

CONNECTED

Trendy

Wymagania i zadania

Przykłady rozwiązań i zastosowań



Bezpieczna transmisja danych
w układach automatyki –
zdalna diagnostyka układów
CNC

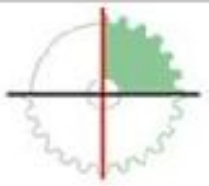
Chcemy stosować nowe technologiczne trendy w Automatyce

Trendy

Wymagania

Przykłady

- **Trendem jest odchodzenie od struktur systemów sterowania scentralizowanych do systemów rozproszonych realizujących zadania lokalnie**
- **Powyższe stwierdzenie**
- **Ethernet jest stosowany na wszystkich poziomach automatyki**
- **Wzrastające zastosowanie otwartych standardów w automatyce**
- **Techniki informatyczne i automatyka rozwijają się ściśle razem**



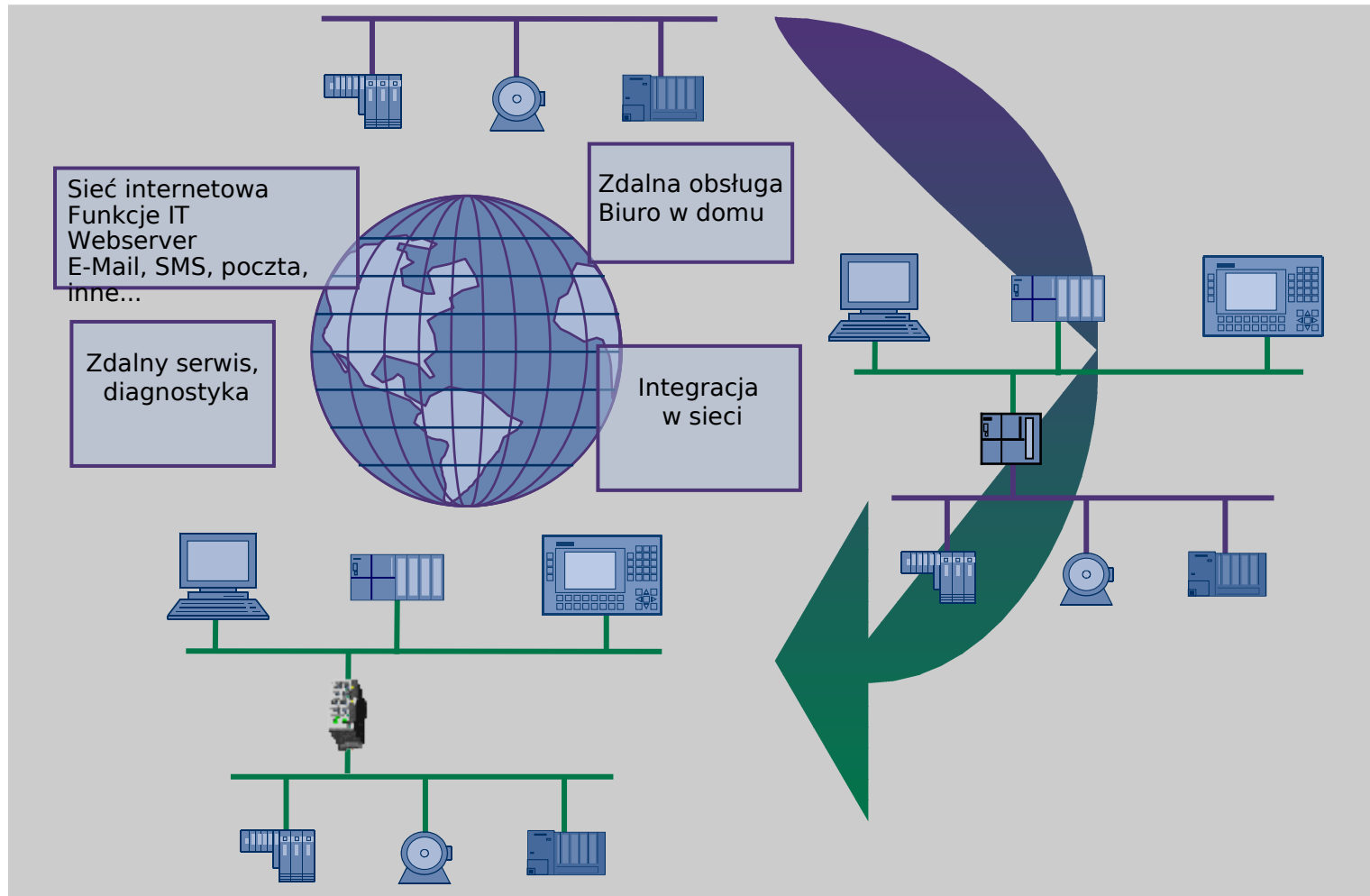
klub paragraf 34

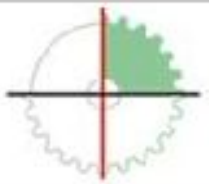
Trendy w Ethernecie...

Trendy

Wymagania

Przykłady





klub paragraf 34

Badania firmy Consultic: Ważność bezpieczeństwa sieci

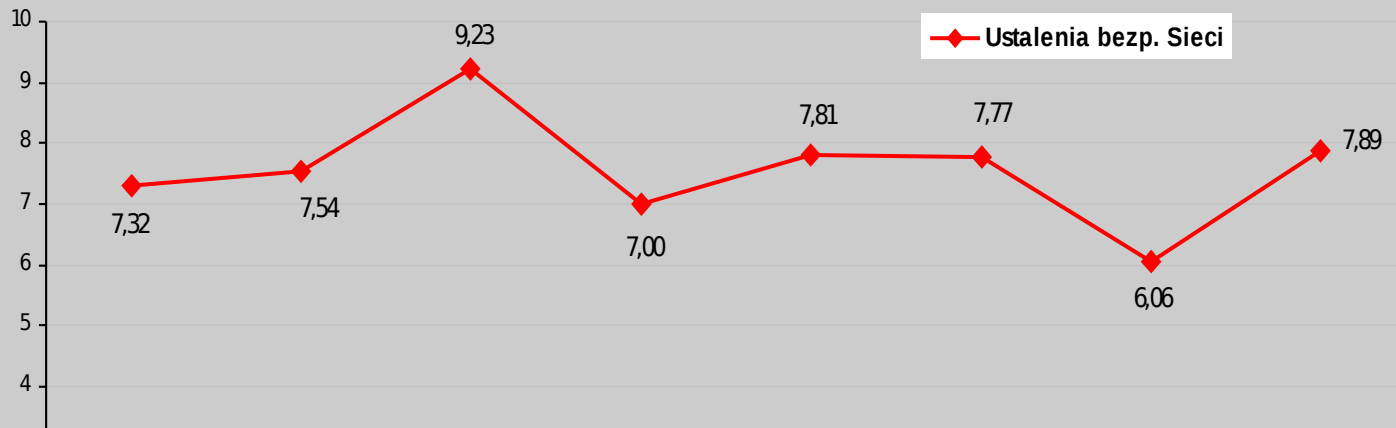
consultic

Trendy

Wymagania

Przykłady

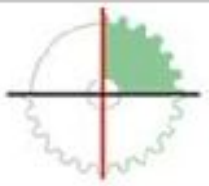
Bardzo ważne



Mało ważne

Przemysł spożywczy Przemysł Chemiczny Przemysł Samochod. Przem. Drukarski Elektrownie Przem. wytwórczy Engineering Budown.

Badania wykonane dla Siemens A.G.



klub paragraf 34

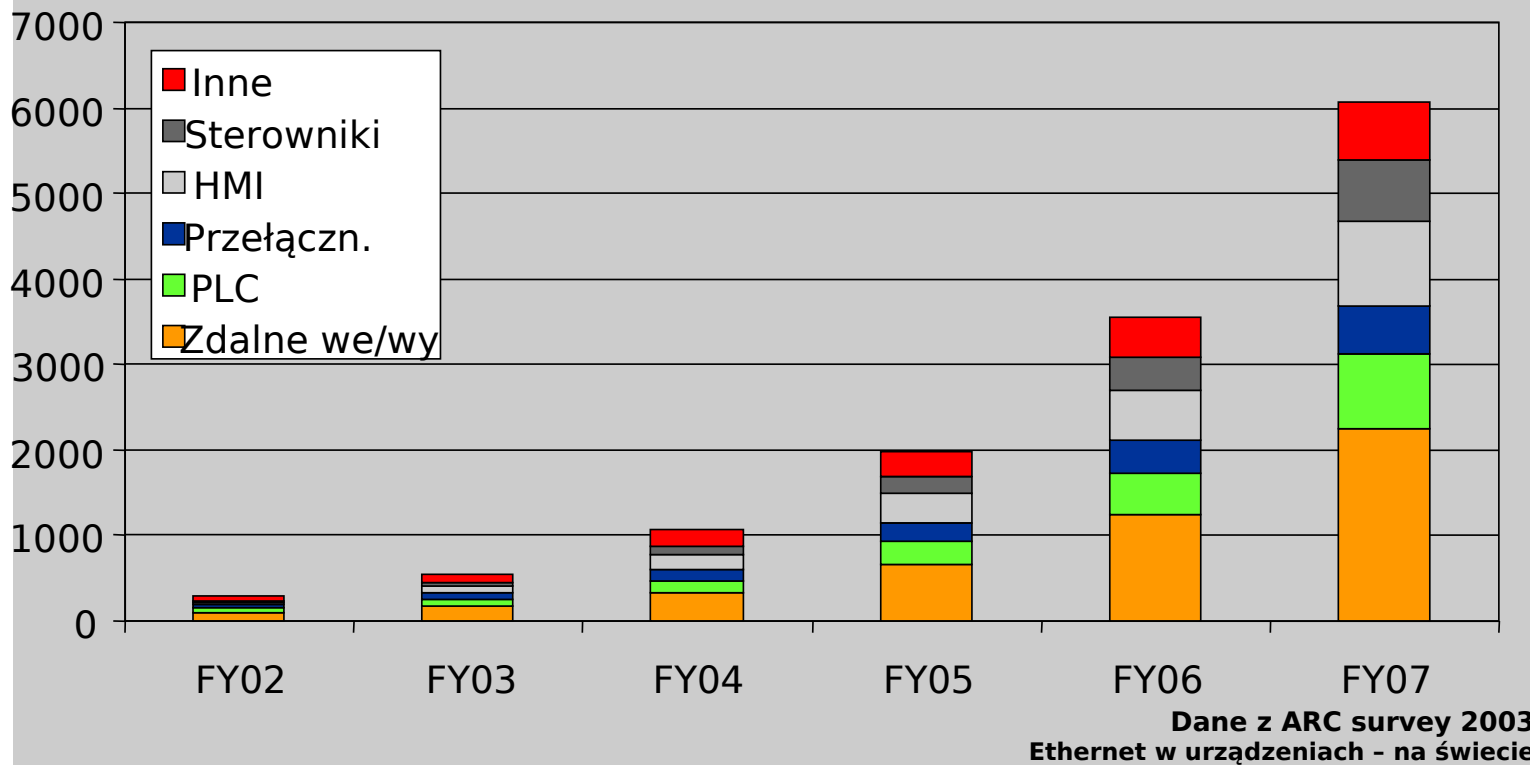
Potencjał dostaw urządzeń Ethernetu dla przemysłu

Trendy

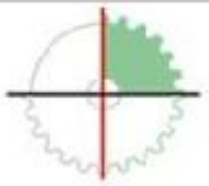
Wymagania

Przykłady

Dostawy urządzeń Ethernetowych na świecie



Silny wzrost o 84 %



klub paragraf 34

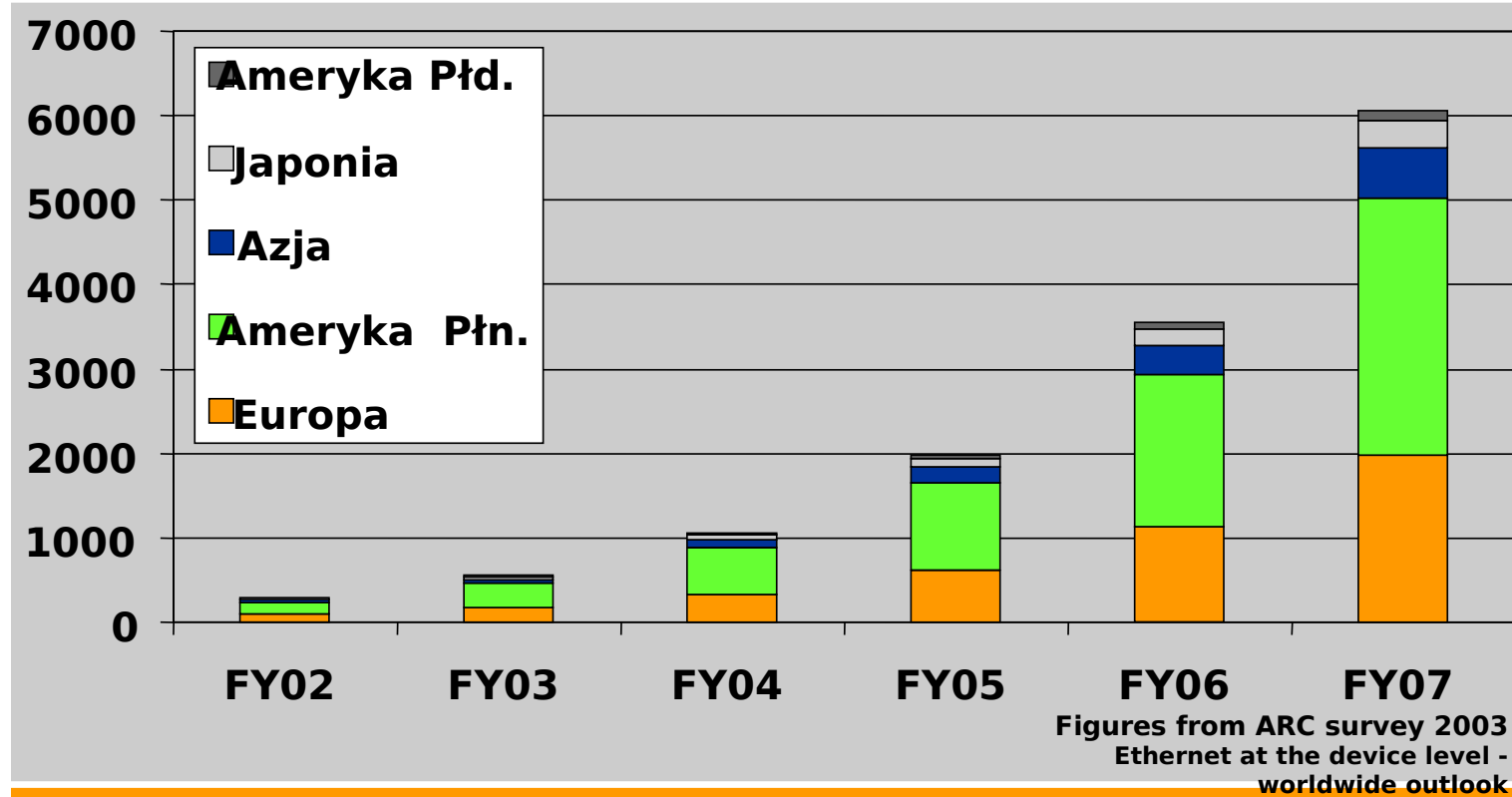
Regionalna dystrybucja urządzeń Ethernet dla przemysłu

Trendy

Wymagania

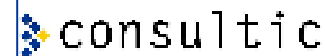
Przykłady

Dostawy urządzeń Ethernet wg. Regionów geograficznych



Ameryka Północna i Europa są największymi rynkami

Badania firmy Consultic : Największe niebezpieczeństwa dla sieci



Trendy

Wymagania

Przykłady

Największe niebezpieczeństwa dla sieci	Procent
Ataki od wewnątrz i z zewnątrz (hakerzy)	35.9%
Wirusy, makra i trojany	33.8%
Błędne operacje przez nieautoryzowany dostęp, niewykwalifikowanego personelu, zaniedbanie	14.8%
Szpiegostwo	9.9%
Sabotaż i manipulacje (dane, maszyny)	9.9%

Źródła niebezpieczeństw Ze względu na wzrost struktury sieci

Trendy

Wymagania

Przykłady

Przemysłowe sieci Ethernet (także fabryczne). Domniemane bezpieczeństwo wynikające z protokołu sieci zostało utracone

Potencjalne narastające niebezpieczeństwo

Wyspy automatyki “rozrastają się” wspólnie na tym samym kablu

Interakcja
Błędne adresowanie

Sieci automatyki są dołączane do sieci biurowych

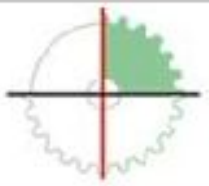
Interakcja
Błędne adresowanie
Nieautoryzowany dostęp

Dostęp klienta zdalnego następuje przez sieć niezabezpieczoną (Internet, WAN, LAN bezprzewodowy, etc.)

Niebezp. ataku (DoS, ..)
Niebezp. szpiegowania
Niebezp. manipulacji

Miejsca są łączone sieciowo jedno z drugim

Niebezp. ataku (DoS, .etc.)
Niebezp. szpiegowania
Niebezp. manipulacji



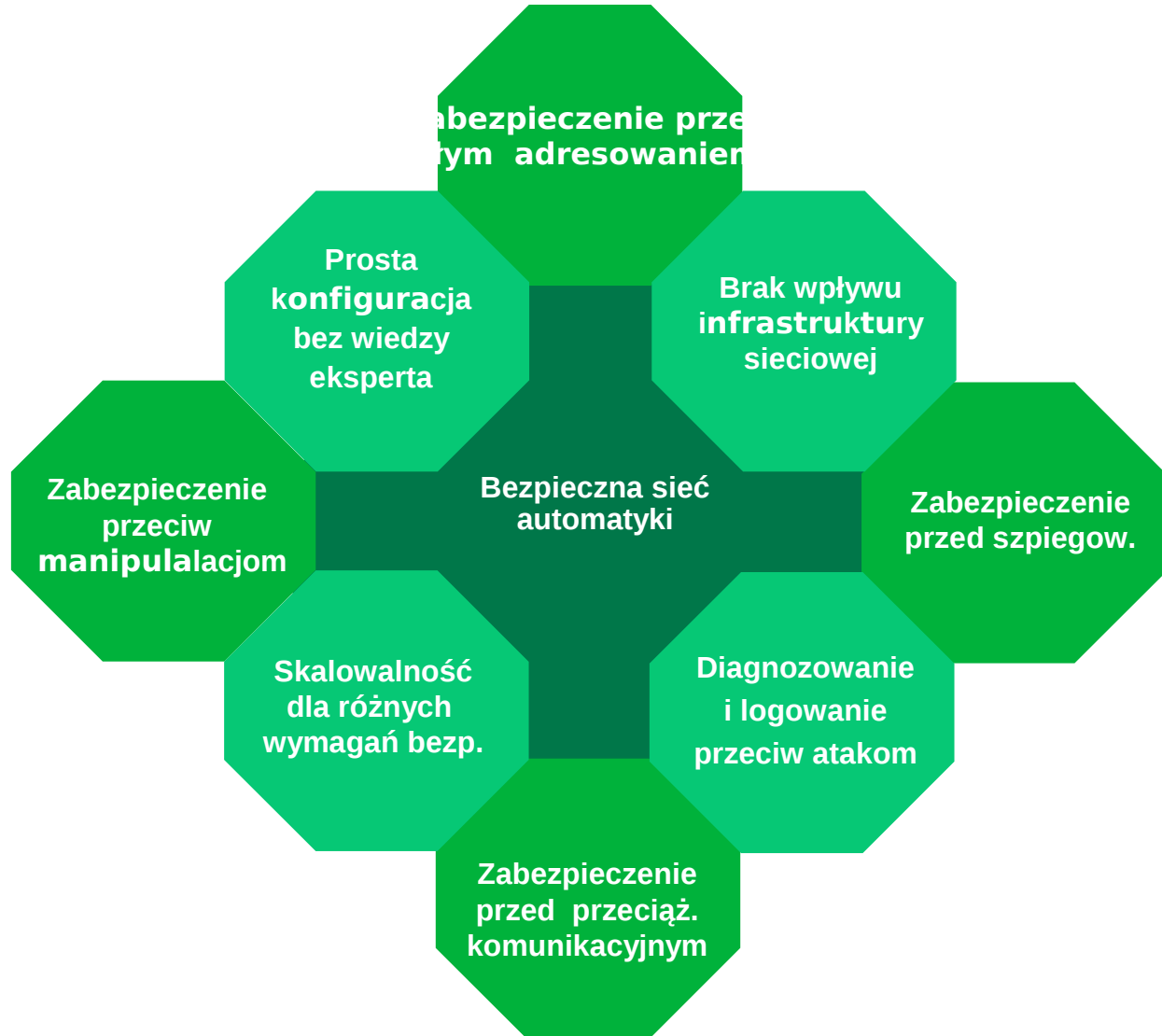
klub paragraf 34

Wymagania bezpieczeństwa w sieciach automatyki

Trendy

Wymagania

Przykłady



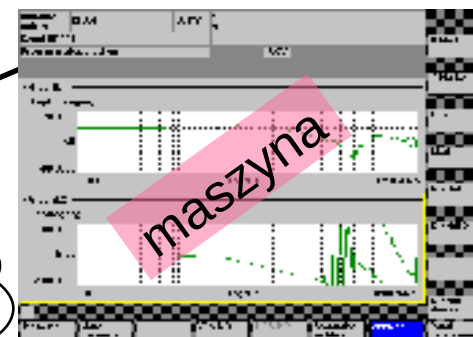
Zdalna diagnostyka - funkcje systemu

Trendy

Wymagania

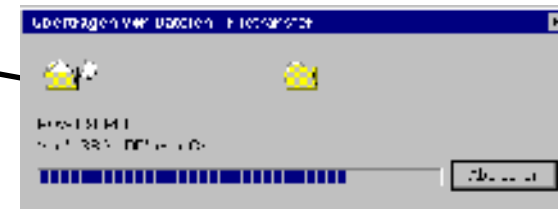
Przykłady

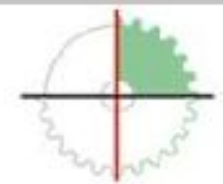
- Zdalna diagnostyka
- Porozumiewanie się - instruowanie oraz transfer informacji tekstowych
- Przesyłanie zbiorów



Komputer-
przeładowarka

Naciskaj przyciski
kierunkowe osi!





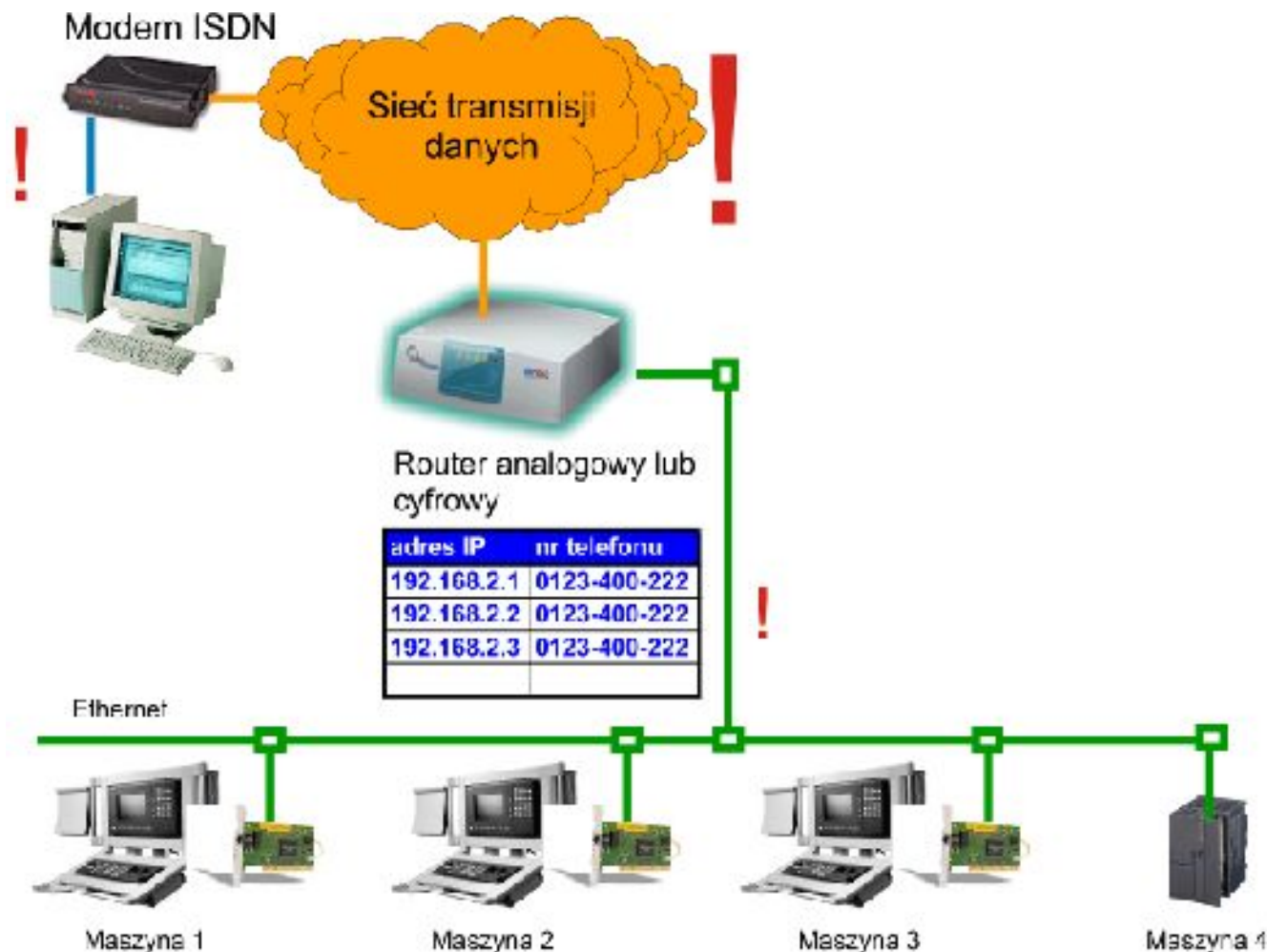
klub paragraf 34

Zdalna diagnostyka a bezpieczeństwo

Trendy

Wymagania

Przykłady

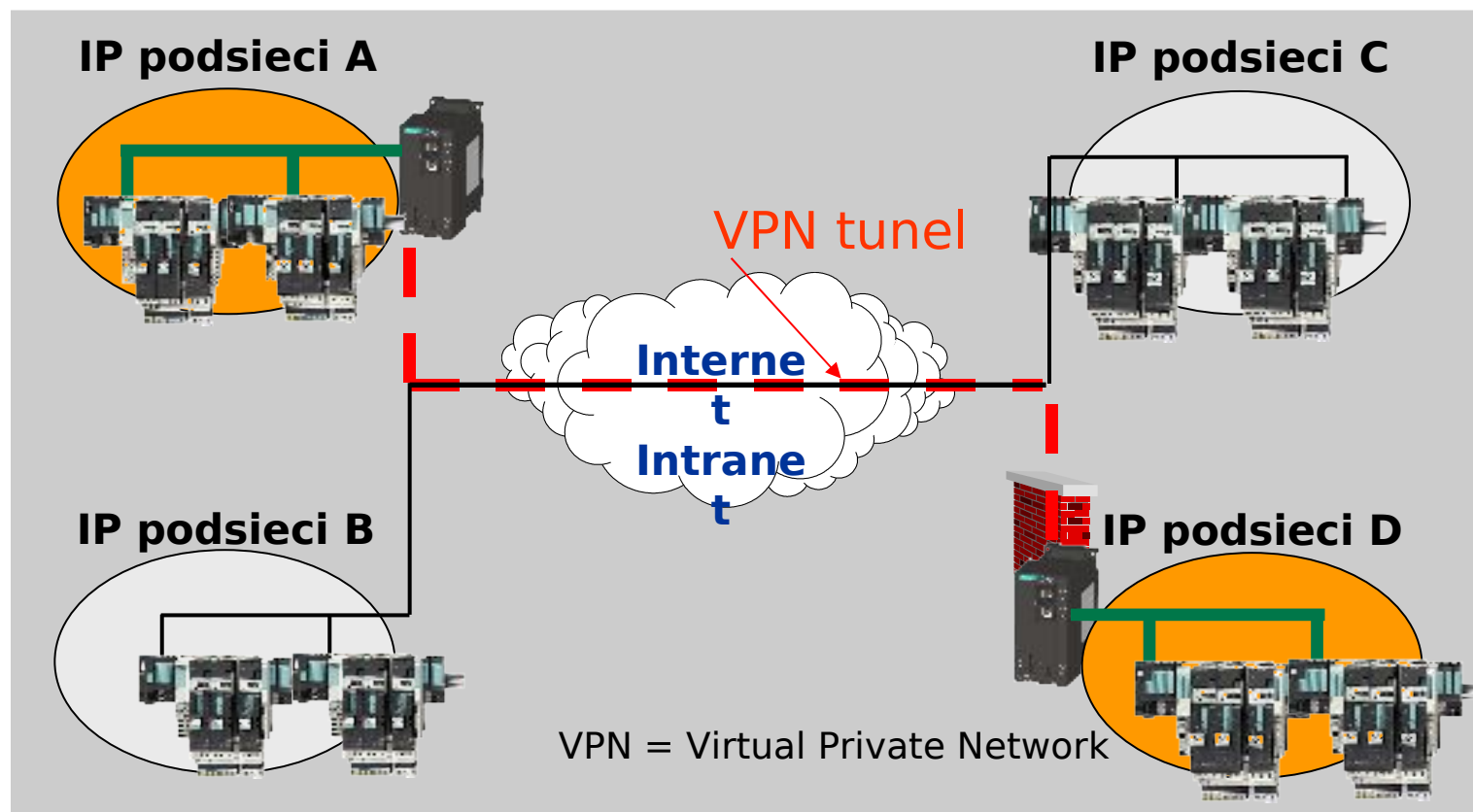


Koncepcja bezpieczeństwa przemysłowego z wykorzystaniem modułów bezpieczeństwa

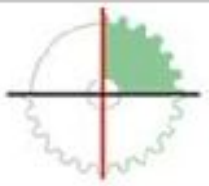
Trendy

Wymagania

przykłady



- **Przepływ danych** pomiędzy zewnętrzną i wewnętrzną siecią jest **sterowany przez moduły bezpieczeństwa**
- **Zdekodowana transmisja danych** pomiędzy bezpiecznymi modułami



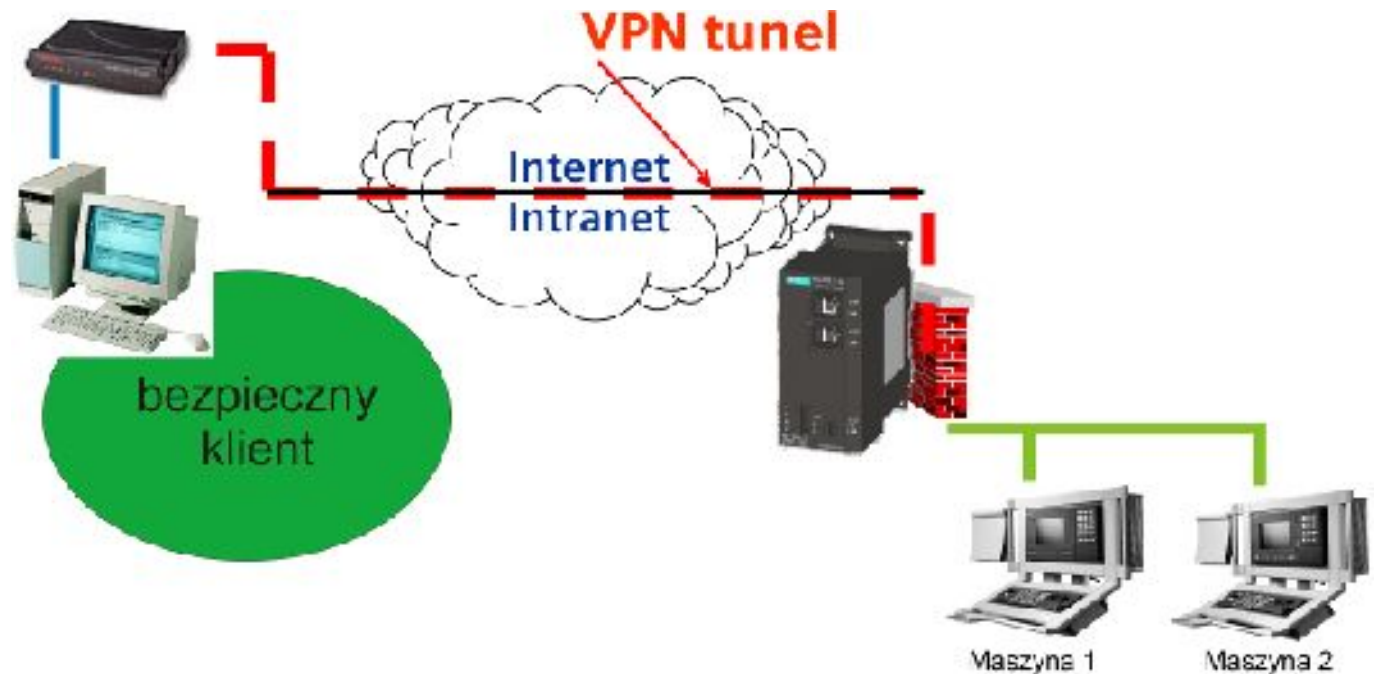
klub paragraf 34

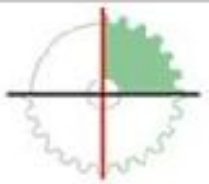
Przykład w układzie zdalnej diagnostyki

Trendy

Wymagania

przykłady





klub paragraf 34

Przykładowy ekran kopii zapasowej systemu CNC

Trendy

Wymagania

przykłady



Zabezpieczenie dostępu wewnątrz i na zewnątrz Instalacji

Zabezpieczenie przeciwko

- Błędnemu adresowaniu
- Nieautoryzowanemu dostępowi
- Szpiegostwu
- Manipulacjom

- Poprzez:

Zastosowanie ochrony przeciwko atakom

Szyfrowana transmisja danych (IPsec, IKE)

Kontrola „ruchu” w sieci – „firewall”

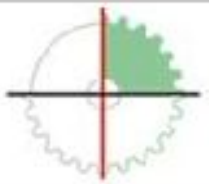
Zabezpieczenie instalacji przed błędnymi operacjami, manipulacjami i szpiegostwem bazuje na standardach bezpieczeństwa

SOFTNET bezpieczny klient

Koncepcja zintegrowanego bezpieczeństwa na przykładzie SCALANCE S i z bezpiecznym klientem SOFTNET

- **Klient VPN dla** PC, PG i noteooka w środowisku przemysłowym.





klub paragraf 34

Konfiguracja modułów bezpieczeństwa

Przykład ekranu konfiguracyjnego:

Nummer	Name	IP-Adresse	Subnetzmaske	Default Port	MFC-Adresse	Status	Typ	Kommentar
01	Mod.01	10.10.10.1	255.255.0.0		01.00.00.00.00	OK	S313	
02	Mod.02					OK Security Client	S313	
03	Mod.03	10.10.10.2	255.255.0.0		01.00.00.00.00	OK	S313	
04	Mod.04	10.10.10.4	255.255.0.0		01.00.00.00.00	OK	S313	

Trendy

Wymagania

przykłady