RealFlex

Abschlussbericht (IHP)

Zuwendungsempfänger:	IHP GmbH
Förderkennzeichen:	01BN0711A
Berichtszeitraum:	01.10.2007 - 30.11.2010
Abgabedatum:	30.07.2011
Version:	1.0
Seiten:	23

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 01BN0711A gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Editor:
Steffen Peter
IHP GmbH
Im Technologiepark 25
15236 Frankfurt (Oder), Germany
email: peter@ihp–microelectronics.com

Inhaltsverzeichnis

I Kurze Darstellung

I.1 Aufgabenstellung

Das Projekt RealFlex adressierte das neue Gebiet der drahtlosen Kommunikationstechnik im Automatisierungsumfeld. Dies beinhaltet sowohl die Interaktion mit Sensor-/Aktorsystemen, als auch die Einbindung in die Systemumgebung der Automatisierungstechnik. Diese, geprägt durch hohe Zuverlässigkeit und Echtzeitfähigkeit, soll um drahtlose Systemkomponenten ergänzt werden, die in Bezug auf ihre Einsatzmöglichkeiten mit drahtgebundenen Komponenten vergleichbar sind. Bei drahtlosen Komponenten muss aber zusätzlich der Einfluss der Umgebung auf den Übertragungskanal berücksichtigt werden. Es müssen entsprechende Mittel in der Architektur vorgesehen werden, um Einschränkungen zu kompensieren. Hierfür ist die Realisierung von autonomen Teilsystemen, die Kommunikationssubsysteme aber auch einzelne Sensoren sein können, vorgesehen. Falls diese Konzepte nicht ausreichen um die Einschränkungen zu kompensieren, werden Mechanismen untersucht, die dem Integrator die Beschränkungen in jedem Fall sichtbar machen. Die Kombination von drahtlosen Kommunikationsmöglichkeiten mit dem Konzept der autonomen Teilsysteme erlaubt die Realisierung einer flexiblen Systemarchitektur sowie den sehr flexiblen Einsatz der entstehenden Lösung. Damit fällt das vorgeschlagene Projekt ins Zentrum der durch die Ausschreibung beabsichtigten Verbesserung der Automatisierungs- und Fertigungstechnik durch den Einsatz drahtloser Kommunikationstechnologien. Das Ziel dieses Projektes ist die Flexibilisierung von Automatisierungssystemen durch die nahtlose Integration drahtloser Kommunikationssysteme. Zur Erreichung dieses Ziels müssen folgende wissenschaftliche und technische Herausforderungen erfolgreich gemeistert werden:

- **Entwicklung einer flexiblen Architektur für drahtlose Automatisierungssysteme und Integration dieser in drahtgebundene Architekturen:** Die Gewährleistung von Systemeigenschaften wie „plug and produce“ und Echtzeitfähigkeit bei Verwendung drahtloser Kommunikationslösungen erfordert eine modulare Architektur mit verteilter Intelligenz. Das Ziel dabei ist es, Teilsysteme zu autonomen Entscheidungen zu befähigen. So können z. B. neue Systemkomponenten weitestgehend ohne menschliches Eingreifen in das System integriert bzw. Sensordaten können lokal ausgewertet werden und entsprechende Aktionen können lokal ausgelöst werden.
  Daher sollen Untersuchungen zur Umsetzung eines integrierten Managementansatzes durchgeführt werden, die überwiegend der Sicherstellung der „plug and produce“ Eigenschaft dienen. Einer der Schwerpunkte hierbei ist die Vereinheitlichung des Managements der Automatisierungsanwendung und des Managements des Kommunikationssystems. Durch diese Management-Komponente wird auch die Umsetzung von Sicherheitskonzepten, wie Authentisierung und Autorisierung, unterstützt.

  Um drahtlose Sensor-/Aktornetzwerke künftig auch in der Wirkungskette von Prozess-Regelungen und Prozess-Steuerungen einsetzen zu können, ist die Echtzeitfähigkeit unabdingbar. Zur Gewährleistung der Echtzeitfähigkeit sollen daher Ansätze untersucht werden, die eine verteilte Realisierung der Steuerungsmechanismen ermöglichen. Diese sollen Teilsysteme aber auch einzelne Sensoren zu autonomen intelligenten Entscheidungen befähigen. So können Zwischensysteme und Sensoren auf der Basis ihrer lokalen Messwerte vordefinierte Aktionen autonom ausführen oder ihre Werte beispielsweise nur dann senden, wenn diese außerhalb vordefinierter Grenzen liegen. Auf diese Weise werden sowohl die zentralen Steuereinheiten der Automatisierungssysteme als auch die Kommunikationssysteme entlastet. Beides trägt auch dazu bei, die Echtzeitfähigkeit des Gesamtsystems zu verbessern, da die Ressourcen entlastet werden.

- **Entwicklung von drahtlosen Kommunikationssubsystemen für Automatisierungssysteme:** Der flexible Einsatz unterschiedlicher Kommunikationsmedien erfordert die Bereitstellung geeigneter Zwischensysteme, die zwei oder mehr Kommunikationsstandards konfliktfrei unterstützen können. Der Einsatz in Automatisierungssystemen erfordert außerdem die Sicherstellung von „Quality of Service“ (QoS), damit die Echtzeitfähigkeit und Zuverlässigkeit des Systems gewährleistet werden kann.

  Im Rahmen dieser Arbeiten sollten Multistandard-Kommunikationsknoten, die z. B. IEE-E802.11 und IEEE802.15.4 und IEEE802.15.4a unterstützen, entwickelt werden und hinsichtlich ihrer Zuverlässigkeit untersucht und getestet. Insbesondere sollten zur Sicherstellung der QoS HCCA-Ansätze für die WLAN-Module untersucht und integriert werden. Für die IEEE 802.15.4a-Module soll die Zuverlässigkeit durch die Integration der Chirp-Technologie erhöht werden.

Für die Multistandard-Kommunikationsknoten sollen geeignete Protokolle und Proxies entwickelt werden. Die Proxies sollen als intelligente autonome Zwischensysteme (vgl. letzter Anstrich) realisiert werden. Hier können also autonome Entscheidungen hinsichtlich der Weiterleitung von einzelnen Paketen erfolgen. So können Stausituationen vermieden und eine hohe Aktualität der weitergeleiteten Daten sichergestellt werden.

Die Einbindung einzelner Sensoren soll durch die Entwicklung einer Version von IO-Link für drahtlose Übertragungstechnologien realisiert werden.

- **Test und Verifikation der Systemeigenschaften:** Die Eigenschaften der neu entwickelten Systemkomponenten (Soft- und Hardware) sollen während der Realisierung mit Hilfe analytischer Methoden und geeigneten Tests verifiziert werden. Die Überprüfung soll möglichst unter realen Bedingungen stattfinden. Um das Zusammenspiel der Komponenten testen und verifizieren zu können, sind gemeinsame Demonstratoren einzuplanen.

I.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das IHP ist ein weltweit führendes Institut im Bereich der drahtlosen Kommunikation und verfügt über eine eigene SiGeC-Technologie sowie einen Klasse-1-Reinstraum. Die Systemabteilung des IHP hat große Erfahrung in der Untersuchung und Realisierung von drahtlosen Kommunikations-systemen und verfügt über Know-how auf allen Ebenen des Protokollstapels. Außerdem hat das IHP Middleware-Plattformen für ortssensitive Dienste in nationalen (Wireless Internet ad hoc und zellular, BMBF) und internationalen Projekten (WINEGLASS, EU) realisiert.

Relevante Vorarbeiten vom IHP:

- IBMS2: am IHP wurde im Rahmen dieses Projektes das weltweit erste 802.11a-Single-Chip-Modem gefertigt.
- im BASUMA-Projekt entwickelt das IHP Sensorknoten, die zur Langzeitüberwachung der vitalen Daten von z. B. chronisch Kranken eingesetzt werden können. Diese Knoten nutzen das IEEE-802.15.4-Protokoll.
- Im Rahmen der Projekte Mobile Internet Business (BMBF) und UbiSecSens (EU) untersucht das IHP Fragestellungen im Bereich Sicherheit für mobile Endgeräte und Sensorknoten. In diesen Projekten wurden Hardwarebeschleuniger für symmetrische und asymmetrische Verschlüsselungsverfahren entwickelt.

I.3 Planung und Ablauf des Vorhabens

Das Projekt sollte vom 01.10.2007 bis zum 30.09.2010 laufen. Es war in drei zeitliche Phasen aufgeteilt, welche die Abhängigkeiten in den geplanten Forschungs- und Entwicklungsarbeiten widerspiegeln. Diese Phasen überlappten sich teilweise um zeitliche Verzögerungen in der Projektbearbeitung zu vermeiden:

Phase 1: Requirement Analyse: Ausgehend von der Beschreibung relevanter Szenarien sollen die technischen Anforderungen an das Gesamtsystem abgeleitet werden. Die analytisch hergeleiteten Anforderungen bilden die Grundlage für die anschließenden Spezifikations- und Designuntersuchungen in den einzelnen Teilgebieten. Um Zeit zu gewinnen wird diese Phase frühzeitig geeignete Anforderungen an die darauf folgenden Arbeitspakete liefern, welche dann in der weiteren Arbeit konkretisiert werden.

Phase 2: Spezifikation und Implementierung: In den Arbeitspaketen 2 - 4 werden die Teilsysteme sowie die notwendigen Protokolle spezifiziert, implementiert und anschließend individuell getestet.

Phase 3: Integration und Evaluierung: Zur Evaluierung werden 1 - 2 der Anwendungsszenarien zu Demonstratorspezifikationen ausgearbeitet. Diese werden in Teilsystemen z. B. als Labor-Demonstratoren realisiert. Dazu werden Systemkomponenten aus den Arbeitspaketen 2 - 4 miteinander integriert. Nach erfolgreichem Abschluss dieser Arbeiten werden die Teilsysteme in den Gesamt-Demonstrator integriert und dort hinsichtlich ihrer Parameter im realen Betrieb evaluiert.

Das Projekt besteht aus fünf technischen und einem administrativen Arbeitspaket. Letzteres dient dem Projektmanagement und der Außendarstellung. Die fünf technischen Arbeitspakete sind:

AP 1 Anwendungsszenarien und Anwendungsanforderungen
AP 2 Systemspezifikation
AP 3 Drahtlose Sensorknoten
AP 4 Protokollentwicklung
AP 5 Demonstrator

AP1 und AP5 bilden den Rahmen des Projektes, ersteres dient der Untersuchung der Systemanforderungen, während letzteres überwiegend der Evaluierung der in den Arbeitspaketen 2 - 4 erzielten Ergebnisse im Hinblick auf die Erfüllung der Systemanforderungen dient. Jedes Arbeitspaket wurde in 3 bis 6 Unterarbeitspunkte unterteilt.

Trotz der sorgfältigen Planung hat es im Laufe des Projektes Verzögerungen gegeben, die zum Ende hin eine kostenneutrale Projektverlängerung um 2-3 Monate notwendig gemacht haben. Gründe hierfür waren:

- der etwas verspäte Start des Projektes - die eigentlichen Arbeiten im Projekt begannen mit 2-3 monatiger Verspätung,
- Komplexe Diskussionen bei der Entscheidung der Gesamtarchitektur in AP2,
- Signifikante gesamtwirtschaftliche Schwankungen, die speziell bei den industriellen Partnern zu Anspannungen bei den verfügbaren Ressourcen geführt haben.
- Wechsel des Betreibers der Biogasanlage, was die Planung und Durchführung der Integration für diesem Demonstrator verzögert haben.

Abgesehen von diesen Verzögerungen konnte der Projektplan direkt umgesetzt werden und die Projektziele erreicht werden.

I.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Zu Beginn des Projektes gab es von der Automatierungsseite kaum Anknüpfungspunkte im drahtlosen Bereich. Allerdings war es notwendig, existierende Protokolle und Standards aus dem drahtgebundenen Bereich zu berücksichtigen.

Die zum damaligen Zeitpunkt sich im Feld befindliche drahtlose Automatisierungssysteme beruhten auf Varianten des IEEE802.11 sowie auf Bluetooth, ZigBee und vielen proprietären Lösungen im Bereich der unteren ISM-Bänder. Diese wurden in der ersten Projektphase umfassend analysiert.

Im Bereich der drahtgebundenen Protokolle wurde mit IO-Link ein erster Versuch unternommen, Sensorenschnittstellen so zu standardisieren, dass eine einfache Integration möglich wird. Die IO-Link-Spezifikation [6] beinhaltet die Übertragungseigenschaften, eine Datenschnittstelle für Prozess- und Bedarfsdaten und Informationen zur Systemintegration und ermöglicht so eine zentrale Diagnose und Parametrierung, eine sehr schnelle Inbetriebnahme und eine einheitliche Verdrahtung der Sensoren/Aktoren. IO-Link bietet einen rückwirkungsfreien und abwärtskompatibler Betrieb von intelligenten binären Sensoren und Aktoren. Allerdings war und ist IO-Link ausschließlich für eine drahtgebundene Infrastruktur konzipiert. Damit es auch für drahtlose Sensoren und Aktoren verwendbar wird, ist eine entsprechende Weiterentwicklung und Anpassung des Protokolls zwingend erforderlich, was im RealFlex Projekt getan wurde.

Wie es im wissenschaftlichen Betrieb üblich ist, wurde zur Lösung der Aufgabe umfassend Literatur genutzt die sich von Tagungsbänden (z.B SPS/IPC/Drives Tagungsbände), Spezialliteratur (Anderson „Security Engineering“ [3]) und Fachjournalen und Magazinen erstreckt. Für Fachartikel wurde umfangreich frei im Internet erhältliche Publikationen als auch die IHP subscription bei dem IEEE explorer Dienst genutzt.

I.5 Zusammenarbeit mit anderen Stellen

Das IHP hat im Rahmen des Projektes mit den Konsortialpartnern direkt zusammen gearbeitet. Diese Zusammenarbeit wurde mit regelmäßigen gesamtkonsortialen Projekttreffen sowie –insofern notwendig– mit bilateralen Entwicklungstreffen und Telefonkonferenzen praktisch umgesetzt.

Darüber hinaus wurde mit Standardisierungsgremien und Nutzerorganisationen wie die PNO (Profinet Nutzer Organisation) zusammengearbeitet. Speziell bei der PNO bekamen wir, aktuelle Ergebnisse reportierend, gutes Feedback bezüglich der Anwendbarkeit der Projektresultate.

Weitere informelle Zusammenarbeiten gab es mit anderen Forschern im Fachbereich. Dieser wissenschaftliche Austausch wurde auf Konferenzen und Workshops (z.B. ETFA [1], SPS/IPC/DRIVES [5]) getätigt.

Innerhalb des IHPs gab es des weiteren noch wertvolle Synergien mit anderen Projekten im Bereich drahtloser Sensornetze und deren Sicherheit.

II Eingehende Darstellung

II.1 Verwendung der Zuwendung

Die Zuwendung wurde konform zur Antragstellung verwendet. Alle Arbeitspakete des IHP sowie der Unterauftrag an das Institut inIT wurden in vollem Umfang bearbeitet. Im folgenden werden die Highlights der Ergebnisse, geordnet entsprechend des Arbeitsplans, eingehend dargestellt.

II.1.1 AP1 - Anwendungsszenarien und Anwendungsanforderungen

Das Ziel dieses Arbeitspaketes war es, die Anforderungen hinsichtlich der Parameter wie Echtzeitverhalten, Zuverlässigkeit und Sicherheit für das Gesamtsystem und auch für seine Teilsysteme zu bestimmen. Hierzu sollen zunächst relevante Anwendungsszenarien spezifiziert werden.

Das IHP war hierbei vor allem im Arbeitspunkt AP1.4: „Ableitung von Sicherheitsanforderungen“ aktiv. Bei dieser Anforderungsanalyse hinsichtlich der Sicherheit haben wir mögliche Bedrohungsszenarien und ihre Folgen beschrieben. Daraus abgeleitet wurden Schutzziele definiert und Sicherheitsmechanismen genannt, die diese Schutzziele durchsetzen. Die Ziele und Sicherheitsanforderungen wurden dann mit Hinblick auf die drei im Projekt zu realisierenden Demonstratoren weiter verfeinert. Die Ergebnisse dieser Untersuchungen und die detaillierteren Anforderungen für jeden der drei Demonstratoren sind Teil des Deliverables D01.

Ein Ergebnis dieser Sicherheitsanalyse ist dass generell hohe bis sehr hoher Anforderungen an die Sicherheit gestellt werden. Dieses Ziel kann prinzipiell durch zeitgemäße Verschlüsselungsmechanismen realisiert werden. Allerdings verbieten andere Anforderungen wie Geschwindigkeit, Antwortzeiten und maximale Größe der zu versendenden Pakete eine direkte Anwendung aktueller Sicherheitprotokolle. Beispielsweise wäre das Verschlüsseln und Signieren eines Ereignisses (1 Bit) mit Standardprotokollen wie AES [4] und ECDSA [2] sehr unökonomisch. Wir verfolgten darum den Weg, die Sicherheitsfunktionalitäten in den Netwerkstacks im Medienzgriffsprotokoll (MAC) unterzubringen.

Die Realisierung dieser Idee wird in Abschnitt II.1.2 beschrieben.

II.1.2 AP2 - Systemspezifikation

Das Ziel dieses Arbeitspaketes war die Entwicklung einer Gesamtarchitektur. Hierfür müssen sowohl die Hardwarebestandteile wie Funksysteme und Sensoren berücksichtigt werden als auch Softwaremodule. Die Arbeit des IHP hat sich hierbei auf alle sechs Unterarbeitspunkte erstreckt, die im folgenden beschrieben weren.

AP2.1 - Spezifikation der Gesamtarchitektur
Die Gesamt-RealFlex-Architektur wurde in enger Zusammenarbeit mit allen Partnern ausgearbeitet. Dies war notwendig um sicherzustellen, dass die entstehende Systemarchitektur auf der einen Seite innovativ, flexibel und erweiterbar ist und auf der anderen Seite auch den Anforderungen der Anwender und Systemintegratoren genügt. Letzteres erfordert zum einen möglichst niedrige Kosten für die Komponenten und zum anderen auch die Möglichkeit, die neuen Komponenten in bestehende Systeme zu integrieren ohne Grundlegende Änderungen der Gesamtanlage durchführen zu müssen.

Des weiteren galt es, vor allem die Anforderungen der drei Demonstratoren und auch die Interessen der einzelnen Konsortialteilnehmer so zu berücksichtigen, dass eine auch nach außen hin kommunizierbare und standardisierbare flexible Architektur entsteht. Im Konsortium sind wir zu einer System-Architektur gekommen, wie sie in Bild 1 dargestellt ist.

An ein Profinet-System wird entweder direkt oder über eine WLAN-Bridge der Mapping Controller angeschlossen. Die Aufgabe dieser Komponente ist das Umsetzen des Profinet Protokolls auf Wireless IO-Link Protokoll. In den unteren Schichten unterscheiden wir eine prototypische Version, die von Phoenix Contact realisiert wird (rechte Seite) und die Wireless IO-Link Realisierung, die eine echte drahtlose IO-Link-Lösung darstellt (linke Seite). Das Wireless IO-Link Protokoll wurde erst später in AP4 implementiert. Daher war die Zwischenlösung von Phoenix willkommen, um schneller einsatzfähige Demonstrationsgeräte zu erhalten und in der Evaluationsphase repräsentative Vergleichswerte nutzen zu können.

Für das Wireless IO-Link existieren, wie im Bild erkennbar, zwei Funklösungen. Die erste ist eine Bluetooth-Lösung und die zweite eine Applikation der WSAF (Wireless Sensor Actor Networks for Factory Automation) Technologie. Bluetooth ist dabei bevorzugt in der Prozessautomatisierung anzuwenden, da es

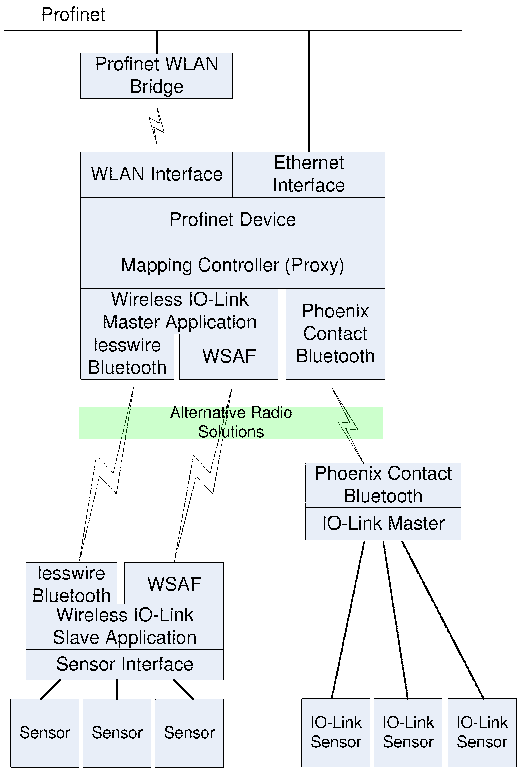


Abbildung 1: Ansatz der RealFlex Gesamtarchitektur

höhere Reichweiten und robustere Verbindungen erlaubt. WSAF ist vor allem für die Fertigungsautomatisierung gedacht, da es kleinere Latenzzeiten für mehr Netzwerkteilnehmer auf engerem Raum ermöglicht.

Unterhalb der Funkschicht gibt es für die Wireless IO-Link Lösung ein Sensor/Aktor-Modul (Block unten links in Bild 1). Die Applikation, die auf solch einem Modul laufen kann, ermöglicht eine Reihe von Diensten (Diagnostik, Parametrierung, Management) aber auch die Integration von Sicherheitsfunktionalitäten. Eine flexible Sensor-Interface-Schnittstelle erlaubt dadurch den Anschluss beliebiger Sensoren, so dass auch ältere Sensoren von den neuen Funktionalitäten profitieren können. Letzteres wurde notwendig, da in existierenden Anlagen ein Austausch von Sensoren oft nicht oder nur sehr schwer möglich ist.

Dass mit dieser Lösung sowohl für die Prozessautomatisierung als auch für die Fertigungsautomatisierung eine globale Architektur geschaffen wurde, die bis auf die eigentliche Funkschnittstelle eine Wiederverwendung der Komponenten und Module erlaubt, ist das herausragende Ergebnis dieses Arbeitspaketes.

Da diese Lösung ein Funkmodul für jeden Sensor benötigt, können die Installationskosten relativ hoch werden. Da oft Sensoren räumlich und kausal eng miteinander verknüpft sind, bietet sich eine alternative Lösung an, die wir ebenfalls anstrebten. Die Sensoren die eng miteinander arbeiten, werden mittels standard IO-Link an eine sogenannte Sammelbox angeschlossen. Diese Box verwaltet und sammelt die Daten der angeschlossenen Sensoren/Aktoren und übermittelt diese Daten kabellos an den Access-Point. Es wird also nur eine Funkverbindung für eine größere Anzahl von Sensoren benötigt. Auch diese Lösung erlaubt eine transparente Integration in bestehende Systeme.

Vergleich der Funktechnologien

Als integraler Teil der Gesamtarchitektur haben wir A nfang des Jahres 2008 gemeinsam mit Lesswire und inIT einen Vergleich verfügbarer Funktechnologien, die auf dem Massenmarkt verfügbar sind, durchgeführt, um ihre Eignung für den Einsatz in Automatisierungsanwendungen zu analysieren. Dabei untersuchten wir IEEE 802.11 WLAN, Bluetooth und IEEE 802.15.4 (Zigbee / Wireless HART). Grundsätzlich sind alle diese genannten Standards geeignet, drahtlose Kommunikation mit garantierten Zykluszeiten im Bereich weniger Millisekunden zu realisieren. Allgemein lässt sich jedoch sagen, dass die Anzahl gleichzeitiger Echtzeitverbindungen sehr beschränkt ist (im Bereich <8) und damit keine gute Skalierbarkeit gegeben ist. Daher war es notwending die in AP3 beschriebenen Anpassungen, die Medienzugriffsschicht betreffend, vorzunehmen.

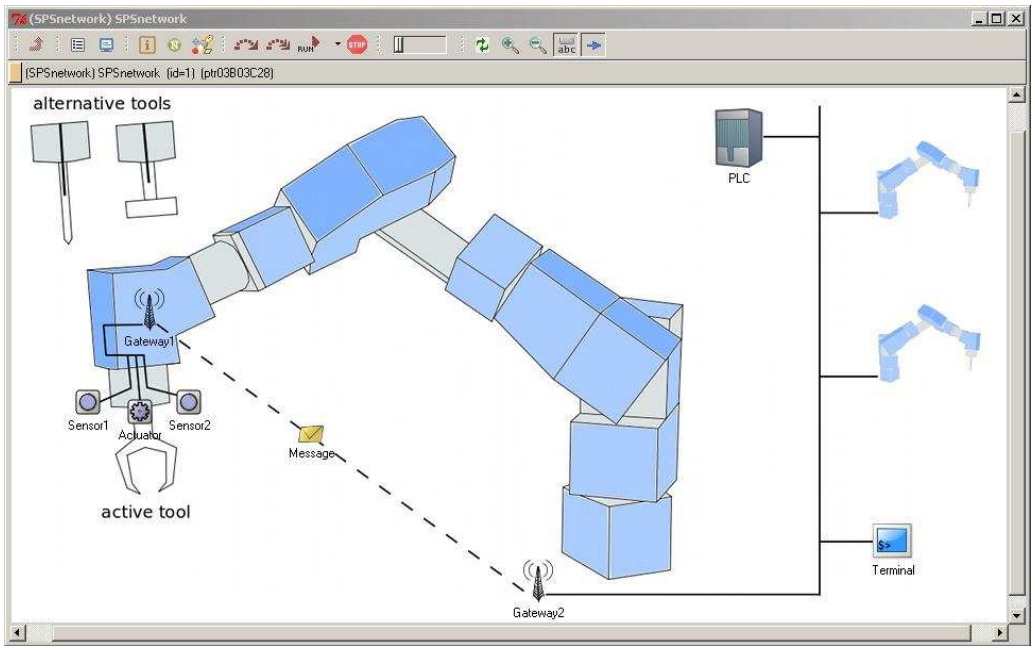


Abbildung 2: Simulationsumgebung am Beispiel des Roboterszenarios

Simulationsumgebung

Im IHP haben wir 2010 begonnen die Komponenten der RealFlex-Archtiektur in einer Simulationsumgebung nachzumodellieren. Das ermöglicht das Testen des Verhaltens des Systems und der Komponenten für die einzelnen Demonstrator-Szenarien im Labor ohne die eigentliche Hardware programmieren zu müssen.

Die Simulationsumgebung kann auch eingesetzt werden um neue Funktionalitäten auf den Komponenten testen zu können. So konnten wir zum Beispiel verschiedene Verschlüsselungsprotokolle auf den Sensoren bzw, dem Gateway integrieren, testen und analysieren. Des Weiteren erlauben die Simulationen das Nachbilden und Testen komplexer Szenarien mit vielen Sensoren und Aktoren. Entsprechend große Testaufbauten wären in der Praxis nur schwer realisierbar, werden aber benötigt um die Leistungsfähigkeit der Systeme auch unter Belastung demonstrieren zu können.

AP2.2 - Spezifikation der autonomen Teilsysteme

In diesem Arbeitspaket wurden die einzelnen Komponenten der Systemarchitektur spezifiziert. Das beinhaltete sowohl Software- als auch Hardware-Spezifikationen.

Neben der Simulationsumgebung und der Fokussierung auf die Sicherheitsprotokolle haben wir uns im IHP hierbei vor allem auf die Sensorseite fokussiert und haben diskutiert, wie man, in der Prozessautomatisierung oft angewandte, „dumme“ Sensoren an die intelligente RealFlex Architektur anbinden kann. Diese

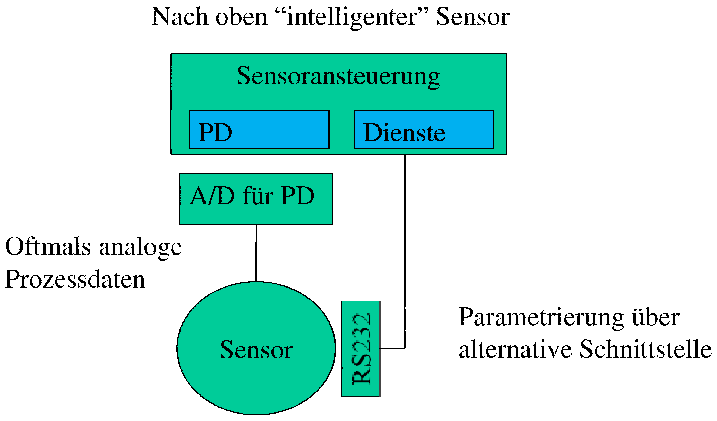


Abbildung 3: Erweiterung eines analogen Sensors mit einer intelligenten Sensoransteuerung

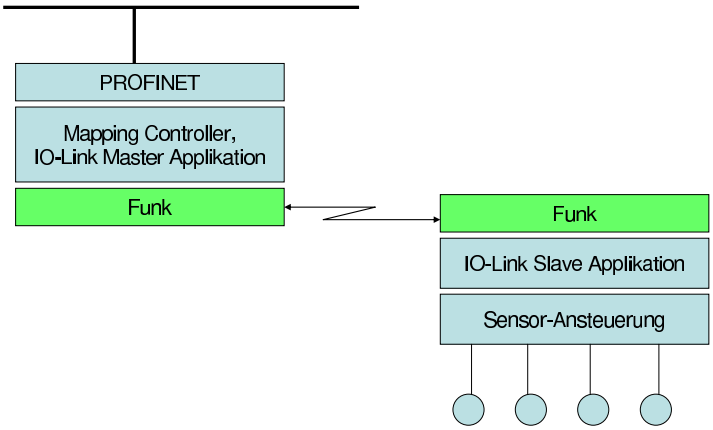


Abbildung 4: Vereinfachte Darstellung der RealFlex Architektur mit Sensorseite (rechts) und Mapping Controller (links)

„dummen“ Sensoren bekommen durch die an sie angeschlossenen RealFlex Boards dann nicht nur die Möglichkeit, drahtlos zu kommunizieren, sondern gewinnen zusätzlich die auf dem IO-Link-Protokoll basierende „lokale Intelligenz“.

In Abbildung 3 ist diese Idee beispielhaft für einen Analogsensor, wie er in den Demonstratoren Wasserwerk und Biogasanlage vorkommt, dargestellt. Neben der Verarbeitung der digitalisierten Messwerte, kann die Sensoransteuerung den Sensor auch über die existierende RS232-Schnittstelle parametrisieren. In heutigen Anlagen wird hierfür noch ein Mitarbeiter benötigt, der vor Ort, also in Sensornähe, mit Hilfe eines Notebooks die Sensoransteuerung vornimmt. Das IO-Link-Protokoll ermöglicht zukünftig, dass solche Arbeiten aus der Ferne ausgeführt werden können. Mit dem Wireless IO-Link, wie er in AP4 vorgestellt wurde, sollte das dann auch drahtlos geschehen.

Diese Sensoransteuerung ist auf der RealFlex Sensorseite die unterste Ebene (siehe Abbildung 4) und ist bewusst flexibel gehalten. Das soll den Anschluss beliebiger Sensortypen erlauben. Darüber gibt es eine IO-Link-Slave Adaptionsschicht.

Prinzipiell verhält sich die Sensorseite, mit der IO-Slave Applikation und der Sensor-Ansteuerung zusammen, logisch wie ein IO-Link-Sensor. Die zu entwickelnde RealFlex Sensorseite verfügt noch über ein Funkmodul dass vor allem von lesswire in AP3 zu entwickelt wurde. Das Funkmodul ist so flexibel gehalten, dass es die unterschiedlichen Anforderungen in der Prozess- und Fertigungsautomatisierung, wie Latenz und Reichweite, entsprechend den Anforderungen der Schnittstelle erfüllt.

AP2.3 - Untersuchung von Mechanismen zur verteilten Entscheidungsfindung

Die drei grundlegenden Teilsysteme (Access-Point, Übertragungsboard und Sammelbox) bieten Angriffspunkte für die Untersuchung von lokalen Intelligenzen und verteilten Entscheidungsfindungen. Eine erste lokale Aufgabe die realisiert wurde ist das lokale Protokollieren von Ereignissen. Diese Funktionalität kann im Falle von Störungen helfen, die Gründe herauszufinden, den Zustand des Systems zu diagnostizieren und das Gesamtsystem schneller wiederherzustellen. Da eine solche Protokollierung kein aktives Eingreifen in das System darstellt, widerspricht es auch nicht dem Wunsch der transparenten Integration.

Ewas weiter gingen die grundlegenden Untersuchungen zur verteilten Entscheidungsfindung in Automatisierungsnetzwerken. In der Automatisierung werden Messwerte durch Sensoren gesammelt und an Speicherprogrammierbare Steuerungen (SPS) übermittelt. Diese steuern wiederum vorhandene Aktoren. In diesem Arbeitspunkt wurde untersucht, wie eine verteilte Entscheidungsfindung auf Sensorknoten im Bereich der Automatisierung implementiert werden kann. An Stelle der SPS wurde mit Sensorknoten und einem Gateway versucht, die Funktionalität einer SPS und einer Intelligenz zu kombinieren, um eine dezentrale Entscheidungsfindung zu ermöglichen. Die Sensorknoten dienen zur Verbindung der Sensoren und Aktoren mit der Steuerung und kommunizieren drahtlos mit dem Gateway. Das Gateway wird für die Übermittlung von Messwerten an die zentrale Steuerung genutzt. Netzteilnehmer mit einer künstlichen Intelligenz heißen Agenten. Ein System aus mehreren Agenten, welche untereinander kommunizieren, kooperieren und versuchen soziales Verhalten nachzustellen, wird als Multi-Agenten-System bezeichnet. Mit einem solchen System wird versucht, eine verteilte

Entscheidung zu realisieren. Jedoch gibt es im Bereich der Automatisierungstechnik einige Beschränkungen, zum Beispiel durch die Nutzung von festgelegten Feldbus-Protokollen, welche eingehalten werden müssen, um eine Integration in der zentralen Steuerung zu ermöglichen. Die Möglichkeit einer Auslagerung von Entscheidungen auf Knoten, welche somit gegebenenfalls auch zur Steuerung von Aktoren genutzt werden können, musste daher zunächst theoretisch analysiert werden. Ziel war es dabei, den entstehenden Traffic im Netzwerk möglichst gering zuhalten. Dazu wurde der ideale Agent als Benchmark definiert, welcher an die Bedingungen, wie zum Beispiel die Kommunikation mit der zentralen Steuerung und des Einsatzgebietes in der Automatisierung angepasst wird.

Mit diesem Benchmark wurden potentielle Lösungen von Sensorknoten verglichen. Die Knoten sind mit einem Betriebssystem wie zum Beispiel RTOS versehen und entsprechend in der Lage als aktive Anwendung Daten abzufragen und selbstständig durch Aktoren oder durch entsprechende Nachrichten im Netzwerk Aktionen auslösen zu können. Hier war es notwendig, dass jeder Parameter dezentral definiert wird. Jedoch ist eine Änderung an dem auszuführenden Programm nur möglich, wenn der Benutzer den entsprechenden Knoten neu programmiert, was in der Praxis schwer durchführbar erscheint. Eine weitere Lösung wäre es, auf dem Sensorknoten ein Betriebssystem zu nutzen, welches beim Starten einer Verbindung eine Anmelde-Nachricht an die zentrale Steuerung schickt. Diese antwortet wiederum mit einer Nachricht, welche die nötigen Parameter für die Konfiguration an den Sensorknoten enthält. Da in dieser Variante verschiedene Parameter zentral abgefragt werden, kann hier der Ablauf eines Programms durch eine Steuerung beeinflusst werden, was eine Anpassung an geänderte Bedingungen ermöglicht.

Zum Vergleich dieser beiden Varianten wurde eine Simulation einer Anlage genutzt, in der Sensorknoten kommunizieren. Vorteilhaft ist eine Aufteilung der beiden Varianten entsprechend der Aufgabe. Somit steigt zwar in Abhängigkeit der Aufteilung der Traffic, aber die Sensorknoten bleiben so in einem gewissen Rahmen autonom und können trotzdem relativ transparent gesteuert werden.

Diese Evaluierung der Machbarkeit einer verteilten Entscheidungsfindung in Automatisierungsanwendungen ist ein wissenschaftlicher Beitrag des RealFlex Projektes, der mit dem Abschluss des Projektes noch nicht abschließend gelöst ist.

Im Bereich intelligente Entscheidungsfindung gab es in RealFlex einen praktischen Schwerpunkt im Biogas-Demonstrator. Es war das Ziel die Geschwindigkeit des Rührers im Fermenter automatisiert einzustellen. Die optimale Geschwindigkeit ist dabei abhängig von Messwerten der Sensoren und einer Bildanalyse der im RealFlex-System integrierten WLAN Kamera. Auch wenn dieser Punkt letztendlich nicht in der Praxis demonstriert werden konnte, so haben Simulationen und theoretsiche Analysen die Machbarkeit auf Basis der RealFlex Architektur gezeigt.

AP2.4.1 - Sicherheitssystem

Nach der Analyse der Sicherheitsanforderungen in AP1 haben wir uns für das Design und die Implementierungen der Sicherheit auf folgende Use-Cases fokussiert

- Übertragung der Prozessdaten
- Anmeldung eines Devices
- Parametrierung eines Devices

Alle drei Anwendungsfälle besitzen sehr unterschiedliche Anforderungen. Für die Prozessdaten darf es keinen Overhead in der Paketgröße oder bei den zu versendenden Daten geben. Bei der Anmeldung eines Devices hat man dagegen mehr Zeit und Mittel. Es ist auch geplant, dass während dieser Anmeldung die Vertrauensbeziehung aufgebaut wird, die eine effiziente Kommunikation für die Prozessdaten erlaubt. Bei der Parametrierung planen wir benutzerabhängige Dienste anzubieten. Das würde zum Beispiel erlauben, Programmcode für Geräte in der Anlage zu aktualisieren. Entsprechende Anfragen müssten von einer berechtigten Person digital unterschrieben sein. Das Gerät kontrolliert diese digitale Unterschrift und führt den Befehl nur aus, wenn die Person berechtigt ist. Eine solche Funktion wäre eine Neuigkeit in der Automatisierungstechnologie, da bisherige Ansätze keine benutzerabhängigen Zugriffe ermöglicht haben.

Die Mechanismen für die Sicherheit wurden für Meilenstein M2.3 untersucht. Wir setzen standardisierte Algorithmen wie AES [4] und ECDSA [2] ein, passen diese allerdings in ihrer Anwendung an, um die spezifischen Anforderungen zu erfüllen. Für die Prozessdaten nutzen wir einen als Stream-Cipher angewendeten rückgekoppelten AES, der durch eine Kopplung zwischen Sender und Empfänger nicht nur die Daten verschlüsselt, sondern auch die Integrität sicherstellt.

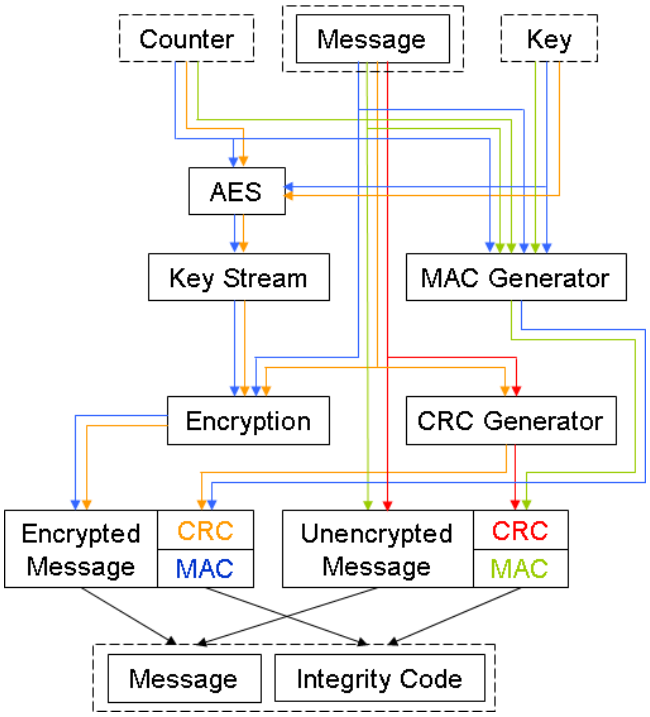


Abbildung 5: Datenflüsse der verschiedene Operationsmodi des Sicherheitsprotokolls. Es ist ersichtlich dass alle Konfigurationsmöglichkeiten in einer einheitlichen Paketstruktur (Message und Integirty Code) münden. Welcher Fluss am Ende gewählt wird, hängt vom jeweiligen Anwendungsfall ab.

Für die digitalen Unterschriften sowie Authentifikationsaufgaben innerhalb des Verbindungsaufbaus diskutierten wir die Nutzung von asymmetrischen Schlüsseln, wobei der Schlüssel auf Device-Seite effizientere Verschlüsselungsoperationen erlaubt. Die Master-Seite muss entsprechend mehr Rechenarbeit leisten, was allerdings kein Problem ist, da sie ausreichend Rechenleistung besitzt. Hier verfolgten wir mehrere Ansätze, wobei letztendlich ECC bevorzugt wurde. Elliptische Kurven Kryptografie (ECC), ist speichereffizient und selbst mit kurzen Schlüssellängen sicher, im Vergleich mit anderen Verfahren, wie zum Beispiel RSA. Eine alterative leichtgewichtige Methode ist die Nachbildung einer asymmetrischen Beziehung über eine dritte Vertrauenspartei unter Nutzung von symmetrischen Verschlüsselungsverfahren. Vorteile sind dass weniger Rechenleistung und wenig Speicherplatz benötigt wird. Nachteilig ist hier die Notwendigkeit der Vertrauenspartei im Netzwerk.

Leichtgewichtiges Sicherheitsprotokoll für Prozessdaten

Ein besonderes Ziel war es, für die Funkübertragungen flexible zuschaltbare Sicherheitsfunktionalitäten im Bereich der Verschlüsselung und Integritätsprüfung zu realisieren. Hierzu werden im Rahmen eines Stufenmodells verschiedene Modi mit optionaler Verschlüsselung und Integrationsprüfung zur Verfügung gestellt. Die Grafik in Abbildung 5 zeigt, wie aus der eigentlichen Nachricht unter Nutzung von verschiedenen Arbeitsblöcken, die zu sendende Nachricht mit Intergrity code entsteht. Welche Blöcke dabei genutzt werden, hängt von den Anforderungen des Nutzers ab.

Dabei werden folgende Modi, wie in der Abbildung 5 ersichtlich, implementiert:

- Ohne Sicherheit, mit einfacher unsicherer Integrität (CRC) (rot)
- Mit Verschlüsselung, mit einfacher unsicherer Integrität (CRC) (gelb)
- Ohne Verschlüsselung, mit Integritätsprotokoll (MAC) (grün)
- Mit Verschlüsselung und mit Integritätsprotokoll (MAC) (blau)

Dabei sind die gestrichelt umrandeten Kästchen die Ein- bzw. Ausgabewerte im Modell. Für einige Modi werden ein Schlüssel oder/und ein Zähler benötigt. Der für die Verschlüsselung benötigte Schlüssel wird über ein geeignetes Schlüsselaustauschverfahren generiert bzw. ausgetauscht. Der Zähler dient der Erkennung valider Nachrichten und kann zur Synchronisierung eingesetzt werden. Die vier Modi arbeiten auf der gleichen

Paketstruktur. Das bedeutet, dass innerhalb der Prozessdaten keine zusätzlichen Informationen gesendet werden müssen. Die hinzu-gewonnene Sicherheit wird allein durch zusätzliche Rechenoperationen erreicht. Der berechnete Integritätscode wird dann an die Nachricht angehängt. Hierbei steigen die Anforderungen an die Hardware bei Nutzung der stärkeren Sicherheitsmodi an.

Bei der ersten Stufe (rot) wird auf eine Verschlüsselung verzichtet und lediglich eine einfache Integritätsprüfung durchgeführt, um fehlerhaft übertragene Pakete erkennen zu können. Dies wird durch einen einfachen Cyclic-Redundancy-Check erreicht. Das Verfahren ist jedoch nicht optimal hinsichtlich der Erkennungsrate und der möglichen Einschleusung absichtlich veränderter Pakete. Aufgrund der fehlenden Verschlüsselung kann es zu einer ungewollten Verbreitung von Prozessdaten kommen.

Durch die in der zweiten Stufe (gelb) aktivierte Verschlüsselung schützt dieser Modus vor der ungewollten Verbreitung von Prozessdaten. Die Weiteren oben beschriebenen Probleme bleiben allerdings noch bestehen.

Die dritte Stufe (ohne Verschlüsselung) (grün) bietet ein zuverlässiges Integritätsprotokoll, welches sowohl zufällig fehlerhafte Pakete als auch absichtlich veränderte Pakete erkennt. Damit wird eine einfache Einschleusung fremder Pakete ins System verhindert. In der letzten Stufe (blau) werden sowohl die Verschlüsselung als auch ein zuverlässiges Integritätsprotokoll aktiviert. Damit wird sowohl das Ausspähen von Prozessdaten verhindert, als auch die Einschleusung bzw. Weiterverbreitung von fehlerhaften Paketen verhindert. Anlagenbetreiber könnten dann anhand ihres Sicherheitsbedürfnisses und der vorhandenen Hardware abwägen, welchen Sicherheitsmodus sie nutzen wollen. Mit steigender Sicherheit verringert sich die Gefahr, dass Prozessdaten ausgespäht oder verändert werden können. Die Möglichkeit eines einfachen Angriffs auf Elemente der Automatisierungsanlage wird somit wirksam verhindert. Der Vorteil der Option ohne Sicherheitsprotokolle ist, dass keine Schlüssel ausgetauscht werden müssen und damit jedes Gerät an jeder Anlage sofort einsetzbar ist. Der Schlüsselaustausch für die sicheren Lösungen ist sowohl hinsichtlich der Hardwareanforderungen als auch von der Protokollseite her eine Herausforderung. Derzeit setzen wir auf einen Diffie-Hellman Schlüsselaustausch, der in Software auf der Applikationsebene implementiert ist. Damit ist er für alle RealFlex Konfigurationen einsetzbar.

Die eigentliche Verschlüsselung der Daten muss effizient geschehen, weshalb mehrere auf die jeweilige Hardware optimierte Implementierungen realisiert wurden, welche auf einem 128 bit AES-Algorithmus basieren. Bei den untersuchten Verfahren für die Integritätsprüfung spielen Laufzeit und Speicherverbrauch hinsichtlich der verwendeten Hardware eine übergeordnete Rolle. Ebenso wurden Interoperabilität und Sicherheit der Algorithmen betrachtet.

Für die Prozessautomatisierung wurden die Protokolle in Software implementiert. Für das WSAF Protokoll, das in der Fertigungsautomatisierung eingesetzt wird und ohnehin schon den Einsatz spezialisierter Hardware erfordert (von lesswire entwickelt), wurden die Sicherheitsprotokolle in Hardware integriert. Dies war notwendig, um die notwendigen Geschwindigkeiten von wenigen Millisekunden im WSAF Protokoll realisieren zu können. Die abschließenden Demonstrationen konnten den Erfolg dieser Arbeit nachweisen.

AP2.4.2 - Managementsystem

Hier haben wir vor allem untersucht wie man in der heterogenen Struktur von Automatisierungsanlagen neue Services auf Gateways und Sensoren integrieren kann, die zum Beispiel Sicherheit und verteilte Entscheidungsfindung ermöglichen können. Mit IO-Link haben wir dabei bereits ein Protokoll, dass Adressen-basiert die Nutzung von Diensten auf den Komponenten erlaubt.

Für das Management war die vornehmliche Frage, wie der Nutzer bestimmte Operationen auf bestimmten Geräten ausführen kann. Durch die inhomogene Struktur von industriellen Netzwerken ist diese Frage nicht trivial und einheitlich zu beantworten. Für das zentrale Management der Endgeräte benötigt man zum Beispiel spezielle FDT-PlugIns deren Aufbau und Arbeitsweise zunächst analysiert werden musste. Diese Ergebnisse sind in M2.3 festgehalten. Der Zugriff auf PROFINET Devices, wie unseren WLAN Proxy oder der Mapping Controller, geschieht allerdings mit anderen Werkzeugen. Hier bieten sich zum Beispiel IP-basierte Dienste wie WEB oder telnet an.

Die Identifikation und Feststellung der Nachbarschaftsbeziehungen innerhalb des PROFINETs werden mit dem PROFINET SNMP und LLDP vollzogen. Für die Dienste auf den Sensoren und Aktoren nutzen wir die IO-Link Schnittstelle, die integraler Bestandteil unserer Architektur ist. Die oberste Priorität hat hierbei, dass wir existierende Standards unterstützen um eine möglichst transparente Integration zu ermöglichen. Zusätzliche Funktionalitäten, wie Funkkanal-Konfiguration, Schlüsselmanagement, Diagnostik, werden auf diesen

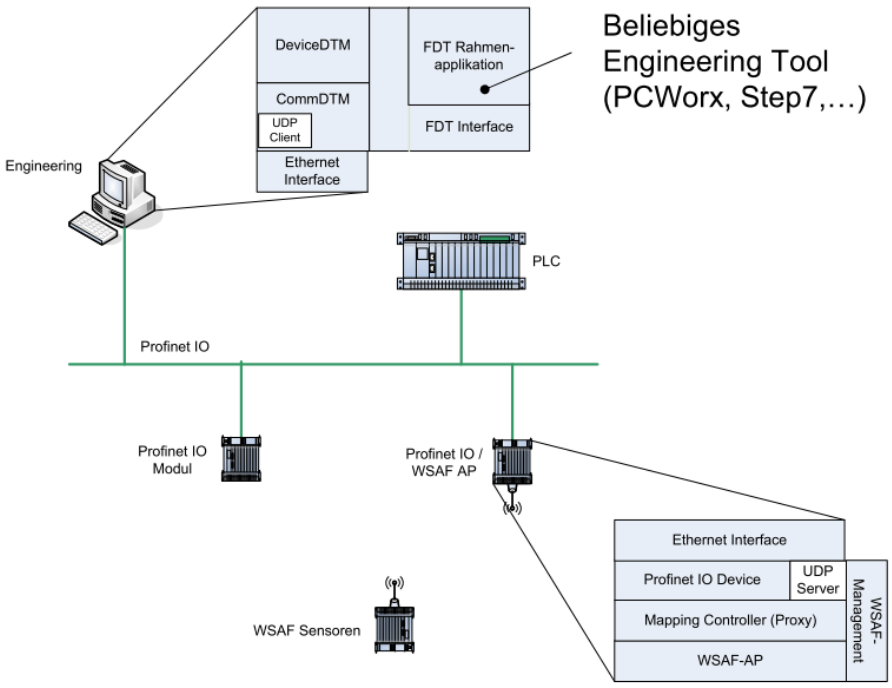


Abbildung 6: RealFlex Management Architektur: Die FDT Rahmenapplikation kann in beliebige Engineering Tools eingebunden werden um die RealFlex Komponenten (in dem Fall WSAF AP) zu konfigurieren.

existierenden Diensten aufgesetzt. Als Beispiel wird die Funkkanal-Konfiguration als IP-basierter Dienst über PROFINET angeboten. Die Diagnostik der Sensoren kommuniziert über IO-Link, dass von dem FDT-PlugIn auf der Managementplattform ausgeführt wird. Durch die Nutzung von LINUX als Betriebssystem auf den Komponenten ist die Integration von IP-basierten Diensten und SNMP wenig problematisch.

Für industrielle Standard Engineering-Software-Systeme wurde ein FDT-PlugIn zur Steuerung und Parametrisierung der Anlage implementiert, was auf Grund des komplexen Interfaces zu den Engineering-Software-Systemen eine besondere Herausforderung darstellte. Wie allerdings in der Abschlusspräsentation am Roboterarm gezeigt werden konnte, wurde die Herausforderung, vorrangig durch die Arbeiten des Unterauftragnehmers inIT, letztendlich gemeistert. Die Management-architektur ist in Abbildung 6 illustriert.

II.1.3 AP3 - Drahlose Sensorknoten

In diesem Arbeitspaket hat das IHP keine Leistungen abgerechnet.

II.1.4 AP4 - Protokollentwicklung

In diesem Arbeitspaket hat das IHP Arbeiten im folgenden Arbeitspunkt Leistungen abgerechnet:

AP4.2 - WLAN Proxy

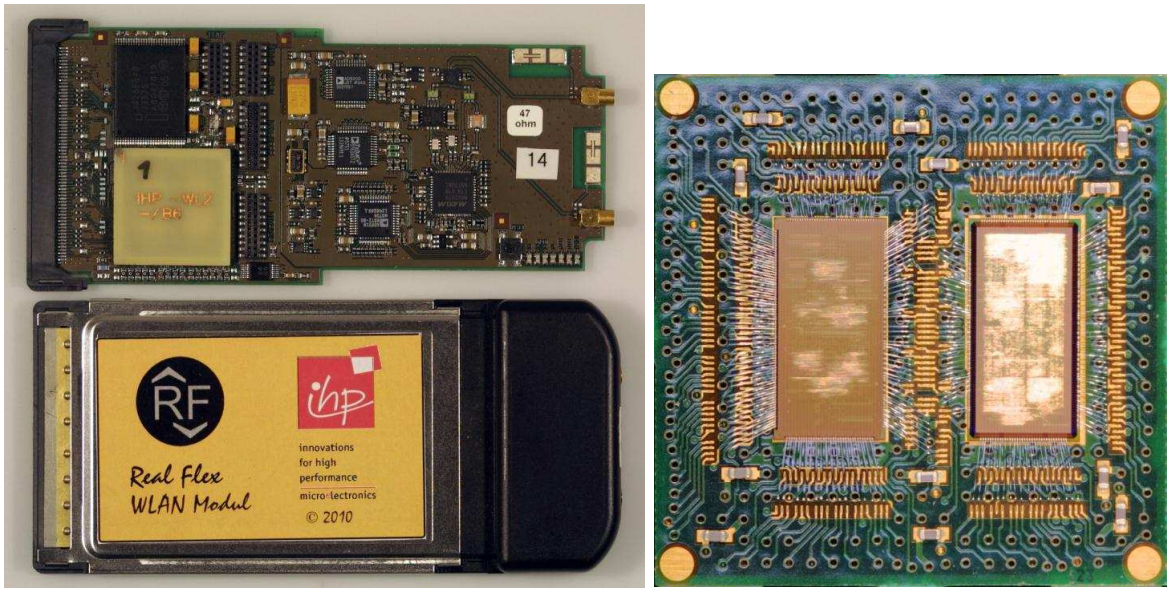
Im Rahmen dieses Teilarbeitspaketes wurde der WLAN-Proxy spezifiziert und anschließend die notwendige WLAN-Hardware implementiert und getestet. Die Spezifikation umfasst einerseits die Vermittlung zwischen den im Gesamtsystem verwendeten Protokollen und andererseits die Sicherstellung von QoS-Parametern, hierzu gehört beispielsweise die Gewährleistung von Echtzeiteigenschaften bei der Übertragung von Nachrichten.

Um die Qualität der Datenübertragung zu gewährleisten, müssen spezielle Funktionalitäten wie PCF (Point Coordination Function) und HCCA (HCF Controlled Channel Access) unterstützt werden. Diese wurden in IEEE 802.11e spezifiziert. Aktuell sind allerdings noch keine entsprechenden Chipsätze verfügbar. Die besonderen zeitkritischen Eigenschaften dieser Standards machen auch eine Hardwareimplementation notwendig.

Dies wurde im IHP auf Basis eines bereits im Institut verfügbaren WLAN Chipsatzes realisiert. Dies erfolgte in zwei Schritten. Zunächst wurde die spezifizierte Funktionalität, die im Wesentlichen im MAC-Protokoll lokalisiert ist, in ein am IHP vorhandenes Simulationsmodell des IEEE 802.11 MAC-Protokolls integriert. Dieses Modell ist in der Sprache SDL geschrieben und erlaubt es, die korrekte Funktion des MAC-Protokolls nebst

Erweiterungen durch SDL-Simulation zu verifizieren. In einem zweiten Schritt wurde das SDL-Modell an die Hardware-Plattform angepasst, dafür compiliert und schließlich erprobt.

Nachdem abschließend neue WLAN Chipsätze gefertigt wurden und Tests erfolgsversprechend verliefen, wurden neue Platinen, mit denen die verbesserte Quality-of-Service demonstriert kann, gefertigt und anschließend getestet.



(a) WLAN Karte (b) Chip der WLAN Karte

Abbildung 7: IHP WLAN Karte und Chip

Ein Prototyp wird in Abbildung 7(a) gezeigt: unten die verpackte Karte und oben mit geöffneten Gehäuse. Der technisch interessanteste Teil befindet sich in dem großen gelben Chip (links unten) auf dem Board. In diesem Chip befinden sich die WLAN Basisband-Verarbeitung sowie die Verarbeitung des Medienzugriffs (MAC).

Um das Risko von Fertigungsfehlern zu reduzieren (doppelte Fläche bedeuted vierfache Fehlerwahrscheinlichkeit), haben wir uns für die Entwicklungsphase für diese Zweichiplösung in einem Gehäuse entschieden. Diese sind in Abbildung 7(b) gut zu erkennen.

Teile des MACs sind mittels einer Firmware programmierbar. Diese Firmware enthält auch die Funktionalitäten zu der verbesserten Quality of Service. Die technischen Arbeiten an der Firmware wurden im Berichtszeitraum erfolgreich abgeschlossen und in der SDL Entwicklungsumgebung getestet und ist im entsprechende Meilenstein M4.5 dokumentiert.

Eine Demonstration auf Laptop Computern konnte die Funktionalität der WLAN-Implementierung nachweisen. Eine Integration in den RealFlex Access-Point konnte nicht realisiert werden, da einzelne technologische Parameter des gefertigten WLAN Chips nicht den Erfordernissen des RF-APs entsprechen.

II.1.5 AP5 - Demonstrator

AP5.1 - Spezifikation Aufbauend auf den Szenarien aus AP1 wurden die drei Demonstratoren spezifiziert. Diese bestehen aus den im Rahmen dieses Projektes entwickelten Teilsystemen und geeigneten Anwendungen, die auf diesen Teilsystemen aufsetzen. Die drei implementierte Szenarien waren:

- Wasserwerk
- Biogasanlage
- Roboterzelle

Als Konsortialführer hat das IHP dafür Sorge getragen, dass die Ergebnisse der einzelnen Arbeitspakete problemlos in den Demonstratoraufbauten zusammenfließen können. Hierbei mussten vor allem potentielle zeitliche Konflikte zwischen Bereitstellung und Nutzung von Komponenten (speziell Sensorboards) identifiziert und aufgelöst werden. Dabei haben sich keine nennenswerten Komplikationen ergeben. Das Dokument D07 - Spezifikation des Demonstrators - dokumentiert diese Demonstratorarbeiten.

	Plan	Gesamt	Diff	diff %
Entgeltgruppe E12-E15	349.505,25	347.192,71	-2.312,54	-0,66
Beschäftigungsentgelte	14.996,00	18.072,40	3.076,40	+20,51
Vergabe von Aufträgen	216.483,00	217.282,99	799,99	+0,37
Dienstreisen	17.350,00	10.858,37	-6.491,63	-37,42
Overhead (GK)	36.502,00	36.526,51	24,51	+0,07
Investitionen	333.800,00	324.938,81	-8.861,19	-2,65
Gesamt:	968.636,25	954.871,79	-13.764,46	-1,42

Tabelle 1: Ausgaben-Übersicht

AP5.3 - Integration der Teilsysteme
Im Bereich der Integration bestand die primäre Aufgabe des IHPs und des Unterauftragnehmers inIT die Sicherheits- und Managementdienste in die Komponenenten die vorrangig von Lesswire entwicklet wurden zu integrieren. Diese tendenziell mechanische Aufgabe lief ohne nennenswerte Komplikationen.

II.1.6 AP 6 Management und Öffentlichkeitsarbeit

AP6.1 - Projektmanagement und Controlling
Als Projektkoordinator und Verantwortlichen für das AP6 „Management und Öffentlichkeitsarbeit“ oblagen dem IHP eine Reihe von administrativen Aufgaben.

- Einrichtung eines Email-Verteilers für die interne Kommunikation innerhalb des Verbundes
- Eine Internet-Domäne “RealFlex-projekt.de” wurde angemeldet und mit aufbereiteten Projektinhalten zur Außendarstellung des Vorhabens auf einem Web-Server angeboten.
- Ausarbeitung des Konsortialvertrags
- inhaltliche und organisatorische Gesamtleitung des Projektes
- Abstimmung mit dem und die Berichterstattung zum BMBF bzw. dem Projektträger
- Organisation und Leitung der regelmäßigen (vierteljährlich) Konsortialtreffen

AP6.2 - Öffentlichkeitsarbeit
Projektergebnisse wurden sowohl auf wissenschaftlichen Konferenzen als auch auf der SPS/IPC/Drives Messe vorgestellt und diskutiert. Gerade die Diskussionen mit Industrievertreten auf der Messe waren vielversprechend. Sowohl Sensorhersteller als auch Anbieter von Kommunikationskomponenten haben allgemein Interesse an drahtloser Kommunikation in Industrieanlagen bekundet und waren auch gezielt an den RealFlex-Ergebnissen in Form des zu erwartenden Wireless IO-Link interssiert.

Zur Promotion dieses Standards hat das IHP das RealFlex-Projekt beim Arbeitskreis “Wireless Sensor and Actor Networks” (WSAN) der PNO vorgestellt. Ziel ist es, die Ergebnisse aus dem RealFlex-Projekt in die Standardisierung eines Funkstandards für die Automatisierungstechnik einzubringen. Dazu soll eine Drahtlos-Variante des IO-Link-Standards (“Wireless IO-Link”) entstehen. Im Rahmen der Zusammenarbeit mit der PNO war auch der Zugang zu technischen Spezifikationen, z. B. von IO-Link, notwendig und vorgesehen. Von der PNO wurde die Zusammenarbeit mit unserem Vorhaben begrüßt, auch wenn sich bis Projektende kein wirklicher Durchbruch in diesem Bereich erzielen lassen konnte.

II.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die Ausgabenübersicht ist in Tabelle 1 dargestellt. Es ist erkennbar, dass vom IHP 1,42% weniger Mittel in Anspruch genommen wurden als initial geplant worden sind. Die signifikantesten Abweichungen gibt es im Bereich Dienstreisen, wo 37 Prozent weniger ausgegeben wurde und im Bereich zusätzlicher Beschäftigungsentgelte, wo für die Intergrationsarbeiten im letzten Jahr mehr Arbeiten von studentischen Hilfskräften genutzt wurden als initial geplant wurde.

II.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Für die im Rahmen dieses Projektes untersuchten Fragestellungen existieren keine allgemein anerkannten oder gar standardisierten Lösungen. Vielmehr wird in einigen Bereichen noch sehr intensiv an ähnlichen bzw. glei-

chen Fragestellungen geforscht. Die Arbeiten waren also aus wissenschaftlich-technischer Sicht notwendig, um Aussagen zur Umsetzbarkeit der Basisidee des zuverlässigen drahtlosen Anschluss von Sensoren und Aktoren im industriellen Automatisierungsumfeld treffen zu können. Zu allen Arbeitspaketen wurden intensive Untersuchungen sowohl theoretischer Natur, speziell im Bereich sicherer Protokolle, als auch experimenteller Art durchgeführt. Der Nachweis der prinzipiellen Machbarkeit des RealFlex System anhand der drei Demosntratoren kann als Basis für anschließende Produktentwicklungen gesehen werden.

II.4 Voraussichtlicher Nutzen

Sowohl die Mapping-Architektur, die das drahtlose IO-Link Protokoll an die Feldbusse anschließt, als auch Funkarchitektur WSAF werden noch aktiv in den Arbeitsgruppen der PNO diskutiert. Dadurch ist es möglich, dass die Projektergebnisse zeitnah in den relevanten Standards Beachtung finden und von den entsprechenden Projektpartnern verwertet werden. Entsprechend sind hier die primären Projektziele, d.h. der praktische Nutzen der Projektergebnisse, gut erreichbar.

Im IHP gibt es derzeit intensive Bestrebungen eine Ausgründung mit dem Hintergrund Sensornetze voranzutreiben. Dies geschieht auch in Richtung der Automatisierungstechnik auf Basis der guten praktischen Ergebnissen des RealFlex Projektes. Nach derzeitigen Planung soll diese Ausgründung im Jahr 2013 selbständig werden.

Zum jetzigen Zeitpunkt ist erkennbar, dass speziell an den Sicherheitsansätzen sowie deren Implementierungen Interesse bei Anbietern von Sensoren und Komponenten besteht. Ein Verkauf oder die Lizenzierung dieser Blöcke ist demnach realistisch.

Das IHP hat im Kontext des Projektes ein Patent angemeldet, das potentielle Verwertung ermöglicht:
D. Dietterle, P. Langendörfer: Protokollbeschleunigermodul mit Paketweiterleitungs-funktion und Betriebsverfahren für einen Senderempfänger zur schnellen Weiterleitung von Datenpaketen Anmeldekennzeichen 10 2009 001 821.2-31

Die wissenschaftliche Verwertung in Lehrveranstaltungen und Publikationen ist nach wie vor geplant und teilweise schon realisiert. Die RealFlex-Demonstratoren geben plastische Beispiele um moderne Konzepte im Bereich Sensor- und Aktornetze greifbarer und anwendungsnah zu gestalten. Gerade im Bereich Sicherheit sind akademische Vorstellungen und Praxis stark divergiert. Hier gibt es die Chance mittels der RealFlex Projektergebnisse Theorie und Praxis anzunähern.

Mit den Simulationen in der offenen und freien Simulationsumgebung OMNET+ besteht nun auch die Möglichkeit die Projektergebnisse einem größeren akademischen Kreis zugänglich zu machen. Davon erwarten wir zum einen ein größeres akademisches Interesse an unseren Ansätzen und zum anderen auch potentielle Zusammenarbeiten im Bereich der Kommunikationssysteme für die Industrieautomatisierung. Wir gehen davon aus dass ein gut dokumentiertes frei zugängliches Framework des zu entwickelnden Wireless IO-Link Protokolls von universitären Einrichtungen angenommen wird und somit die Reichweite der Projektergebnisse multipliziert wird.

II.5 FE-Ergebnisse von dritter Seite

Von der HART Communication Foundation wurde im Oktober 2007 der Drahtlos-Standard "Wireless HART", der für die Prozessautomatisierung ausgelegt ist, verabschiedet. Um eine Einordnung dieses globalen Standards für die Ziele des RealFlex-Verbundes vorzunehmen, wurde diese Technologie mit den ursprünglich im Projektantrag anvisierten Wireless-Technologien für die Umsetzung von Sensor- und Aktoranbindungen verglichen, wobei wir auf GRund der fehlenden anwendbarkeit in der Fertigungsautomatisierung Abstand von dieser Technologie nahmen.

In der PNO schien sich derweil das von ABB entwickelte WSAN als bevorzugte Lösung für die Fertigungsautomatisierung durchzusetzen. Als Resultat dieser Entwicklung haben wir sichergestellt, dass

- unsere Systementwicklungen und Protokolle gegebenenfalls mit diesem Standard zusammen arbeiten können. Dies gilt insbesondere für das IO-Link Mapping und die Sicherheitskomponenten,
- der von uns entwickelte Funkstandard WSAF basis-technologisch dem WSAN Standard ähnelt und so eine Integration von beiden Systemen in Produkten möglich machen sollte, und

- als Abgrenzung vor allem die Prozessautomatisierung (weniger Sensoren, größere Reichweiten) angesehen wird, die nicht das Ziel der WSAN-Technologie ist.

Es zeichnet sich ab, dass dieser Standard aktuell keine Sicherheitsfunktionalitäten unterstützt. Hier sehen wir gute Chancen auf Umsetzungen unserer Projektergebnisse.

II.6 Veröffentlichungen

Innerhalb des RealFlex Projektes gab es eine Reihe von Veröffentlichungen die im folgenden aufgelistet sind:

- Homepage: www.RealFlex-projekt.de
- Filmpräsentation und Messedemonstrator für die Messe SPS/IPC/Drives 2010 in Nürnberg
- Graeser, Olaf; Trsek, Henning; Jasperneite, Jürgen; Investigations on Traffic Patterns for Timing Requirements of an Industrial Real-Time System in Factory Automation; 2nd Junior Researcher Workshop on Real-Time Computing (JRWRTC 2008) (in conjunction with the 16th International Conference on Real-Time and Network Systems (RTNS 2008)) Rennes, France, Oct 2008.
- Hameed, Mohsin; Trsek, Henning; Graeser, Olaf; Jasperneite, Jürgen: Performance Investigation and Optimization of IEEE802.15.4 for Industrial Wireless Sensor Networks; 13th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA2008) Hamburg, Germany, Sep 2008.
- J. Krimmling, St. Peter, D. Schmidt, M. Mahlig: Test einer Bluetooth-Funkstrecke für die Prozessautomatisierung; Proc. SPS/IPC/Drives Kongress 2010, Ed.: K. Bender, W. Schumacher, A. Verl, 167 (2010)
- Peter, Steffen; Stecklina, Oliver; Langendörfer, Peter: An Engineering Approach for Secure and Safe Wireless Sensor and Actuator Networks for Industrial Automation Systems; ETFA 2009 - 14th IEEE International Conference on Emerging Technologies and Factory Automation; Session: Security for industrial applications; September 22 - 26, 2009; Mallorca, Spain.
- Peter, Steffen; Vater, Frank; Langendörfer, Peter: Sicherheits-Engineering am Beispiel von drahtlos angebundenen Sensor/Aktor-Systemen in der Automatisierungstechnik; SPS/IPC/Drives 2009, Proceedings of SPS/IPC/DRIVES, Elektrische Automatisierung, Systeme und Komponenten '09, Nuernberg, Germany, November, 2009.
- Pressemitteilung über die Abschlusspräsentation des Projektes bei Phoenix Contact Electronics im Rahmen der Messe SPS/IPC/Drives 2010 in Nürnberg
- Presseinformation von Phoenix Contact: SZuverlässige Datenübertragung von Sensor- und Aktordaten- über Funksysteme nachgewiesen"(3.12.2010)
- Pressemitteilung der Hochschule Ostwestfalen-Lippe: "RealFlex: Neuartige Management-, Sicherungs- und Verschlüsselungskonzepte"(21.12.2010)
- Patent: D. Dietterle, P. Langendörfer: Protokollbeschleunigermodul mit Paketweiterleitungs-funktion und Betriebsverfahren für einen Senderempfänger zur schnellen Weiterleitung von Datenpaketen Anmeldekennzeichen 10 2009 001 821.2-31

Literatur

[1] IEEE International Conference on Emerging Techonologies and Factory Automation, 2009. http://etfa2009.org/.

[2] American National Standards Institute (ANSI). AMERICAN NATIONAL STANDARD X9.62-2005. Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.

[3] R. Anderson. *Security Engineering - A guide to building dependable distributed systems*. Wiley, 2008.

[4] FIPS. Specification for the advanced encryption standard (AES). Federal Information Processing Standards Publication 197, 2001.

[5] mesago. SPS/IPC/DRIVES, 2010. http://www.mesago.de/sps.

[6] PROFIBUS Nutzerorganisation. Spezifikation IO-Link Physik/Kommunikation, 2005.