Why put security into automation networks?
Total Shipment of Industrial Ethernet Devices

(Thousands of Units)

CAGR = 51.4 Percent

Source: 2005

Security System

Authentication

Identification

Access Control

Authorisation

Switch / Router: MACH, MICE, RS

Firewall: EAGLE mGuard

Availability

Security

Tunnelling

Encryption
Typical scenarios in factory automation networks

At field level, **external employees** have unrestricted access to unused Ethernet ports for maintenance or repair purposes.
Maintenance By Third Parties

• Step 1 – Issue an IP address using DHCP
• Step 2 – Use firewall rules to limit access
The most dangerous hackers work in your own company.
EAGLE mGuard (1)

**Industrial Power**
- 9.6 ... 60 V DC
- redundant power supply
- signalling contact

**Optical Indication**
- status LEDs
- signalling contact

**Industrial Design**
- rail mountable
- no fan
- cUL508, GL

**USB Port**
- auto configuration adapter

**Serial Port**
- V.24 console
- remote dial-in

**Various Interfaces**
- twisted pair
- multi-mode
- single-mode
- long haul

EAGLE mGuard (2)

**Hardware & Software**
- Intel XScale IXP, 533 MHz
- 16 MB Flash, 64 MB DRAM
- hardware encryption
- Linux

**Various Topologies**
- routing
- multi-client transparent (stealth mode)
- 1:1-NAT
- router redundancy
- redundant ring coupling
- dual homing, STP

**Broad Functionality**
- stateful inspection firewall
- router & IP-masque
- VPN (250 tunnels)
- virus scanner

**Features**
- MAC-Filter
- VLAN support
- L3 redundancy
- DHCP relay
- X.509-support
- virus scan http, ftp, smtp, pop3

**Secure Management**
- GUI (https), CLI (ssh)
- HiDiscovery
- HiVision (LLDP)
- SolSoft plug-in (ISCM)
How can I protect my network?

**Functions**

- **Basic**
  - Protects against attacks from insecure networks
  - Hides the internal network structure

- **Advanced**
  - **Access control:**
    When and how may computers communicate with each other
  - **User control:**
    Which users can access which services
  - **Protocol and Services control:**
    Which protocols and services can run over which port
  - **Data control:**
    Which data can be transmitted and received
  - **Logging, Accounting and Auditing**
  - **Alarming during attacks**
  - **Antivirus support**
Function: Stateful Inspection

Insecure → Secure

Reply ← Ping → Reply

Ping ← X → Reply

Function: Packet Filtering

• Accept or discard data based on IP address or protocol
• 99% wire speed
Function: MAC Address Filtering

- Accept or discard data based on source/destination MAC address

Function: Site to Site VPN

- Hardware encryption
- 70 Mbps throughput
- Multiple VPN tunnels
- Pre-Shared Key (PSK) or Certificates
EAGLE Remote Access with Service Network

Office Network

Service Network

Laptop (hotel, home...)

DSL-Modem

Router/Firewall Option

DSL-Modem Public IP address

Internet

PTSN

GPRS

PC

Factory Network (Option)

Factory Network 1

Trusted side

Untrusted side

Eagle

PLC

DSL-Modem Dynamical IP Address

Connection to the Internet

Factory Network 2

Trusted side

Untrusted side

Eagle

PLC

DSL-Modem Dynamical IP Address

Connection to the Internet
EAGLE Remote Access without Service Network

Office Network
- VPN client software needed inside all PC.
- (Klinkmann instructions are made for NCP Secure Entry Client)

Laptop (hotel, home...)

Internet

DSL-Modem

Public IP address
(port forwarding)

Connection to the Internet

Factory Network (Option)

PC

Untrusted side

Trusted side

Factory Network 1

Eagle

PLC

Factory Network 2

Eagle

PLC

Connection to the Internet

DSL-Modem

Public IP address
(port forwarding)

Internet

GPRS

PTSN

Modem

Untrusted side
Pre-Shared key (PSK)

- User defined key
- To achieve a good security level, the key should be approx. 30 characters long (made up of upper and lower case letters and digits).
- Both ends of the tunnel will use the same key
- EAGLE needs public IP address at both ends of tunnel.
EAGLE Authentications

X.509v3 Certificate

- This method is supported by most of the newer IPsec implementations and is currently considered the most secure.

- Private and public certificate are needed for each EAGLE. For example:
  
  - Private certificate of EAGLE 1 is installed as Machine certificate to the EAGLE 1 and it is used for decryption for data coming from EAGLE 2.
  
  - Public certificate of EAGLE 1 is installed to EAGLE 2 as connection certificate and it is used for encryption of data which is sent to the EAGLE 1.

  - Private certificate of EAGLE 2 is installed to the EAGLE 2 and public certificate of EAGLE 2 is installed to the EAGLE 1

- No public IP address needed in remote side
EAGLE X509 Certificates

Service Network

PC

Eagle 1

Trusted side

Untrusted side

DSL-Modem
Public IP address

Internet

Eagle 1

Trusted side

Eagle 1 Private Certificate for decryption
.P12 or pfx file

Eagle 1 public Certificate for encryption
.pem or .cer file

Internet

Factory Network (Option)

PC

Eagle 2

Trusted side

Eagle 2 Private Certificate for decryption
.P12 or pfx file

Eagle 2 public Certificate for encryption
.pem or .cer file

Factory Network 1

Untrusted side

DSL-Modem
Dynamical IP Address

Connection to the Internet

PLC
EAGLE IP Addressing

• VPN tunnel connects service network and factory networks from remote sites to the same network

• Eagle work as router between those networks

• Remote sit addressing can be made using Direct Addressing or using 1-1 NAT

Direct addressing

• Each remote site gets own subnet

• Remote sites are accessible same address locally and from service network

1.1 NAT

• Each remote sites use locally same Subnet addresses

• EAGLE will Transfer remote sites to individual subnet addresses using 1-1 NAT

• Site is accessible different address locally and from service network
EAGLE Direct Addressing

Service Network

PC
IP 10.0.0.2/24
PC
IP 10.0.0.3/24

DSL-Modem
Public IP address

Untrusted side

Internet

Connection to the Internet
DSL-Modem
Dynamical IP Address

PC

Factory Network (Option)

PC

Factory Network 1

Eagle
IP 10.0.1.1/24

PLC 1
IP 10.0.1.3/24

PLC 2
IP 10.0.1.4/24

Factory Network 2

Eagle
IP 10.0.2.1/24

PLC 1
IP 10.0.2.3/24

PLC 2
IP 10.0.2.4/24
EAGLE 1-1 NAT Addressing

Service Network

Internet

DSL-Modem
Public IP address

Eagle
Untrusted side

IP 10.0.0.1/24

PC

IP 10.0.0.2/24

PC

IP 10.0.0.3/24

Internet

Connection to
the Internet

DSL-Modem
Dynamical IP
Address

Factory Network
(Option)

PC

Factory Network 1

Eagle
IP 10.0.1.1/24

PLC 1
IP 10.0.1.3/24

PLC 2
IP 10.0.1.4/24

1-1 NAT from
10.0.11.0/24 to
10.0.1.0/24

1-1 NAT from
10.0.12.0/24 to
10.0.1.0/24

Factory Network 2

Eagle
IP 10.0.1.1/24

PLC 1
IP 10.0.1.3/24

PLC 2
IP 10.0.1.4/24

1-1 NAT from
10.0.11.0/24 to
10.0.1.0/24

1-1 NAT from
10.0.12.0/24 to
10.0.1.0/24

Factory Network (Option)

Connection to
the Internet

DSL-Modem
Dynamical IP
Address