Security Issues and Quality of Service in Real Time Wireless PLC/SCADA Process Control Systems

Dr. Halit Eren & Dincer Hatipoglu
Curtin University of Technology
(Perth – Australia)

PRESENTATION

- Current state of wireless sensor networks
- Technological issues on the wireless sensor deployment in industrial applications
- Security and management of large networks
- Case study
- Conclusions

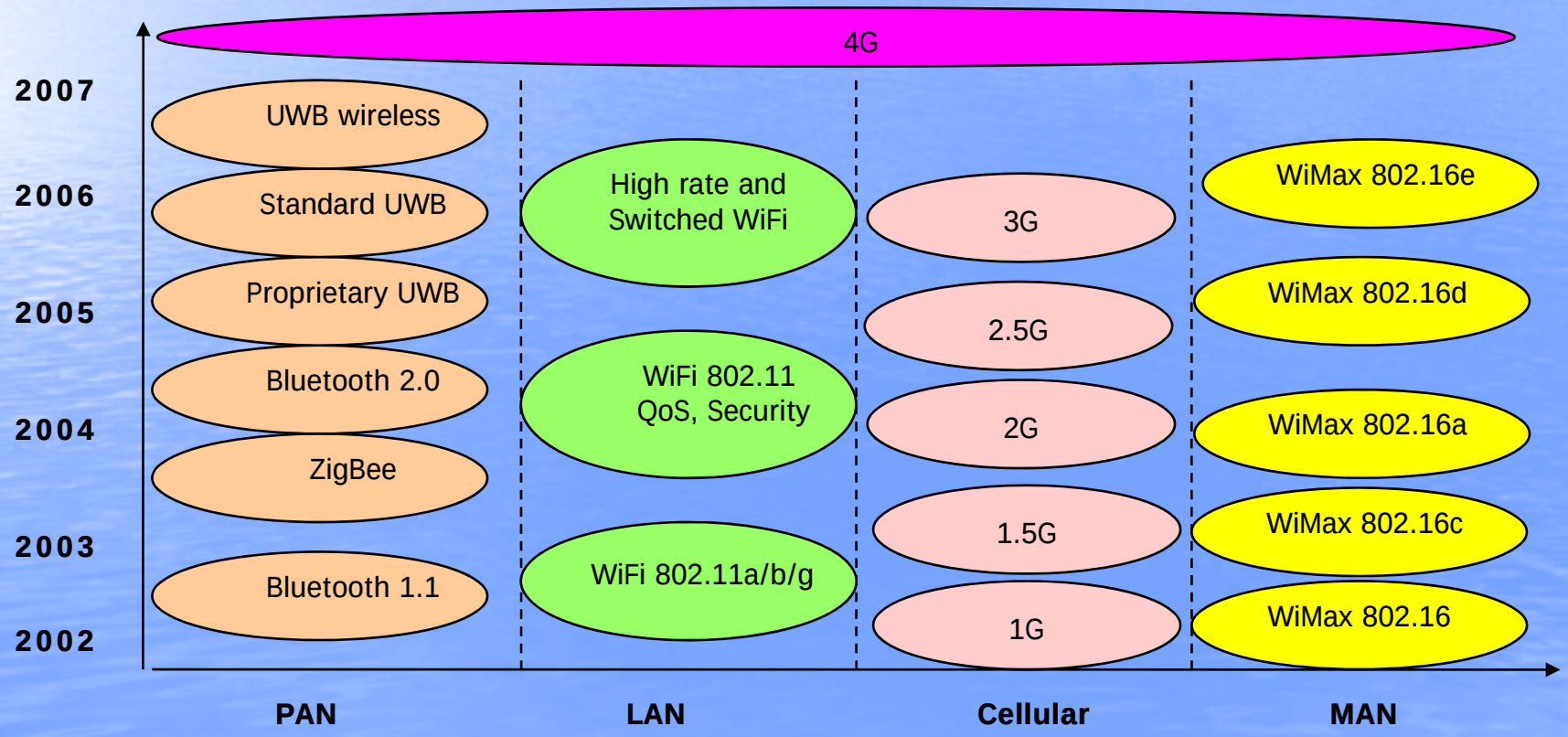
Definitions:

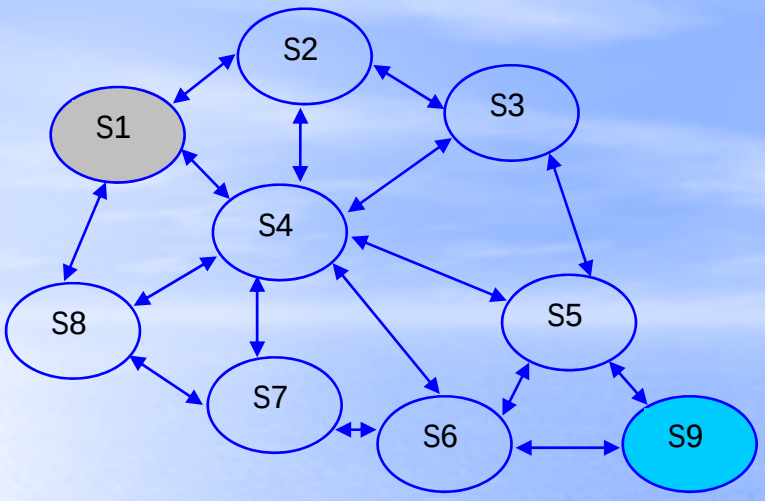
- **Wireless sensor network (WSN)** is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, motion or pollutants, at different locations. (Wikipedia,2008).

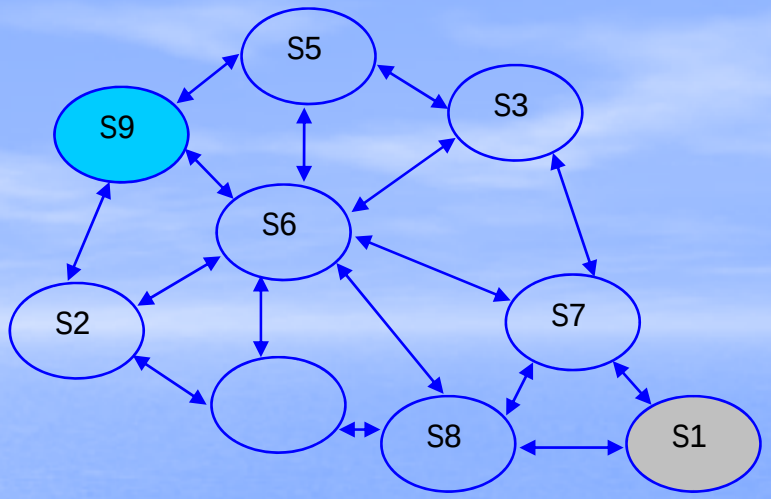
- **Quality of Service:** The ability of a network (including applications, hosts, and infrastructure devices) to deliver traffic with minimum delay and maximum availability.

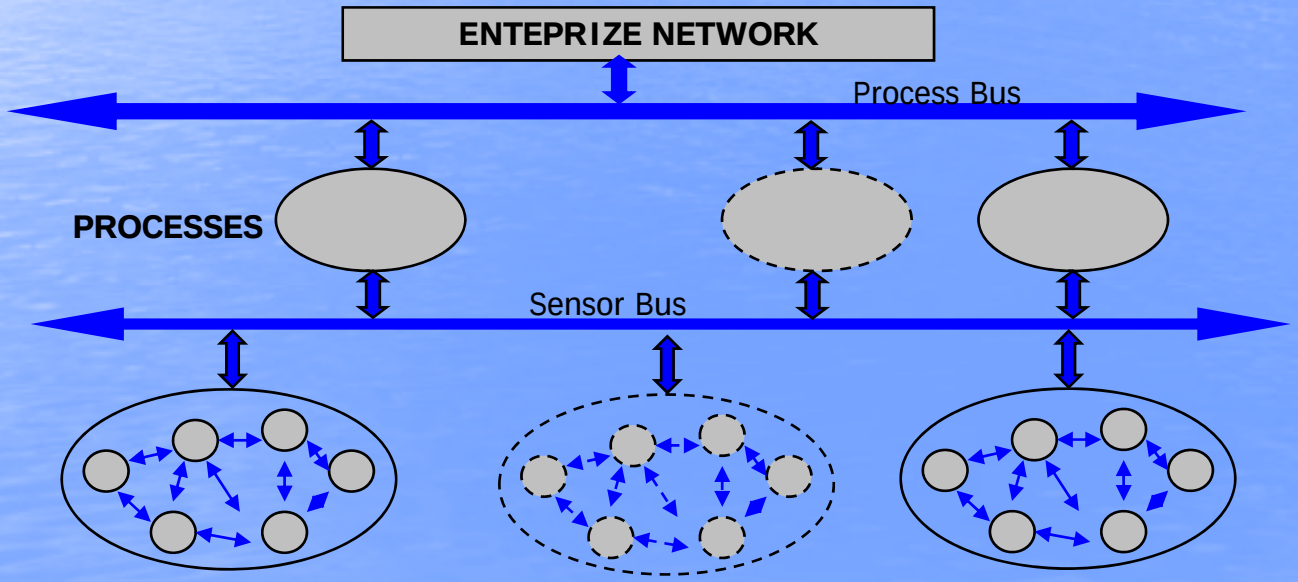
There are a few types of wireless sensor networks:

- Personal Area Networks (PANs)
- Local area Networks (LANs)
- Mobile networks such as cellular networks
- Extended LANs and Metropolitan (MAN) networks
- Telemetry, ultra-long distance, satellites, etc.




S1
S2
S3
S4
S5
S6
S7
S8
S9


S9
S5
S3
S6
S2
S7
S8
S1


ENTEPRIZE NETWORK
Process Bus
PROCESSES
Sensor Bus

Concerns of the industry

- ***Security*** is a major concern. Connecting a control system to web aggravates the concern. There have been cases of attacks that impacted control systems. (Encryption, frequency hopping, coding, etc.)
- ***Robustness, reliability and safety*** are major concerns. Failure of control systems can not be tolerable.
- ***Industrial espionage and cyber-terrorism***
- **Level of Quality of service**

PLCs

- Programmable Logic Controllers (PLCs) are extensively used and play important role in monitoring and controlling operations.
- Modern PLCs are use communications ports such as the RS232, RS485, usb, Ethernet.
- PLCs transfer real-time data to the system.
- Programming of PLCs is easy and effective coupled with the SCADA systems.
- Most PLC control systems are based on wired communication networks.

SCADA

- Supervisory Control and Data Acquisition (SCADA) is a term adopted by the process control industry to describe a collection of computers, sensors and other equipment suitably interfaced in order to monitor and control processes.

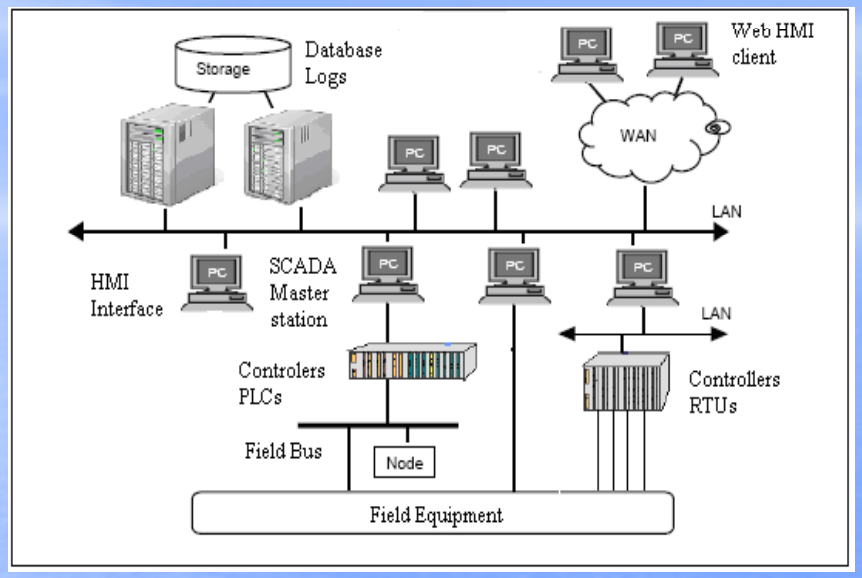
- Remote Terminal Units (RTUs) provide a Human Machine Interface (HMI) using Graphic User Interface (GUI). Operators, at the central stations are familiar with HMI software for the display of information coming from the sensors and transducers and other field device and they control of the process by using HMI.

- Data Storage is easy thus giving historical information about the performance of a particular sensor node

Case study

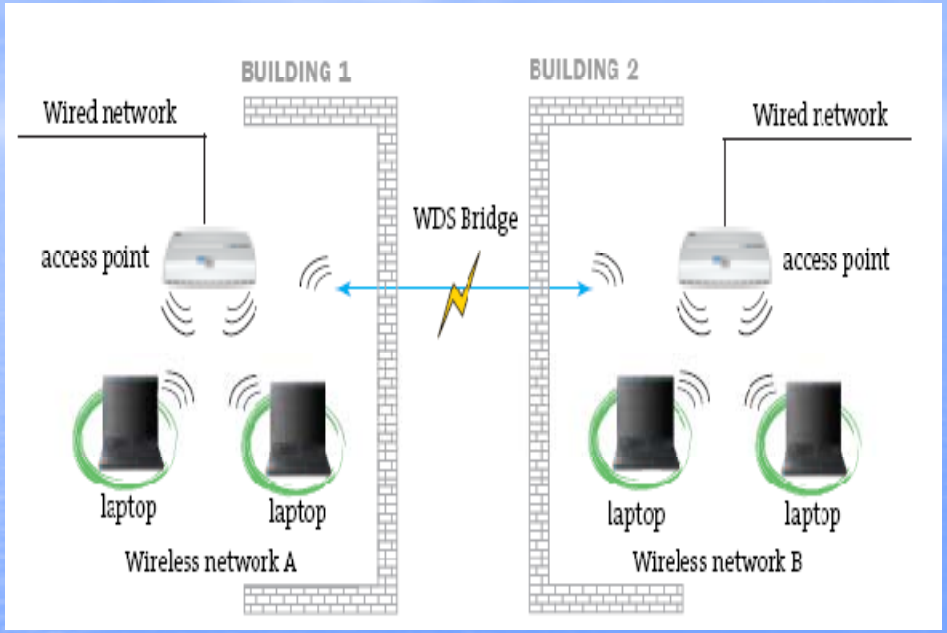
- A wireless network with 20 PLC/SCADA formed a Local Area Network, LAN.
- The link between PLCs and SCADA is based on OMRON Factory Intelligent Network Services (FINS) Gateway.
- FinsGateway allows instructions from one network to another, regardless of the protocol used on the network.
- FINS Commands are defined in the application level and do not depend on lower levels hence can be used across a variety of networks and CPU buses, specifically with Ethernet, Controller Link, and Host Link networks, and between CPU Units and CPU Bus Units.

System configuration



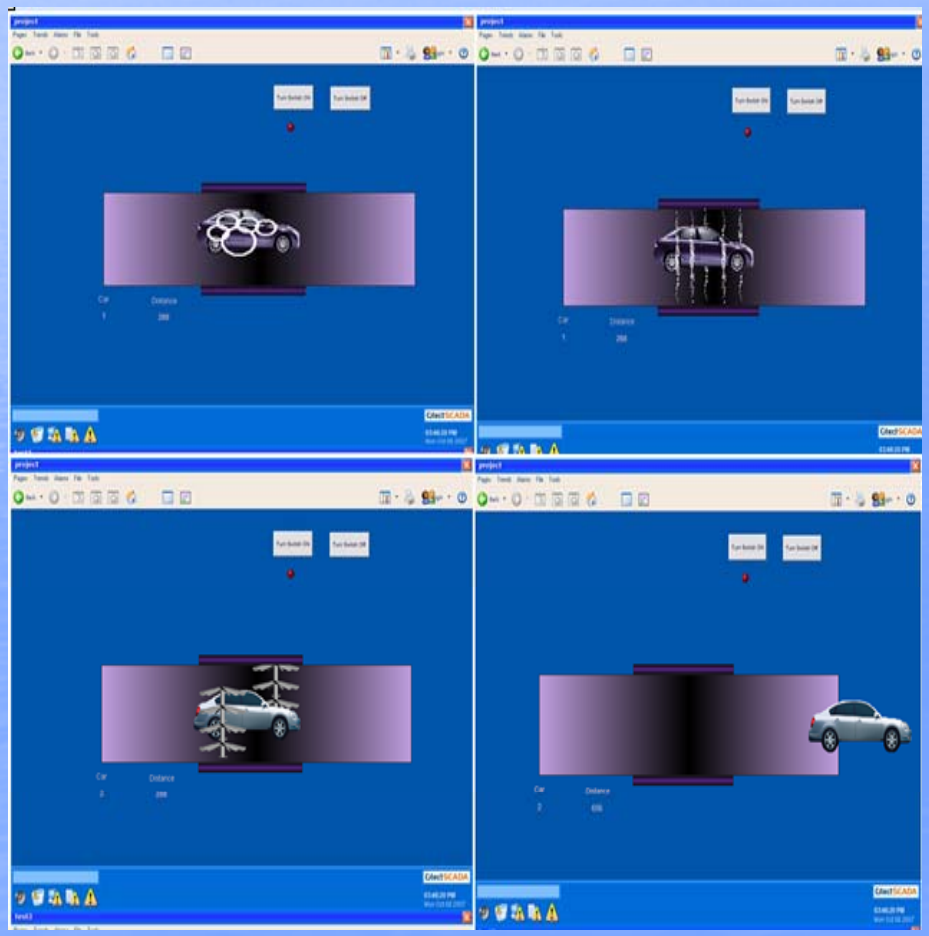
- **Wired configuration:** 20 computers and 20 PLCS communicate by Ethernet
- Any computer can access any PLC
- Computers communicate among themselves (but not PLCs)
- **Wireless configuration:** Any computer can access any PLC wirelessly

Experimental procedure

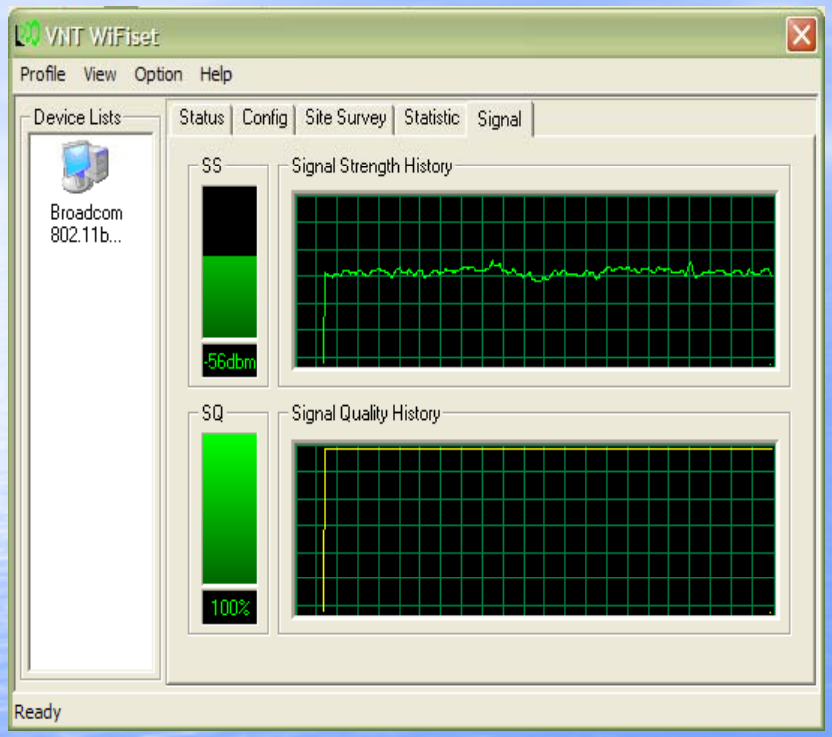


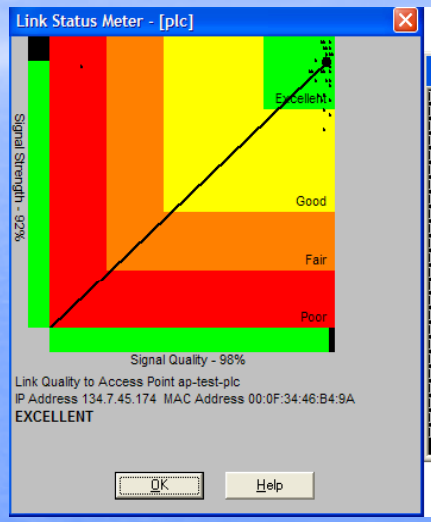
- Communication system was based on IEEE 802.11 standards Wi-Fi.
- The nodes were equipped with wireless Ethernet using RS-232 ports based on Cisco Airnet 1200.

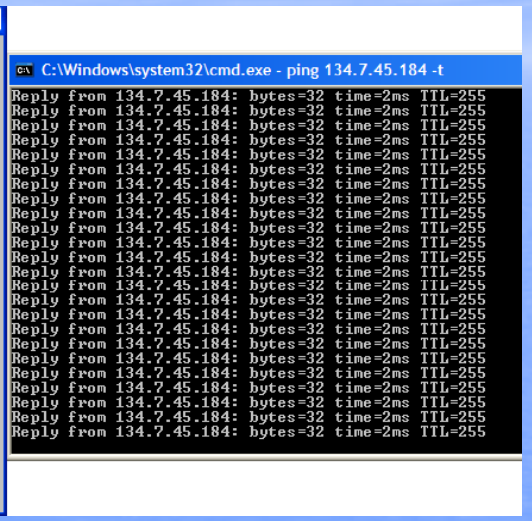
- PLC, SCADA and Wireless Network were integrated and ready to run the simulation of a Car Washing Process. The simulation could be operated by the PLC as well as from the control buttons on the HMI terminal.



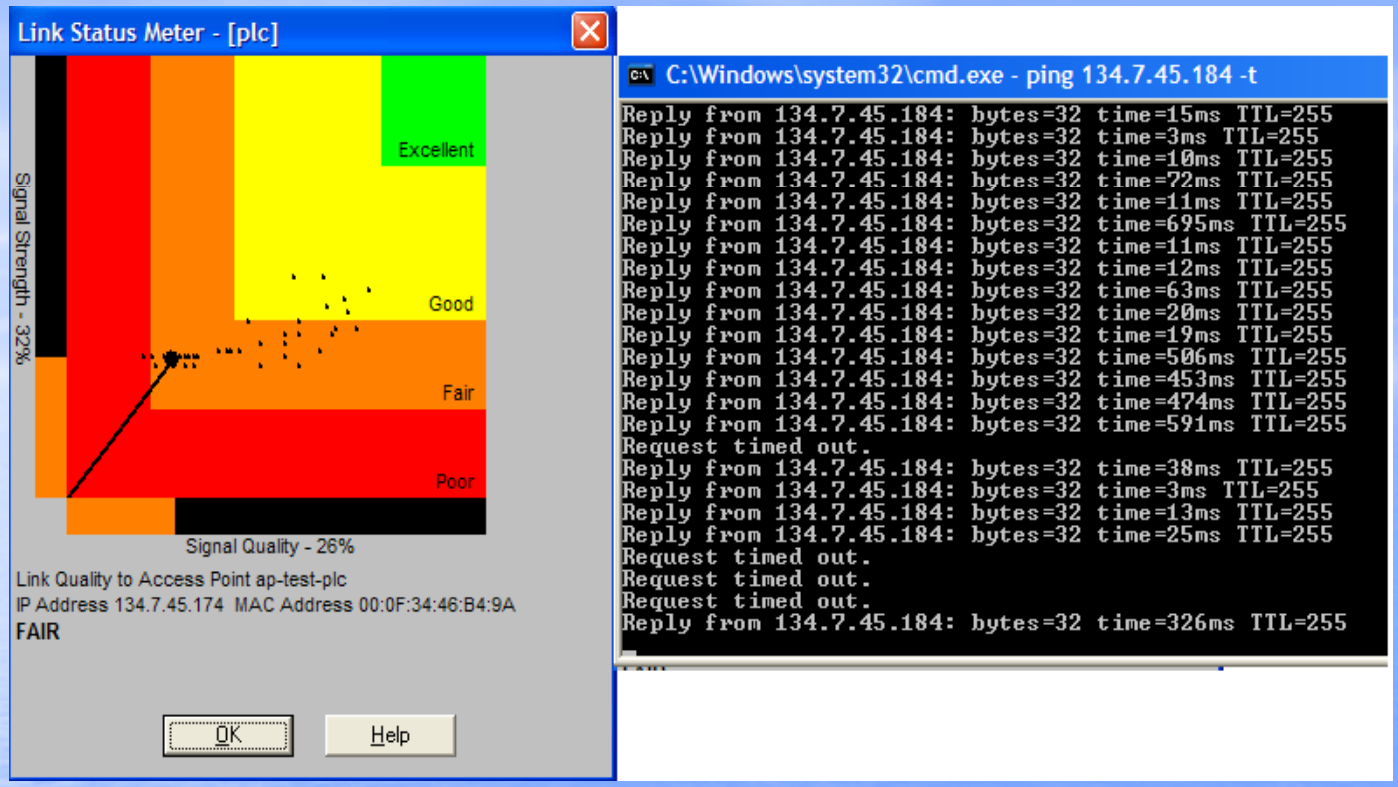
Results







- When the distance between the Access point and the wireless client was 10m the signal strength was measured as 92% with the response time of 2ms.



- When the distance between the Access point and the wireless client was 50m the signal strength was measured as with an inconsistent the response time. It was noted that after 600ms the connection dropped

- When the connection has dropped out, the tags in the output file did not match the tags results of the base file.
- When the laptop was moved few meters towards the Access Point, the connection was re-established.
- However, after the re-establishing connectivity the SCADA simulation did not run without re-initializing the FinsGateway services. When the error on the FinsGateway was cleared the application restarted.
- Restoring the FinsGateway services was about 30s, which may be unacceptable in industrial applications.
- Recovery (self-healing) of system is possible.

Conclusions

- Wireless industrial systems exist but not common.
- Security, reliability, and network management present problems not only from communication point of view but from the complete system integration point of view.
- Integration of the existing wireless technology with industrial requirements requires custom design and more research.
- For successful applications of Wireless systems in process control application characteristics and limitations must be determined carefully.