Schlussbericht

Sensoren für eine kooperative Netzwerküberwachung

ESCI

Förderprogramm	Unternehmen Region ForMaT2
Förderer	BMBF
Förderkennzeichen	03FO3102
Projektlaufzeit	01.04.2011 - 31.03.2013
Stand	30.09.2013
Autoren	Oliver Stecklina, Jana Krimmling, Andreas Paul, Franka Schuster, Oliver Maye, Stefan Lange, Prof. Dr. Peter Langendörfer
Zuwendungsempfänger	IHP GmbH

Das diesem Bericht zugrundeliegende Vorhaben wurde durch Mittel des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 03FO3102 gefördert. Die inhaltliche Verantwortung dieses Berichtes liegt bei den Autoren.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Kurze Darstellung

1.1. Aufgabenstellung

Ziel des Projektvorhabens „Sensoren für eine kooperative Netzüberwachung“ war die Erstellung einer Plattform für eine ganzheitliche Sicherheit in der industriellen Informationstechnik (IIT). Hierbei sollten insbesondere die Systeme kritischer Infrastrukturen adressiert werden, da diese als besonders schutzbedürftig angesehen werden.

Aufgrund der heterogenen Technik innerhalb der IIT können bereits existierende Ansätze aus der klassischen IT nicht ohne Anpassungen für die industrielle Informationstechnik übernommen werden. So müssen die spezifischen Protokolle und die Realzeit-Anforderungen von den zu entwickelnden Sicherheitssystemen berücksichtigt werden. Hierzu müssen für die Systeme der IIT neue Techniken zum Monitoring und zum Selbstschutz der einzelnen Komponenten und des Gesamtsystems erstellt werden. Die Komponenten umfassen hierbei insbesondere eingebettete Systeme, wie digitale Sensoren, speicherprogrammierbare Steuerungen oder Koppelsysteme. Für einen ganzheitlichen Schutz moderner IIT ist eine allgegenwärtige, flexible und offene Sicherheitsarchitektur zwingend erforderlich. Diesem Bedürfnis sollte im Rahmen des Projektvorhabens mit der Erstellung einer „verteilten und reaktiven Sicherheitsplattform“ (VRS-Plattform) nachgekommen werden. Diese Plattform sollte eine globale Sicht auf das System erlauben, die heterogenen Beziehungen der verschiedenen Komponenten berücksichtigen und zusätzlich geeignete, mitunter maßgeschneiderte, Techniken zum Schutz der einzelnen Teilsysteme bereitstellen.

Innerhalb des Projektvorhabens sollte das Forschungsvorhaben durch drei Gruppen unter den folgenden Aspekten bearbeitet werden:

Netzsensoren: Es sollten Sensoren für die Erkennung von Angriffen, zum Einleiten von Gegenmaßnahmen und zum Selbstschutz für den Einsatz in allen Systemklassen der IIT untersucht und umgesetzt werden.

Kooperatives Monitoring: Für eine globale Sicht auf die Systeme der IIT sollten die Sensoren über ein Overlay-Netzwerk kooperieren. Hierzu sollten Mechanismen für eine sichere Kommunikation, zum Aufbau von Vertrauensbeziehungen und geeignete, verteilte Angriffsmechanismen untersucht und umgesetzt werden.

System- und Sicherheitsmanagement: Für den Aufbau einer wirksamen Sicherheitsplattform ist eine sorgfältige Planung unumgänglich. Hierzu sollten Werkzeuge untersucht und gegebenenfalls entwickelt werden, die eine Auswahl der notwendigen Sicherheitsmodule sowie eine Platzierung der Komponenten der VRS-Plattform und das Definieren von Sicherheitsregeln erlauben.

Die Erforschung und die Entwicklung der VRS-Plattform sollten in enger Zusammenarbeit mit den in der Phase I ermittelten Projektpartnern (Lead-Users) erfolgen. In der Zusammenarbeit sollten die im Rahmen des Vorhabens entwickelten Mechanismen evaluiert und Ergebnisse diskutiert werden.

1.1. Vorhabensvoraussetzungen

Das IHP ist ein Forschungsinstitut der Leibniz-Gemeinschaft und beschäftigt im Jahr 2013 ca. 300 Mitarbeiter aus 25 verschiedenen Nationen. Der Schwerpunkt der Forschung am IHP liegt in der Entwicklung von Hochfrequenzschaltungen und deren Anwendung. Das Institut ist in die vier Abteilungen Materialforschung, Technologie, Schaltungsentwurf und System Design gegliedert und verfolgt erfolgreich einen vertikalen Forschungsansatz, in dem die einzelnen Abteilungen durch die Nutzung von Synergien effizienter und schneller Forschungsthemen bearbeiten können.

Die Abteilung System Design verfügt zu Beginn des Forschungsvorhabens bereits über mehrjährige Erfahrungen im Design und bei der Umsetzung von Sicherheitslösungen für eingebettete Systeme. So wurden in anderen Forschungsvorhaben (WSAN4CIP, REALFLEX, TANDEM) bereits eingebettete Systeme im Bereich der kritischen Infrastrukturen untersucht und Ansätze für eine Sicherheitsplattform entwickelt. Zusätzlich konnte durch eine enge Kooperation mit dem Lehrstuhl Rechnernetze und Kommunikationssysteme der BTU Cottbus das Wissensportfolio um die Bereiche *Intrusion Detection und Response Systeme* und *Overlay-Netzwerke* erweitert werden. Als weitere Partner gehörte der Lehrstuhl Marketing und Innovationsmanagement der BTU Cottbus zum Forscherteam. Der Lehrstuhl Marketing und Innovationsmanagement verfügt über langjährige Erfahrungen im Bereich des Lead-Users-Managements. Durch eine enge Zusammenarbeit mit Universitäten und Fachhochschulen in Berlin und Brandenburg bestehen sehr gute Möglichkeiten zur wissenschaftlichen Verwertung der Ergebnisse in Forschung und Lehre.

1.2. Planung und Ablauf des Vorhabens

Das Forscherteam bestand aus drei Forschergruppen und einem kaufmännischen Mitarbeiter. Den Forschergruppen entsprechend, wurde das Vorhaben in die drei Themenkomplexe: *Netzsensoren*, *kooperatives Monitoring* und *System- und Sicherheitsmanagement* aufgeteilt. Zu Beginn der Projektlaufzeit sollte das Gesamtsystem von allen technischen Mitarbeitern in einer zweimonatigen Spezifikationsphase gemeinsam entworfen und spezifiziert werden. Hierbei sollten Abhängigkeiten zwischen den einzelnen Systemkomponenten sowie deren Schnittstellen definiert werden. Anschließend sollte die Entwicklung in den einzelnen Forschergruppen fortgeführt werden. Der vereinfachte Gantt- Plan des Projektablaufes ist in Tabelle 1dargestellt.

Projektmonat / **Aufgabe**	**1-2**	**3-5**	**6-15**	**16-21**	**22-24**
Spezifikation					
Feinspezifikation					
Entwicklungsumgebung					
Implementierung					
Optimierung					
Aufbau Prototyp					

Tabelle 1: Vereinfachter Gantt-Plan des Projektverlaufes

Nach dem Abschluss der Spezifikationsphase war ein Lead-User-Workshop zur Evaluierung der Ergebnisse geplant. Anschließend sollten die einzelnen Forschergruppen aufbauend auf den Ergebnissen aus den ersten Projektmonaten eine Feinspezifikation erstellen. In dieser Phase sollten insbesondere die Protokoll- und Systemspezifika der IIT mit einbezogen werden. Außerdem war geplant, etwas zeitversetzt mit dem Aufbau der Entwicklungs- und Evaluationsplattform und ersten Implementierungen zu beginnen. In den ersten Monaten des zweiten Projektjahres sollten die

Arbeiten an den Implementierungen soweit abgeschlossen werden, dass in einem zweiten Workshop eine Präsentation für die Lead-User durchgeführt werden kann. Die Ergebnisse dieser Präsentation sollten in die anschließende Optimierungsphase einfließen. Ziel des Projektes war der Aufbau eines Demonstrators zur Präsentation der Ergebnisse bei potentiellen Kunden. Für den abschließenden Aufbau dieses Demonstrators waren die letzten drei Projektmonate vorgesehen.

Das Projekt wurde, wie in der Planung vorgesehen, mit der Spezifikationsphase gestartet. Jedoch zeigte sich hier bereits frühzeitig, dass die Komplexität der Systeme eine eingehendere Untersuchung notwendig macht. Insbesondere der enge Kontakt mit den Lead-Usern und der Workshop haben dem Forscherteam viele Erkenntnisse gebracht, die in der Spezifikationsphase genutzt werden konnten. Allerdings hat dadurch die Systemspezifikation drei Monate länger dauert als geplant, so dass nachfolgende Arbeiten teilweise erst verspätet gestartet werden konnten. Darüber hinaus konnte der Aufbau der Entwicklungs- und Evaluationsumgebung nicht im avisierten Zeitraum durchgeführt werden. Da zunächst für Testzwecke ein Demonstrator bei einem der Lead-User vorgesehen war und dieser im Laufe des Projektes nicht wie geplant zur Verfügung stand, hat das Arbeitspaket wesentlich mehr Zeit beansprucht, als im Antrag geplant. Stattdessen wurden vom Forscherteam Systemkomponenten für einen Inhaus-Demonstrator ausgewählt.

Um den Verzögerungen entgegenzuwirken, wurden Teile der Plattform auf anderen Systemen umgesetzt. So konnten die Arbeiten zur Virtualisierungsplattform und zur sicheren Kommunikation auf bereits am IHP vorhandenen Komponenten oder mit Standard-PC-Technologie umgesetzt werden. Darüber hinaus wurden die Arbeiten zur Simulationsumgebung umfangreicher als ursprünglich geplant bearbeitet. Die Gespräche mit Lead-Usern haben gezeigt, dass insbesondere eine Simulationsumgebung zum Evaluieren von neuen Konzepten einen großen Bedarf hat. Hiermit konnten Sicherheitskonzepte zeitnah getestet und deren Auswirkungen auf die Infrastruktur evaluiert werden. Nichtsdestotrotz haben die Verzögerungen dazu geführt, dass der Aufbau des Demonstrators viel später als geplant begonnen werden konnte. So konnten die Arbeiten auch nicht wie geplant im Rahmen des Projekts abgeschlossen werden. Da diese Verzögerung jedoch frühzeitig bekannt war, wurde der Termin für die Fertigstellung mit der Hannover Messe 2013 festgelegt. Diese Messe ist die Leitmesse im Bereich der IIT und wurde durch das Projektteam mit einem eigenen Stand besucht, auf dem die Ergebnisse der Forschung präsentiert werden konnten.

1.3. Wissenschaftlicher und technischer Stand

Sicherheitslösungen für SCADA-Systeme sind bereits am Markt bekannt und übernehmen klassische und bekannte Algorithmen aus dem Office-LAN in die SCADA-Netze. Kommerzielle Anbieter klassischer IT-Sicherungssysteme sind beispielsweise McAffee (Intel), Symantec, ABB und viele weitere. Wie aktuelle Vorfälle belegen, funktionieren diese Ansätze jedoch nur unzureichend. Aufgrund der Verbindung heterogener Technologien und dem weiterhin verstärkten Einsatz von eingebetteten Systemen verfehlen klassische Ansätze wie Firewalls und IDS-Systeme jedoch ihre Wirkung (siehe Abbildung 1). Diese schützen lediglich bekannte Netzzutrittspunkte. Durch die zunehmende Vernetzung werden auch teilweise unbekannte temporäre Netzverbindungen ausgebildet, die ungeschützt sind. Weiterhin stellen eine Vielzahl von Diensten, die zunehmend auf Automatisierungsgeräten ausgeführt werden, zusätzliche Angriffspunkte dar. Darüber hinaus laufen diese Ansätze den internen und externen Angreifern in den Lücken und Methoden hinterher. Zudem können hierbei verschiedene Kundenanforderungen nicht befriedigt werden.

Zu diesen Anforderungen zählen:

- keine Verschlechterung der Verfügbarkeit und Echtzeitfähigkeit,
- keine Steigerung der Komplexität des Netzwerks,
- gleichbleibender Betriebs- und Wartungsaufwand,
- Reduzierung von Fehlalarmen (False-Negatives, False-Positives),
- Einsatz in industriellen Bedingungen (raue Umgebungen) und
- Zusatznutzen (z. B. zur schnellen Inventur der Anlagenkomponenten).

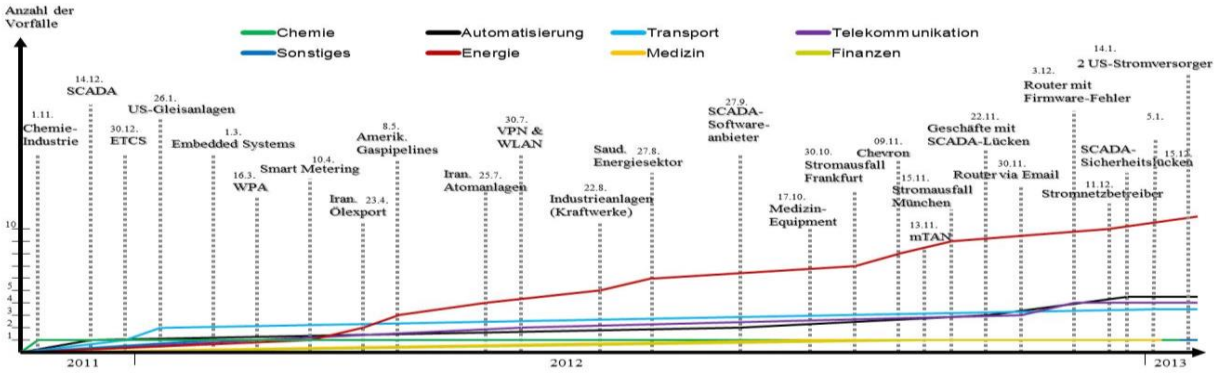

Abbildung 1: Angriffe auf kritische Infrastrukturen seit September 2011 (Sänn, Stecklina 2013)

Bisher werden Schäden durch Sicherheitsvorfälle oftmals erst zu spät erkannt und deren Ursache ist dann nicht mehr nachvollziehbar. Zusätzliches Chaos wird dabei durch die Vielzahl an verfügbaren und immer noch verwendeten traditionellen Feldbusprotokollen weiterhin in die bestehende Automatisierungslandschaft eingebracht. Die industrielle Automatisierung durchläuft jedoch gegenwärtig einen Wandel von traditionellen Feldbussen wie Profibus, Modbus hin zu Industrial Ethernet als Kommunikationsbasis. Hierbei ist das Protokoll Profinet in Europa die vorherrschende Ausprägung von Industrial Ethernet. Modernere Ansätze, wie zum Beispiel von Siemens erhältlich, schützen immerhin direkt die Steuerungstechnik mit lokalen Firewall- oder IDS-Modulen innerhalb des Netzes, statt lediglich den Netzzugangspunkt. Dabei werden allerdings die Sensoren und Aktoren ebenfalls nicht mit einbezogen. Intelligente Sensoren sind jedoch einer der Wachstumsmärkte der nächsten Jahre. Die Einbeziehung der Sensoren und Aktoren ist daher notwendig und erfordert verteilte Strukturen. Dies ist im Hinblick auf den aufkommenden Standard IEC 61449 für verteilte Automatisierungssysteme bedeutend. Hierzu werden momentan Forschungsarbeiten von verschiedenen Gruppen vorangetrieben. Der weit verbreitete Standard IEC 61131 für programmierbare Steuerungen ist hinsichtlich aktueller Entwicklungen durch seine zyklische Request-Response-Arbeitsweise begrenzt. Intelligente Sensoren und Aktoren sind jedoch sinnvoll mit dem Standard IEC 61449 und der zugrunde liegenden auf Events basierenden Arbeitsweise einzusetzen, was kooperative Strukturen ermöglicht und spätestens dann eine verteilte IT-Sicherheitslösung zwingend notwendig macht. Deshalb müssen vollständig neue Techniken zum Schutz der einzelnen Komponenten und des Gesamtsystems entwickelt werden.

In dem Projekt WSAN4CIP wurden bereits Forschungsarbeiten auf den Gebieten Jamming- und Intrusion Detection, Code Attestation und verteilte Datenspeicherung durchgeführt. Als Zielplattform dienten drahtlose Sensorknoten mit sehr geringer Rechenleistung und geringer Speicherkapazität. Es konnte gezeigt werden, dass insbesondere für statische, industrielle Anlagen derartige Systeme

umsetzbar sind. Aufbauend auf diesen Ergebnissen ist damals ein Konzept für eine verteilte Sicherheitsplattform zur Erkennung von Systemanomalien entstanden. Darüber hinaus wurde in dem Projekt die konzeptionelle Grundlage für ein Planungswerkzeug einer verteilten Sicherheits-architektur gelegt.

1.4. Zusammenarbeit mit anderen Stellen

Bereits frühzeitig hat das IHP einzelne Projektergebnisse auf Konferenzen, Ausstellungen und in Journalen präsentiert. Die aktuell brisante Ausrichtung des Forschungsthemas hinterließ auch Spuren in der bundesweiten Presse (siehe dazu „BLACKOUT - Morgen ist es zu spät“ von Marc Elsberg). So wurde das Projektteam unter dem Titel „Hacks mit schweren Folgen“ im Deutschlandfunk zu einem Interview gebeten. Unter dem Stichwort „Anfällige Anlagen“ berichtete die Zeitschrift Technology Review – „MIT´s Magazine of Innovation“ im Jahr 2011 über laufende IHP-Projekte und deren Problemstellung. Die Dechiffrierung von WPA2-Schlüsseln zur Drahtloskommunikation wurde ferner durch das Projektteam gezeigt. Dies machte die Themenstellung „Schutz kritischer Infrastrukturen“ im Jahr 2012 zum „Hot Topic“ des CAST e. V., dessen Workshop durch das Projektteam organisiert wurde und der Vertreter der Forschung (Leibniz, Fraunhofer, Universitäten), der Industrie sowie der öffentlichen Einrichtungen (BBK, BSI) zusammenbrachte. Im Rahmen des Workshops konnte das Projektteam den Ansatz der verteilten Sicherheitsplattform einem erweiterten Publikum präsentierten. Hierbei waren sowohl Vertreter der Wirtschaft sowie nationaler Behörden anwesend. In weiteren Vorträgen von Teilnehmenden wurden sowohl Hintergründe als auch andere Projektansätze vorgestellt. So bot der Workshop dem Projektteam eine sehr gute Plattform zur Diskussionen und zum Austausch von Erfahrungen. Die Initiative zu dem Workshop kam vom Arbeitskreis (AK) KRITIS der Gesellschaft der Informatik (GI). Der AK trifft sich vierteljährlich und versucht, theoretisches und praktisches Wissen zum Themengebiet „Sicherheit in KRITIS“ zu strukturieren und damit die Grundlagen zur Erstellung von Standards auf diesem Gebiet zu schaffen. An den Sitzungen des AKs nahmen regelmäßig Mitarbeiter des Forscherteams teil.

Durch die enge Zusammenarbeit mit Experten der Wirtschaft und Forschung konnten viele Kundenanforderungen bereits bei der Auswahl und Definition der Forschergruppen für das ForMaT-Projekt berücksichtigt werden. Es wurden auf empirischer Basis Vertreter von 52 Unternehmen aus verschiedenen Branchen der Automatisierungstechnik und KRITIS befragt, darunter die Abteilungen IT-Sicherheit, Information und Kommunikation, wie auch externe Beratungsunternehmen und Serviceagenturen. Im Zuge des ForMaT-Projekts unterstützte uns die BTC AG im direkten Austausch. Michael Pietsch ist seitens der BTC Ansprechpartner. Weitere Zusammenarbeit erfolgte auch mit der Universität Bochum bzw. unserem Partner Dirk Schadt, IT-Sicherheitsexperte und Lehrbeauftragter für IT-Sicherheit an der Ruhr-Universität Bochum.

Aufgrund enger Kontakte der Projektpartner zu lokalen Unternehmen der Energie- und Wasserwirtschaft wurde der Bedarf einer Sicherheitslösung für KRITIS und Cyber-Physical-Systems bereits frühzeitig aufgezeigt. Dies konnte im Rahmen des Sensornetztages am IHP durch Fachgespräche mit weiteren Unternehmen und Einrichtungen bestätigt werden. In Zusammenarbeit mit dem Branchenverband BITKOM und dem KRITIS-Experten, Herrn Dirk Schadt, konnten Abhängigkeiten zwischen den einzelnen Bereichen kritischer Infrastrukturen und deren wirtschaftlicher Bedeutung aufgezeigt werden. Der Branchenverband BITKOM unterstützte das Projektteam durch einen regelmäßigen Abgleich der Forschungsarbeiten mit dem weiterführenden Bedarf der Industrie und generierte Feedback aus den einzelnen Arbeitskreisen.

Am Institut für Energietechnik der BTU Cottbus engagierten sich verschiedene Lehrstühle in branchenspezifischen Forschungs- und Industrieprojekten. So konnten enge Kontakte zu Vattenfall Europe und den Stadtwerken Cottbus hergestellt werden. Die Kontakte bestätigten die Relevanz des Forschungsthemas und zeigten Interesse zu einer Unterstützung des Projektteams. Darüber hinaus wurden Kontakte zu überregionalen Unternehmen wie den Stadtwerken Jena-Pößneck und envia Netze hergestellt.

Mit Hilfe der Resultate konnten die Spezifikation des Systems detailliert beschrieben und die nächsten Schritte der Planungsphase festgelegt werden. Dies geschah in Zusammenarbeit mit den Lead-Usern im Rahmen eines zweitägigen Workshops, der am 25. und 26. August 2011 am IHP durchgeführt wurde. Darüber hinaus wurden weiterführende Diskussionen mit den Lead-Usern angestrebt und Fachmessen besucht. Im Ergebnis wurde eine Risikoanalyse durchgeführt, um die wesentlichen Risiken der IIT aus praktischer Sicht bewerten zu können. Zur Einbindung eines größeren Anwenderkreises in diese Risikoanalyse wurde durch das Innovationslabor eine Internetumfrage erstellt, die über die Internetpräsentation des Projektes www.esci-vrs.de erreichbar ist. Sie soll dem gesamten Projektteam genauere Einblicke in die Anforderungen und Bedürfnisse möglicher Anwender geben.

Neben den Arbeiten zur Entwicklung der Sicherheitsplattform hat sich das Forscherteam auch weiterhin mit potentiellen Lead-Usern getroffen. Hierzu wurde am 20. Juni 2012 in Cottbus ein zweiter Lead-User-Workshop durchgeführt. Im Rahmen des Workshops wurden mit Vertretern aus der Energiewirtschaft erste Ergebnisse des Projektes und weiterführende Lösungen diskutiert. An dem Workshop nahmen sowohl Teilnehmer des ersten Workshops als auch neue Partner teil.

Aktuelle Ergebnisse und wichtige Nachrichten aus dem Projektumfeld können zeitnah auf der Internetseite des Projektes verfolgt werden. Ein kleines, durch den Betriebswirtschaftler organisiertes Redaktionsteam kümmert sich fortlaufend um die Aktualität der Inhalte. Das schließt die Einbindung neuer Informationen und Kontakte sowie die Darstellung der Projektfortschritte gegenüber den Partnern ein. Dazu wurden unter Anderem soziale Netzwerke genutzt. Darüber hinaus wurde die bereits im ersten Jahr erstellte Online-Umfrage zur Sicherheit in kritischen Infrastrukturen erweitert bzw. an aktuelle Ergebnisse angepasst. Zum Erreichen eines erweiterten Teilnehmerkreises wurde die Umfrage bei einem Besuch der Hannover Messe 2012 durch einen Mitarbeiter bei verschiedenen Ausstellern und Besuchern präsentiert. Durch diese und weitere Aktionen konnte die Umfrage im zweiten Jahr bei einem erweiterten Teilnehmerkreis bekannt gemacht und die Qualität der Ergebnisse verbessert werden.

2. Verwendung der Zuwendung und erzielte Ergebnisse

Die zu entwickelnde VRS-Plattform (siehe Abbildung 2) soll den Anwender bei der Erfassung des Soll- und der Überwachung des Ist-Zustandes unterstützen und als Overlay-Netzwerk agieren. Hier ist vorgesehen, den Soll-Zustand in einem semi-automatischen Prozess aus den vorhandenen Planungsunterlagen des Anlagenbetreibers zu gewinnen und den Ist-Zustand mit Hilfe von eingebetteten Sensoren zu erfassen und ortsnah auszuwerten.

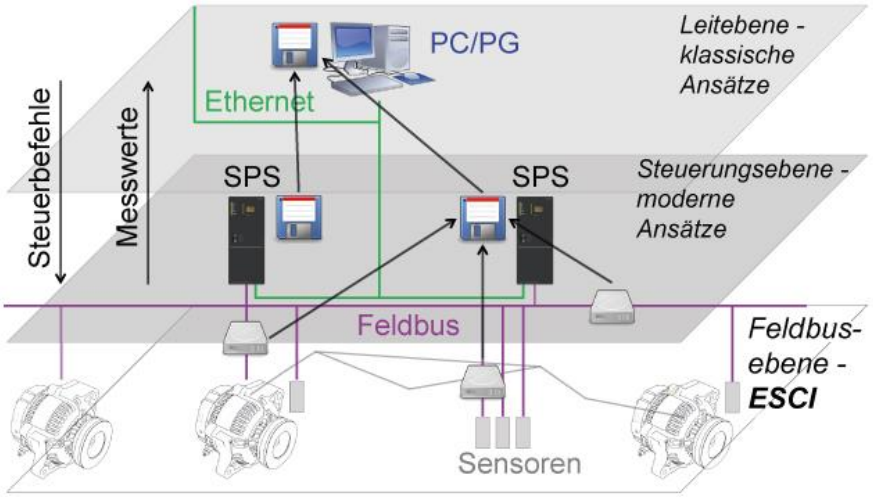

Abbildung 2: Overlay-Netzwerk des ESCI-Vorhabens und Aufgabenstellung

Besondere Herausforderungen stellen die komplexen Sicherheitsalgorithmen, die knappen Ressourcen der vorhandenen Feldbuskomponenten sowie der minimal-invasive Ansatz dar. Diese Herausforderungen müssen zu jedem Zeitpunkt berücksichtigt werden und gehen weit über den aktuellen Stand der Technik hinaus. Daraus ergibt sich die im Folgenden dargestellte wissenschaftlich-technische Aufgabenstellung.

2.1. Erzielte Ergebnisse aus den einzelnen Arbeitspaketen

Im Zuge des ForMaT-Projektes wurde das Konzept der verteilten Sicherheitsplattform aus dem Vorläuferprojekt WSAN4CIP aufgegriffen und hinsichtlich eines Einsatzes in kritischen Infrastrukturen evaluiert und weiterentwickelt. Im zweiten Jahr des Projektes wurden die Ergebnisse der Spezifikationsphase in den jeweiligen Forschergruppen umgesetzt. Es entstanden die nun zugrunde liegenden Implementierungen des Planungswerkzeuges, des Expertensystems und der Kommunikationsplattform. Anschließend sollten diese und die bereits im ersten Jahr erzielten Resultate zu einem Demonstrator zusammengeführt werden. Eine genauere Beschreibung zu den einzelnen Ergebnissen erfolgt in den Unterabschnitten dieses Kapitels.

Für die verteilte Architektur des ESCI-Projekts wurden verschiedene Ansätze für den Aufbau der Kommunikationsstruktur des Systems hinsichtlich ihrer Eignung betrachtet. Hinsichtlich der prinzipiellen Bauweise wurde ein modularer Ansatz einem monolithischen Ansatz vorgezogen. Der modulare Ansatz bietet die Möglichkeit, einfach und unkompliziert Module auszutauschen, ist jedoch von der Art der Implementierung her häufig aufwändiger, da zahlreiche Schnittstellen definiert werden müssen. Hierfür bieten sich vor allem objektorientierte Sprachen wie Java und C++ aufgrund ihrer Abstraktionsmöglichkeiten hervorragend an. Zudem galt es, zwischen Performance und Plattformunabhängigkeit abzuwägen. Seit dem Aufkommen von embedded Java besteht die Möglichkeit, auch plattformunabhängige eingebettete Anwendungen einzusetzen. Der Einsatz von Java für die Implementierung macht diese teilweise weniger performant, jedoch dafür plattformunabhängiger. Da zu erwarten ist, dass auch drahtlose ressourcenbeschränkte Systeme in Zukunft von gestiegener Rechenleistung profitieren werden, bietet Java eine gute Basis für zukünftige Entwicklungen in diesem Bereich. So können Geräte unterschiedlichster Art, die Java unterstützen, in die Architektur eingebunden werden. Ebenso ist durch den Einsatz von Java eine

robuste Implementierung wahrscheinlicher, da wesentliche Bestandteile von Java, wie die Garbage Collection und der Verzicht auf Zeiger zur Robustheit einer Implementierung beitragen, was insbesondere im industriellen Umfeld wichtig ist. Aus diesem Grund wurde Java als Grundlage für die Implementierung der ESCI-Architektur gewählt.

Netzsensoren

Durch die Forschergruppe „Netzsensoren“ wurde zunächst eine Analyse der Protokolle der IIT durchgeführt. So wurde das Protokoll ProfiNet detailliert analysiert. Hierbei wurden verschiedene Angriffsmöglichkeiten identifiziert und hinsichtlich einer Erkennung durch die VRS-Plattform untersucht. Der Untersuchung der Protokolle ging eine Analyse des Marktes der IIT voraus, in der die zu untersuchenden Protokolle auf Grundlage ihrer Marktrelevanz identifiziert wurden. So wurden die Protokoll Profibus, IO-Link, WirelessHART (bzw. Zigbee) und Bluetooth genauer betrachtet und als geeignete Vertreter der verschiedenen IIT-Protokolltypen für den Demonstrator ausgewählt. Darüber hinaus konnten in einer im Rahmen des Projektes betreuten Diplomarbeit sehr gute Ergebnisse zur Erkennung von Jamming-Angriffen auf IEEE802.15.4 basierte Funknetzwerke erzielt werden. Daneben wurden in einem Bluetooth-Netzwerk und einem IEEE802.15.4-Netzwerk Verfahren zur Rekonfiguration von Verbindungswegen entwickelt und erprobt. Für die Umsetzung einer einheitlichen Plattform auf den verschiedenen Geräten der IIT wurden verschiedene Virtualisierungstechniken und Integrationsstrategien untersucht. Als Ergebnis daraus wurde mit Takatuka und OCAPI eine Java VM für ressourcenbeschränkte Systeme umgesetzt. Durch den Einsatz der Java VM wird der Einsatz einer einheitlichen Implementierung der VRS-Plattform auf Systemen aller Leistungsklassen möglich.

Die Forschergruppe „Netzsensoren“ beschäftigte sich intensiv mit der Umsetzung der Module zur Erkennung von Anomalien. So wurde mit der Implementierung der Deep Packet Inspection begonnen. Hierbei konzentrierte sich die Forschung auf das Protokoll ProfiNet. Die Ergebnisse der Umfragen haben ergeben, dass dieses Protokoll insbesondere nachgefragt wird und in allen Bereichen der industriellen Informationstechnik eine weite Verbreitung findet. Das Modul wurde zunächst für Microsoft Windows umgesetzt, da dieses Betriebssystem im SCADA-Umfeld die bestehende Plattform darstellt. Für das Abgreifen der Daten aus dem Datenstrom wurde SNORT eingesetzt. Dieses wurde mit speziellen Regeln für das Protokoll ProfiNet ausgestattet. Die Verwendung von SNORT hat den Vorteil, dass damit eine Portierung auf andere Systemumgebungen, wie z. B. Linux, leicht möglich ist. Für die Erstellung des Soll-Zustandes wurde bei der Deep Packet Inspection der Ansatz des maschinellen Lernens verfolgt. Dieser Ansatz hat den Vorteil, dass genaue Kenntnisse über die korrekten Protokollabläufe nicht theoretisch ausgearbeitet werden müssen. Stattdessen wird anhand eines bestehenden Systems der Soll-Zustand erfasst und zu einem späteren Zeitpunkt mit dem Ist-Zustand abgeglichen. Für die Umsetzung des maschinellen Lernens wurden zunächst verschiedene Bibliotheken hinsichtlich ihrer Eignung für das Projekt untersucht und anschließend mit der Integration einer passenden Bibliothek begonnen. Im Berichtszeitraum konnten auch bereits erste Ergebnisse erzielt werden, die im Folgenden weiter untersucht werden sollen und die Basis für mögliche Optimierungen darstellen.

Neben der Deep Packet Inspection wurde mit der Umsetzung einer Hardwareplattform als Sensor für Feldbusgeräte begonnen. Der entwickelte Sensor verfügt über eine ProfiBus-Schnittstelle und kann damit direkt in den Feldbus integriert werden. Er kann hier sowohl aktiv an der Kommunikation teilnehmen als auch passiv eine reine Überwachungsfunktion erfüllen. Darüber hinaus ist der Sensor

mit einem Bluetooth-Modul ausgestattet, womit ein privates Netzwerk zum Übertragen von Analyseergebnissen aufgebaut werden kann. Der Sensor als Proof-of-Concept dient der Evaluierung der Integrationsmöglichkeiten der Plattform. Für die softwaretechnische Einbettung des Protokolls wurde für OCAPI eine Implementierung der ProfiBus-Variante DP-V0 erstellt. Aufbauend auf der im ersten Projektjahr portierten Java Virtual Machine (JavaVM) Takatuka wurde in dem Berichtszeitraum mit JSR-94, Java Specification Request, eine Java Rule-Engine umsetzt. Im Gegensatz zu bereits existierenden Umsetzungen dieser Rule-Engine nutzt die vom Forscherteam erstellte Implementierung lediglich Funktionen der Java Platform Micro Edition (Java ME) und ist damit nahezu auf allen Java-basierten Systemen einsetzbar.

Kooperatives Monitoring

Die Forschergruppe „Kooperatives Monitoring“ beschäftigte sich mit dem Entwurf und der Implementierung von Mechanismen zum Datenaustausch zwischen den Monitorkomponenten, der Untersuchung von Verfahren für eine verteilte Analyse von Systemereignissen und der Entwicklung einer Bibliothek zur sicheren und vertrauenswürdigen Kommunikation.

Die heterogene Struktur von industriellen Informationssystemen erfordert den Einsatz einer Vielzahl von verschiedenen Sensoren. Hierbei unterscheiden sich die Systeme hinsichtlich ihrer Architektur als auch ihrer unterstützten Protokolle. Um eine ganzheitliche Überwachung gewährleisten zu können, war eine Normierung der Daten notwendig. Von den Mitarbeitern der Forschergruppe wurden hierzu Datenstrukturen entwickelt, die eine Abstraktion und damit einen Austausch der Daten ermöglichen. Die Schnittstellen wurden anschließend in das Deep-Packet-Inspection-Modul integriert. Auf Basis dieser Implementierung können die Schnittstellen hinsichtlich ihrer Eignung für die angedachten Anwendungsszenarien evaluiert werden.

Als Ergebnis der Diskussionen mit den Lead-Usern wurde die Forschung bzgl. der Entwicklung eines geeigneten Simulationsmodells für die IIT und insbesondere für die IIT in Verbindung mit der VRS-Plattform vertieft. So beschäftigt sich die Forschergruppe „Kooperatives Monitoring“ intensiv mit der Entwicklung eines Simulationsmoduls auf der Basis von OMNeT++. Ergebnisse dieser Forschung konnten auf internationalen Konferenzen präsentiert werden. Grundlagen zur verteilten Analyse mittels kooperativer Sensoren wurden im Rahmen von zwei durch das Projektteam betreute Diplom- bzw. Masterarbeiten geschaffen. Hierbei wurden sowohl PC-Systeme als auch Sensornetzwerke untersucht. Die Erkenntnisse aus den Arbeiten wurden im Folgenden durch die Studenten als Mitarbeiter des Projektteams weiterverfolgt und auf die IIT übertragen.

Für den Einsatz in der Automatisierungstechnik wird normalerweise zwingend die Echtzeitfähigkeit von Geräten vorausgesetzt. Dies stellt jedoch im Fall einer verteilten Architektur eine enorme Herausforderung dar, wenn die Koordinierung zwischen den einzelnen Komponenten ebenfalls in Echtzeit erfolgt. Sinnvoll ist in diesem Fall eine Beschränkung der Echtzeitfähigkeit auf die Teile der Architektur, die im direkten Kontakt mit dem zu untersuchenden System stehen. Diese Vorgehensweise ermöglicht eine flexiblere Konfiguration der verteilten Architektur, welche sich dann einfacher in bestehende Systeme integrieren lässt. Der Schwerpunkt des Systems wurde in dieser Hinsicht eher auf die Flexibilität des Systems gelegt. Weiterhin wurden Anforderungen an die Komplexität und Laufzeit der Algorithmen hinsichtlich des Einsatzes in ressourcenbeschränkten Systemen betrachtet. Bedingt durch den Einsatz von Java erhöht sich durch die benötigte Java-Laufzeitumgebung wie oben erwähnt teilweise die Laufzeit der Programmkomponenten. Dies kann

wiederum durch eine Beschränkung auf weniger komplexe Algorithmen ausgeglichen werden, um einen Mittelweg zwischen Komplexität und Laufzeit zu finden. Normalerweise sind die Anforderungen an Geräte im Automatisierungsbereich vor allem geprägt durch ihre Echtzeitfähigkeit und Verfügbarkeit. Im Bereich der ressourcenbeschränkten drahtlosen Systeme sind diese beiden Anforderungen zurzeit jedoch nicht in voller Ausprägung erfüllbar. Die Implementierung des Systems ist zum einen durch die begrenzte Rechenleistung und den verfügbaren Speicher begrenzt und zum anderen schon allein aufgrund der Einschränkungen bei der Drahtloskommunikation der verteilten Architektur, wie schwach gekoppelte Verbindungen und schwankende Übertragungszeiten und Datenmengen. Für diese Einschränkungen wurden im Rahmen des Projektes die folgenden Lösungen erarbeitet. Die Protokollscanner (Netzsensoren) am Bus arbeiten in Echtzeit, um Anomalien in den synchronen und asynchronen Datenströmen auf dem Bus zu erfassen und als Events an die verteilte Architektur zu liefern. Dabei müssen die Timing-Anforderungen des jeweiligen Feldbusses eingehalten werden. Aufwärts von den Protokollscannern funktioniert die Kommunikation zwischen den verteilten Komponenten mittels Events. Damit ist dieser Teil der Architektur nicht den Einschränkungen durch die Echtzeitfähigkeit unterworfen (kritische Timing-Anforderungen). Starke Laufzeitschwankungen durch die Bearbeitung von Events auf unterschiedlich performanter Hardware können somit ausgeglichen werden. Durch die verteilte Architektur ist auch die Verfügbarkeit einzelner Komponenten des Monitoringsystems nicht als kritisch anzusehen, da sowohl eine redundante Datenaufnahme als auch eine Auswertung von gesammelten Daten innerhalb der Architektur erfolgt.

Für das kooperative Monitoring wurde somit eine modulare verteilte Architektur unter Verwendung von Java entworfen und implementiert. Diese besteht aus verschiedenen Modulen, wie Event Scanner, Event Korrelator und Nachrichtenverteiler. Diese Module sind über definierte Schnittstellen verbunden und können einfach durch Module mit gleicher Funktion aber mit anderer Implementierung ausgetauscht werden. Dies ist vor allem hinsichtlich der Anpassung auf das zu beobachtende System wünschenswert, da nur so eine optimale Integration in das zu beobachtende System nach den jeweils vorhandenen Gegebenheiten erfolgen kann. Das Event-Scanner-Modul nimmt dabei die von den Protokollscannern (Netzsensoren) und dem Java-Expertensystem erzeugten Events auf. Dabei wurde berücksichtigt, dass für unterschiedliche Feldbusprotokolle auch teilweise unterschiedliche Events von den Protokollscannern generiert werden, weshalb dieses Modul zusammen mit den Protokollscannern auf den jeweils zu beobachtenden Feldbus angepasst werden muss. Der Event-Scanner reicht die aufgenommenen Events an den Event-Korrelator weiter. Dieser korreliert nun die eintreffenden Events abhängig vom Einsatzgebiet des zu beobachtenden Systems und generiert daraus bei Bedarf komplexe Events. Die komplexen Events werden durch den Bewertungsalgorithmus hinsichtlich ihrer Relevanz für das zu beobachtende System zunächst lokal bewertet und diese Information wird dann durch das Nachrichtenverteilungsmodul im Monitoringsystem verteilt. Diese Information fließt in den anderen Knoten wiederum in den Bewertungsalgorithmus ein und kann somit den Gesamtzustand des Monitoringsystems beeinflussen.

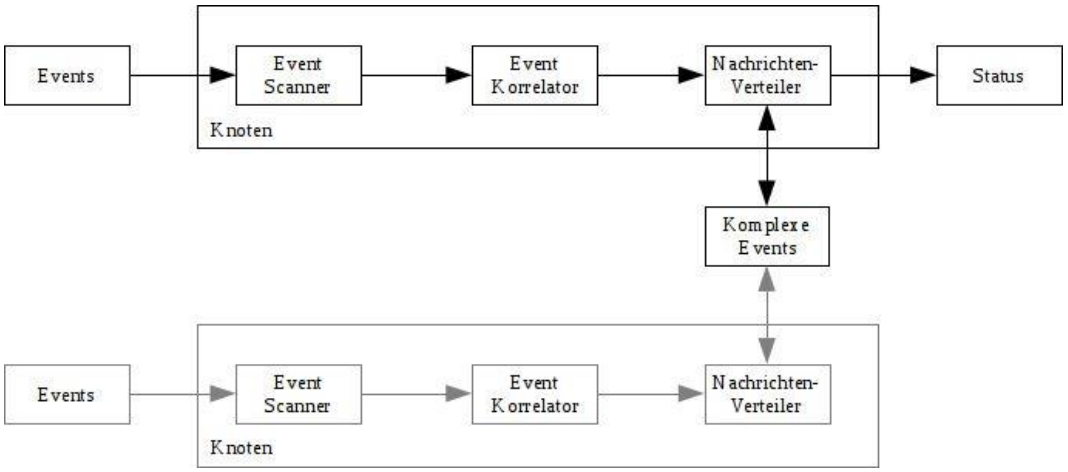

Abbildung 3: Event-Verarbeitung innerhalb der VRS-Plattform

Für eine sichere und vertrauenswürdige Kommunikation zwischen den Komponenten der Sicherheitsplattform wurde eine einheitliche Bibliothek entwickelt. Die Bibliothek basiert auf der frei verfügbaren CyaSSL-Bibliothek. Die CyaSSL-Bibliothek ist eine leichtgewichtige C-basierte SSL/TLS-Bibliothek, die speziell für den Einsatz in eingebetteten Systemen entwickelt wurde. Sie besitzt OpenSSL-kompatible Schnittstellen und erlaubt damit eine leichte Portierung von bereits vorhandenen Algorithmen. Neben der CyaSSL-Bibliothek wurden zusätzlich leichtgewichtige Verfahren für eine asymmetrische Kryptographie erforscht. Als Ergebnis dieser Arbeit entstand mit ShortECC ein Kryptosystem für eine geschlossene Gruppe, das einen verringerten Rechenaufwand benötigt, eine reduzierte Blockgröße besitzt und dabei trotzdem ein vergleichbares Maß an Sicherheit bietet. Die Sicherheitsbibliothek wurde erfolgreich für einen 16-bit-Mikrocontroller (MSP430F5438A) von Texas Instruments umgesetzt und getestet.

Für den Aufbau von Vertrauensbeziehungen wurden von den Mitarbeitern der Forschergruppe „Kooperatives Monitoring“ zunächst Untersuchungen und Implementierungen zum Aufbau von Vertrauensbeziehungen ausgeführt. Hierbei wurden insbesondere die Geräte mit beschränkten Ressourcen betrachtet. Mit der Entwicklung und Umsetzung des ShortECC-Verfahrens in Software wurde diese auf asymmetrischer Kryptographie basierende Methode zur Authentifizierung auf Geräten mit sehr wenig Rechenleistung einsetzbar. Darüber hinaus wurden Algorithmen und Softwarebibliotheken für die Umsetzung und die Speicherung der Vertrauensbeziehungen innerhalb einer einheitlichen VRS-Plattform untersucht und ausgewählt.

System- und Sicherheitsmanagement

Das Forscherteam „System- und Sicherheitsmanagement“ beschäftigte sich mit der Untersuchung von Beschreibungssprachen für IIT Systeme. Hierbei wurden verschiedene Systeme diverser Hersteller untersucht und letztendlich AutomationML als herstellerunabhängiges System ausgewählt. Anschließend wurde mit der Umsetzung des ESCI-Editors als zentrales System- und Sicherheitsmanagementwerkzeug begonnen.

Das System- und Sicherheitsmanagement dient zum einen der Erfassung des Soll-Zustandes der Anlage und zum anderen der Auswahl von geeigneten Methoden für eine sicherheitstechnische Instrumentierung des Systems. Die Arbeiten wurden im ESCI -Editor zusammengefasst. Der ESCI-Editor ist ein graphisches Werkzeug, welches dem Anwender das Einlesen von vorhandenen Planungsunterlagen ermöglicht und diese graphisch darstellt. Anhand der graphischen Darstellung

können anschließend Komponenten zur sicherheitstechnischen Instrumentierung ausgewählt werden. Für diese Komponenten wurde aus den Daten der Planungsunterlagen eine Regelbasis erstellt, die anschließend durch das JSR-94 der IDS-Komponenten (Netzsensoren) verarbeitet werden kann. Die Forschergruppe hat hierzu AutomationML als Beschreibungssprache für die Planungsunterlagen und RuleML für die Beschreibung der Regeln ausgewählt. Für beide Sprachen existieren frei verfügbare Werkzeuge, welche eine Verarbeitung der Daten wesentlich vereinfachen bzw. Bibliotheken, die in neuen Anwendungsprogrammen genutzt werden können. Im Projektzeitraum konnten die wesentlichen Bestandteile des Editors erstellt werden, so dass ein Proof-Of-Concept für den gewählten Ansatz existiert, der einen Grundsatz der notwendigen Funktionen umfasst und für eine Diskussion von weiterführenden Ansätzen mit Lead-Usern genutzt werden kann.

Neben der Umsetzung des ESCI-Editors hat sich das Forscherteam während des Berichtszeitraums mit der CORAS-Risikoanalyse beschäftigt. Ziel war die Identifizierung von Assets und möglichen Bedrohungen für industrielle Informationssysteme. Die Ergebnisse dieser Analyse sind in die Online-Umfrage eingeflossen. Darüber hinaus wurde ein Ansatz zur direkten Nutzung von Ergebnissen einer CORAS-Risikoanalyse im ESCI-Editor ausgearbeitet und umgesetzt.

2.2. Technische Beschreibung der Ergebnisse

Protokollanalyse

Insbesondere die Echtzeitkommunikation als spezielle Anforderung der in industriellen Steuerungssystemen eingesetzten Technologien lässt den Einsatz etablierter Maßnahmen zur Gewährleistung klassischer Schutzziele in diesem Bereich nicht zu. So weisen auch die eingesetzten Kommunikationsprotokolle fehlende Mechanismen zur Gewährleistung einer authentifizierten Kommunikation unter Wahrung der Datenintegrität auf. Obwohl diese Probleme seit geraumer Zeit bekannt sind, mangelt es derzeit an wissenschaftlichen Abhandlungen, in denen konkrete protokollspezifische Angriffsszenarien beschrieben werden.

Im Rahmen dieses Projekts wurde das Industrial-Ethernet-Protokoll Profinet IO hinsichtlich der Ableitung von Nachrichtenfolgen, die einen effektiven Angriff darstellen, untersucht. Als Grundlage der Protokollanalyse wurde die Profinet-IO-Protokollspezifikation verwendet. Neben den Nachrichtenformaten sind in der Spezifikation die genauen Kommunikationsabläufe zwischen den jeweils diensterbringenden Instanzen beschrieben. Entsprechend der bereitgestellten Funktionalität können diese Kommunikations- oder Protokollabläufe in Sequenzen zur Initialisierung des Automatisierungsprozesses (Systemhochlauf) und Abläufe der Betriebsphase (z. B. zyklischer Austausch von Prozessdaten) eingeteilt werden. Im Rahmen der durchgeführten Protokollanalyse konnten vier Angriffe auf die Prozessinitialisierung und ein Angriff auf die Betriebsphase abgeleitet werden. Diese Angriffe zielen sowohl auf eine gezielte Unterbindung von Protokollfunktionalitäten (Denial of Service) als auch auf die unbemerkte Umleitung der Nachrichten über einen Angreifer (Man in the Middle) ab. Details zu den abgeleiteten Angriffen können der Veröffentlichung [20] entnommen werden.

Deep Packet Inspection

Ein Ansatz zur Erkennung protokollspezifischer Angriffe am Beispiel des analysierten Protokolls Profinet IO wird ebenfalls in [20] diskutiert. In dem Beitrag wird verdeutlicht, dass eine effektive Angriffserkennung eine Analyse des Netzwerkverkehrs unter folgenden Aspekten erfordert:

A1: Dekodierung von Netzwerknachrichten. Voraussetzung der Analyse ist eine Unterscheidung zwischen verschiedenen Nachrichtentypen (z. B. *read-request, write-request*, etc.) sowie eine typspezifische Dekodierung der entsprechenden Protokollfelder bis auf Anwendungsebene (Deep Packet Inspection – DPI).

A2: Berücksichtigung der Nachrichtenreihenfolge. Da es sich bei den zur Angriffsdurchführung versendeten Netzwerknachrichten jeweils um protokollkonforme Nachrichten handelt (sowohl typ- als auch inhaltskonform), können diese Angriffe durch getrennte Analyse jeder einzelnen Nachricht (Single Packet Inspection) nicht erkannt werden. Die Analyse muss daher eine zusammenhängende Reihenfolge der Netzwerknachrichten berücksichtigen (Multi Packet Inspection).

Die Architektur der im Rahmen des Projekts prototypisch implementierten Analysekomponente (OpMon) ist in [6] beschrieben. Im Wesentlichen besteht die Analysekomponente aus folgenden Komponenten:

DPI-Komponente: Diese Komponente ist für die Umsetzung von Aspekt A1 verantwortlich. Hierzu wird das netzbasierte Intrusion-Detection-System Snort um Module (Präprozessoren) zur Dekodierung der vom System zu unterstützenden Protokolle erweitert. Im Rahmen des Projekts wurde ein Präprozessor für das Industrial-Ethernet-Protokoll Profinet IO entwickelt. Die DPI-Komponente stellt außerdem die dekodierten Netzwerkdaten zur weiteren Verarbeitung der nachfolgend beschriebenen Lern- und Angriffserkennungskomponente in Form von *Events* zur Verfügung.

Lern- und Angriffserkennungskomponente: Bei der Analyse der Netzwerkdaten wird zwischen einer Lern- und einer Angriffserkennungsphase unterschieden. In der Lernphase wird zunächst aus den erhaltenen Events mit Hilfe eines Lernalgorithmus (Support Vector Machine) ein Modell des Soll-Zustandes generiert. Hierzu müssen die dekodierten Informationen der Netzwerknachrichten (Nachrichtentyp und Inhalte der Protokollfelder) in ein für den Lernalgorithmus bearbeitbares Eingabeformat überführt werden. Ferner ist die Reihenfolge der Netzwerknachrichten (vgl. Aspekt A2) in geeigneter Form abzubilden. Ansätze hierzu werden in [21] diskutiert. Zur Angriffserkennung wird das generierte Modell über das Normalverhalten mit den in der Erkennungsphase erhaltenen Events abgeglichen. Dabei führt jede detektierte Abweichung zur Generierung einer Alarmmeldung.

Simulationsumgebung

Zur Evaluierung der Analysekomponente wurde eine Simulationsumgebung entwickelt, deren Prinzip in Abbildung 4 dargestellt ist.

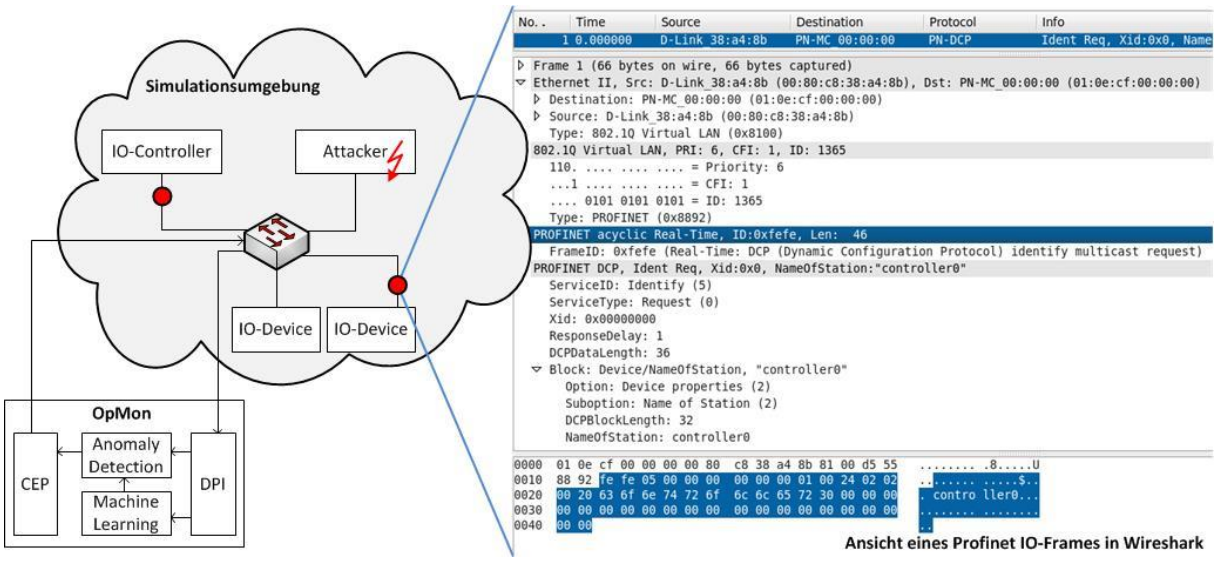

Abbildung 4: Prinzip der Simulationsumgebung

Mit der Umgebung wurde eine rudimentäre Simulation von Profinet-Anlagen realisiert. Dies beinhaltet die Simulation relevanter Abläufe des Systemhochlaufs sowie der zyklischen Übertragung von Prozessdaten (vgl. [20]). Des Weiteren lassen sich Angriffskomponenten konfigurieren, mit denen – entsprechend der spezifizierten Angriffsszenarien – reguläre Protokollabläufe manipuliert werden können. Die während einer Simulation generierten Netzwerkdaten können der OpMon-Komponente zur Analyse bereitgestellt werden. Hierzu werden Profinet-IO-konforme Nachrichten im pcap-Dateiformat generiert. Die direkte Anbindung der OpMon-Komponente an die Simulationsumgebung erfolgt über einen Unix Domain Socket. Ferner besteht die Möglichkeit, die generierten Nachrichten zur späteren bzw. wiederholten Analyse in eine separate Datei zu schreiben.

Zur Erprobung des verfolgten Lernansatzes wurde zunächst mithilfe der Simulationsumgebung der Systemhochlauf eines Profinet-IO-Netzwerks simuliert und der so generierte normale Netzwerkverkehr der Analysekomponente zugeführt (Lernphase). Anschließend wurden die in [20] vorgestellten Angriffe durch eine im Simulationsmodell integrierte Angreiferkomponente simuliert und der resultierende Angriffsverkehr wiederum der Analysekomponente zugeführt (Überwachungsphase). Die Erkennungsrate in der Überwachungsphase war abhängig von der konkreten Konfiguration des Lernalgorithmus. Bei allen Konfigurationen wurden sämtliche Angriffssequenzen als solche erkannt (keine False-Negatives). Entscheidend ist bei dem verfolgten Analyseansatz jedoch die Rate der Falschalarme (False-Positives). Sie lag im besten Fall bei 12 %. Aus den Ergebnissen wurde geschlussfolgert, dass der verfolgte lernbasierte Analyseansatz grundsätzlich vielversprechend für das Anwendungsgebiet ist. Für den Einsatz in realen Systemen muss jedoch die Analyse grundlegend verfeinert werden. Dazu müssen die in [21] dargelegten Aspekte in zukünftigen Arbeiten evaluiert werden.

ESCI-Editor

Als zentrale Planungskomponente entstand der ESCI-Editor. Die Software analysiert einen Anlagenentwurf hinsichtlich möglicher Schwachstellen und gibt Verbesserungsvorschläge. Durch die Nutzung des Dateiformats AutomationML ist eine nahtlose Integration in bestehende Entwurfsprozesse möglich.

Dabei werden die drei Sichten von AutomationML genutzt, was die Modellierung (1) der

Komponenten der Anlage (2), der ver- und bearbeiteten Rohstoffe und Produkte und (3) der Prozesse in der Anlage erlaubt. Die Sichten sind untereinander verknüpft. So ist z. B. ein Prozess mit den Komponenten, die ihn ausführen, verknüpft oder ein Rohstoff mit den Prozessen und Komponenten, die ihn verarbeiten, verknüpft. Damit ist nicht nur eine Analyse der physikalischen Anlagenstruktur möglich, sondern so können auch Prozesse und Rohstoffe in die Analyse einfließen.

Die Analyse auf Schwachstellen und Verbesserungsmöglichkeiten erfolgt mit Hilfe einer Regeldatenbank. So speichert die Datenbank Muster, welche später beim Anlagenentwurf auf Übereinstimmung geprüft werden können. Darüber hinaus lassen sich Implikationen, die sich aus dem Vorhandensein des Musters ergeben, ableiten. Eine Implikation kann sowohl eine Eigenschaft, z. B. die Anlage ist sicher, oder eine Bearbeitungsvorschrift, z. B. Ersetzen bestimmter Komponenten durch sichere Bauteile, sein.

Realisiert sind Analyse und Regeldatenbank als logische Programmierung. Der ESCI-Editor konvertiert den Anlagenentwurf in ein logisches Programm, das die Anlage beschreibt. Implementiert wurde die Umwandlung als XSLT 1.0-Skript von AutomationML zu RuleML 1.0. Die Regeldatenbank besteht aus einer Menge Ableitungsregeln und Abfragen. Die Datenbank wurde vollständig in RuleML 1.0 kodiert. Zur Analyse wird die logische Anlagenbeschreibung mit zusätzlichen Ableitungsregeln aus der Regeldatenbank in eine Logik-Engine geladen. Anschließend werden die Abfragen durch die Logik-Engine ausgewertet.

Die logischen Formeln sind auf Horn-Klauseln beschränkt, wie dies z. B. in der logischen Programmiersprache Prolog der Fall ist. Dadurch sind Anfragen immer in polynominaler Zeit entscheidbar.

Die Implementierung des ESCI-Editors erfolgte ebenfalls in der Programmiersprache Java. Hierbei wurden die folgenden Bibliotheken verwendet:

- die XML-Parser-Bibliothek Apache Xerces-j,
- die XLST-Bibliothek Apache Xalan-j,
- die Logik-Bibliothek jOODrew als Logik-Engine und
- die Grafik-Bibliothek Prefuse zur Visualisierung der Topologie.

Durch die Verwendung von Java ist die Plattform für die Ausführung des ESCI-Editors nicht vorgegeben. Sie lässt sich unter Microsoft Windows als auch unter Linux/Unix-Systemen nutzen.

Java-Expertensystem

Um die in der Zielstellung avisierte Plattformunabhängigkeit zu erreichen, wurde Java als Programmiersprache für das Expertensystem ausgewählt. Java erfordert zur Ausführungszeit eine Laufzeitumgebung, auch virtuelle Maschine (JVM) genannt. Je nach Mächtigkeit der Zielplattform liegen diese JVMs grundsätzlich in einer von drei standardisierten Editionen vor: Java Enterprise Edition (Java EE) ist dafür vorgesehen, Application-Server auf dafür vorgesehenen Geräten besonderer Leistungsstärke zu betreiben. Die Java Standard Edition (Java SE) ist für Geräte der PC-Klasse vorgesehen. Schließlich adressiert die Java Micro Edition (Java ME) besonders mobile Endgeräte mit ihren teilweise stark eingeschränkten Rechenleistungen und Speicher- bzw.

Netzwerkressourcen. Diese Edition wurde aufgrund der besten Übereinstimmung mit der Zielplattform für die weitere Entwicklung ausgewählt.

Innerhalb der Micro Edition wird anhand sogenannter Profile oder Konfigurationen die Leistungsfähigkeit weiter ausdifferenziert, um die große Variabilität zwischen z. B. Smartphone und Smartcard abbilden zu können. Connected Device Configuration (CDC), Mobile Information Device Profile (MIDP) oder Connected Limited Device Configuration (CLDC) sind Beispiele etablierter Profile. Wiederum aufgrund einer guten Übereinstimmung, aber auch wegen der schlichten Verfügbarkeit fiel die Wahl auf das CLDC-Profil.

Java virtuelle Maschinen (JVMs) für Sensorknoten sind derzeit noch relativ selten. Mit Takatuka und Darjeeling sind derzeit zwei OpenSource JVMs verfügbar, die sowohl auf Atmels ATmega als auch auf TI's MSP430-Prozessoren lauffähig sind und in etwa den Funktionsumfang von Java ME, CLDC bieten. Die weiteren Betrachtungen wurden auf Takatuka und die MSP430-Plattform konzentriert.

Zusätzliche Funktionen, die nicht durch die Edition oder das Profil standardisiert sind, werden in Java durch zahlreiche Java Specification Requests (JSRs) spezifiziert. Es handelt sich dabei um Zusatzpakete mit standardisierter Schnittstelle. Je nach Entwicklungsstand des JSRs liegen dazu Referenz- oder Beispiel-Implementationen vor. Im Rahmen der Weiterentwicklung von Java können JSRs auch in spätere Versionen einer Edition einfließen oder darin aufgehen.

Eine gängige Ausprägung von Expertensystemen sind Rule Engines. Eine entsprechende Rule-Engine-API ist zwar nicht direkt Bestandteil einer Java-Edition, aber durch das JSR 94 („Java Rule Engine API") immerhin als Zusatzpaket spezifiziert. Leider setzt das JSR 94 mindestens die Standardedition Java SE voraus.

Im Rahmen der Projektarbeit wurde zunächst umfänglich nach einer offenen JSR94-Implementation für Java ME recherchiert. Es existieren zahlreiche JSR94-Implementationen wie z. B. Jess, JRules oder OpenRules. Die meisten Funde schieden aus, weil sie mindestens Java SE benötigen. Im Ergebnis wurde lediglich Witmate (www.witmate.com), ein kommerzielles Produkt der japanischen Firma Witsign Ltd. ausfindig gemacht. Dessen Quellen liegen leider nicht offen. Eine Probelizenz für Evaluierungszwecke war nicht zu bekommen.

Um eine europäische und vorzugsweise quelloffene Lösung zu ermöglichen, wurde deswegen mit einer eigenen Implementierung begonnen. Diese Gesamtaufgabe wurde in drei Teilpakete unterteilt und schrittweise gelöst. Zunächst musste die API als solche (JSR94) auf Java ME portiert werden. Im zweiten Schritt wurde die vorhandene API mit einer Implementation (Provider) unterlegt. Schließlich wurden mit der entstandenen Implementation Regeln und Konfigurationen erarbeitet, um anhand einer realen Laufzeitumgebung den Effekt und die Arbeitsweise der Java Rule Engine prototypisch zu demonstrieren.

Die API an sich (JSR94) abstrahiert von der konkreten Implementierung. Letzteres wird durch sogenannte Provider vorgenommen. Das JSR94 stellt allgemeine Methoden zur Instanziierung eines Providers und zum Handling der dazu notwendigen Parameter bzw. der daraus resultierenden Ergebnisse bereit. Dazu bedient es sich entsprechend allgemeiner Techniken und Datenstrukturen. Einige dieser Techniken und Strukturen sind in Java ME leider nicht verfügbar und erforderten eine entsprechende Anpassung. Im Ergebnis entstand eine API, die formal vom JSR94 abweicht, funktional

jedoch eine Untermenge von diesem abbildet und, wo nötig, auf eng verwandte Datenstrukturen ausweicht. Die Tabelle 2 gibt einen Überblick über die wichtigsten Anpassungen des JSR94 für Java ME.

Problem im original JSR 94	Anpassung für Java ME
Nutzt Java Reflection für dynamische Instanziierung anhand des Klassennamens	Instanziierung nur für vorher festgelegte Klassennamen möglich (statisch, hard-coded)
Verwendet `java.util.List`	Ersetzt durch `java.util.Vector`
Verwendet `java.util.Map`	Ersetzt durch `java.util.Hashtable`
Methode `javax.rules.admin.RuleExecutionSetProvider.createRuleExecutionSet(Element)` verwendet `org.w3c.dom.Element`	Methode wurde nicht implementiert.
Verwendet `java.io.Serializable` interface (tagging)	Verzichtet ersatzlos auf `Serializable`
Verwendet `java.rmi.RemoteException`	RemoteExceptions werden nicht benutzt. Entsprechende Fehler müssten durch den Provider zunächst lokal aufgefangen und in Eigenregie signalisiert werden

Tabelle 2: Liste der Anpassungen von JSR94 für Java ME

Für die entstandene API wurde ein leichtgewichtiger Provider namens „Manatee“ implementiert, der nur die notwendigsten Funktionen für eine lokale Regelauswertung bereitstellt. Die Regelsprache unterstützt dabei lediglich einfachste algebraische Ausdrücke, Boolesche Logik, Vergleiche sowie das Konzept benamter Variablen und Referenzen. Dies genügt, um die für die Zielplattform typischen Kriterien, wie z. B. „wenn GEWICHT1 + GEWICHT2 > 300 und TEMPERATUR < 80, dann…“ abzubilden. Kernstück von Manatee ist die Auswertelogik, die letztendlich das Eintreffen einer Regel oder eines Regelsatzes feststellt.

Für die entstandene JSR94-Implementation – einschließlich Provider Manatee – wurde abschließend und beispielhaft ein Regelsatz implementiert. Die darin enthaltenen variablen Eingangsgrößen wurden zur Laufzeit aus Profibus-Protokoll-Mitschnitten extrahiert und in die Rule Engine gespeist. Das Ergebnis wurde mittels einer Konsole-Anwendung auf einem PC visualisiert. So konnte die Funktionsfähigkeit von Manatee zusammen mit Takatuka auf einem Sensorknoten mit MSP430-Prozessor erfolgreich demonstriert werden.

Netzsensoren

Wie oben beschrieben, wurde die verteilte Kommunikationsstruktur unter Verwendung der Programmiersprache Java entworfen und implementiert. Durch den Einsatz von Java ist das System weitestgehend plattformunabhängig und damit auf nahezu jeder Hardware lauffähig, die auch Java unterstützt. Die Architektur besteht aus verschiedenen austauschbaren Modulen, wie Event Scanner, Event Korrelator und Nachrichtenverteiler, die dem jeweiligen Einsatzzweck angepasst werden können.

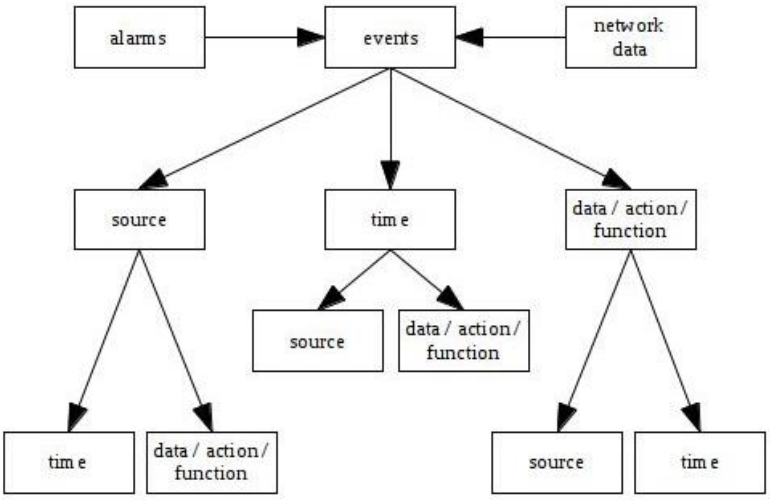

Abbildung 5: Schematischer Aufbau der Event Korrelation

Event Scanner

Die von den Protokollscannern und dem Java-Expertensystem (Netzsensoren) gelieferten Daten können über verschiedene Kommunikationswege an die Event Scanner in den korrelierenden Knoten verteilt werden, hierzu gehören drahtlose Verbindungen wie WLAN, BT, IEEE 802.15.4-Verbindungen und andere. Hierzu bedienen unterschiedliche Implementierungen von Event Scannern die Aufnahme von Events über verschiedene Kommunikationswege und Abstrahieren diese für den Event Korrelator.

Event Korrelator

Der Event Korrelator nimmt die vom Event Scanner aufgenommenen Events auf und generiert daraus komplexe Events, beispielsweise aus einer bestimmten zeitlichen Abfolge von eintreffenden Events oder dem Auftreten bestimmter Events zu einem Zeitpunkt. Im Rahmen des ESCI-Projektes wurde ein auf Profibus/Profinet angepasster Event Korrelator umgesetzt. Für diese Implementierung wurde auf eine Vorarbeit von Czejdo[1] zurückgegriffen. Hierzu werden die Events in Tabellen organisiert und bei Eintreffen von neuen Events auf ungewöhnliche Anhäufungen untersucht. Eine Einordnung der Events erfolgt bei der zunächst für Profibus umgesetzten Implementierung nach einem vorgegebenen Schema, welches an die Funktionsweisen von Profibus/Profinet angepasst ist. Diese Vorgehensweise ist in Feldbussen sinnvoll, da ein großer Teil der Kommunikationsverbindungen synchron abläuft und somit zumindest teilweise vorhersagbar ist. Auch sind die am Bus teilnehmenden Geräte in aller Regel bekannt und können mit den eintreffenden Daten abgeglichen werden.

Nachrichtenverteiler

Die generierten komplexen Events sowie weitere Events von anderen Knoten werden im Nachrichtenverteiler verarbeitet. Wenn ein Sicherheitsvorfall vorliegt, werden andere Knoten per Event über den Vorfall informiert. Hierzu stehen wie beim Event Scanner verschiedene

[1] Czejdo, B.D., Ferragut, E.M., Goodall, J.R., & Laska, J. (2012). Network Intrusion Detection and Visualization using Aggregations in a Cyber Security Data Warehouse. International Journal of Communications, Network and System Sciences, 5.

Kommunikationswege zur Verfügung. Hierzu gehören wiederum drahtlose Verbindungen wie WLAN, BT, IEEE 802.15.4-Verbindungen und andere, aber auch drahtgebundene Kommunikationswege wie Ethernet.

Sichere Kommunikation

Für die Kooperation zwischen den IDS-Komponenten ist ein sicherer und vertrauenswürdiger Kommunikationskanal zwingend erforderlich. In IP-basierten Netzwerken kann die Kommunikation mittels der Protokollerweiterung IPsec abgesichert werden. IPsec ist Bestandteil des IPv6-Protokolls oder eine Erweiterung für IPv4 und sowohl für windowsbasierte als auch unixbasierte Systeme verfügbar, ist es allerdings auf das Internetprotokoll beschränkt.

Der Einsatz von IP in der IIT ist wenig verbreitet. Insbesondere in Feldbussystemen werden aufgrund der Realzeitanforderungen weniger komplexe Protokolle verwendet. Die Sicherung wird hierbei direkt in den Medium Access Layer oder in das Anwendungsprotokoll integriert. Außerdem ist der Einsatz von komplexen Protokollen in den Feldbusgeräten aufgrund ihrer beschränkten Ressourcen nicht möglich. Im Rahmen des Forschungsvorhabens wurde die CySSL-Bibliothek zur Sicherung der Datenübertragung ausgewählt. Die CySSl-Bibliothek beinhaltet ein SSL/TLS-kompatibles Interface und kann damit analog zur sehr weit verbreiteten OpenSSL/TLS-Bibliothek verwendet werden. Darüber hinaus hat die CySSl-Bibliothek einen sehr geringen Speicherbedarf und kann damit auch auf kleinen Geräten verwendet werden.

Für den Einsatz der CySSL-Bibliohtek in der VRS-Plattform wurde eine Bibliothek auf den MSP430 Microcontroller portiert. Hiermit konnte gezeigt werden, dass die notwendigen Mechanismen zur Sicherung des Datenverkehrs bereitgestellt werden können. Darüber hinaus konnte eine Kompatibilität zu leistungsstärkeren Systemen gewährt werden, ohne zusätzliche Implementierungen vornehmen zu müssen.

Aufbau von Vertrauensbeziehungen – shortECC

Für den Aufbau von Vertrauensbeziehungen zwischen den Komponenten des IDS ist zum einen die CySSL-Bibliothek vorgesehen. Da jedoch insbesondere digitale Sensoren über sehr beschränkte Ressourcen verfügen und damit die Verwendung von asymmetrischer Kryptographie nahezu unmöglich wird, wurde nach einem Verfahren gesucht, das die Eigenschaften von öffentlichen und privaten Schlüsseln unterstützt und trotzdem auf Sensoren verwendet werden kann. Hierbei ist insbesondere wichtig, dass das Bilden und das Verifizieren von Signaturen in akzeptabler Zeit durchgeführt werden kann. Im Rahmen des Forschungsvorhabens wurde hierzu das shortECC-Verfahren entwickelt.

Das shortECC-Verfahren ist ein leichtgewichtiges asymmetrisches Kryptoverfahren für ressourcen-beschränkte Geräte. Es diente der Authentifizierung, dem Integritätsschutz und der Sicherung von Vertraulichkeit. Es basiert auf der Elliptischen-Kurven-Kryptographie, benutzt aber Kurven über einem endlichen Körper mit n Elementen, wobei n eine 32 Bit lange Primzahl ist. Nach dem shortECC-Verfahren können Pakete mit einer Länge von genau 32 Bit gesichert werden. Damit eignet sich das Verfahren insbesondere für Geräte mit kleinen Datenpaketen, wie sie bei digitalen Sensoren in der Regel anfallen. Das shortECC-Verfahren ist sehr gut für geschlossene Gruppen geeignet. Die Geräte teilen die geheimen shortECC-Parameter untereinander mit und benutzen sie für den sicheren Austausch von Daten.

Zu den geheimen shortECC-Parametern gehören:

- die Gleichung der elliptischen Kurve,
- die Anzahl der Punkte auf der Kurve sowie
- der Basispunkt der Kurve.

Jedes vertrauenswürdige Gerät hat darüber hinaus ein Schlüsselpaar, das aus einem öffentlichen Schlüssel und einem privaten Schlüssel besteht. Die öffentlichen Schlüssel sind nur denjenigen Knoten bekannt, die sich in der vertrauenswürdigen Gruppe befinden.

Als digitale Signatur wird die modifizierte Version von ECDSA verwendet. Es wird keine Hashfunktion verwendet, da die Ausgabe einer kryptographischen Hashfunktion mit 160 Bit zu lang ist. Der Unterschriftsalgorithmus verknüpft/verwebt die originale Nachricht mit der zugehörigen Unterschrift, so dass diese nicht zusätzlich beigefügt werden muss. Die digitale Unterschrift kann entweder eine 1-zu-1- oder eine 1-zu-n-Relation herstellen. In der 1-zu-1-Kommunikation wird die Nachricht mit dem privaten Schlüssel des Senders unterschrieben und anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. In der 1-zu-n-Kommunikation wird ein gemeinsamer Schlüssel der ganzen Gruppe als öffentlicher Schlüssel des Empfängers benutzt. Für die Verifikation der Unterschrift benutzt der Empfänger seinen privaten Schlüssel (bzw. den privaten Gruppenschlüssel) für die Entschlüsselung der Nachricht und anschließend den öffentlichen Schlüssel des Absenders zur Überprüfung der Unterschrift. Der Vorteil von dieser Methode gegenüber den Standard Message Authentication Codes oder Verschlüsselungsmethoden ist der Verzicht auf Schlüsselpaare pro Gerätepaar aus der Gruppe.

	shortECC	**AES**
Initial Trust	Basiert auf ECC, innerhalb der vertrauenswürdigen Gruppe braucht man kein Schlüsselaustauschprotokoll	
Synchronisierung	nein	Verschlüsselung von kurzen Paketen braucht Synchronisierung
Funktion	Verschlüsselung und digitale Unterschrift	AES – nur Verschlüsselung, AES CCM – verschlüsselte Authentifizierung
Hashfunktion	nein	SHA2 produziert 256 Bits
Verschlüsselung (32 Bit langer Input)	Output 66 Bits	Output 128 Bits
Digitale Unterschrift (32 Bit langer Input)	Output 98 Bits	CCM min 64 Bits + Verschlüsselung 128 Bits
Länge des empfangenen Pakets	Wird nicht benötigt	wird benötigt in AEC CMM
Nonce history	Nein	AES CCM ja

Tabelle 3: Vergleich von AES mit ShortECC

Die Authentizität einer Nachricht kann durch alle Geräte in der Gruppe, die den öffentlichen Schlüssel des Senders kennen, verifiziert werden. Für die Verschlüsselung wird der ElGamal-Algorithmus verwendet. Um den Datenverkehr abhörsicher zu machen, sind im shortECC-System periodische Änderungen aller Sicherheitsparameter möglich. Selbst in Kenntnis der zuvor

verwendeten (und kompromittierten) Parameter können die neuen shortECC-Parameter nicht bestimmt werden. Die Generierung neuer Parameter ist rein zufällig. Hierzu wird ein leichtgewichtiger, kryptographisch sicherer Zufallsgenerator verwendet. Der Generator wurde auf Basis einer logischen Gleichung entwickelt und an ressourcenbeschränkte Geräte angepasst. Als Primzahltest für 32 Bit lange Zahlen kann die deterministische Version des Miller-Rabin-Algorithmus verwendet werden. Das Testen ist weniger aufwendig als probabilistisches Testen von großen Zahlen, wie sie für gewöhnliche digitale Signaturalgorithmen erzeugt werden.

2.3. Präsentation auf der Hannover Messe 2013

Die Hannover Messe ist die Leitmesse im Bereich der IIT und wurde durch das Projektteam im April 2013 mit einem eigenen Stand besucht, auf dem die Ergebnisse der Forschung präsentiert werden konnten.

3. Nutzen und Verwendbarkeit der Ergebnisse

3.1. Verwendung in weiteren Forschungsprojekten

Das IHP und dessen Abteilung System Design sind stetig aktiv an verschiedenen Forschungsprojekten beteiligt. Ein Schwerpunkt liegt hierbei beim Entwurf und der Entwicklung von eingebetteten Systemen im sicherheitskritischen Umfeld. Die gewonnenen Erkenntnisse aus dem Forschungsvorhaben können direkt und indirekt wiederverwendet werden. Zusätzlich ermöglichen Gemeinsamkeiten zwischen den Projekten die Nutzung von Synergien. So werden insbesondere die JavaVM und die Simulationsumgebung in anderen Projekten wiederverwendet. Die Rule-Engine des ESCI-Editors wird im Netzwerkanalysator des Projekts Sens4U wiederverwendet. Die Regeldatenbank wird dem Projektziel, das Deployment von drahtlosen Sensornetzen zu automatisieren und zu erleichtern, angepasst.

Das Thema IT-Security ist von großer wirtschaftlicher Bedeutung und wird von vielen Firmen kritisch eingeschätzt. Daher wird für die Weiterentwicklung von ESCI im Januar erneut ein EXIST-Antrag durch die Kollegen Jana Krimmling, Stefan Lange und Alexander Sänn eingereicht. Von vielen Seiten wurde ein wachsendes Interesse für das ESCI-Projekt bekundet. Es liegen LOI von verschiedenen Interessengruppen vor, die den EXIST-Antrag unterstützen. Wie schon die Marktuntersuchung zur Laufzeit der ForMaT-Forschung zeigte, ist dieser Ansatz noch einzigartig und wird sonst nur zu Forschungszwecken verfolgt.

3.2.Nutzung in Forschung und Lehre

Das IHP verfügt über enge Kooperationen mit Hochschulen in Berlin und Brandenburg. So werden unter anderem zwei Lehrstühle an der BTU Cottbus-Senftenberg durch Mitarbeiter des IHPs geleitet. Die Forschungsinhalte des Lehrstuhls „Sicherheit in pervasiven Systemen“ stehen in direktem Zusammenhang mit den Forschungszielen des Forschungsvorhabens. Die Entwicklung von sicheren eingebetteten Systemen ist auch hier zentraler Schwerpunkt der Forschung. So können Projekterkenntnisse direkt in der Lehre wiederverwendet werden.

Darüber hinaus werden für Studierende der Hochschulen Berlin/Brandenburg Praktika und Abschlussarbeiten am IHP angeboten. Die zu bearbeitenden Themen sind hierbei oftmals auf den Bereich der sicheren eingebetteten Systeme ausgelegt. Mit dem ESCI-Demonstrator kann den Studierenden hierfür Hardware zur Verfügung gestellt werden, die sie selbständig weiterentwickeln

und erproben können.

Nachdem sich herausgestellt hat, dass der lernbasierte Ansatz zur Erkennung protokollspezifischer Angriffe grundsätzlich vielversprechend für das Anwendungsgebiet ist, wird die zukünftige Evaluierung der in [21] dargestellten Lernaspekte zur Verfeinerung der Analyse für den Einsatz in realen Systemen angestrebt. Für die Evaluierung wird die Implementierung der in [6] beschriebenen Analysekomponente weiterhin sukzessive fortgeführt. Ziel ist es, die Analysekomponente für den Einsatz in realen industriellen Netzwerken vorzubereiten und dort zu erproben. Aufgrund der modularen Architektur der Analysekomponente ist dazu eine Erweiterung auf andere gängige Automatisierungsprotokolle gut umsetzbar.

4. Fortschritte bei anderen Stellen

Aktuelle Vorfälle, siehe Abbildung 1, und Studien zeigen, dass es in der industriellen Informationstechnik (IIT) an der Sensibilisierung zur IT-Sicherheit mangelt. Das steigende Bedrohungspotenzial und die Schwierigkeit der Abwehr von Angriffen sind heute offensichtlich. So belegt der Bericht zur Lage der IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) diese Problematik. Die Herausforderungen werden durch den vermehrten Einsatz von drahtloser Kommunikation zusätzlich verstärkt.

Innerhalb des Forschungsvorhabens wurde die Beobachtung des Marktes wie bereits zu Beginn des Projektes fortgeführt. So konnte auf Messen und nationalen als auch internationalen Konferenzen ein sehr starker Bedarf nach einer derartigen Sicherheitslösung identifiziert werden. Darüber hinaus haben persönliche Gespräche gezeigt, dass renommierte Branchevertreter, wie z. B. Siemens, ABB und Beckhoff, an ähnlichen Ansätzen für IT-Sicherheitslösungen für die IIT arbeiten. Jedoch werden hierbei nur Umsetzungen für eigene Produktserien betrachtet. Eine herstellerunabhängige Architektur wird von diesen Unternehmen nicht angestrebt.

Das Produktportfolio von NitroSecurity ist durch einen Übernahmeprozess an McAfee und damit letztendlich an Intel übergegangen. Intel verfügt zudem mit der Übernahme von Windriver über Know-How im Bereich der eingebetteten Systeme. Allerdings haben persönliche Gespräche gezeigt, dass die aktuelle Ausrichtung auf Informationssysteme im Banken- und Telekommunikationssektor beschränkt ist und sich damit wesentlich von ESCI abgrenzt.

Als unabhängiger Hersteller von Sicherheitskomponenten für die industrielle Informationstechnik konnte bisher lediglich Tofino identifiziert werden. Allerdings ist Tofino ein kanadischer Hersteller und damit auf die Systeme Nordamerikas, die sich wesentlich von europäischen Systemen unterscheiden, fokussiert. Zusätzlich bietet das System keinen ganzheitlichen Ansatz, der auch eine direkte Verarbeitung von bereits bestehenden Planungsunterlagen unterstützt. Damit bestehen weiterhin für ESCI wesentliche Wettbewerbsvorteile gegenüber den Produkten von Tofino.

5. Erfolgte und geplante Veröffentlichungen

[1] Klasse statt Masse

Alexander Sänn 2011: Innovationsmanager 16, S. 66-67

[2] Lead Users and Non-Lead Users: Do Their Preference Really Differ in Product Design?

Alexander Sänn und Daniel Baier: Proceedings of the 18th IPDM Conference, June 2011, Delft (The Netherlands).

[3] Customer Innovation: A Combined Lead User and Conjoint Analysis Approach

Alexander Sänn: Marketing Science, June 2011, Houston (USA).

[4] Ubiquitous Computing asks for Ubiquitous Line of Defense

Oliver Stecklina und Peter Langendörfer: KSVS 2011 Workshop über IT-Sicherheit in kollaborativen und stark vernetzten Systemen, Oktober 2011, Berlin (Deutschland).

[5] Mobile XMPP and Cloud Service Collaboration: An Alliance for Flexible Disaster Management

Ronny Klauck, Michael Kirsche, Jan Gaebler und Sebastian Schoepke: Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2011), October 2011, Orlando (USA).

[6] A Distributed Intrusion Detection System for Industrial Automation Networks

Franka Schuster: 17th IEEE International Conference on Emerging Technologies & Factory Automation (ETFA 2012), Krakau (Polen).

[7] Profinet IO Vulnerability Assessment and Attack Derivation

Andreas Paul: 7th International Conference on Critical Information Security (CRITIS 2012), Lillehammer (Norway).

[8] Topologieüberwachung von drahtlosen Sensornetzen in der Automatisierung

Stefan Lange und Oliver Stecklina: 11. GI/ITG KuVS Fachgespräch “Drahtlose Sensornetze”, Darmstadt (Germany).

[9] Complex Product Development: Using a Combined VoC Lead User Approach

Alexander Sänn: The 36th Annual Conference of the German Classification Society (GfKl), Hildesheim, Germany.

[10] A Lightweight Pseudorandom Number Generator for Wireless Sensor Networks

Anna Sojka and Krzysztof Piotrowski: In Proceedings of the 9th International Joint Conference on e-Business and Telecommunications, Rome (Italy).

[11] Erweiterte Sicherheit für kritische Infrastrukturen (ESCI)

Oliver Stecklina und Alexander Sänn: ISI4people Innovationsforum, Berlin (Germany).

[12] Lead Users And Non-Lead Users: Breakthrough Preferences Measured By Online Analysis

Alexander Sänn: ISMS Marketing Science Conference, 2012, Boston (USA).

[13] Lead Users And Non-Lead Users: Breakthrough Preferences Measured By Online Analysis

Alexander Sänn: The R&D Management Conference, 2012, Grenoble (France).

[14] XMPP to the Rescue: Enhancing Post Disaster Management and Joint Task Force Work

Ronny Klauck and Michael Kirsche: In Proceedings of the 2nd International Workshop on Pervasive Networks for Emergency Management (PerNEM) in Cooperation with the 10th IEEE Conference on Pervasive Computing and Communication (PerCom 2012), Lugano, Switzerland.

[15] Bonjour Contiki: A Case Study of a DNS-Based Discovery Service for the Internet of Things

Ronny Klauck and Michael Kirsche: In Proceedings of the 11th International IEEE Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW 2012), Belgrad (Serbien).

[16] Distributed Shared Memory as an Approach for Integrating WSNs and Cloud Computing

Peter Langendörfer, Krzysztof Piotrowski M. Diaz and B. Rubio: In Proceedings of the NTMS Workshop on Wireless Sensor Networks: Architectures, Deployments and Trends (WSN-ADT 2012), Istanbul (Türkei).

[17] Enhanced DNS Message Compression - Optimizing mDNS/DNS-SD for the Use in 6LoWPANs

Ronny Klauck and Michael Kirsche: In Proceedings of the 9th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing 2013 (PerSeNS 2013), co-located with the 11th IEEE Conference on Pervasive Computing and Communication (PerCom 2013) , March 2013, San Diego (USA).

[18] Moversight: An Approach to Support Mobility in Collaborative Applications

Jan Gaebler and H. Koenig: Poster presented as part of the 10th Annual Conference on Wireless On-Demand Network Systems and Services (WONS 2013), March 2013, Banff (Kanada).

[19] Intrusion Detection Systems for (Wireless) Automation Systems

Jana Krimmling and Peter Langendoerfer: The State of the Art Intrusion Prevention and Detection (to be published in 2014), CRC Press, (USA).

[20] Towards the Protection of Industrial Control Systems - Conclusions of a Vulnerability Analysis of Profinet IO

Andreas Paul, Franka Schuster, Hartmut König 2013: Detection of Intrusions and Malware, and Vulnerability Assessment - 10th International Conference (DIMVA 2013), S. 160-176

[21] Towards Learning Normality for Anomaly Detection in Industrial Control Networks

Franka Schuster, Andreas Paul, Hartmut König 2013: Emerging Management Mechanisms for the Future Internet - 7th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2013), S. 61-72

Berichtsblatt

1. ISBN oder ISSN geplant	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel Sensoren für eine kooperative Netzwerküberwachung - ESCI	
4. Autor(en) [Name(n), Vorname(n)] Stecklina, Oliver; Krimmling, Jana; Paul, Andreas; Schuster, Franka; Maye, Oliver; Lange, Stefan; Langendörfer, Peter	5. Abschlussdatum des Vorhabens März 2013
	6. Veröffentlichungsdatum geplant
	7. Form der Publikation Broschüre
8. Durchführende Institution(en) (Name, Adresse) IHP GmbH Im Technologiepark 25 15236 Frankfurt (Oder)	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 03FO3102
	11. Seitenzahl 29
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben
	14. Tabellen 4
	15. Abbildungen 5
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Der Schlussbericht des Projektes „Sensoren für eine kooperative Netzwerküberwachung“ beschreibt die angestrebten und erreichten Ziele des Projektes.

Das Projekt hatte sich zum Ziel gesetzt eine verteilte, reaktive Sicherheitsplattform für eine ganzheitliche Sicherheit für die Systeme der industriellen Informationstechnik (IIT) zu erstellen. Die Plattform nimmt hierbei den Soll-Zustand einer Anlage aus den Planungsunterlagen oder mittels maschinellen Lernens auf und vergleicht diesen Zustand anschließend mit dem Ist-Zustand der Anlage. Der Ist-Zustand wird hierbei mittels Sensoren, die in die reale Anlage eingebracht werden, erfasst.

Durch die Heterogenität der Systeme der IIT konnten klassische Ansätze der IT-Sicherheit aus der Informationstechnik nicht ohne Modifikationen übertragen werden. So gelten in der IIT insbesondere andere Anforderungen bzgl. der Verfügbarkeit, der Reaktionsfähigkeit und der Flexibilität der Systeme sowie bei den Protokollen. Darüber hinaus ist die IIT geprägt durch eine Vielzahl an verschiedenen Protokollen und Systemumgebungen, die teilweise Hersteller-spezifisch sind. Die VRS-Plattform setzt hierzu auf einen modularen Ansatz und verwendet die Java Systemumgebungen. Damit sind eine unkomplizierte Portierung und ein flexible Erweiterung der Plattform möglich. Hierbei wurde insbesondere die beschränkten Ressourcen der Geräte berücksichtigt und eine Java Virtual Machine gewählt, die auf allen Geräteklassen lauffähig ist.

Darüber hinaus wurden Verfahren für eine sichere und vertrauenswürdige Kommunikation zwischen den Komponenten der VRS-Plattform entwickelt. Hierbei lag der Fokus auf Systeme mit sehr geringen Ressourcen, da insbesondere für diese Klasse and Geräte keine adäquaten Lösungen zur Verfügung stehen.

19. Schlagwörter
Sicherheit, Industrielle Informationstechnik, Intrusion Detection, Deep Packet Inspektion

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN planned	2. type of document (e.g. report, publication) Final report
3. title Sensors for cooperative network monitoring - ESCI	
4. author(s) (family name, first name(s)) Stecklina, Oliver; Krimmling, Jana; Paul, Andreas; Schuster, Franka; Maye, Oliver; Lange, Stefan; Langendörfer, Peter	5. end of project March 2013
	6. publication date Planned
	7. form of publication Brochure
8. performing organization(s) (name, address) IHP GmbH Im Technologiepark 25 Frankfurt (Oder)	9. originator's report no.
	10. reference no. 03FO3102
	11. no. of pages 29
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references
	14. no. of tables 4
	15. no. of figures 5
16. supplementary notes	
17. presented at (title, place, date)	

18. abstract

The final report of the project "Sensors for cooperative network monitoring" presents the originally planned as well as the really achieved project goals.

The project aims the development of a distributed, reactive security platform for a ubiquitous line of defence for systems of industrial information technology. Especially in small systems in the area of industrial automation or critical infrastructures the behaviour of a node is strictly predefined and regular. Exploiting feature of this type of systems allows us to provide a clear definition of the expected behaviour. The VRS platform provides a toolset for generating the ruleset from the planning documents and by an autonomous learning. During operation the generate ruleset is compared with the current system state. Any deviation can be considered an anomaly, which indicates that something goes wrong.

Due to the heterogeneous systems of the IIT classical approaches like IP-based firewalls and intrusion detection systems cannot be used one-to-one for this class of networks. The IIT has different requirements regarding availability, response time and flexibility of a system or protocol. Furthermore, the IIT covers a broad variety of industrial protocols and systems, which often deeply influenced by manufactures. Therefore, the VRS platform uses a modular system architecture and Java virtual machines. Thereby, an easy porting and a flexible extension become feasible. The implementation of the Java virtual machine takes the restricted resources of systems into account.

In addition, a library for a secure and trustworthy communication among the VRS components was developed. The development was focused on small systems because of the missing of suitable solutions.

19. keywords
Security, industrial information technology, intrusion detection, deep packet inspection

20. publisher	21. price