Submission Title: Application requirements and proposed solutions  
Date Submitted: 18 March, 2008  
Source: Ludwig Winkel, Siemens AG  
Address Siemensallee 74, Karlsruhe, 76187, Germany  
Voice: +49 721 595 6098, FAX: +49 721 595 893 6098, E-Mail:ludwig.winkel@siemens.com  
Re: IEEE P802.15.SG4a Call For Applications, see 15-07-0936-00-004e-call-applications-tg4e.doc

Abstract: Requirements of factory automation and proposed solution

Purpose: Provide P802.15.4 application for Process automation and Factory automation

Notice: This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

Release: The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.
.4e application

Ludwig.Winkel@siemens.com

March 18, 2008

Orlando
Integration of wireless in wired infrastructure

Bussystems for the Industry

Industrial Ethernet

PROFIBUS PA

PROFIBUS

Manufacturing Execution System

MES, SCADA, Monitoring

Controller

Remote I/O

Networking components

Field Devices

Sensors + Actors (Factory Automation)
Industrial Wireless LAN (IWLAN) enables industrial mobile Communication

- Industrial Mobile Communication

**Reliable**
- Cyclic data transmission (Deterministic, low latency)
- Redundancy
- Control of radio link
- Stable radio link

**Robust**
- Metal housing with high environmental protection class
- Protection against vibration and shock
- Extended Temperature range

**Secure**
- Easy configuration
- Access control (Authentication)
- Encryption, etc.

**Safe**
- Safety communication even on the same medium as non-safety related communication
IWLAN Reaction times allow even a fail safe communication via PROFIISafe

- Up to Safety Category 4 according to EN 954-1
- SIL3, see IEC/EN 61508

Wireless – even in safety applications!
2. Use Cases – How can wireless meet current customers’ requirements

Use Cases are

• No. 1: Asset management
• No. 2: Increase process information by additional sensors for monitoring
• No. 3: Wireless field device in control
• No. 4: All wireless field devices in one network
Use Case 1 Asset Management

- **Current situation**
  - Modern field devices have lots of diagnostics data
  - These data are available in most cases only per costly on-site inspection
- **How wireless supports customers**
  - Wireless units allow central access to field devices
- **Customers benefits**
  - No changes, only add-ons
  - Higher plant availability
  - Predictive instead of preventive maintenance reduces costs
  - Quick Return of Invest
  - Wireless even in backbone buses (also in following use cases)
Use Case 2- Increase process knowledge by additional monitoring TAGs

- **Current Situation**
  - Due to high installation costs only most important field devices are installed

- **How wireless supports customers**
  - Due to lower total cost of ownership (TCO) users can add additional wireless measurement points

- **Customers benefits**
  - Higher performance …
  - Better product quality …
  - Less energy and material input …
  - Increased productivity …

through enhanced process knowledge via additional monitoring field devices
Use Case 3

Wireless field devices in process control

- **Current Situation**
  - Customers want to have experience with new technology before using it in mission critical applications

- **How wireless supports customers**
  - After getting experience with wireless field devices in monitoring applications a user may add wireless devices in control

- **Customers benefits**
  - Same wireless technology for monitoring and control
  - Change from monitoring to control results in no new investment, just add an existing/new wireless device into control strategy
Use Case 4
All Wireless Field Devices in One Network

• **Current Situation**
  – Customers have a rich set of tools, templates, standards, experience with device out of 1+ classes (e.g. HART, PROFIBUS, FF)

• **How wireless supports customers**
  – Wireless devices can be easy integrated in this unchanged environment

• **Customers benefits**
  – No new device types
  – No additional training
  – No additional networking components like routers
3. Resulting technical / commercial requirements

- Two major types of Applications
  - Process Automation
  - Factory Automation
- Stability against noisy Environment
- Use of Standard Radio Technologies for monitoring and control
- Simplicity
- Minimize Lifecycle Costs & Easy Integration in existing automation solutions
- Secure operation with wireless technology
Two major types of Applications
Process Automation

Requirements from process automation
• high number of devices in one wireless cell
• moderate performance requirements (latency times 500+ ms)
• relative long distances
• Redundant communication paths
• Functional Safety
Two major types of Applications

Factory Automation

Requirements from factory automation

- smaller number of devices in one wireless cell
- high performance requirements (latency times < 10 ms)
- relative short distances
- Redundant communication paths
- Functional Safety
Stability against noisy Environment

Robust Communication over the air

- Coexistence with other wireless technologies, e.g.
  - IEEE 802.11 (WLAN)
  - IEEE 802.15.1 (Bluetooth)
  - Future specifications

- Robust against interference sources
  - E.g. micro wave oven

- E.g. infrastructure laptops
- …

- 802.11x
- 802.15.4e
- 802.15.1
- EMC
- cell phones
- PDAs
- keyboard & mouse
- …
Use of Standard Radio Technologies for monitoring and control

• Interoperability from an end-user’s perspective
  – Free choice of supplier, e.g. for field devices
  – Devices from different suppliers run in the same wireless network

• Interoperability from an supplier’s perspective
  – More than one chip vendors for wireless components
  – Cheap wireless components (e.g. ASICs)
  – Wide-spread technology
Simplicity

- Easy installation without special tools, e.g. for site surveys, and without special training
- Simple expandability of the network by new devices
- Simple network management
- Common infrastructure (unique radio technology)
- Minimum number of infrastructural networking components
Simplicity

- Easy installation without special tools, e.g. for site surveys, and without special training
- Simple expandability of the network by new devices
- Simple network management
- Common infrastructure (unique radio technology)
- Minimum number of infrastructural networking components
Minimize Lifecycle Costs & Easy Integration in existing automation solutions

- Minimum Lifecycle Costs
  - Battery life time 5+ years
    - Excessive and configurable usage of sleep modes
    - Low power consumption of the radio
  - Self-configuring networks
  - Self-Healing networks
- Easy wireless integration in existing automation solutions
  - Used tools
  - Used templates
  - Industry and Customer standards should be able to be used by customers, e.g. for integration and parameterization of HART, PROFIBUS and FF devices
Secure operation with wireless technology

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>The protection of devices or system resources against unauthorized access.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Assurance of the identity of a device or a system resource.</td>
</tr>
<tr>
<td>Availability</td>
<td>The property of a device, a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Assurance that information is not disclosed to unauthorized individuals, processes, or devices.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Property that data has not been changed, destroyed, or lost in an accidental manner.</td>
</tr>
<tr>
<td>Data Authenticity</td>
<td>Assurance that the origin and/or the source of data are correctly identified.</td>
</tr>
</tbody>
</table>
4. Siemens’ proposal baseline

- Meshed Networking (TDMA)
- High Performance (TDMA)
- Frequency Agility
- IEEE 802.15.4 on 2.4 GHz Band
- Coexistence with IEEE 802.11
- Wireless Backbone based on IEEE 802.11 and IEC 61784-2, CP 3/4 (PROFInet Conformance Class A wireless)
- Security
Meshed Networking

Requirements are
- Reliability & Robustness
- Huge Coverage
- Simplicity
- Self-organizing
- Self-healing
- Long distances

Gateway

Device
High Performance is met by Star Topology

Requirements are
- TDMA based
- fulfills the req. from factory automation
- deterministic behavior
- required for high performance cyclic communication
- allows acyclic traffic (contention period)

Sync Beacon from Gateway

10 ms cycle time

Scheduled Timeslots

Contestion period, optional

Gateway Device
Frequency Agility to enable robustness and availability

Frequency usage over time for one dedicated link

Requirements are
- Robustness against interferences
- Availability of the network
IEEE 802.15.4 on 2.4 GHz Band

• Standard Technology, specified by IEEE
  – Cheap
  – Multi vendor
  – Low power
  – Scalable

• 2.4 GHz Band
  – High performance
  – Worldwide usability enabled

Requirements are
  – Interoperability from an end-user’s and supplier’s perspective
  – Lifetime >5 years
Coexistence with IEEE 802.11

WLAN (IWLAN) and 802.15.4 RF Spectrum

IEEE 802.11
- Channel 1
  - 2412 MHz
- Channel 6
  - 2437 MHz
- Channel 11
  - 2462 MHz

Clear channels

IEEE 802.15.4
- Channel 15
  - 2425 MHz
- Channel 20
  - 2450 MHz
- Channel 25
  - 2475 MHz
- Channel 26
  - 2480 MHz

Standard should allow to enable only selected channels (e.g. in the gaps of running WLAN)
Security

- AES encryption (Advanced Encryption Standard)
  - Open and accepted encryption technology

- Authentication and key update approach suitable for mesh networks as well
  - Scalable technology, applicable for simple devices (primitive sensors) as well

- Security on Wireless should be based on available standard technologies
Overall Approach

Dual Mode approach

• Unique hardware platform

• Minor difference in FW stack
  – Optimization for advanced mesh (AM) functionality
  – Optimization for advanced performance (AP) functionality
Overall Approach

- **Software**
  - Advanced Mesh (AM)
  - Advanced Performance (AP)
  - MAC extensions for mesh
  - MAC – part from 802.15.4
  - MAC extensions for star
  - MAC – part from 802.15.4

- **Hardware**
  - Medium Access Layer (MAC) – lower part from 802.15.4
  - Physical Layer (PHY)
Your Questions and Comments

Thank you for your attention

Questions

Comments
das ist eine wiederholung von oben, dann besser weglassen
adbire0; 06.09.2006