

**T&E**

Technology & Engineering

# Security Aspects in Wireless Control

WIB Mini-seminar 26 April 2006

By Jos Berkien



## Agenda

- Akzo Nobel Technology & Engineering
- Wireless Standards
- Wireless Equipment for the Process Control
- Where Wireless in Process Control
- Risks of Wireless networks
- Wireless Security Risks
- Protecting Wireless Networks
- Case: Wireless Security at Organon
- Summary
- Questions

On April 1, 2006 the following departments were integrated into the new Akzo Nobel Technology & Engineering organisation:

- Akzo Nobel Engineering (AE)
- Akzo Nobel Manufacturing Services (ManS)
- Health, Safety & Environment (ManS HSE)
- Manufacturing Technology Department (ManS MTD)
- Materials Technology Center (ManS AMC)
- Manufacturing & Engineering Services (ManS MES)
- Akzo Nobel Manufacturing Support Center A/P (MSC A/P)
- Akzo Nobel Safety Services
- Akzo Nobel Sustainable Development (SD)
- Akzo Nobel SHERA Americas
- Akzo Nobel Chemicals Environmental Research (CER)
- Akzo Nobel Powder Technology Department (PTD)

Akzo Nobel Technology & Engineering serves customers (Akzo and non-Akzo) throughout the world with; Safety, Health, Regulatory, Toxicology, and Environmental Services, Process & Manufacturing Support, and Project & Design Management.

Focusing on the various process industries, Akzo Nobel T&E delivers knowledge-driven sustainable solutions.

## Wireless Standards

- **GSM**  
(Global System for Mobile Communications)
- **DECT**  
(Digital Enhanced Cordless Telecommunications)
- **Bluetooth (IEEE 802.15.1)**
- **WLAN (IEEE 802.11)**  
(Wireless Local Area Network)
- **ZigBee (IEEE 802.15.4)**
- **WiMAX (IEEE 802.16)**  
(Worldwide Interoperability for Microwave Access)



## Wireless Equipment for the Process Control



Control Stations



Barcode Scanners



PDA's



Remote Terminals

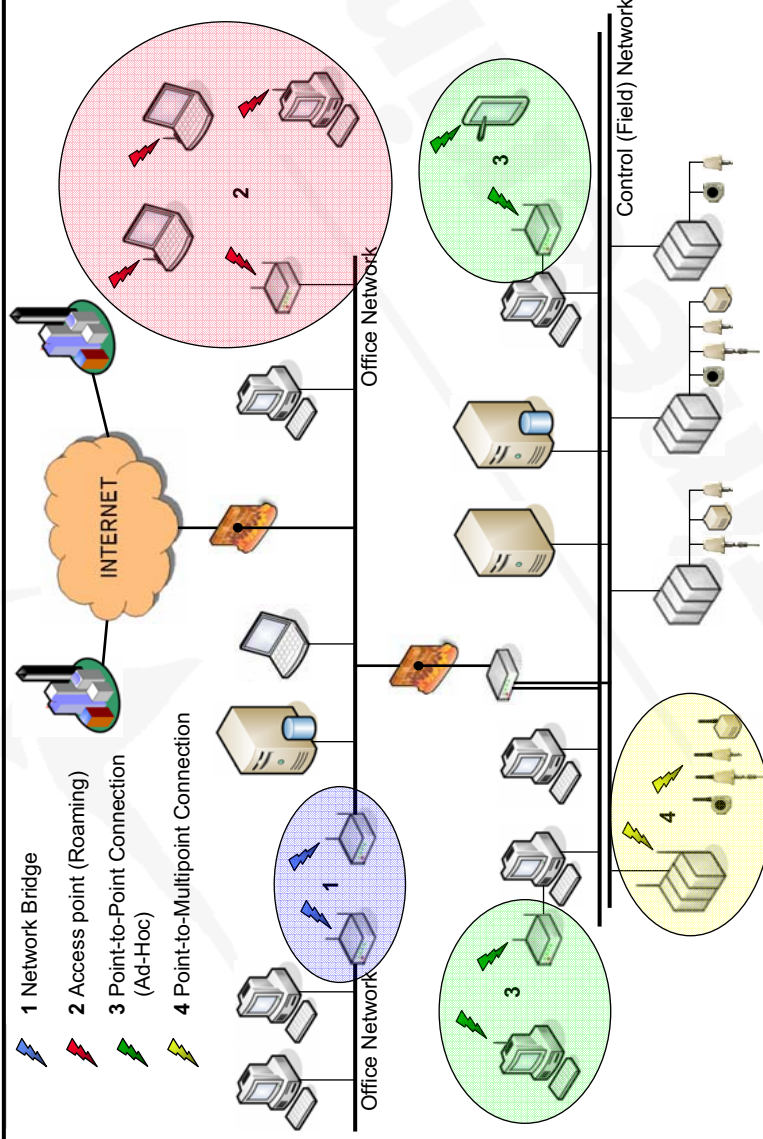


PC Peripherals



Instrumentation

## Where Wireless in Process Control

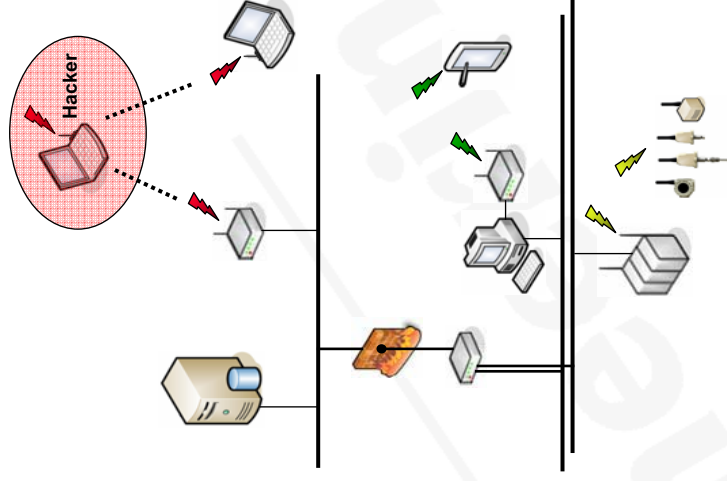


## Risks of Wireless Networks

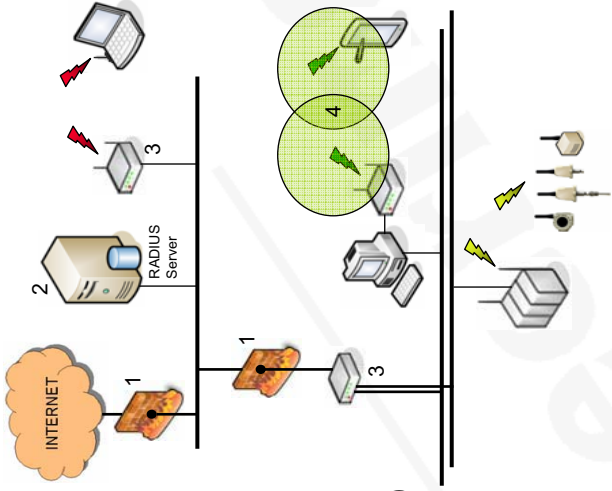
- **Reliability / Availability**
  - Wireless networks are susceptible to the environment (line of site, weather conditions, signal disturbance)
- **Maintainability**
  - Extra technology requires more knowledge
  - More security is required
- **Security**
  - Next sheet

## Wireless Security Risks

- **Man-in-the-Middle**  
Act as an Access Point, relay traffic to a real AP while filtering it.
- **Denial of Service**  
Overload Access Points to cause denial of network access or even a crash of the AP
- **Network Injection**  
Re-configuration of routers, switches etc. to bring down that network
- **Identity Theft (MAC Spoofing)**  
Cloning of a MAC ID to gain access
- **Unauthorized access**  
Gaining access to private company data



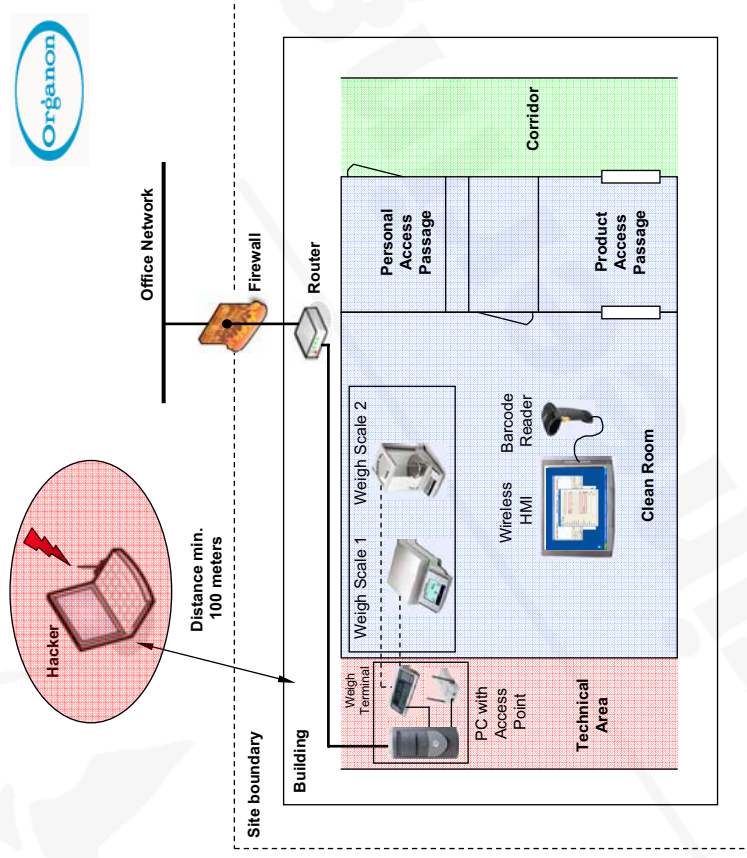
- **Standard network protection**
  - Force User Identification<sup>(1)</sup>
  - Activate and Position Firewalls<sup>(2)</sup>
  - Configure a Network Infrastructure<sup>(3)</sup>
- **Wireless coverage area**
  - Limit the transmitter/receiver range<sup>(4)</sup>
- **Technical Wireless Protection**
  - next sheet



- **Change default Access Point names and passwords**
  - Change factory settings of wireless equipment
- **Enable MAC address filtering**
  - Use the unique Media Access Control number of each network device to enable network access
- **Enable Wireless Network Encryption**
  - Use data encryption tools
    - WEP (Wired Equivalency Privacy)
    - WPA (Wi-Fi Protected Access)
    - WPA2 (Wi-Fi Protected Access version 2)
- **Disable the SSID broadcast option**
  - Make the wireless network identification (Service Set ID) invisible to the outside world



1. Distance between sender / receiver
2. WEP Data Encryption
3. User identification
4. Router installed
5. Firewall installed
6. Only operator operations, no system control
7. Value of information



## Summary

- **Wireless Communication is a fast growing & moving technology, is a useful technology and needs extra knowledge**
- **Wireless Communication is prone to security risks**
- **Not one protection method for Wireless Communication is sufficient on its own, it is necessary to combine protection methods**
- **A Wireless network can never be 100% secure**



---

# Thank you for your attention

# Questions?



**Ing. J. (Jos) Berkien**

*Process automation engineer  
Project & Design Management*

Akzo Nobel Technology & Engineering bv  
Velperweg 76, PO Box 5136, 6802 EC Arnhem, The Netherlands  
Phone +31 26 366 3260, Fax +31 26 366 5877  
E-mail [Jos.Berkien@AkzoNobel.com](mailto:Jos.Berkien@AkzoNobel.com)  
[www.akzonobel-te.com](http://www.akzonobel-te.com)