White paper:

Security concepts

based on EAGLE system

Contents

Security concepts

based on EAGLE system

Contents

Security-concepts based on EAGLE system

1 Introduction

1.1 The company's own employee – a security risk?

In the year 2004 a 17 year-old schoolboy detected a lack of security loop in Windows XP operating system and created the "Sasser" worm, allowing access to terminals and switching them off, because Microsoft inadvertently had not secured port 445.

The expenditure of time for programming this worm was probably just one night, the resulting damage however amounted to millions. Meanwhile, the technical inadequacies were eliminated by Microsoft responding with a patch, and worms from external networks are now usually trapped by a company's central firewall.

The above case of Sasser affected the production departments of many company's to the same extent as the administration departments, since today many industrial controls are based on Microsoft operating systems. In this case, the security model of the central firewall failed, because the malicious software was inadvertently brought along by employees using their laptops outside of the company. Thus the infected laptops - after re-connecting them within the company – allowed the worm to infect the entire network. The company's own employee – a security risk without intention.

The scenario can be extended: from employees to suppliers, who are often also inside the company, to visitors, who find access to a companies' network in the conference rooms. The source of danger does not necessarily arise in combination with the malicious software. Often times access via a standard browser is sufficient to inadvertent connect to the network. Therefore only a local security mechanism can offer effective protection of production or manufacturing facilities which must be permanently in operation.

1.2 Which customer problem is solved?

In factory default the EAGLE is configured for transparent mode and “stateful-inspection”. Thus, only data requested from inside reaches the secured network. Additionally rules can be defined with port filters, in order to close the known gaps. In the previously mentioned example with “Sasser”, the worm would not have been transmitted through the EAGLE, because port 445 would have been inaccessible.

The EAGLE can limit network access to specific IP addresses and services. Only authorised users have access to the secured net from outside.

Using the EAGLE family together with various security services, an open, industrial specific and defined communication from the management level to the field level is supported. Through network segmentation, the EAGLE family provides comprehensive protection for all current and future applications.

1.3 Identification of the potential

Security implementations for industrial networks often require features which are above and beyond those normally used in a standard office environment. These features are relevant to all of Hirschmann’s focus industries such as process, factory and traffic automation. In addition as the result of vertical integration, more and more industrial applications will be developed with Ethernet.

Decentralised security architecture based on the EAGLE family is particularly of interest, when data security in industrial networks is required, to protect unintentional and unwitting attacks from inside the network:

- Secure remote access to machines (tooling and printing-machines)
- Inter location networking of factories (including via the “insecure” Internet)
- Networking of wind parks (also off-shore)
- Secure cell separation in networks in the automotive or mechanical engineering industries

As a matter of fact the EAGLE stands on one hand for a supplementation of existing security mechanisms like centralised firewalls and virus-scanning software and on the other hand for an independant factory security policy attempt.

2 Safety factor in your company’s network: The EAGLE system.

2.1 Made for Security

The EAGLE family was conceived as a series of individual devices for security applications, and the operating system, management, etc., reflects this purpose.

Advantage: The security mechanisms can be designed into the network decentrally, therefore providing a better overview. A reference to the respective and to be protected cell or the to be protected end-device can be established. In addition no complex access lists or firewall rules need to be maintained in the backboneLocal and remote logins provide the ability to analyze and constantly optimize the data transmission.

The system supports Hirschmann’s Redundant Ring Coupling and Dual Homing redundancy mechanisms.

2.2 Feature overview

2.2.1 Scalability of the security functionality

- Firewall
- Firewall with VPN functionality

The firewall is for defining ports in the operating system. A port typically is a protocoll (like FTP, HTTP, SNMP) whit the options of access allowed and denied. For using Eagle as firewall, please refer to User Scenario 3.1 „Secured Service Port“. For using Eagle in combination with a VPN tunnel, please refer to User Scenario 3.5 „Remote access via V.24 interface and external modem“.

2.2.2 Simplest integration in existing networks without changes of IP addresses

- Single client transparent mode (SCT)
- Multi client transparent mode (MCT)

Single and multi client transparent modes are used in Layer-2 networks especially. The modes will provide security to a network configured as „flat“ L2 architecture without the need to change configuration in terms of IP address assignment. For using Eagle in combination with single and multi client transparent modes, please refer to User Scenario 3.1 „Secured service port“ or 3.2 „Secure cell separation“.

2.2.3 Separation of sub-networks – generating „Compartments“

- Router mode
- 1:1 NAT (Network Address Translation)

Router mode is used in Layer-3 networks especially. The modes will provide security to a network configured as performant L3 architecture typically due to the very high amount of ports and users being part of network. Router mode typically causes the need of changing configuration in terms of IP address assignment. For using Eagle in combination with router mode, please refer to User Scenario 3.3 „Secure connection of networks compartments“. For using Eagle in combination with NAT, please refer to User Scenario 3.4 „Operating identical network segments by using 1:1 NAT“.

2.2.4 Support of Hirschmann redundancy scenarios

- Redundant Ring Coupling
- Dual Homing
- Virtual Router Redundancy Protocol (VRRP)
- Spanning Tree Protocol (STP)

Redundancy protocols are typically used to enhance the reliability of networks and finally the availability of network services. There are several protocols to name. . For using Eagle in combination with VRRP, please refer to User Scenario 3.6 „Router Redundancy using VRRP“. For using Eagle in combination with STP, please refer to User Scenario 3.9 „Supporting STP (Spanning Tree Protocol.) Redundancy“.

2.2.5 Simplest implemention

- Support of HiDiscovery
- Support of auto configuration adapter

2.2.6 Industrial design

- Redundant 24V power supply
- DIN Rail mountable
- IP 20 (without fan)

2.2.7 Extensive diagnostic facilities

- Web-based management
- Status LED’s
- Alarm Relay
- Logging on SysLog Server
- Integration in HiVision

For using Eagle in combination with Alarm Relay, please refer to User Scenario 3.8 „Security providing by optical indication“.

2.2.8 Migration in existing networks

Twisted Pair and fibre connections for
- Secured port
- Unsecured port

2.2.9 Remote access to the network

- Remote Access via V.24

For using Eagle in combination with Remote Access via V.24, please refer to User Scenario 3.5 „Remote access via V.24 interface and external modem“.

3 Typical user scenarios

The most frequently used applications in industry require the operation of the EAGLE in one of the following modes:

- Transparency mode on layer 2 (multi client, single client)
- Router mode on layer 3

Typical user scenarios:

- Secured service port
- Secure cell separation
- Secure connection of networks
- Remote access over VPN tunnel

3.1 Secured service port

Secure access for initial configuration or external employees is realized using an integrated DHCP server.
Configuration:
Network mode of the EAGLE: SCT, MCT or router mode

- Within the router mode the EAGLE needs to be configured as the standard gateway on the secured port of the connected client computer.
- Configuration of the EAGLE as DHCP server: enter the MAC IP relationship on the unsecured port
- Definition of firewall rules for the IP addresses provided by the DHCP server

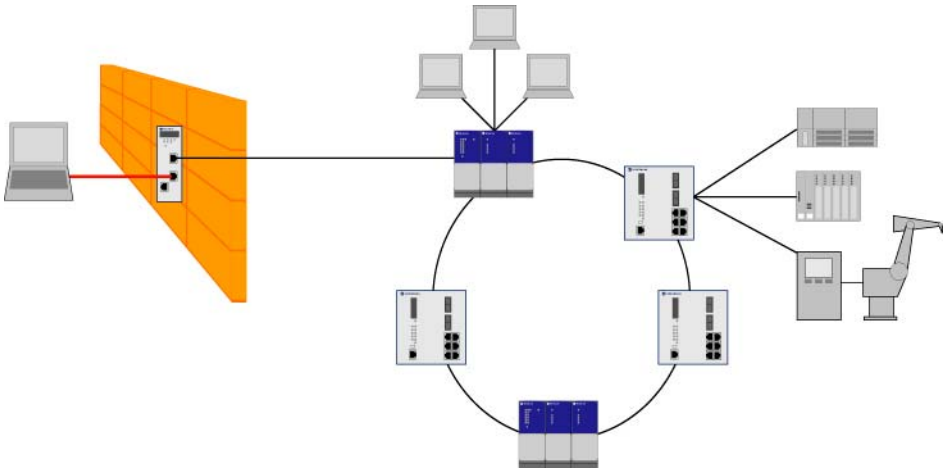


Figure Security-1: Example of the secured service port

3.2 Secure cell separation

Configuration 1:

Network mode of the EAGLE: multi-client transparency mode

- Use in existing networks without modification of current IP configurations.
- Establish firewall rules for controlled access between backbone and cell or between the cells.

Configuration 2:

Network mode of the EAGLE: router-mode

- Within the router mode the EAGLE needs to be configured as the standard gateway on the secured port of the connected client computer.

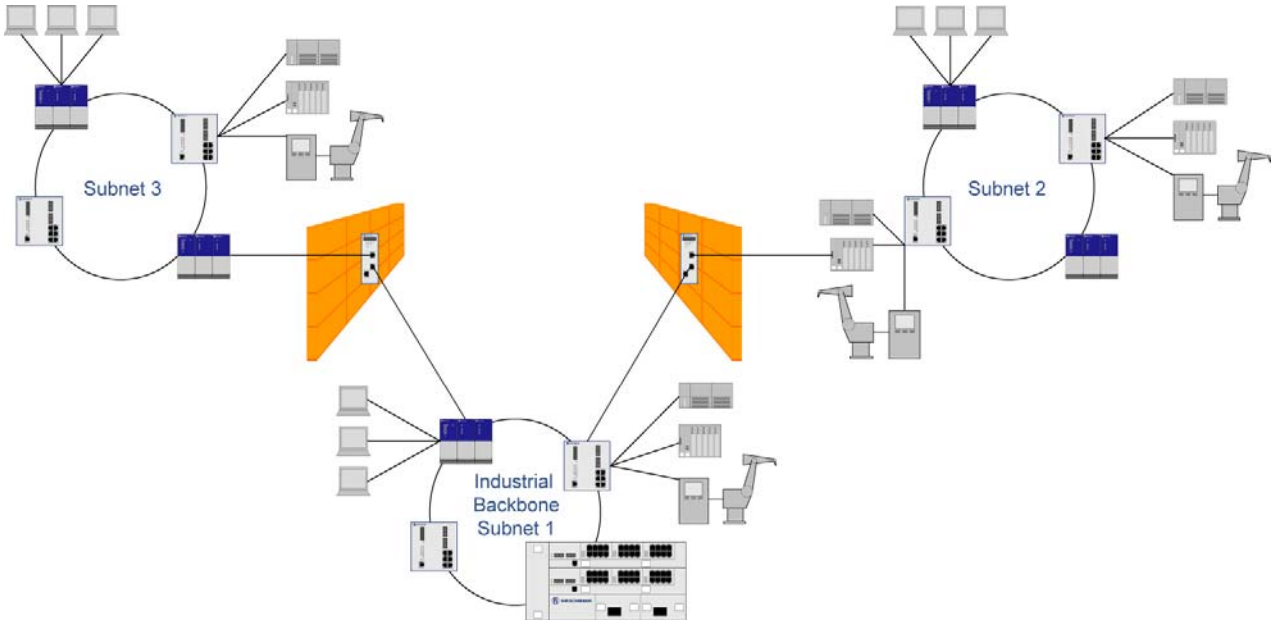


Figure Security-2: Example for secure cell separation

3.3 Secure connection of networks compartments

Configuration:

Network mode of the EAGLE: Router

- Within the router mode the EAGLE needs to be configured as the standard gateway on the secured port of the connected client computer.
- When using a DSL modem, PPPoE settings need to be configured

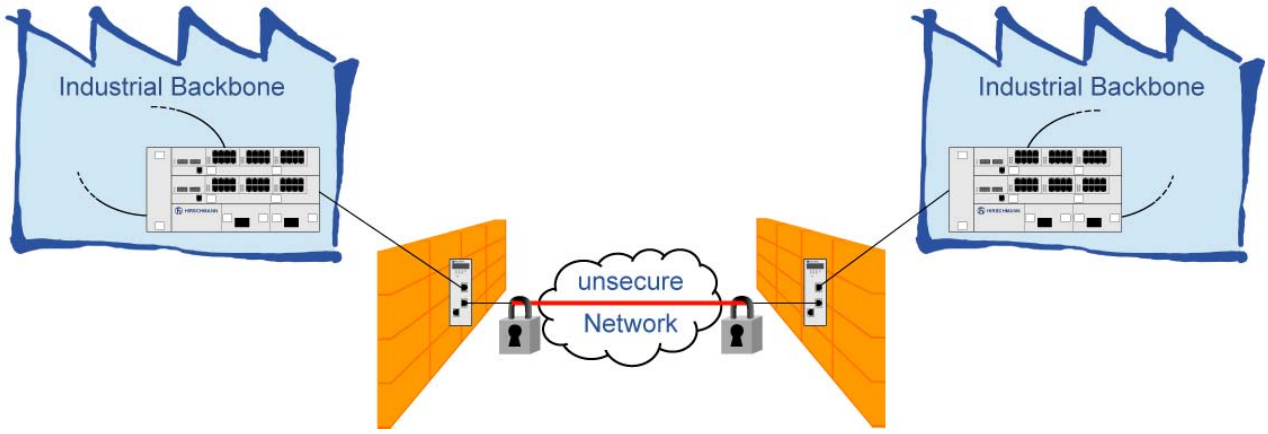
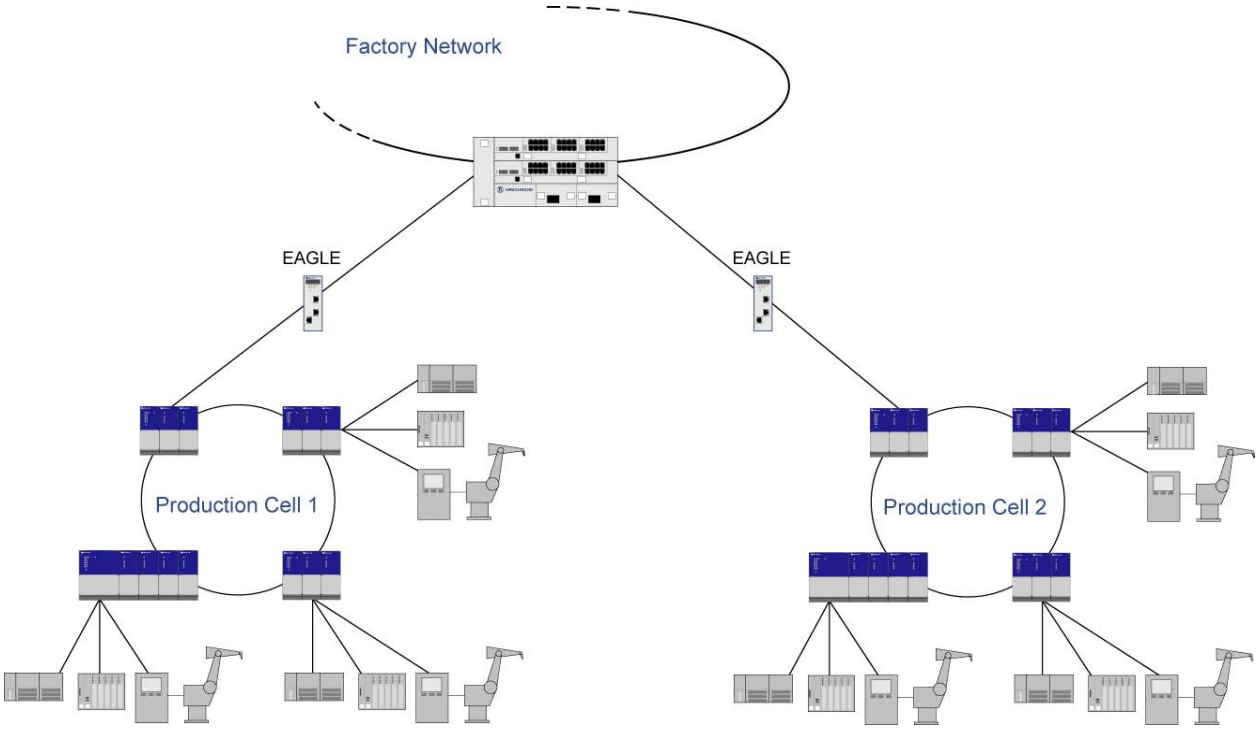


Figure Security-3: Example of a secure connection between networks

3.4 Operating identical network segment by using 1:1 NAT

In some special applications it is appropriat to configure network compartment identically, even by using the same IP addresses. In order to do so, the device connecting this compartment to the overlayed network need to support a mechanism for masquerading IP addresses. The Eagle is capable of performing this feature by supporting 1:1 NAT (Network Address Translation).

Configuration:



3.5 Remote access via v.24 interface and external modem

On the remote computer an extra VPN client needs to be installed. Windows 2000/XP contains the VPN client.

Configuration:

Network mode of the EAGLE: single client transparency or router

- Within the single client transparency mode no modification of the connected computer's TCP/IP configuration is necessary.
- Within the router mode the EAGLE needs to be configured as the standard gateway on the secured port of the connected client computer.

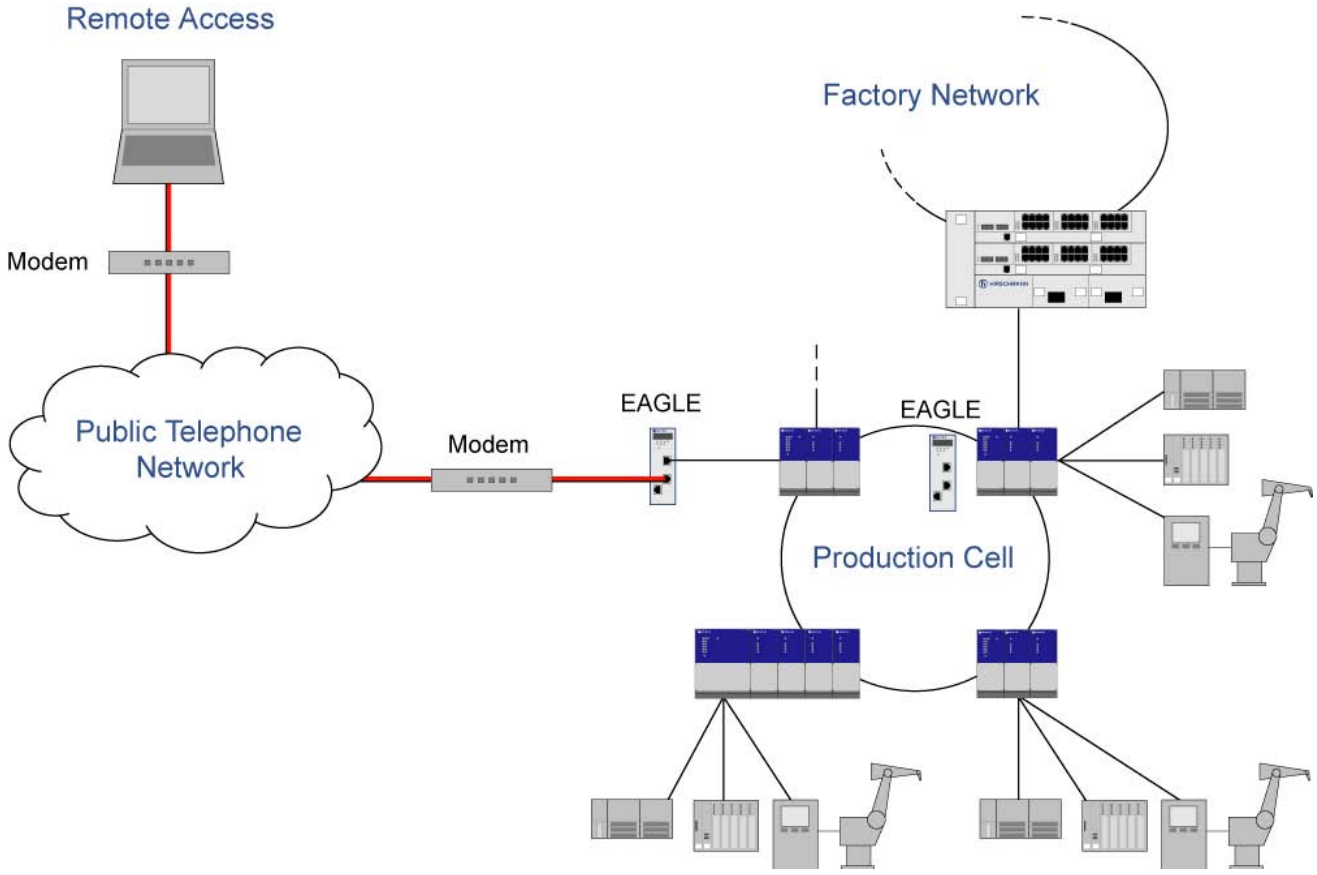
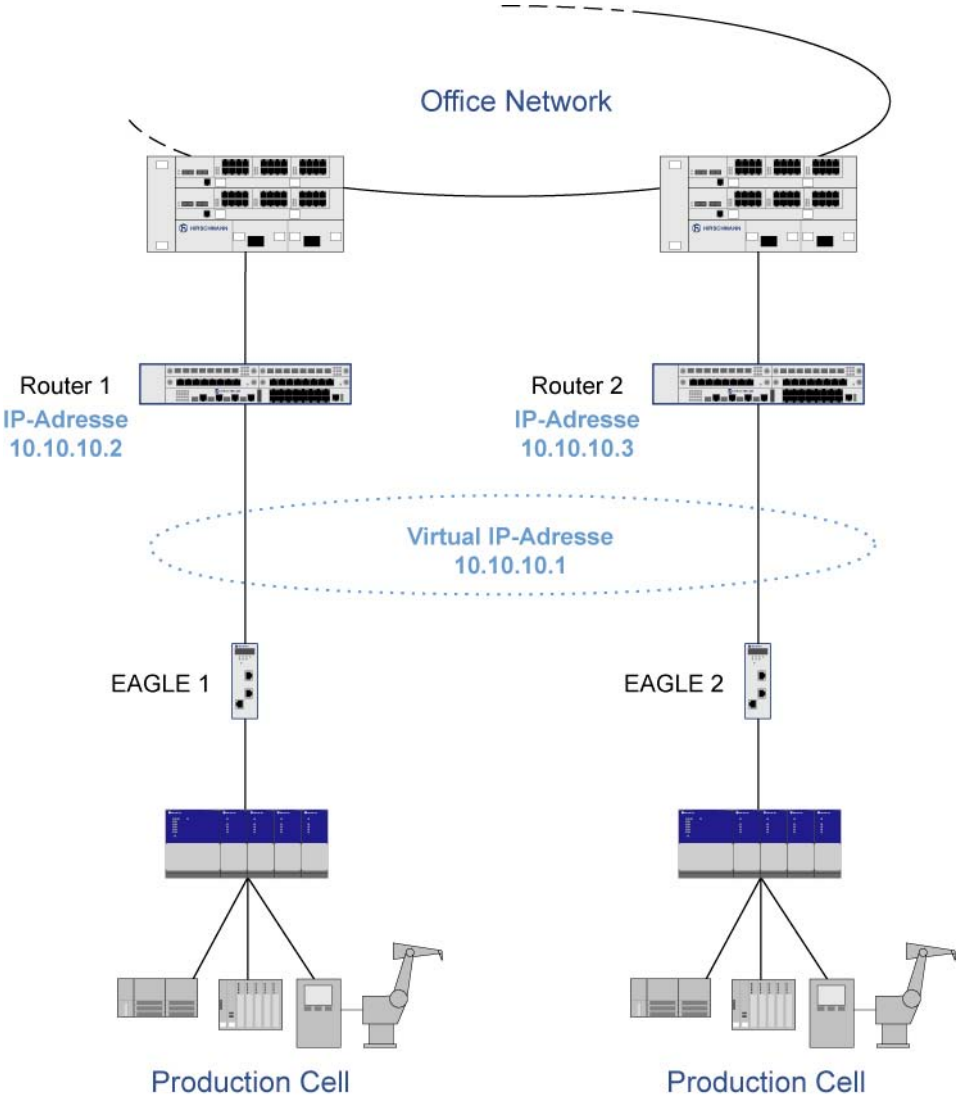


Figure Security-4: Example of remote access using a VPN tunnel

3.6 Router Redundancy using VRRP

Large networks oftentimes are configured as Layer-3 topologies. When adding redundancy to a Layer-3 network, it is very common to use the Virtual Router Redundancy Protocol (VRRP). In order to be able adding security to an existing L3 network operating VRRP, the Eagle supports the VRRP protocol.

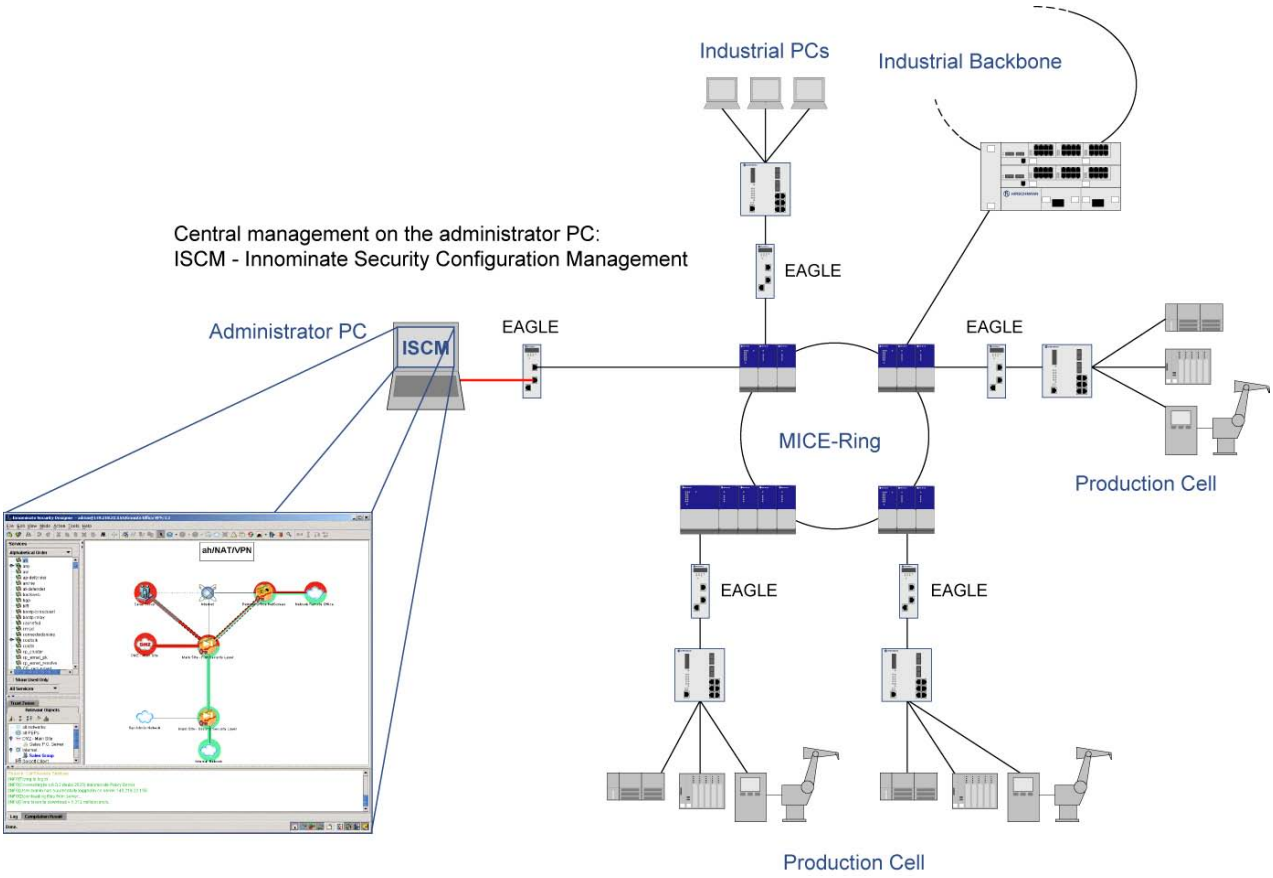
Configuration:



3.7 Centralized Management

In large network installations, the amount of compartment and even the amount of Eagle devices are that high that configuration and especially reconfiguration of security options is time consuming. In order to minimize the efforts for this kind of network, it is possible to use the centralized management shell ISCM (Innominate Security Configuration Management).

Configuration:

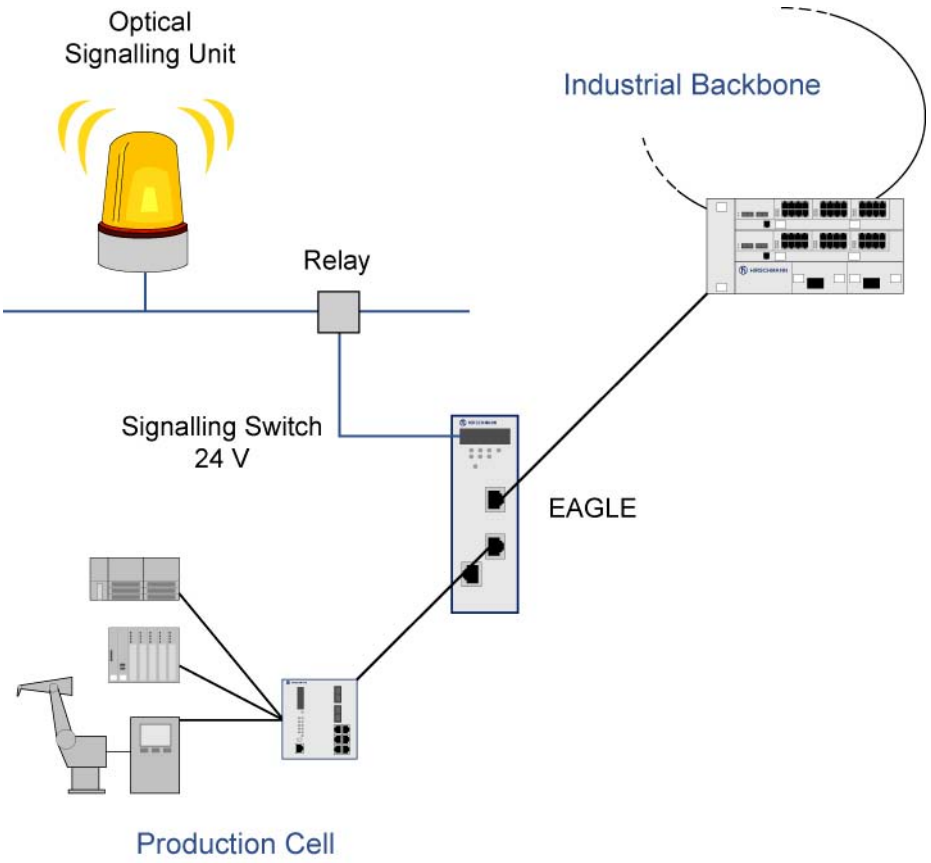


3.8 Security providing by optical indication

A flashing alarm lamp or a warning beacon will indicate an infringement of firewall rules, i. e.

- attempt to access to a network compartment illegally (identified by MAC or IP address)
- attempt to use a not allowed port of the network (for example using the protocol FTP although firewall rules declining access)

Configuration:



3.9 Supporting STP (Spanning Tree Protocol) Redundancy

Eagle system is supporting STP redundancy by allowing BPDU (bridge protocol data unit) to pass. BPDUs are data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. Eagle system is transparent for these BPDUs, and as a result, STP can be supported.

The end user will profit by being able to use existing redundant network topologies without the need to reconfigure due to adding network security. Especially if large topologies are configured as “flat” L2 networks, it could be high effort to change this network architecture from L2 to L3.

Configuration: