ForMaT
UNTERNEHMEN REGION
Die BMBF-Innovationsinitiative Neue Länder

innovations for high performance microelectronics

Abschlußbericht zum Vorhaben

Sensoren für eine kooperative Netzwerküberwachung

Phase I

Zuwendungsempfänger:	**Förderkennzeichen:**
IHP GmbH	03F03101
Vorhabensbezeichnung:	
Sensoren für eine kooperative Netzwerküberwachung	
Laufzeit des Vorhabens:	
1.10.2009 bis 31.03.2010	
Berichtszeitraum:	
1.10.2009 bis 31.03.2010	

Autor : Peter Langendörfer, Oliver Stecklina

Version : 1.0

Datum : 04.11.2010

INHALTSVERZEICHNIS

I. Aufgabenstellung

Ziel des Vorhabens war es, wissenschaftlich-technische Ansätze für neuartige kooperative Netzwerkmonitoring-Lösungen zu identifizieren. Das wirtschaftliche Potential der identifizierten Lösungen sollte mit Hilfe der Lead-User-Methode evaluiert werden.

II. Wissenschaftlicher und technischer Stand

Obwohl in der Vergangenheit bereits vielfach Sicherheitsvorfälle in kritischen Infrastrukturen aufgetreten sind [1], [3], wird die IT-Sicherheit in diesem Bereich erst in den letzten Jahren durch die Forschung adressiert. So wurden in Deutschland im Rahmen der Nationalen Roadmap Embedded Systems [2] für den Bereich der eingebetteten Systeme sechs Forschungsschwerpunkte identifiziert, von denen vier das Thema der Sicherheit direkt adressieren.
Diese vier Forschungsschwerpunkte (autonome Systeme, verteilte Echtzeitsituationserkennung und Lösungsfindung, sichere Systeme sowie Virtual-Engineering) stehen in einem direkten Bezug zu einer verteilten und reaktiven Sicherheitsplattform (VRS-Plattform), wie sie im Rahmen dieses Projektes entwickelt wird. Dass in diesem Bereich ein großer Forschung- und Entwicklungsbedarf besteht, zeigen die in diesem Abschnitt zu dem Themenbereich „Intrusion Detection Systeme (IDS) für Sensorknoten und/oder drahtlose Ad-hoc Netzwerke“ vorgestellten Arbeiten.
Zur detaillierten Betrachtung wird zunächst eine Klassifizierung der Komponenten eines verteilten Sensornetzwerkes vorgenommen und der aktuelle Stand der Technik vorgestellt.

1 Klassifizierung der Komponenten eines Sensornetzwerkes

Aktuelle Sensornetzwerke zur Überwachung, Steuerung sowie Datenerfassung im Industrieautomatisierungs- und Energiebereich (SCADA – Supervisory Control and Data Acquisition) setzen sich aus Geräten verschiedener Leistungsklassen zusammen. Zur Realisierung eines ganzheitlichen Lösungsansatzes muss die VRS-Plattform entsprechend den verfügbaren Ressourcen der einzelnen Geräteklassen angepasste Komponenten bereitstellen. Für die von uns im Rahmen des Projektes avisierte Lösung klassifizieren wir die Geräte eines Sensornetzwerkes wie folgt:

Low-Power 8- und 16-bit-Mikrocontroller bilden die Grundlage für viele aktuell verfügbare Sensorknoten. Mikrocontroller verfügen über sehr wenige Ressourcen und eine geringe Verarbeitungsgeschwindigkeit [4], [5], [6]. Darüber hinaus werden die Geräte meist mittels Batterien oder einer anderen begrenzten Energiequelle versorgt, so dass die Bearbeitungszeit und der Energieverbrauch einzelner Operationen genau beachtet werden müssen.

Verbindungsknoten werden in Netzwerken eingesetzt, bei denen größere Entfernungen überbrückt und/oder kleine Sensornetze aggregiert werden müssen. Sie realisieren oft einen Übergang zwischen verschiedenen Übertragungstechniken und sind im Gegensatz zu Sensorknoten mit leistungsstarken 32-bit-Mikroprozessoren ausgestattet [7], [8], [9]. Sie werden meist durch eine permanente bzw. unbegrenzte Energiequelle versorgt.

PC-basierte Kontroll- und Monitoring-Systeme bilden die Schnittstelle vom Sensornetz zum Nutzer des Systems. Hierbei handelt es sich in der Regel um Standard-Hardware mit Standard-Betriebssystemen.

2 Sicherheitskomponenten Ressourcen-beschränkter Systeme

Bis vor wenigen Jahren wurden Sicherheitsmechanismen auf dem Gebiet der Informationssicherheit für die Klasse der Low-Power-Mikrocontroller kaum bis gar nicht betrachtet. Mit der zunehmenden Migration von Sensorknoten in den Bereich der Cyber-Physical-Systems wurde deutlich, dass hier ein starkes Defizit besteht. Zur Lösung dieses Problems wurden in den letzten Jahren vermehrt Untersuchungen zum Einsatz kryptographischer Verfahren [10], [11], [12], [13], [14] und/oder Trusted Computing [15], [16] durchgeführt.
Die Arbeiten zu starken kryptographischen Mechanismen auf Sensorknoten haben gezeigt, dass diese verwendet werden können, insbesondere dann, wenn sie durch geeignete Hardware unterstützt werden [17]. Im Bereich Trusted Computing[1] für Sensorknoten sind aktuell weniger vielversprechende Ergebnisse vorhanden, jedoch zeigen die Forschungsarbeiten, dass dieses Thema zunehmend an Bedeutung gewinnt.

Eingesetzte Protokolle und Sicherheit: Die Datenübertragung zwischen den einzelnen Knoten von Automatisierungsnetzwerken erfolgte in der Vergangenheit fast ausschließlich über herstellerabhängige Protokolle. Vereinzelt sind auch standardisierte Protokolle (Modbus-ASCII/RTU, Profibus) vorzufinden. Seit Mitte der 90er Jahre ist eine Verschiebung zu Ethernet-basierten Kommunikationsprotokollen zu beobachten (Modbus-TCP, Profinet, EtherNet/IP, DNP3+TCP/UDP). Im Bereich der drahtlosen Übertragungsprotokolle beginnt sich IEEE802.15.4[2] als „Standard“ zu etablieren. So wird es unter anderem von der Hart Communication Foundation für Automatisierungsnetze als Basis definiert.
Infolge dieser Entwicklungen verschieben sich die Sicherheitsrisiken der traditionellen IT-Infrastruktur immer mehr in die Nähe der SCADA-Systeme. Aber auch IEEE802.15.4 wurde in der Vergangenheit bereits erfolgreich angegriffen [18]. Darüber hinaus ist insbesondere das Routing in drahtlosen Sensor- und Ad-hoc-Netzwerken immer wieder Ziel von Angriffen. So wurden in den letzten Jahren erfolgreich Sybill[3]- und Wormhole[4]-Angriffe [19], [20] entdeckt und erste Ansätze zur Vermeidung dieser entwickelt [21]. Die Angriffe und Gegenmaßnahmen hängen jedoch stark vom verwendeten Protokoll ab. Aus diesem Grund sind Techniken von IP-basierten Systemen nur bedingt auf den Bereich der drahtlosen Sensor- und Ad-hoc-Netzwerke übertragbar.

***Intrusion Detection*:** Mit der zunehmenden, allgegenwärtigen Bedrohung von IT-Infrastrukturen kommt zu den klassischen, präventiven Maßnahmen die reaktive Erkennung und Bekämpfung von IT-Sicherheitsverletzungen hinzu. Hierbei wird den Intrusion Detection Systemen (IDS) für die automatische Erkennung von Angriffen eine wachsende Bedeutung beigemessen [22]. Ein bedeutender Vertreter aus diesem Bereich ist das open-source IDS SNORT [32]. SNORT analysiert den Datenverkehr in IP-Netzwerken in Echtzeit. Zur Erkennung von Sicherheitsverletzungen werden die Datenpakete mit charakteristischen Mustern bekannter Angriffe verglichen. Diese Muster

---

[1] **Trusted Computing** ist eine Technologie, die PCs, aber auch andere computergestützte Systeme wie Mobiltelefone mit einem zusätzlichen Chip ausstattet, der mittels kryptographischer Verfahren die Integrität sowohl der Software-Datenstrukturen als auch der Hardware messen kann und diese Werte nachprüfbar abspeichert.

[2] Der Standard **IEEE 802.15.4** beschreibt ein Übertragungsprotokoll für Wireless Personal Area Networks (WPAN). Er definiert die untersten beiden Schichten des OSI-Modells, den Bitübertragungs- und den MAC-Layer. Entwicklungsziele für das Protokoll sind eine geringe Leistungsaufnahme für einen langen Betrieb über eine Batterieversorgung, kostengünstige Hardware, sichere Übertragung, Nutzung der lizenzfreien ISM-Bänder und Parallelbetrieb mit anderen Sendern. Durch diese Eigenschaften eignet sich der Standard IEEE 802.15.4 vor allem für drahtlose Sensornetze (WSN).

[3] Der **Sybil-Angriff** beschreibt multiple Identitäten eines Knotens, um bspw. Suchanfragen fehlzuleiten oder Mehrheitsabstimmungen im Netzwerk zu manipulieren. Damit wird das Routing verlangsamt, was als Vorbereitung für andere Angriffe dienen kann. Klassische Sicherheitsansätze auf Basis von Mehrheitsentscheidungen werden ebenfalls ausgehebelt.

[4] Der **Wormhole-Angriff** beschreibt das bewusste Fehlleiten von Datenpaketen innerhalb eines Sensornetzwerkes. Damit wird das Routing über einen speziellen Knoten verstärkt, was sich negativ auf seine Ressourcen auswirkt und bis zur Abschaltung des Knotens führen kann.

werden allgemein als Signaturen bezeichnet. Für IP-basierte Netzwerke ist eine Vielzahl an Signaturen, bis zu einigen tausend, verfügbar. Ein Einsatz von SNORT in Sensornetzwerken ist jedoch wegen seines zentralistischen Ansatzes, seiner Ausrichtung auf IP-basierte Kommunikationssysteme und seines Ressourcenbedarfes nicht möglich.
Im kommerziellen Bereich sind bereits Firewall- und IDS-Produkte verfügbar, die um Filterregeln für Ethernet-basierte SCADA-Protokolle erweitert wurden. Entsprechende Systeme sind Bestandteil der Produktportfolios von Branchengrößen wie Juniper, Cisco, Symantec, McAfee, IBM-ISS und Fortinet. Allerdings adressieren diese Systeme die häufig eingesetzten Übertragungsstandards wie z. B. Modbus-ASCII/RTU sowie drahtlose Sensornetze nicht.
Im Bereich drahtloser Sensornetze gibt es hinsichtlich der Erkennung von Angriffen nur erste Ansätze. Diese beruhen in der Regel darauf, dass das Verhalten einzelner Sensorknoten von anderen Sensorknoten bewertet wird. So werden z. B. Sensorknoten, die durch ein anormales Verhalten auffallen, aus dem Netzwerk ausgeschlossen. Diese Verfahren basieren auf der Annahme, dass nur ein Teil der Sensorknoten auffällig ist [23], [24]. Hier wird häufig davon ausgegangen, dass eine korrekte Funktion des Sensornetzwerkes sichergestellt ist, solange der Anteil auffälliger Knoten einen vom Ansatz abhängigen Prozentsatz nicht übersteigt. Im Bereich des Schutzes kritischer Infrastrukturen, aber auch bei Automatisierungssystemen kann jedoch die gezielte Kompromittierung einiger weniger Knoten in einem bestimmten Bereich für einen erfolgreichen Angriff ausreichen. Das heißt, hier sind Ansätze, die auf statistischen Betrachtungen beruhen, nicht geeignet. Einen anderen Ansatz verfolgt der regelbasierte Ansatz aus [25]. Hier wird das aktuelle Verhalten des Netzwerkes mit einem als korrekt erlernten Verhalten verglichen. Bei Abweichungen werden diese als Angriff erkannt. Die Anwendbarkeit dieses Verfahrens wird durch die Voraussetzung, dass während der Lernphasen keine Angriffe stattfinden, stark eingeschränkt.

Peer-to-Peer[5]-basierte Overlay-Netzwerke: Für ein Lagebild über die Sicherheit in dem zu schützenden System und geeignete Reaktionsmöglichkeiten auf erkannte Vorfälle sind verteilte Netzsensorik-Konzepte erforderlich. Um eine kontinuierliche Überwachung, eine hohe Anpassungsfähigkeit, Skalierbarkeit und dynamische Rekonfigurierbarkeit sicherzustellen, müssen im Bereich drahtloser Netze alle Knoten gleichberechtigt arbeiten und hierzu über gleichartige Algorithmen verfügen. Gleichberechtigte Überwachungsstrukturen können über P2P-Ansätze gut umgesetzt werden. In [26] und [27] wurden erste Anwendungen des P2P-Prinzips zur Erkennung von Virus-Epidemien und Angriffsversuchen durch Informationsaustausch vorgestellt. Solche Monitoring-Strukturen bestehen aus einem Netzwerk kooperierender Sensoren (Netzsensoren) unter Verwendung von P2P-Mechanismen in Form eines so genannten Overlay-Netzwerkes. Die Netzsensoren erfassen sicherheitsrelevante Daten, werten diese aus oder leiten sie an dafür spezialisierte Knoten weiter und initiieren, wo dies möglich ist, geeignete Gegenmaßnahmen.

Verwandte Projekte auf diesem Gebiet sind:

FIDeS: Das Frühwarn- und Intrusion-Detection-System (FIDeS) untersucht Methoden der künstlichen Intelligenz zur Analyse und Vorhersage von Angriffssequenzen. Das Ziel hierbei ist es, Systemadministratoren bei der Auswahl geeigneter Gegenmaßnahmen zu unterstützen. Das Projekt betrachtet allerdings „normale“ Internet-Angriffe und adressiert die Bereiche der kritischen Infrastrukturen und eingebetteten Systeme nicht.

RealFlex: Das Projekt befasst sich mit der Integration zuverlässiger drahtloser Kommunikationssysteme in Sensor- und Aktornetzen in Automatisierungsanwendungen. Hierbei wird in Teilarbeitspaketen die Integration von Sicherheitsmechanismen in Automatisierungsnetze untersucht. Fragestellungen hinsichtlich der Erkennung von Angriffen werden jedoch nicht betrachtet. Der Schwerpunkt des Projektes liegt auf dem Aspekt der Zuverlässigkeit.

---

[5] Ein **Peer-to-Peer**-Netzwerk (P2P) zeichnet sich durch eine gleichberechtigte (engl. peer) Kommunikationsbeziehung der Netzwerkteilnehmer aus. Teilnehmer eines P2P-Netzwerkes können sowohl Dienste nutzen als auch anbieten. Eine explizite Rollenverteilung existiert nicht.

SPES 2020: Das Projekt Software Platform Embedded Systems (SPES) 2020 ist ähnlich dem Projekt Realflex und hat als Ziel die Entwicklung einer Methodik für den Entwurf „eingebetteter Systeme“. Die zu dem Projekt verfügbaren Informationen sind sehr gering, jedoch lässt die Benamung des Arbeitspaketes AP4: „Sicherheitsnachweis, Zertifizierung und Qualitätssicherung nicht funktionaler Anforderungen“ den Schluss zu, dass hier Sicherheit nicht im Sinne von IT-Sicherheit betrachtet wird. Die Ausrichtung des gesamten Projektes stützt die Vermutung, dass „Sicherheit“ im Sinne von Zuverlässigkeit und Betriebssicherheit im Vordergrund steht.

Auch im 7. Rahmenprogramm der EU untersuchen einige Projekte Sicherheitsaspekte, die relevant für das hier vorgeschlagene Projekt sind. Das Projekt AWISSENET (Ad-hoc personal area network & WIreless Sensor SEcure NETwork) hat eine Architektur zur Angriffserkennung in drahtlosen Sensornetzen vorgeschlagen, die eine zentrale Komponente zur Auswertung von Angriffssequenzen nutzt. Dieser Ansatz erscheint aufgrund der beschränkten Ressourcen und der Echtzeitanforderungen im Bereich der Leitsysteme und Automatisierungsanwendungen nicht anwendbar. Auch im Projekt WSAN4CIP (Wireless Sensor and Actor Networks for Critical Infrastructure Protection) werden Sicherheit und Zuverlässigkeit in Sensornetzen untersucht. Die Untersuchungen zur Angriffserkennung berücksichtigen jedoch nur isolierte Knoten und eine Erkennung von Angriffssequenzen ist ebenfalls nicht geplant. Das hier vorgeschlagene Projekt geht mit der verteilten Angriffserkennung und der Einleitung von Gegenmaßnahmen deutlich über die Ansätze von AWISSNET und WSAN4CIP hinaus.

III. Erzielte Ergebnisse

In einem ersten Schritt wurden potentielle Anwendungsgebiete untersucht. Der Rest dieses Abschnittes führt in das Themengebiet ein, welches für am relevantesten identifiziert wurde.

In den letzten Jahren ist in der industriellen Informationstechnik (IT) ein starker Trend weg von den proprietären, kabelgebundenen und abgeschlossenen Bussystemen[6] hin zu drahtlosen, standardisierten und offenen Verbindungsnetzwerken zu verzeichnen. Damit werden in der industriellen Informationstechnik die folgenden drei, grundlegend verschiedenen Technologien miteinander verbunden:

- proprietäre, drahtgebundene Bussysteme,
- drahtlose Automatisierungssysteme und
- standardisierte und offene Verbindungsnetzwerke.

Durch die Verbindung dieser Technologien werden die Systeme, die Phänomene der realen Welt überwachen, in das gemeinschaftliche Netz eingebunden. Derartige Systeme werden als **Cyber-Physical-Systems**[7] bezeichnet. Dies führt zu tiefgreifenden Veränderungen sowohl im regulären Betrieb als auch beim Gefährdungspotenzial der Systeme durch Angriffe Dritter. Das steigende Bedrohungspotenzial und die Schwierigkeit der Abwehr von Angriffen sind bereits heute anhand der weiten Verbreitung schädlicher Phänomene im Internet ablesbar [29]. So belegt der Bericht zur Lage der IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [28], dass im Jahr 2008 40 % aller Organisationen und Unternehmen Ziel finanziell motivierter Angriffe durch organisierte Kriminalität waren. Diese Problematik wird durch den vermehrten Einsatz von drahtloser Kommunikation zusätzlich verstärkt.

---

[6] Bei einem **Bussystem** handelt es sich um ein Verbindungsnetzwerk innerhalb von Computern oder industriellen Anlagen. Hierbei werden Komponenten zum Austausch von Daten und Informationen über einen gemeinsamen Übertragungsweg (Bus) miteinander verbunden.

[7] Eingebettete Systeme erheben nicht nur Daten und verarbeiten sie vor Ort, sondern leiten Daten auch weiter, kommunizieren mit anderen eingebetteten Systemen und mit Zentralrechnern. Sie werden Teil des Cyberspace und bilden als physikalische Objekte die neuen **Cyber-Physical Systems**. Es geht also um die Verschmelzung der realen physischen Welt und digital-virtuellen Welten.

Aufgrund der Verbindung heterogener Technologien verfehlen klassische Ansätze ihre Wirkung. So müssen für die Verbindung der drei einführend genannten Technologien vollständig neue Techniken zum Monitoring[8] und zum Selbstschutz der einzelnen Komponenten und des Gesamtsystems entwickelt werden.
Für einen ganzheitlichen Schutz moderner industrieller IT ist eine allgegenwärtige, flexible und offene Sicherheitsarchitektur zwingend erforderlich. Diese wurde im Projekt als **„verteilte und reaktive Sicherheitsplattform“** (VRS-Plattform) für den Schutz drahtloser, standardisierter und offener Verbindungsnetzwerke der industriellen IT definiert. Eine derartige Plattform muss eine globale Sicht auf das System erlauben, eine gleichberechtigte Beziehung der verschiedenen Komponenten unterstützen und zusätzlich geeignete, mitunter maßgeschneiderte Techniken für die einzelnen Teilsysteme bereitstellen.

1 Themen und Ziele für weitere Arbeiten

Bei der Definition der Forschungsthemen wurden speziell kritische Infrastrukturen[9] (KRITIS), die eine Ausprägung von Cyber-Physical-Systems darstellen, untersucht. Ausgehend von den Anforderungen an deren Schutz und dem Schutz von industriellen IT-Systemen für den Entwurf und die spätere Umsetzung eines ganzheitlichen Konzeptes für die Gestaltung von Sicherheitslösungen in Form einer verteilten und reaktiven Sicherheitsplattform sollen die im Folgenden kurz beschriebenen Themenkomplexe untersucht werden:

Entwicklung von Netzsensoren[10]: Es sollen Netzsensoren für die Erkennung von Angriffen, zum Einleiten von Gegenmaßnahmen und zum Selbstschutz der in der industriellen IT eingesetzten Systemklassen, Mikrocontroller, Verbindungsknoten und untersucht und umgesetzt werden.

Entwicklung kooperativer Monitoring-Lösungen: Für den Aufbau einer netzwerkweiten Sicherheitslösung sollen die beteiligten Netzsensoren über ein Overlay-Netzwerk[11] kooperieren. Zu diesem Zweck müssen zunächst Mechanismen für eine sichere Kommunikation, zum Aufbau von Vertrauensbeziehungen und geeignete, verteilte Angriffserkennungsmechanismen untersucht und umgesetzt werden.

---

[8] **Monitoring** ist ein Überbegriff für alle Arten der unmittelbaren systematischen Erfassung von Vorgängen oder Prozessen mittels technischer Hilfsmittel.

[9] Als **kritische Infrastruktur** werden Organisationen und Einrichtungen einer Gesellschaft bezeichnet, denen eine zentrale Bedeutung für die stabile Funktionsweise des Gemeinwesens zukommt [1]. Hierzu zählen Energie-, Wasser- und Lebensmittelversorgung, Gesundheitswesen, Verkehrs- und Transportsystem, Bankwesen, die Telekommunikationsinfrastruktur und andere Versorgungsstrukturen. Der Ausfall dieser Systeme kann zu kaskadierenden Effekten führen, die das Funktionieren des Gemeinwesens massiv beeinträchtigen.

[10] Im Rahmen dieses Projektes zeichnen wir Hardware- und Software-Komponenten, die in der Lage sind, sicherheitsrelevante Informationen in verteilten Infrastrukturen aufzuzeichnen, als **Netzsensor**.

[11] Ein **Overlay-Netzwerk** beschreibt ein Netzwerk, das auf ein bestehendes Netzwerk aufgelegt wird. Es ist meist ein logisches Netzwerk mit einer eigenen Adressierung der Teilnehmer und einem eigenen Wegewahlverfahren (Routing).

Entwicklung eines System- und Sicherheitsmanagements: Der Aufbau einer wirksamen Monitoring-Struktur erfordert eine sorgfältige Planung. Diese soll durch entsprechende Werkzeuge unterstützt werden. Hierfür müssen Mechanismen entwickelt werden, die ein Auswählen der notwendigen Sicherheitsmodule sowie ein Platzieren der Netzsensoren unterstützen und das Definieren von Sicherheitsregeln erlauben.

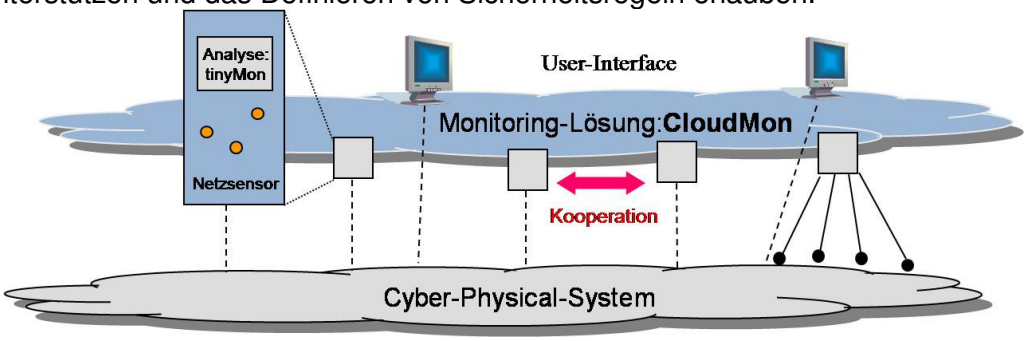

Abbildung 1: Schema der verteilten und reaktiven Sicherheitsplattform

2 Verifikation des Marktpotentials durch Anwendung der Lead-User-Methode

Im Rahmen der **ersten Phase** der Lead-User-Methode wurde die Zielstellung des Projektes konkretisiert. 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 bestätigt. Dies konnte im Rahmen des Sensornetztages am IHP durch Fachgespräche mit weiteren Unternehmen und Einrichtungen weiter gefestigt 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. In der **zweiten Phase** wurden mittels Tiefeninterviews die relevanten Geschäftsfelder überprüft. Am Institut für Energietechnik der BTU Cottbus engagierten sich verschiedene Lehrstühle in branchenspezifischen Forschungs- und Industrieprojekten. Mit ihnen konnten enge Kontakte zu Vattenfall Europe und den Stadtwerken Cottbus hergestellt werden. Die Kontakte bestätigten die Bedeutung 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.
Die in der ersten ForMaT-Phase durchgeführten Gespräche bestätigten den Trend zur Einführung von drahtlosen, standardisierten und offenen Verbindungsnetzen in der industriellen IT und damit den Übergang zu Cyber-Physical-Systems. Die Entwicklung wird im Wesentlichen durch das Fehlen von Sicherheitslösungen verzögert. So bestätigten die Kontakte, dass insbesondere der Einsatz von drahtlosen Verbindungen sehr attraktiv ist, allerdings viele Bedenken hinsichtlich der Sicherheit und der Verfügbarkeit einer solchen Lösung existieren. Die Schnittmenge der vorgestellten Märkte der IT-Sicherheit und eingebetteter Systeme stellt das Zielsegment des Forschungsvorhabens dar. Überträgt man allein für Deutschland den Anteil der IT-Sicherheit am IT-Gesamtmarkt [30] auf den zukünftigen Markt für Sicherheitslösungen im Bereich der eingebetteten Systeme [31], so ergibt sich für das Jahr 2020 ein Gesamtumsatz von 450 Mio. EUR.

IV. Zusammenarbeit

Die **Gruppe drahtlose Sensornetze** des IHP beschäftigt sich seit knapp zehn Jahren mit Fragestellungen der Sicherheit mobiler und drahtloser Systeme. Sicherheitsaspekte in kontextsensitiven

Plattformen und Hardwarebeschleuniger für kryptographische Verfahren untersuchte das IHP in dem Projekt Mobile Internet Business (bmbf) sehr erfolgreich. Aufbauend auf diese Arbeiten wurden erfolgreich mehrere EU-Projekte - UbiSecSens und WSAN4CIP - durchgeführt. Weitere Expertise im Bereich Intrusion Detection und Peer-to-Peer-Kommunikation wurde über einen Unterauftrag an die BTU Cottbus, Lehrstuhl Rechnernetze und Kommunikationssysteme, Prof. Dr. H. König, in die Untersuchungen eingebunden. Der Lehrstuhl forscht seit 1993 kontinuierlich auf dem Gebiet der Intrusion Detection und seit 2003 im Bereich der Peer-to-Peer-Netzwerke. Die betriebswirtschaftliche Expertise wurde ebenfalls über eine Kooperation mit der BTU Cottbus sichergestellt. Der Lehrstuhl für Marketing und Innovationsmanagement, Prof. Dr. D. Baier, forscht seit Jahren mit den Themen Innovationsmarktforschung, Innovationsmanagement und IT-Management im Grenzbereich zwischen der Informatik und den Wirtschaftswissenschaften. Alle eingebundenen Arbeitsgruppen verfügen über eigene Erfahrungen mit Ausgründungen.

Die Zusammenarbeit mit dem Unterauftragnehmer BTU Cottbus verlief erwartungsgemäß, produktiv und reibungsfrei. Kooperationsfördernde Kommunikationstechniken wie Projekttreffen wurden wöchentlich durchgeführt. Unter Ausnutzung synergetischer Effekte wurde das gemeinsam vorhandene Know-how wirkungsvoll in die Projektarbeit eingebracht. Die Einbeziehung der Wirtschaftsunternehmen wurde problemlos erreicht, teilweise wurden hierfür bereits existierende Kontakte aus anderen Projekten genutzt.
Der BITKOM unterstützte das Projektteam durch einen regelmäßigen Abgleich der Forschungsarbeiten mit dem weiterführenden Bedarf der Industrie und generiert Feedback aus den einzelnen Arbeitskreisen.

Zusammenfassend kann festgestellt werden, dass die Zusammensetzung der Arbeitsgruppe hervorragende Voraussetzungen für eine erfolgreiche Bearbeitung des Vorhabens geboten hat.

V. Referenzen

[1] American Water Works Association, Homland Security: Roadmap to Secure Control Systems in the Water Sector, p. 14, 2008
[2] Achatz, Reinhod; Beetz, Klaus; Broy, Manfred; Dämbkes, Heinrich; Damm, Werner; Grimm, Klaus; Liggesmeyer, Peter: Nationale Roadmap Embedded Systems, 2009
[3] U.S.NRC: Status Of The Accident Sequence Precursor (ASP) Program And The Development Of Standardized Plant Analysis Risk (SPAR) Models, p. 6, 2004
[4] Texas Instruments; www.ti.com
[5] Atmel; www.atmel.com
[6] Microchip; www.microchip.com
[7] ARM; www.arm.com
[8] MIPS Technology Inc.; www.mips.com
[9] www.freescale.com
[10] K. Piotrowski, P. Langendörfer, St. Peter: How Public Key Cryptography Influences Wireless Sensor Node Lifetime, Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Oktober 2006
[11] David J. Malan, Matt Welsh, and Michael D. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In Proceedings of the First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Washington, DC, USA, 2004. IEEE Computer Society.
[12] Vipul Gupta, Matthew Millard, Stephen Fung, Yu Zhu, Nils Gura, Hans Eberle, and Sheueling Chang Shantz. Sizzle: A standards-based end-to-end security architecture for the embedded internet (best paper). In PERCOM ’05: Proceedings of the Third

IEEE International Conference on Pervasive Computing and Communications, pages 247–256, Washington, DC, USA, 2005. IEEE Computer Society.
[13] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324–328, Washington, DC, USA, 2005. IEEE Computer Society.
[14] Ronald Watro, Derrick Kong, Sue fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. Tinypk: securing sensor networks with public key technology. In SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pages 59–64, New York, NY, USA, 2004. ACM Press.
[15] Claude Castelluccia, Aurélien Francillon, Daniele Perito, Claudio Soriente: On the difficulty of software-based attestation of embedded devices, CCS'09: Proceedings of the 16th ACM conference on Computer and Communications Security, November 2009
[16] Arvind Seshadri, Adrian Perrig, Leendert van Doorn and Pradeep Khosla. SWATT: SoftWare-based ATTestation for Embedded Devices. Appears in the 2004 IEEE Symposium on Security and Privacy.
[17] St. Peter, P. Langendörfer, K. Piotrowski: Public key cryptography empowered smart dust is affordable, International Journal of Sensor Networks (IJSNET), Inderscience Vol.4, No.1/2, 2008
[18] O. D. Radosveta Sokullu and I. Korkmaz, "On the IEEE 802.15.4 MAC layer attacks: GTS attack," in Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on, pp. 673–678, Aug. 2008.
[19] J. R. Douceur, "The Sybil Attack," in IPTPS'02:1st International Workshop on Peer-to-Peer Systems, (New York, NY, USA), IPTPS, 2002.
[20] J. Yang, Y. Chen, and W. Trappe, "Detecting sybil attacks in wireless and sensor networks using cluster analysis," in Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on, pp. 834–839, 29 2008-Oct. 2 2008.
[21] Murat Demirbas, Youngwhan Song, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks, Proceedings of Advanced EXPerimental activities ON WIRELESS networks and systems (EXPONWIRELESS) Workshop (as part of WOWMOM 2006), Buffalo, NY, pages 564-570, June 2006.
[22] BMBF (2009): Embedded Systems. Embedded Software - Herausforderung und Chancen für die deutsche Wirtschaft. Bundesministerium für Bildung und Forschung. Berlin. Online verfügbar unter http://www.pt-it.pt-dlr.de/_media/Embedded_Systems_Infoblatt.pdf, zuletzt geprüft am 09.03.2010.
[23] João P. Vilela and João Barros, A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol. IEEE Communications Society/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm'07), Nice, France, September 2007
[24] Felix Freiling, Ioannis Krontiris, Tassos Dimitriou Towards Intrusion Detection in Wireless Sensor Networks 13th European Wireless Conference, Paris, France, 2007-04-01
[25] Ana Paula R. da Silva, Marcelo H.T. Martins, Bruno P.S. Rocha, Antonio A.F. Loureiro, Linnyer B. Ruiz, Hao Chi Wong, Decentralized Intrusion Detection in Wireless Sensor Networks, ACM International Workshop on QoS and Security for Wireless and Mobile Networks
[26] V. Vlachos, S. Androutsellis-Theotokis, and D. Spinellis. Security applications of peer-to-peer net-works. Computer Networks, 45(2):195–205, 2004.
[27] R. Janakiraman, M. Waldvogel, and Q. Zhang. Indra: A peer-to-peer approach to network intrusion detection and prevention. In WETICE, pages 226–231. IEEE Computer Society, 2003.
[28] Bericht zur Lage der IT-Sicherheit in der Bundesrepublik Deutschland http://www.bsi.bund.de/literat/lagebericht/lagebericht2007.pdf

[29] Symantec (2010b): State of Enterprise Security 2010. Online verfügbar unter http://www.symantec.com/content/de/de/about/downloads/PressCenter/2010_State_of_Enterprise_Security_report_small_-_final_-_2010-02-14_01.pdf, zuletzt geprüft am 09.03.2010.
[30] IDC (2009b): IDC prognostiziert für 2010 moderates Wachstum der IT-Ausgaben und eine fundamentale Umgestaltung der ITK-Branche. Unter Mitarbeit von Edith M. Horton. IDC. Online verfügbar unter http://www.idc.de/downloads/pdf/pm2009/22_IDC%20IT%20Trends%202010_final.pdf, zuletzt geprüft am 02.03.2010.
[31] A.T. Kearney (2009): Die IT-Industrie im Jahre 2020. Geht die deutsche IT-Industrie als Sieger aus der Finanzkrise hervor? A.T. Kearney.
[32] SNORT; www.snort.org

Berichtsblatt

1. ISBN oder ISSN --	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht

3. Titel
Sensoren für eine kooperative Netzwerküberwachung

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 31.03.2010
Langendörfer, Peter Stecklina, Oliver	6. Veröffentlichungsdatum 24.11.2010
	7. Form der Publikation Abschlussbericht
8. Durchführende Institution(en) (Name, Adresse) IHP GmbH, Frankfurt (Oder)	9. Ber. Nr. Durchführende Institution --
	10. Förderkennzeichen 03F03101
	11. Seitenzahl 11
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung 10115 Berlin	13. Literaturangaben 32
	14. Tabellen 0
	15. Abbildungen 1

16. Zusätzliche Angaben
___

17. Vorgelegt bei (Titel, Ort, Datum)
Technische Informationsbibliothek und Universitätsbibliothek Hannover. 22.11.2010

18. Kurzfassung

Das übergeordnete Ziel des vom BMBF im Rahmen von "ForMaT" geförderten Projektes „Sensoren für eine kooperative Netzwerküberwachung“ bestand in der Evaluierung potentieller Anwendungsgebiete für eine Peer-to-Peer-basierte, kooperative Netzüberwachung sowie der Entwicklung von Forschungsideen, deren Umsetzung in folgenden Projekten eine Realisierung derartiger Ansätze ermöglicht. Für die Evaluierung wurde die Lead-User-Methode angewendet und über 160 Telefoninterviews mit potentiellen Anwendern durchgeführt. Dabei haben sich der Schutz kritischer Infrastrukturen sowie Automatisierungsnetzwerke als besonders vielversprechende Anwendungsgebiete gezeigt. Es wurden Forschungsaufgaben in den Gebieten lokale Überwachung von Sensorknoten, kooperative Überwachung von Sensorknoten sowie die Entwicklung von Werkzeugen zur Anpassung von Netzüberwachungstechniken an reale Netze aus den Anwendungsgebieten identifiziert.

19. Schlagwörter
Drahtlose Sensornetze, Peer-to-Peer Netzwerke, Automatisierungstechnik, kritische Infrastruktur, Sicherheit, Intrusion Detection

20. Verlag ---	21. Preis ---

Document Control Sheet

1. ISBN or ISSN ----	2. type of document (e.g. report, publication) Report
3. title Sensors for cooperative network monitoring	
4. author(s) (family name, first name(s)) Langendörfer, Peter Stecklina, Oliver	5. end of project 31.03.2010
	6. publication date 24.11.2010
	7. form of publication Report
8. performing organization(s) (name, address) IHP GmbH, Frankfurt (Oder)	9. originator's report no. --
	10. reference no. 03F03101
	11. no. of pages 11
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung 10115 Berlin	13. no. of references 32
	14. no. of tables 0
	15. no. of figures 1
16. supplementary notes ----	
17. presented at (title, place, date) Technische Informationsbibliothek und Universitätsbibliothek Hannover. 22.11.2010	
18. abstract The goal of the project named Sensors for cooperative network monitoring " was to evaluate the potential application areas for a peer-to-peer based cooperative network monitoring. In addition potential research fields for later investigation in follow-up projects have been identified. The project used the lead user method for the evaluation process. In this activity more than 160 phone interviews with potential end users have been executed. Automation control and critical infrastructure protection have been identified as the most promising application areas. The following research areas have been identified: local monitoring of individual sensor nodes, cooperative monitoring of sensor nodes, and the development of a tools chain for designing the monitoring network.	
19. keywords Wireless sensor network, intrusion detection, peer-to-peer, automation control, critical infrastructure protection	
20. publisher ---	21. price ---