Angepasste Benutzerschnittstellen für das Wearable Computing im Projekt SiWear

Marc Ronthaler, Mehmet Kus, Karsten Sohr, Katja Wind, Richard Sethmann, Michael Lawo[1]

Mobile Research Center Bremen

Zusammenfassung

In diesem Positionspapier werden die grundlegenden Ideen zu einer angepassten Benutzerschnittstelle für das Wearable Computing im Projekt SiWear, gefördert durch das BMWi im Förderschwerpunkt SimoBIT (www.simobit.de) vorgestellt[2]. Neben der Darstellung der Gesamtarchitektur werden die Aspekte der sicheren Kommunikation, die Authentisierung und Zugriffskontrolle, Lokalisierung sowie die benutzbare und der Situation entsprechende Benutzungsschnittstellen dargestellt.

1 SiWear Gesamtsystem

Kern von SiWear ist die Entwicklung einer mehrstufigen Integrationsplattform (Abb. 1), deren eine Komponente die Service- orientierte Wearable Enterprise Plattform bzw. die hinterlegten Arbeitsprozesse sind und dessen zweite Komponente das Wearable- Endgerät mit einer ebenfalls service- orientierten Plattform ist. Das System basiertl auf einem gezielten „Push“ von Informationen, um den Nutzern zum richtigen Zeitpunkt am rechten Ort mit der rechten Information zu versorgen und um die Kommunikation der teamorientierten Zusammenarbeit zu unterstützen.

---

[1] Die Autoren danken dem BMWi für die Förderung im Rahmen des Forschungsschwerpunkts SimoBIT und allen Projektpartnern für die gute Zusammenarbeit.

[2] Förderbeginn: 1.8.2004, Laufzeit: 30 Monate

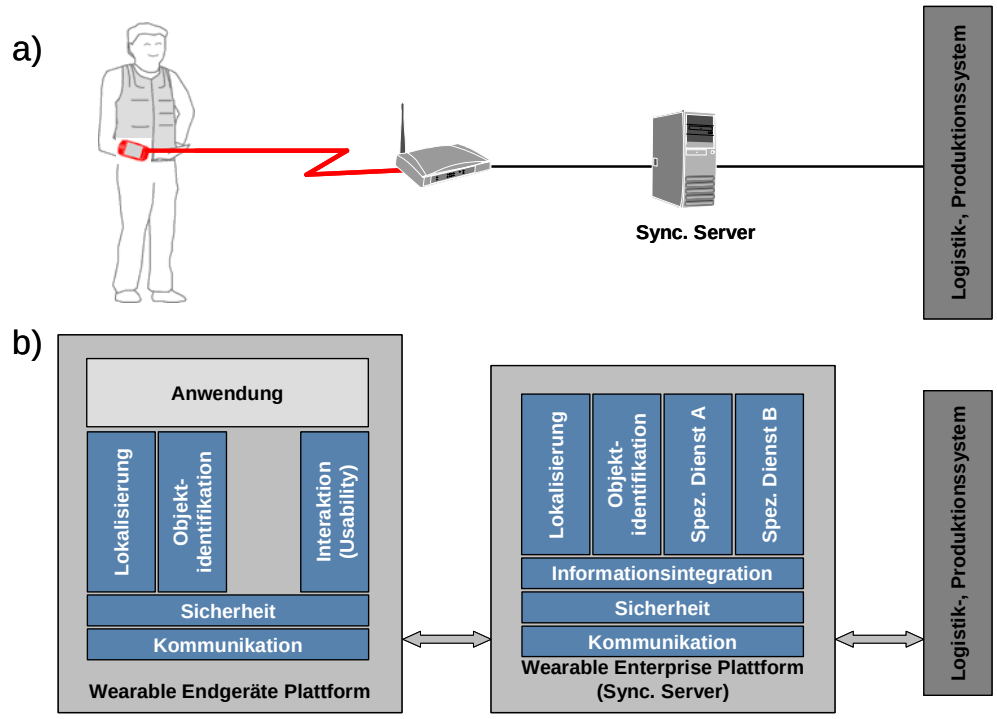

Abb. 1: SiWear Gesamtsystem, a) physikalische Darstellung, b) funktionale Darstellung

Ausgangsbasis sind in einer Anforderungsanalyse identifizierte Arbeitsprozesse und die Modellierung der Gesamtarchitektur sowie Funktionsdemonstratoren zur Evaluation.

Folgende Bereiche werden abgedeckt, jeweils mit dem Fokus auf die Benutzbarkeit und die Sicherheit des Gesamtsystems:

- durchgängig **sichere Kommunikation** zwischen der service- orientierten Plattform und mobilen Endgeräten – Datensicherheit und Datenintegrität,
- **sichere Authentifizierung** Nutzer und **sichere Lokalisierung** von Nutzern, Objekten und Artikeln
- **benutzbare und der Situation entsprechende Benutzungsschnittstellen** – die eine einfache und konsistente Benutzbarkeit der Anwendung auf dem Wearable- Endgerät erlauben.

2 Sichere Kommunikation

Technologisch wird größtenteils auf vorhandene Sicherheitskomponenten zurückgegriffen wie z.B. (mobile) VPN, WLAN- Absicherung (z.B. mittels WPA 2), GPRS-/UMTS-

Absicherung, Trusted Network Connect-Technologien, Virenschutz für mobiles Endgeräte und Web-Service-Sicherheit. Neue mobile Endgeräte, heterogene Netze und die Forderung nach sicheren, skalierbaren und effizienteren Arbeitsabläufen führen zu völlig neuen Anforderungen an das Service Management von Kommunikationssystemen. Verfahren der Selbstorganisation und der adaptiven Netze sind Lösungsansätze für eine sichere und stabile Kommunikation. In Abhängigkeit der Ergebnisse einer Bedrohungs- und Risikoanalyse und unter Berücksichtigung der modellierten Sicherheitsarchitektur werden somit geeignete Sicherheitsmechanismen adaptiert und bereitgestellt.

2.1 Authentisierung und Zugriffskontrolle

Um einen sicheren Zugriff auf Daten und die sichere Kommunikation zwischen verschiedenen Kommunikationspartnern zu gewährleisten, werden Technologien ermittelt, die es ermöglichen, sowohl Personen als auch Objekte und Artikel zu identifizieren bzw. zu authentisieren. RFID- Technologie ermöglicht Personen bzw. das von Personen genutzte Wearable-Endgerät sowie Objekte eindeutig zu identifizieren. Existierende RFID- Systeme sind auf Verträglichkeit mit den herrschenden Umgebungsbedingungen und Einsatzzweck zu untersuchen. Investitionssicherheit und Zukunftssicherheit der Systeme sind für die Beurteilung der Wirtschaftlichkeit zu beachten. Biometrische Authentisierungsverfahren wie z.B. Fingerabdruckscanner und Sprechererkennung bei sprachgesteuerten Systemen werden ferner betrachtet. Zur gegenseitigen Authentisierung zwischen Clients und Servern werden gängige Authentisierungsverfahren wie z.B. Challenge- Response- Protokolle verwendet. Hier existieren Lösungen, da Technologien wie WLAN solche Verfahren unterstützen. Der Zugriff auf die Daten (und auf Services im Sinne von SoA) wird über ein rollenbasiertes Konzept für die Zugriffskontrolle geregelt. Bei der rollenbasierten Zugriffskontrolle erhalten Nutzer Zugriff auf Daten und Services in Abhängigkeit der Rollen, die sie innehaben. Schließlich wird auch in der Modellierung und Architektur des Gesamtsystems darauf geachtet werden, dass entsprechende Mechanismen zur Verwaltung und Bereitstellung der Authentisierungs- und Autorisierungsdaten eingesetzt werden (Identitätsmanagement).

2.2 Lokalisierung

Die Lokalisierung dient als Zugangskontrolle für Mitarbeiter, und dem Qualitätsmanagement des Materialflusses, also der Kontrolle, an welchem Ort zu welchem Zeitpunkt welche Materialien und Artikel zu finden sind. In der Kommissionierung von Produktionsmitteln lassen sich durch Einsatz geeigneter Lokalisierungsmechanismen die Effizienz, aber besonders auch die Effektivität steigern sowie die Fehleranfälligkeit reduzieren. Hierzu können zur Lokalisierung ähnlich der Authentisierung auch RFID-Technologien eingesetzt werden sowie auch die Lokalisierung per WLAN. Besonderes Augenmerk wird bei der Lokalisierung von Personen auf datenschutzrechtliche Fragestellungen und sozio- ökonomische Aspekte gelegt. Die diesen Aspekt betreffenden Arbeitsprozesse werden identifiziert und bei der Auswahl der Basistechnologien berücksichtigt, z.B. durch geeignete Auswahl von Reichweiten, geschützte Bereiche, bzw. Anonymisierung bestimmter Datenarten.

3 Benutzbare und der Situation entsprechende Benutzungsschnittstellen

Benutzungsschnittstellen sollen den Anwender bei seiner in der „realen Welt“ auszuführenden Aufgabe unterstützen, indem sie ihm den effizienten, aufgabenorientierten und kontextsensitiven Zugriff auf benötigte Informationen gestatten und die jeweils adäquate Interaktionsform zur Navigation in der Anwendung und zur Datenerhebung zur Verfügung stellen. Die Kommunikation zwischen Nutzer und Endgerät, also die „letzte Meile“ in der Kommunikation zwischen Mensch und IT-Infrastruktur ist sicherzustellen, d. h. auch hier sind Datensicherheit und –integrität zu gewährleisten.

Die Basistechnologien setzen an verschiedenen Stellen der Systemarchitektur an (vgl. Abbildung 2).

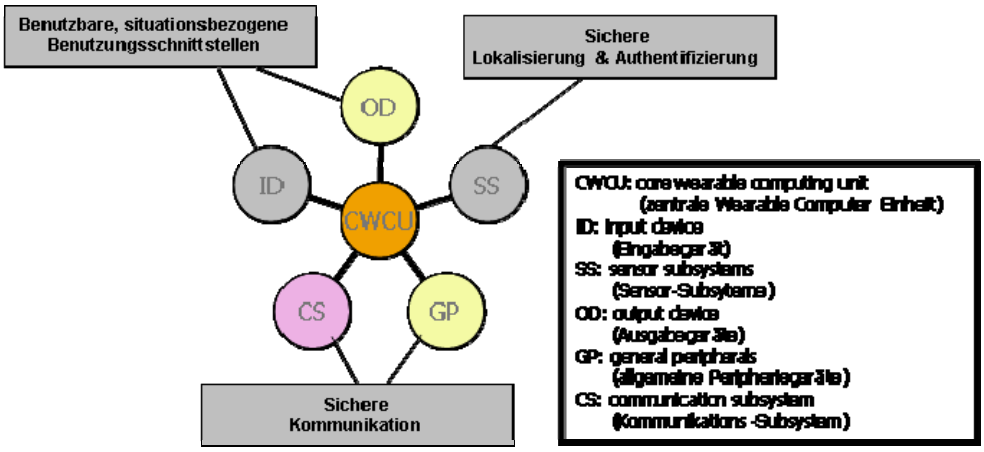

Abb. 2: SiWear Systemarchitektur (basierend auf wearIT@work[3])

Die anwendungsspezifische Systemintegration unter Verwendung von **COTS**[4] Komponenten wird in Benutzbarkeitsstudien evaluiert. Hierzu werden aus kommerziell erhältlichen Hardwarekomponenten Funktionsdemonstratoren entwickelt, die erlauben Komponenten und deren Kombination zu bewerten und in Labor- und unter Realbedingungen zu testen. Die Demonstratoren sollen auch für den Test und die Evaluierung der softwareseitigen Anwendungskomponenten genutz werden.

[3] www.wearitatwork.com

[4] Comercial-off-the-shelf