Automatisierungs- und Kommunikationssysteme und entsprechend zur Verringerung der Risiken grossen finanziellen Schadens oder sogar der Schädigung der körperlichen Unversehrtheit von Menschen sind demnach wohlbegründet und gerechtfertigt.

Industrielle Automatisierungssysteme haben gewisse sicherheitsrelevante Eigenschaften mit kommerziellen und Bürokommunikations- und Informationstechnologie gemeinsam, aber sie weisen auch beträchtliche Unterschiede auf (siehe Kapitel 2). Diese Unterschiede sind sowohl Herausforderung, als auch Chance in Bezug auf IT-Sicherheit.

Dieser Beitrag stellt einige neuartige Schutzkonzepte und -mechanismen vor, die auf die besonderen Bedürfnisse von Automatisierungssystemen ausgerichtet sind.

2 Sicherheitsrelevante Eigenschaften von Automatisierungssystemen

Dieses Kapitel erläutert die sicherheitsrelevanten Eigenheiten industrieller Automatisierungssysteme und Unterschiede zur kommerziellen Informationstechnik.

2.1 Anforderungen

Die Sicherheitsanforderungen für Büroinformationssysteme sind hauptsächlich bestimmt von Anforderungen in bezug auf Vertraulichkeit und Datenschutz. Für Automatisierungssysteme hingegen ist die Hauptanforderung in erster Linie die Gewährleistung der Betriebssicherheit (Safety), d.h. die Vermeidung von Schäden an Leib und Leben, und danach an zweiter Stelle Verfügbarkeit: Prozess und Automatisierungssystem müssen kontinuierlich über lange Zeiträume und mit harten Echtzeitanforderungen im Millisekundenbereich antwortbereit sein. Dies macht die Installation von SW-Updates und -Patches, z. B. zum Schliessen von neu entdeckten Sicherheitsschwachstellen in der Automatisierungsanwendung oder dem Betriebssystem schwierig oder sogar unmöglich. Andererseits ist, im Gegensatz zu e-Commerce Anwendungen, für Automatisierungssysteme die Netzwerkanbindung zur Aussenwelt (Intranet und Internet) typischerweise nicht unbedingt notwendig, und auch längere Verbindungsunterbrechungen sind zwar lästig, haben aber keine schwerwiegenden Konsequenzen für das Unternehmen – schliesslich ist heutzutage immer noch der grösste Teil der Automatisierungssysteme überhaupt nicht mit dem Rest des Unternehmens vernetzt.

2.2 Betriebsbedingungen

Topologie und Konfiguration sowohl der Hardware als auch der Software von Automatisierungssystemen oder zumindest des Teils, der sicherheitskritisch (Safety) ist, werden vergleichsweise selten verändert. Deshalb sind alle beteiligten Geräte und Anwendungen ebenso wie ihre normalen und legitimen Kommunikations- und Interaktionsmuster (Kommunikationspartner, -häufigkeit, Nachrichten-grösse, Interaktionssequenzen) gut bekannt, so dass die Schutz- und Angriffserkennungsmechanismen genau auf sie zugeschnitten werden können. Veränderungen des Systems sind so selten, dass der zusätzliche Aufwand zur Rekonfiguration der Sicherheitseinstellungen tolerierbar ist. Auf diese Weise wird eine gewisse Verringerung des Wartungskomforts aufgewogen durch eine höhere Vorhersag-

barkeit des Systemverhaltens, z. B. in Form von statisch festgelegten Tabellen mit den Adressen von Kommunikationspartnern in allen Geräten anstelle von DHCP. Dies vereinfacht die Erkennung von Anomalien.

Die Computer und Geräte im Automatisierungssystem werden nicht für allgemeine oder persönliche Datenverarbeitungsaufgaben benutzt. Dies schliesst die Risiken durch Applikationen wie Email, Instant Messaging, Büroanwendungen und Viren für deren Makrosprachen weitgehend aus. Häufig handelt es sich sogar um dedizierte eingebettete Systeme, die auf die Automatisierungsfunktionalität spezialisiert sind, zum Beispiel elektronische Schutzrelais für Stromübertragungs-Schaltanlagen.

Alle notwendigen technischen und organisatorischen Massnahmen sind etabliert, um sicherzustellen, dass nur vertrauenswürdige und autorisiertes Personal direkten Zugang zu den Automatisierungsgeräten hat. Das Personal ist schon aus Sicherheitsgründen (Safety) gewohnt, einen höheren Grad an Sorgfalt an den Tag zu legen und eine etwas umständlichere Bedienung des Computersystems zu tolerieren, als man dies von Bürocomputerbenutzern erwarten kann. Dies erhöht die Akzeptanz und Wahrscheinlichkeit korrekter Befolgung von sicherheitsrelevanten Prozessen, auch wenn diese etwas kompliziert und unbequem sind.

Die weit verbreitete hierarchische Gliederung von Automatisierungssystemen in mehrere Netzwerkebenen (oder -zonen) zwischen dem Firmenintranet mit Anschluss an öffentliche Netze und den Sensoren/Aktoren, die mit dem physikalischen Prozess interagieren, bietet eine allgemein anerkannte Grundlage für die Realisierung einer tiefengestaffelten Sicherheitsarchitektur im Automatisierungsnetzwerk [2].

In vielen Anlagen stehen aus Gründen der Fehlertoleranz und Betriebssicherheit (Safety) neben dem an das Netzwerk angeschlossenen, computerisierten Automatisierungssystem noch weitere, unabhängige Steuerungsmechanismen zur Verfügung, um die Folgen eines Ausfalls des Automatisierungssystems zu begrenzen.

Rund um die Uhr ist Personal verfügbar, das die Anlage überwacht und bei Problemen sofort reagieren kann.

2.3 Herausforderungen

Die Eigenheiten von Automatisierungssystemen begründen aber auch spezielle Probleme mit Blick auf IT Sicherheit.

Die Betriebssysteme bieten in vielen Fällen keine oder nur sehr geringe Unterstützung für Authentifizierung, feingranulare Zugriffskontrolle, und Speicherschutz zwischen Prozessen.

Die Geräte habe oft schwache Prozessoren verglichen mit Bürocomputern, was z. B. die Anwendbarkeit weit verbreiteter Verschlüsselungsalgorithmen oder auch optionaler Sicherheitsmechanismen im Betriebssystem beschränkt.

Besonders in Fernüberwachungsanwendungen (z. B. SCADA bei Stromversorgern) werden zum Teil Kommunikationskanäle mit geringer Bandbreite (Mobiltelefon oder Satellitentelefon) verwendet. Es ist deshalb notwendig, dass die Sicherheitsmechanismen die Nachrichtengröße und -latenz nicht wesentlich erhöhen.

Automatisierungssysteme haben eine lange Lebensdauer. Dies bedeutet für viele der heute verwendeten Systeme, dass sie im Vertrauen auf „security by obscurity“ und/oder der Annahme eines isolierten Betriebes weitgehend ohne Berücksichtigung von Sicherheitsaspekten entwickelt und implementiert wurden. Eine andere Folge der langen Lebensdauer ist auch, dass das Gesamtsystem häufig sehr heterogen sowohl in Bezug auf die enthaltenen Produkttypen und Fabrikate, als auch Produktgenerationen ist.

Für heute neu entwickelte Systeme bedeutet die Aussicht auf lange Lebensdauer, dass die Kommunikations- und Sicherheitsfunktionalität (z. B. Authentifizierung, Verschlüsselung) so entworfen werden muss, dass sie mit vertretbarem Aufwand auch mit Mechanismen und Protokollen zusammenarbeiten kann, die erst in 10 bis 20 Jahren auf den Markt kommen werden.

Und nicht zuletzt werden Automatisierungssysteme von Prozesstechnikern und -ingenieuren betrieben, die durch ihr Training und ihren Werdegang eine ganz andere Grundhaltung gegenüber Informationstechnik und Informationssicherheit haben, als die Mitarbeiter der IT-Abteilung des Unternehmens. Hier muss gegenseitiges Misstrauen überwunden werden, um eine wirksame Sicherheitsarchitektur zu realisieren.

3 Spezifikation von Sicherheitsanforderungen

Es ist vergleichsweise einfach, zu definieren und zu beschreiben warum und in Bezug worauf ein bestimmtes System „unsicher“ ist. Dagegen ist es schwierig, genau zu spezifizieren, wie ein „sicheres“ System für eine spezielle Anwendung aussehen muss. Um diese Aufgabe etwas zu vereinfachen, bietet sich die Verwendung einer Strukturierung der An-

forderungsbeschreibung in Paare aus Sicherheitsziel und Gegenstand des Sicherheitszieles an, zum Beispiel <Vertraulichkeit; Benutzerpasswörter> oder <Integrität; Sollwertvorgabe>.

Während die jeweiligen Gegenstände der Sicherheitspezifikation natürlich stark vom betrachteten System abhängen, so können die Sicherheitsziele für die meisten Systeme durch die folgenden acht Kategorien hinreichend beschrieben werden:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentifizierung
- Autorisierung/Zugriffskontrolle
- Nachvollziehbarkeit
- Nachweisbarkeit
- Schutz Dritter vor Angriffen von einem eigenen Informationssystem.

Eine nähere Beschreibung jedes dieser Sicherheitsziele findet sich [3].

4 Neue Sicherheitsmechanismen

Dieses Kapitel stellt einige innovative Lösungen zur Sicherung von Automatisierungssystemen gegen Netzwerkangriffe vor. Wie diese und andere, konventionelle Sicherheitsmechanismen im Rahmen einer Sicherheitsarchitektur mit tiefengestaffelter Verteidigung angewendet und installiert werden können, wird z. B. in [3] diskutiert.

4.1 Überwachungsmonitor für Automatisierungsnetzwerke

Einige der obengenannten speziellen Eigenschaften von Automatisierungssystemen sind: Beschränkte Anzahl von Programmen, weitgehend statische Netzwerktopologie, und deterministische Verkehrsmuster. Ausgehend hiervon kann man einen neuen Typ von Netzwerkmonitor entwickeln, dessen Funktion über die von konventionellen Firewalls angebotene Filterung nach Adresse, Port und Protokoll hinausgeht. Ein derartiger Netzwerkmonitor kann seine Entscheidung, ein Paket zu verwerfen oder einen Alarm auszulösen zusätzlich zu den Firewall-Kriterien auch von applikationsspezifischen Paketeigenschaften abhängig machen, wie

- maximale oder minimale Länge der Mitteilung,
- minimale Zeit zwischen zwei Meldungen bestimmten Typs,
- seitens der Anwendung erforderliche Sequenz von Mitteilungen bestimmter Kommunikationspartner.

Ausgedrückt in der Form der in Kapitel 3 beschriebenen Sicherheitsziele deckt ein derartiges Gerät die Anforderungen <Authentifizierung; Mitteilung>, <Autorisierung; Mitteilung>, und <Schutz Dritter; interne und externe Systeme> ab.

4.2 Sicherheitsadapter für einzelstehende Automatisierungsgeräte

Industrielle Regelungs- und Steuergeräte, insbesondere für Anwendungen der Leistungselektronik, zum Beispiel in der Energieerzeugung, in der Energieverteilung, in industriellen Prozessen (Frequenzumrichter, Gleichrichter, Antriebssysteme,...) und in Verkehrssystemen, werden oft in Form einzelner Geräte über eine grössere geographische Region verstreut installiert. Der Fernzugriff zu solchen Geräten, z. B. über das Internet, für ferngesteuerten Betrieb und Fernwartung ist wirtschaftlich interessant.

Es gilt jedoch, dass derartige Regelungsgeräte oft rund um die Uhr ohne geplante oder ungeplante Ausfälle betrieben werden müssen. Dies macht die Installation von SW-Updates zum Schliessen neu entdeckter Sicherheitslücken ausserhalb des jährlichen Wartungsfensters impraktikabel. Ein entsprechendes Vorgehen wie bei Bürocomputern ist also nicht möglich. Erschwerend kommt hinzu, dass diese Regelungsgeräte meist auf spezielle Echtzeitbetriebssysteme aufbauen, die keine oder nur sehr schwache Sicherheitsfunktionalitäten aufweisen.

Ausserdem besteht noch die Problematik, dass das selbe Gerät mit dem selben Prozessor einerseits für

den zeitkritischen, hochverfügbaren Regelungs- oder Sicherheits- (Safety) Task zuständig ist und andererseits den möglicherweise nichtdeterministischen Verkehr an der Kommunikationsschnittstelle bearbeiten muss, der –beabsichtigt oder unbeabsichtigt – in Bezug auf Mitteilungsgrösse, -rate oder -inhalt die Kapazität des Kommunikationstreibers überschreiten kann und somit die eigentliche Regelungsfunktionalität unterbrechen oder zumindest stören kann.

Eine Lösung hierfür ist es, zwischen das Kommunikationsnetzwerk (Internet, LAN oder Telefon) und das Automatisierungsgerät einen Sicherheitsadapter zu schalten. Dieser Adapter basiert auf einem handelsüblichen Betriebssystem, z. B. einer gehärteten Variante von Linux, und stellt alle die Sicherheitsfunktionen zur Verfügung, über die das Automatisierungsgerät auf Grund seines Designs oder Leistungsfähigkeit seines Prozessors nicht selbst verfügt. Beispiele sind: Firewall, Virtual Private Network (VPN), starke Authentifizierungs- und Zugangskontrollmechanismen, Ereignisarchivierung, netzwerkbasierende und rechnerbasierte Angriffserkennung (NIDS/HIDS)

Das Automatisierungsgerät und das öffentliche Netzwerk sind je über eine eigene Netzwerkschnittstelle mit dem Sicherheitsadapter verbunden, so dass jedes Paket, welches das Automatisierungsgerät erreicht, garantiert nur vom Sicherheitsadapter erzeugt worden sein kann.

Die Problematik nichtdeterministischer, von menschlichen Benutzern generierter Mitteilungen, die möglicherweise vom Kommunikationstreiber des

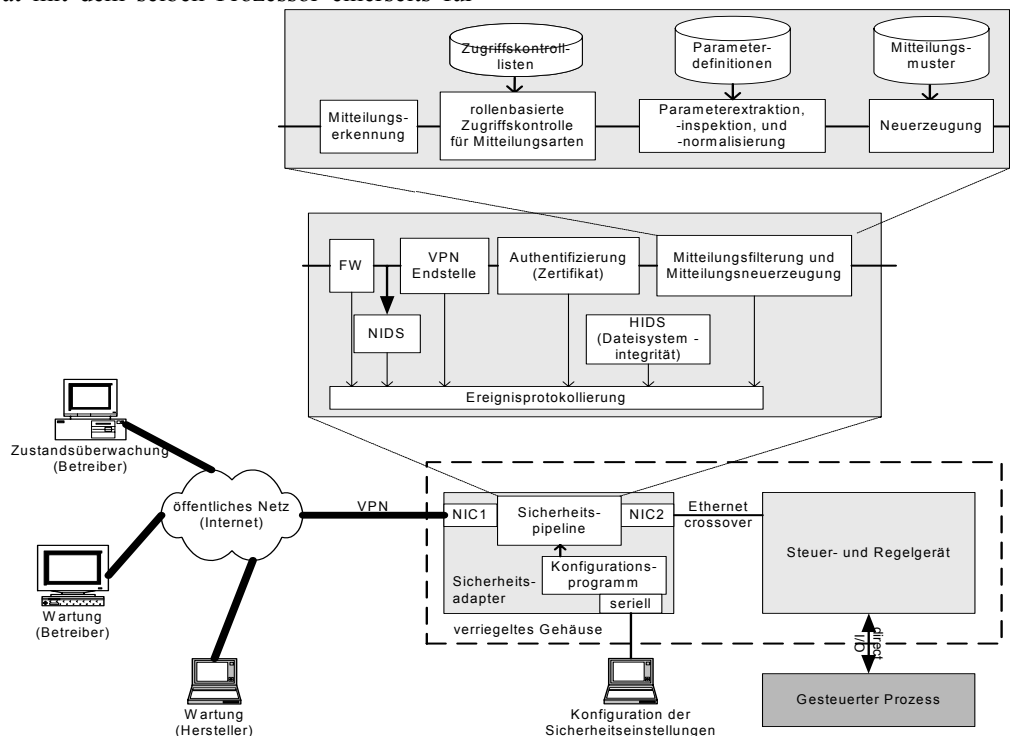


Bild 1 Architektur des Sicherheitsadapters

Automatisierungsgeräts nicht bearbeitet werden können, wird durch ein Programm auf dem Sicherheitsadapter gelöst, das auf Anwendungsebene alle vom öffentlichen Netz her eingehenden Mitteilungen an der anderen Netzwerkschnittstelle neu erzeugt. Nur bestimmte Mitteilungsarten können an das Automatisierungsgerät geschickt werden, und dieses wurde streng daraufhin getestet, dass es alle Pakete innerhalb der Spezifikationen dieser Mitteilungsarten problemlos und ohne Beeinflussung des Automatisierungstasks bearbeiten kann.

Der Mitteilungsfilter auf dem Sicherheitsadapter-Rechner versucht für jede eingehende Mitteilung, einen passenden vordefinierten Mitteilungstyp zu finden. Ist dies nicht erfolgreich, wird die Mitteilung verworfen. Im Erfolgsfall wird gemäss dem Muster des Mitteilungstyps eine neue Mitteilung erzeugt und der variable Inhalt aus der ursprünglichen Nachricht extrahiert und untersucht bevor er in die neue Mitteilung eingesetzt wird. Das neue Nachrichtenpaket wird dann an das Automatisierungsgerät gesandt. Auf diese Weise kann kein Paket an das Automatisierungsgerät gelangen, das nicht der Spezifikation entspricht.

Da die externe Kommunikationsverbindung für das Funktionieren des Automatisierungsgeräts nicht permanent verfügbar sein muss, kann der Sicherheitsadapter jederzeit abgeschaltet, die installierte SW erneuert oder ergänzt und der Rechner neu gestartet werden.

Abb. 1 zeigt eine schematische Darstellung der Architektur eines solchen Sicherheitsadapters.

Der Sicherheitsadapter deckt die Sicherheitsanforderungen

- <Vertraulichkeit; Kommunikation zwischen Automatisierungsgerät und fernsteuerndem Benutzer>,
- <Integrität; Kommunikation zwischen Automatisierungsgerät und fernsteuerndem Benutzer>,
- <Vertraulichkeit; Authentifizierungsinformationen>,
- <Authentifizierung; Benutzer des Automatisierungsgerätes>,
- <Zugriffskontrolle; Automatisierungsgerät>,
- <Nachvollziehbarkeit, Fernsteuerungssitzung>,
- <Nachweisbarkeit; Befehle des Benutzers an das Automatisierungsgerät>,
- <Schutz Dritter; externe System> und
- <Verfügbarkeit; Echtzeitfunktionalität> ab.

Der hier vorgestellte Sicherheitsadapter ist keine Aussensicherung für ein ganzes LAN wie in [4], sondern ein spezifischer Schutz für einen einzigen Typ von Automatisierungsgerät, und die Systemtopologie und

–konfiguration gestatten es nicht, weitere Geräte and das Netzwerksegment zwischen Automatisierungsgerät und Sicherheitsadapter anzuhängen. Der Sicherheitsadapter kann deswegen eher als eine Art Co-Prozessor für das Automatisierungsgerät angesehen werden. Die Kombination aus Sicherheitsadapter mit seinen verschiedenen Sicherheitsfunktionen und Automatisierungsgerät in der oben beschriebenen Konfiguration, zusammen mit den Sicherheitsmechanismen im Automatisierungsgerät selbst – soweit vorhanden – realisiert eine tiefgestaffelte Verteidigungsarchitektur auch für einzelstehende Geräte, die die Funktionsbereiche Verzögerung einen Angriffs, Erkennung, und in begrenztem Umfang auch Reaktion umfasst.

4.3 Angriffserkennung über die Benutzeroberfläche eines Prozesskontrollsystems

Ein Problem beim Einsatz von Intrusion Detection Systemen (IDS) zur Erreichung des Sicherheitszieles <Zugriffskontrolle; Netzwerkverkehr> ist, dass sie viele Fehlalarme – d.h. Alarme für Pakete, die nicht wirklich Teil eines Angriffs sind - produzieren während gleichzeitig typischerweise in einem Unternehmen die Mitarbeiter nicht die Zeit haben, den Meldungen des IDS gründlich nachzugehen.

Die Forschung im Bereich IDS konzentriert sich darauf, die algorithmische „Intelligenz“ der Anwendungen zu verbessern um die Erkennung echter Angriffe zu optimieren.

In industriellen Systemen, insbesondere in Prozesskontrollsystemen, ist die Situation etwas anders: Einerseits sind, wie in Kapitel 2 dargestellt, die Eigenschaften des Verkehrs im Netzwerk sehr gut bekannt, andererseits ist normalerweise ein Operator rund um die Uhr anwesend, der die Aufgabe hat, die verschiedenen Prozessparameter zu beobachten und zu überwachen. Ausserdem ist eine Unterbrechung der Netzwerkverbindung zwischen dem Automatisierungssystem und dem Firmenintranet sogar für die Zeitspanne von mehreren Stunden in den meisten Fällen akzeptabel.

Diese Situation ist der Ausgangspunkt für einen neuartigen Ansatz zur Angriffserkennung in Prozesskontrollsystemen [7]: Die Grundidee hierbei ist, die fehlalarmanfällige künstliche Intelligenz des IDS zu umgehen und stattdessen die ausgeprägte menschliche Fähigkeit zur Erkennung von Anomalien in visuellen Mustern zu nutzen. Konkret werden dazu die Ausgangsgrößen verschiedener sicherheitsrelevanter Geräte und Mechanismen im Netzwerk, wie zum Beispiel

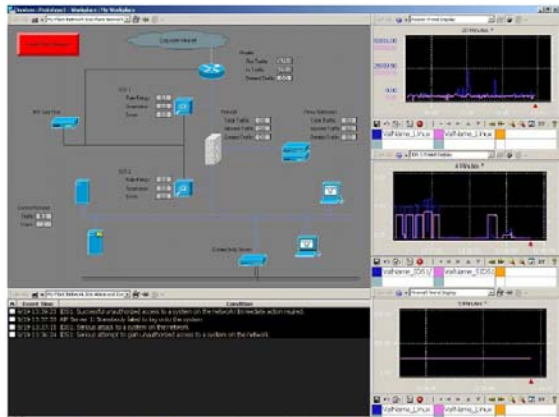


Bild 2 Bildschirm des Prototypen für die Integration von Angriffserkennung und Prozesskon-

- Anzahl eingehender und ausgehender Pakete per Protokoll und Port pro Zeiteinheit,
- Anzahl vom Firewall durchgelassener und zurückgewiesener Pakete pro Zeiteinheit,
- Anzahl Log-Einträge pro Zeiteinheit bezüglich Benutzerverwaltungsoperationen,
- Anzahl Log-Einträge pro Zeiteinheit bezüglich Änderungen von Zugangsrechten,
- Anzahl angemeldeter Benutzer,
- u.v.a.m.

zentral erfasst und als quantitative Trendkurven in der Benutzerschnittstelle des Prozesskontrollsystems wie alle anderen Prozessgrößen angezeigt.

Vom Prozessoperator, der typischerweise weder ein Informationstechnik- noch IS-Sicherheitsexperte ist, wird nur erwartet, dass er die Trendkurven beobachtet und, sobald er eine Anomalie erkennt, Experten bezieht und/oder das Prozesskontrollnetzwerk gegenüber der Aussenwelt isoliert, um die <Verfügbarkeit; Automatisierungssystem> zu gewährleisten. Die Einbindung eines Menschen in den Angriffserkennungsprozess ist sehr wirkungsvoll, da er nicht nur langfristige Muster und Trends besser erkennt als ein Computerprogramm, sondern auch flexibel sein Wissen über normale tägliche, wöchentliche oder monatliche Muster, ebenso wie seine Kenntnis über spezielle ungewöhnliche, genehmigte Aktivitäten wie Wartung oder Umbauten mit in seine Betrachtung einbeziehen kann, ohne dass eine arbeitsintensive und aufwendige Änderung von Konfigurationsdateien notwendig ist.

Unsere - allerdings begrenzten - bisherigen Experimente haben gezeigt, dass verschiedene Typen von typischen Angriffen oder Bestandteilen von Angriffen, ausgeführt z. B. mit Werkzeugen wie Nmap oder Nessus, deutlich erkennbare und unterscheidbare visuelle Anomalien erzeugen (siehe Abb. 2). Ähnlich deutliche Anzeigen erwarten wir z. B. für Angriffe durch Würmer.

5 Zusammenfassung

Dieser Beitrag hat die Notwendigkeit von Massnahmen zur Informationssicherheit auch für Automatisierungssysteme motiviert, eine konzeptionelle Struktur zur Spezifikation solcher Massnahmen basierend auf acht grundlegenden Sicherheitszielen vorgestellt, und einige spezielle Eigenschaften von Automatisierungssystemen aufgezeigt, welche die Auslegung von Sicherheitsmechanismen positiv und negativ beeinflussen können. Anschliessend wurden drei Beispiele für innovative automatisierungsspezifische Sicherheitsmechanismen näher vorgestellt.

Weitere Forschung auf dem Gebiet der Informationssicherheit für Automatisierungs- und Infrastrukturkontrollsysteme ist dringend notwendig [8], zum Beispiel um der Herausforderung durch neue, auf XML Web Services basierenden Kommunikationsprotokollen im Automatisierungsbereich (z. B. OPC-XML) angemessen begegnen zu können.

6 Literatur

- [1] Computer Virus Strikes CSX Transportation Computers - Freight and Commuter Service Affected. CSX Transportation press release, http://www.csx.com/?fuseaction=company.news_detail%20&i=45722&news_year=-1, 8/2003.
- [2] M. Naedele. IT Security for Automation Systems - Motivations and Mechanisms. atp, 45(5), Mai 2003.
- [3] M. Naedele. Industrial IT Handbook (R. Zurawski, ed.), chapter: Security for Automation Systems. CRC Press, 2004.
- [4] P. Palensky and T. Sauter. Security considerations for FAN-Internet connections. In Proc. IEEE Int. Workshop on Factory Communication Systems, September 2000.
- [5] K. Poulsen. Slammer worm crashed Ohio nuke plant net. August 2003. <http://www.securityfocus.com/news/6767>
- [6] C. Jenkins. Sasser eyed over train outage. 3.5.2004. http://news.com.au/common/story_page/0,4057,9455677%255E15306,00.html
- [7] M. Naedele. Ein Ansatz zur Intrusion Detection für Prozessautomatisierungssysteme, Workshop Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA'04), Juli 2004
- [8] M. Naedele. Herausforderungen bei der Sicherung von Automatisierungssystemen gegen netzwerkbasierte Angriffe, Workshop Sicherheit industrieller Rechnersysteme, September 2004