5th BICSI SOUTHEAST ASIA CONFERENCE 2007

Industrial Wireless ETHERNET

TAN Aik Hong
Regional Key Account Manager
Hirschmann Automation and Control
Industrial Wireless LAN
Wireless LAN planning

- On-site conditions
- Link to plant network
- General requirements
- Planning
- Device selection
- Disturbing factors
### Technology Overview

<table>
<thead>
<tr>
<th>Technology</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11a/h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wave band (MHz)</td>
<td>2400.0 - 2483.5</td>
<td>2400.0 - 2483.5</td>
<td>5150 - 5350, 5470 - 5725</td>
</tr>
<tr>
<td>Spectrum</td>
<td>83.5 MHz</td>
<td>83.5 MHz</td>
<td>455 MHz</td>
</tr>
<tr>
<td>Non overlapped channels</td>
<td>3</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>Transmitting power (mW)</td>
<td>100</td>
<td>100</td>
<td>200 - 1000</td>
</tr>
<tr>
<td>Data rate gross (Mbit/s)</td>
<td>11</td>
<td>54</td>
<td>54</td>
</tr>
<tr>
<td>Data rate net (Mbit/s)</td>
<td>5</td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td>Used for</td>
<td>indoor, outdoor</td>
<td>indoor, outdoor</td>
<td>indoor, outdoor</td>
</tr>
<tr>
<td>Range</td>
<td>up to 300 m</td>
<td>up to 300 m</td>
<td>up to 70 m</td>
</tr>
<tr>
<td>Modulation process</td>
<td>DSSS</td>
<td>OFDM</td>
<td>OFDM</td>
</tr>
</tbody>
</table>

DSSS (Direct Sequence Spread Spectrum)  DFDM (Orthogonal Frequency Division Multiplexing)
Range problem

The range depends on:

- Antennas characteristics
- AP transmitting power
- HF cable properties
- Sources of interference
- Construction demands

<table>
<thead>
<tr>
<th>Speed</th>
<th>open</th>
<th>open / closed</th>
<th>closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>54/11 Mbit/s</td>
<td>150 Meter</td>
<td>30 Meter</td>
<td>20 Meter</td>
</tr>
<tr>
<td>5,5 Mbit/s</td>
<td>250 Meter</td>
<td>70 Meter</td>
<td>35 Meter</td>
</tr>
<tr>
<td>2 Mbit/s</td>
<td>400 Meter</td>
<td>90 Meter</td>
<td>40 Meter</td>
</tr>
<tr>
<td>1 Mbit/s</td>
<td>500 Meter</td>
<td>115 Meter</td>
<td>50 Meter</td>
</tr>
</tbody>
</table>

AP = Access Point
HF = High Frequency
Wireless LAN

Task: Link mobile users via access points to the existing Ethernet infrastructure
Wireless LAN

Important Note
WLAN is a “potentially insecure” method compared to wired networks
Industrial Wireless LAN - Applications

Area of Applications

- Transportation – Data Transfer, Traffic Monitoring
- Factory Automation – Production, Service
- Energy – Data Transfer, Management
- Minerals & Mining
- Process Automation
Real-time in Ethernet
What Is Real-Time?

- A system is real-time if it is able to react
  - under all operating conditions
  - to all events correctly
  - within the expected time constraints

Real-time ability

- to fulfill time demands of an application
- defined timing characteristics – under all operating conditions
Categories Of Real-Time

Determinism and Jitter

- Determinism
  - The exact predictability of a system’s timing

- Jitter
  - The tolerable deviation from a deadline when executing a command

Categories Of Real-Time

- Timeliness
  - An action has to be executed within a maximum time

- Synchronism
  - An action has to be executed within a specified time frame.
Four Criteria for Real-time Ability

1. Propagation time, cycle time, reaction time
   ➞ define upper time limit, not to exceed under all circumstances

2. Jitter
   ➞ timing fluctuation, deviation from set point

3. Synchronistic
   ➞ Simultaneity of actions

4. Throughput
   ➞ amount of data to transmit within a time unit
## IAONA Real-Time Classes

### Industrial Automation Open Networking Alliance

<table>
<thead>
<tr>
<th>Real-Time Class</th>
<th>Description</th>
<th>Time-Synchronisation: Maximum Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>properties of today available standard products</td>
<td>&gt; 1 ms</td>
</tr>
<tr>
<td>2</td>
<td>real-time optimized products conform to today's standards</td>
<td>100 μs to 3 ms</td>
</tr>
<tr>
<td>3</td>
<td>products with added new functionality realised in software combined with standard hardware</td>
<td>10 μs to 400 μs</td>
</tr>
<tr>
<td>4</td>
<td>products with added new functionality realised in hard- and software</td>
<td>0.5 μs to 15 μs</td>
</tr>
</tbody>
</table>
Solutions
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Shared medium</td>
<td>1. Switching</td>
</tr>
<tr>
<td>2. Collisions</td>
<td>2. Full duplex</td>
</tr>
<tr>
<td>4. Transmission speed</td>
<td>4. 10Mb/s, 100Mb/s, 1Gb/s</td>
</tr>
<tr>
<td>5. Protocol</td>
<td>5. UDP</td>
</tr>
</tbody>
</table>
QoS on Layer 2: IEEE 802.1D and Q

- QoS solution of IEEE with Expedited Traffic Classes as well as priority transfer
- Distinguishing traffic by type or application
- Identification by user_priority
- 8 priority classes
- Implementation in components: optimum 8 queues, often less
- Bandwidth allocation to queues: different concepts

<table>
<thead>
<tr>
<th>Type of Traffic</th>
<th>Acr</th>
<th>user_prio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>BK</td>
<td>1</td>
</tr>
<tr>
<td>free</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Best-Effort</td>
<td>BE</td>
<td>0 (default)</td>
</tr>
<tr>
<td>Excellent-Effort</td>
<td>EE</td>
<td>3</td>
</tr>
<tr>
<td>Controlled-Load</td>
<td>CL</td>
<td>4</td>
</tr>
<tr>
<td>Video</td>
<td>VI</td>
<td>5</td>
</tr>
<tr>
<td>Voice</td>
<td>VO</td>
<td>6</td>
</tr>
<tr>
<td>Network control</td>
<td>NC</td>
<td>7</td>
</tr>
</tbody>
</table>
Scalable ETHERNET

Realtime in ETHERNET is possible today!

- All you need is ...
  - Full duplex operation / full switched (Example: 1000 stations)
  - Non-blocking Network Architecture
  - non-critical overall delay!

Only Problem: „many-to-one traffic“
Real-Time for Wireless LAN?
IEEE 802.11e defines a set of Quality of Service (QoS) enhancements for wireless LAN applications through modifications to the Media Access Control (MAC) layer.

*Wireless Multimedia Extensions (WME)*
*Wi-Fi Multimedia (WMM)*

Defines four categories for prioritization
- Voice
- Video
- Best effort
- Background
Fast Roaming

- Background scanning
- Pre-authentication
- PMK Caching (Pair-wise Master Key)
  - “Fast Roam Back”
- 30ms hand-over
Wireless LAN Security
Definitions: Safety and Security

- **Safety**
  - Protection of people and material

- **Availability**
  - Stability (MTBF, specifications, ...)
  - Fail-safety (redundancies, ...)

- **Security**
  - Access protection
  - Authentication
  - Authorization
Security objectives and mechanisms

Access Control
- Authorisation
- Confidentiality
- Integrity
- Auditability
- Availability
- Non-reputability
- Third party protection

Authentication
- Identification

Firewall

Intrusion Detection/Prevention

Tunnelling

Encryption
Authentication

- 802.1x
- RADIUS* (Client and Server)
- EAP (Extensible Authentication Protocol)
- LEPS (LANCOM Enhanced Passphrase Security)
  - allows each client to have each passphrase

1. Client asks for authentication at the access point
2. Access point communicates with 802.1x server and allows client access to network after receiving authentication by server
Access Control

Permission Policy, Authorisation Policy

Host-based ↔ Network-based

ACLs
Virtual LANs
VPNs

OS-based ↔ Access Control Device

Host-based Firewalls
Host-based IDS

Perimeter Firewalls
Routers
Switches

Customer service representative
Server and database admin

HR database
R&D file server
Common file server
Firewall

- Stateful Inspection
- Port Filters
- Protocol Filters
- Intrusion Detection
- Denial Of Service Protection

Implementations:
- Dedicated Hardware Appliances
- Integrated into Routers and Gateways
- Software Packages on top of general OS (Server)

Deny all!
Allow specified
Protocols, Ports, IP addresses...

Hide internal information
NAT, PAT, 1-to-1-NAT
Tunnelling

Virtual Private Network

Remote Access VPN
Client-to-Site VPN

Site-to-Site VPN
Encryption

- **802.11i** defines highest possible security level for WLAN
- **AES (Advanced Encryption Standard)** – Hardware Encryption
- **WPA2 Personal / Enterprise (Wi-Fi Protected Access)**

WEP64 3000 packets to crack
WEP128 about a million packets to crack
Secure Wireless LAN – Multiple SSID

- Up to 8 independent WLAN’s simultaneously per wireless interface
  - VLAN-Tagging for every SSID
  - Own MAC-Address-Filter, WEP-encryption, VPN-connection etc.
  - Simultaneously use of open and private networks
  - Management access by HotSpots
  - Migration from WEP → WPA → 802.11i

- Maximum security with 802.11i/AES
- Open network without encryption
- WEP128 encryption to support high number of clients
- WPA/TKIP acceptable security level to allow access to clients that don’t support AES
HIRSCHMANN

Industrial Wireless Ethernet
Industrial Wireless LAN e.g. BAT54-Rail

- **Industrial Features**
  - Robust Metal Enclosure, IP 40, DIN Rail / Wall Mounting
  - Temperature Range of -20°C up to +50°C
  - Redundant Power Supply
    - 2x Power-over-Ethernet
    - 2x Dual 24 Vdc
    - 1x AC adapter

- **Secure Transmission Features**
  - Dual Wireless LAN according to IEEE 802.11a/b/g/h
  - Redundant WLAN Connections
  - Bandwidth up to 108MBit/s per WLAN Interface
  - Fast Roaming
  - IEEE802.11e/QoS

- **Security Features**
  - Highest Possible Security Level using IEEE 802.11i and IEEE 802.1x
  - Firewall & VPN
Steel Plant in Japan

Overview

- Wireless network is used to monitor & control 26 unmanned conveyer cranes at iron ore station (the area highlighted in blue)

- Hirschmann Industrial Ethernet solutions
  - Wireless: BAT54-RAIL
  - Wired: MICE, SPIDER and Industrial HiVision NMS

- Redundant Plant network both in wired and wireless using Hirschmann HiPER-Ring technology & Redundant Wireless Bridge

Field Survey & Test
- Distance test
- Communication quality test
Steel Plant in Japan

System Overview

IP Camera
PLC
On crane

BAT54 RAIL
+ ANTN14G
In field panel

Gigabit HiPER-Ring
(MM Fiber and UTP)

MS30
MS30
MS30
MS30

Redundant Coupling

MELSEC PLC
MELSEC PLC

ENG Station Process Computer

Material Center (CCR)

Elec. Room A

UTP
MM Fiber
Steel Plant in Japan

Redundancy both in wired and wireless networks

Wired:
- HiPER-Ring (among L2SWs) < 200ms
- Redundant Coupling (between L2SW & L3SW)

Wireless:
- Redundant Wireless using different radio frequency
- RSTP for failover action

- Master WLAN AP
- Root Bridge in RSPT
- Slave WLAN AP

Frequency Band 1
Frequency Band 2
Industrial Wireless LAN – Security everywhere
Questions?
Thank you for your attention!