

# Security Integrated

**Create Sustainable Value**

## PC-baserede systemer

**Pc-baserede systemer** (HMI, teknisk og pc-baseret kontrol) skal sikres i industrielle automatiseringssystemer ved hjælp af antivirussoftware, whitelisting og integrerede security-mekanismer

## Controller/HMI Systems

**Kontrolniveauet** er beskyttet mod manipulation ved hjælp af flere integrerede effektive foranstaltninger

## Kommunikationssystemer

**Kommunikation** skal observeres ved hjælp af systemer til overvågning af netværksindtrængen og underopdeles intelligent af firewalls (cellebeskyttelseskoncept)

## PC-baserede systemer - Security @ SCADA-niveau

**Virusscanner**

**Whitelisting**

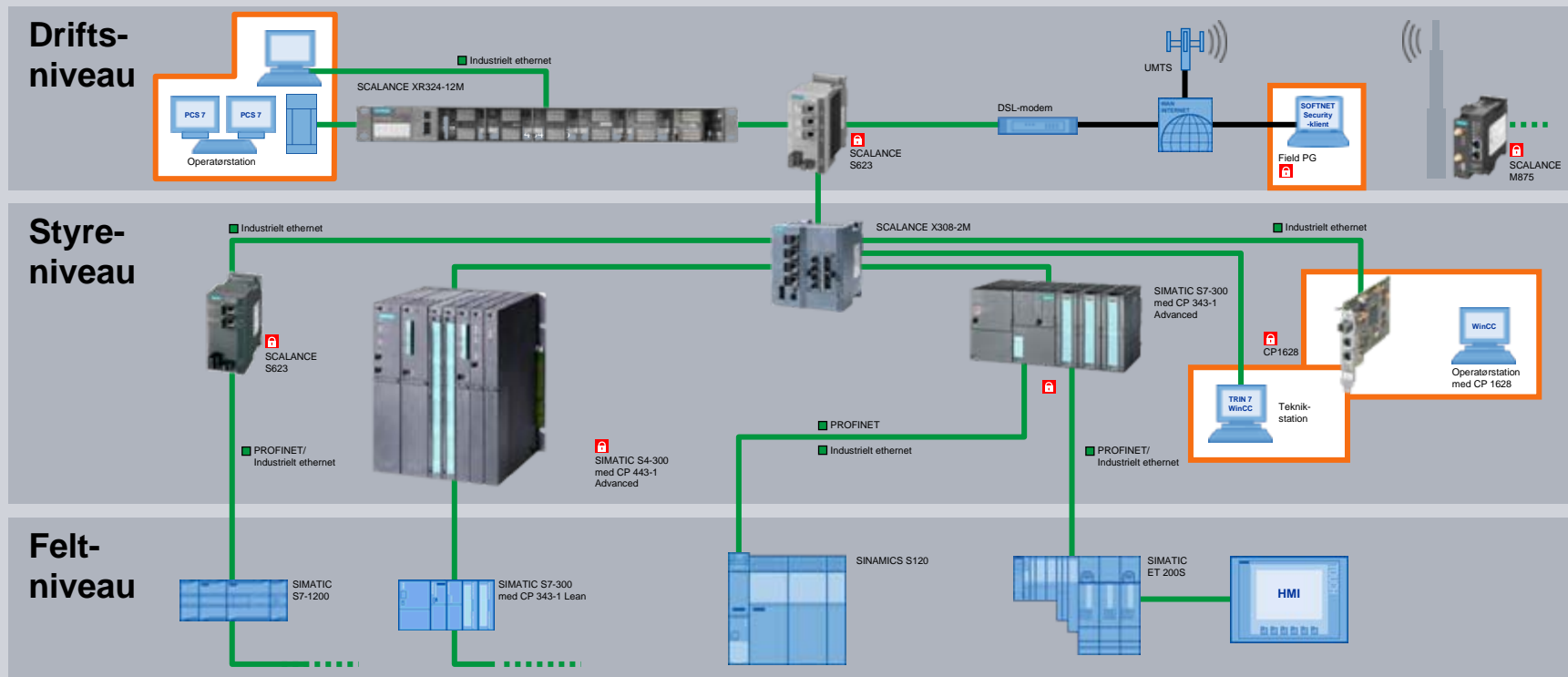
**Deaktivering af tjenester**

**VPN-klientsoftware**

**Brugerstyring**

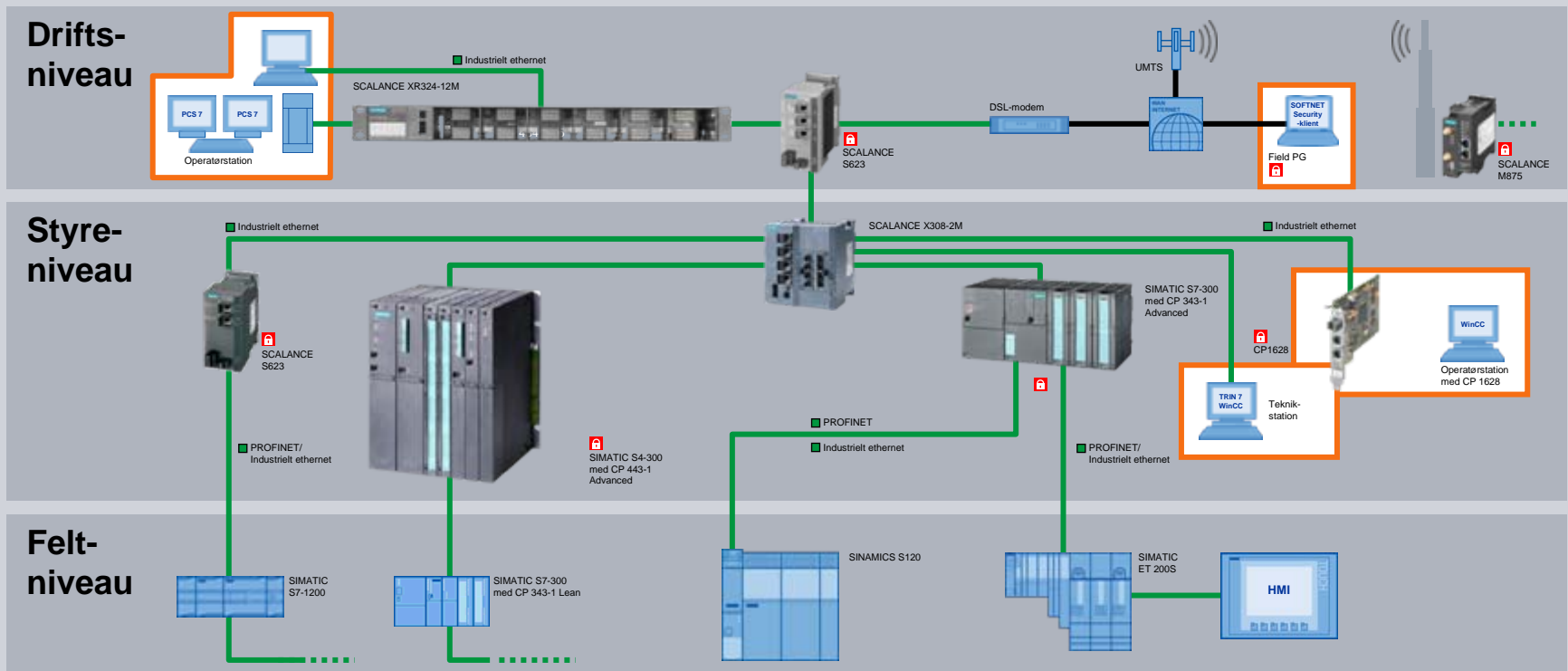
## Virusscanner

Brug af virusscannere i kontor-pc'er, teknik- og operatørstationer samt i pc-baserede styreenheder som SINUMERIK og SIMOTION



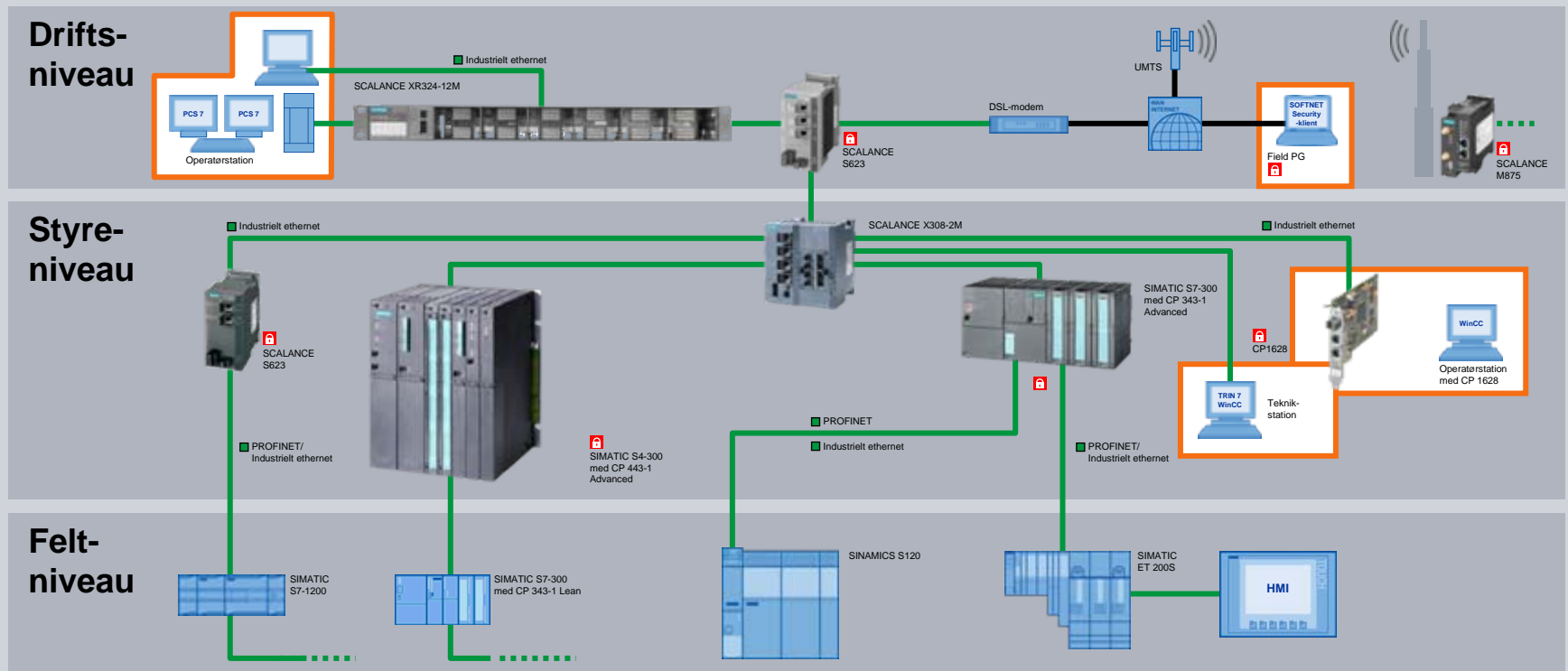
## Whitelisting

Brug af whitelisting-software i kontor-pc'er, teknik- og operatørstationer. Kun tilladt software kan anvendes



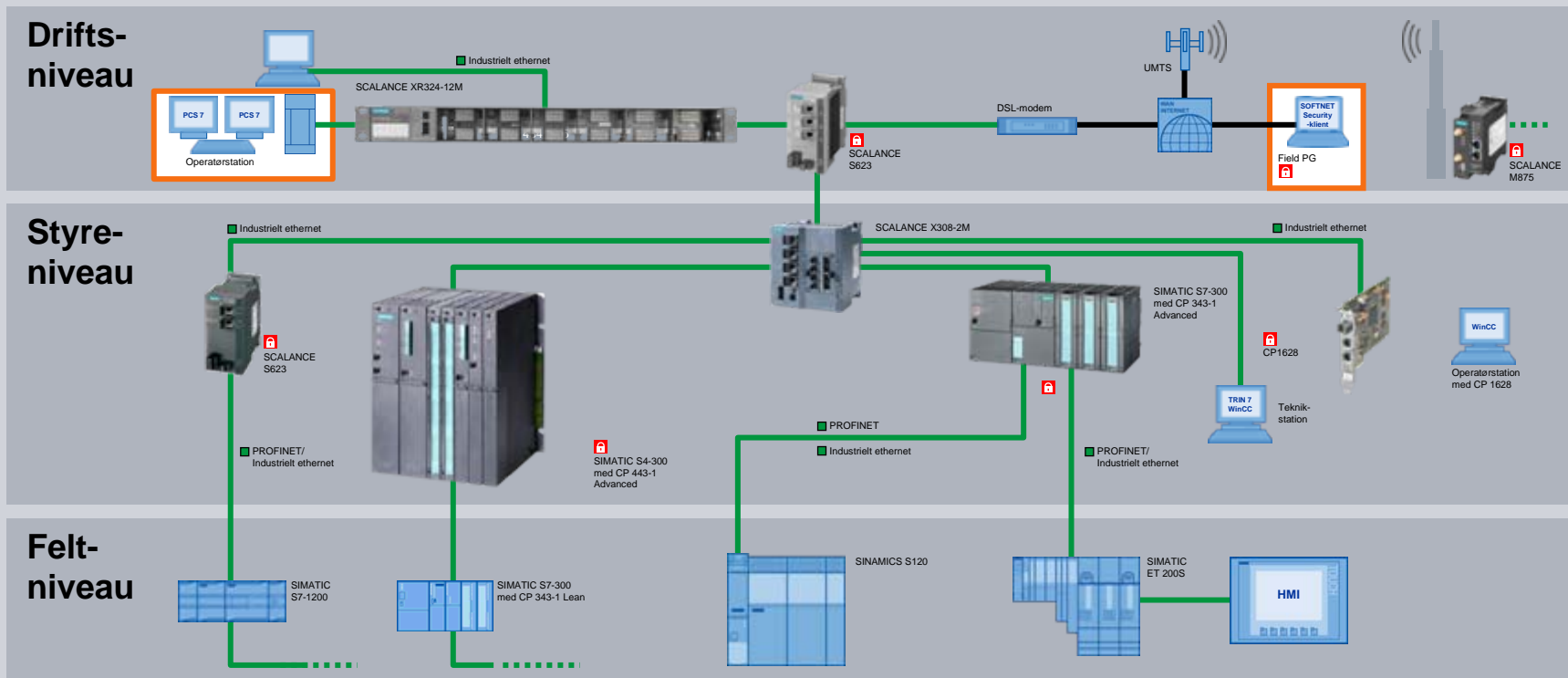
## Deaktivering af tjenester

Deaktivering af ubenyttede tjenester som fjernadgang på kontor-pc'er, teknik- og operatørstationer



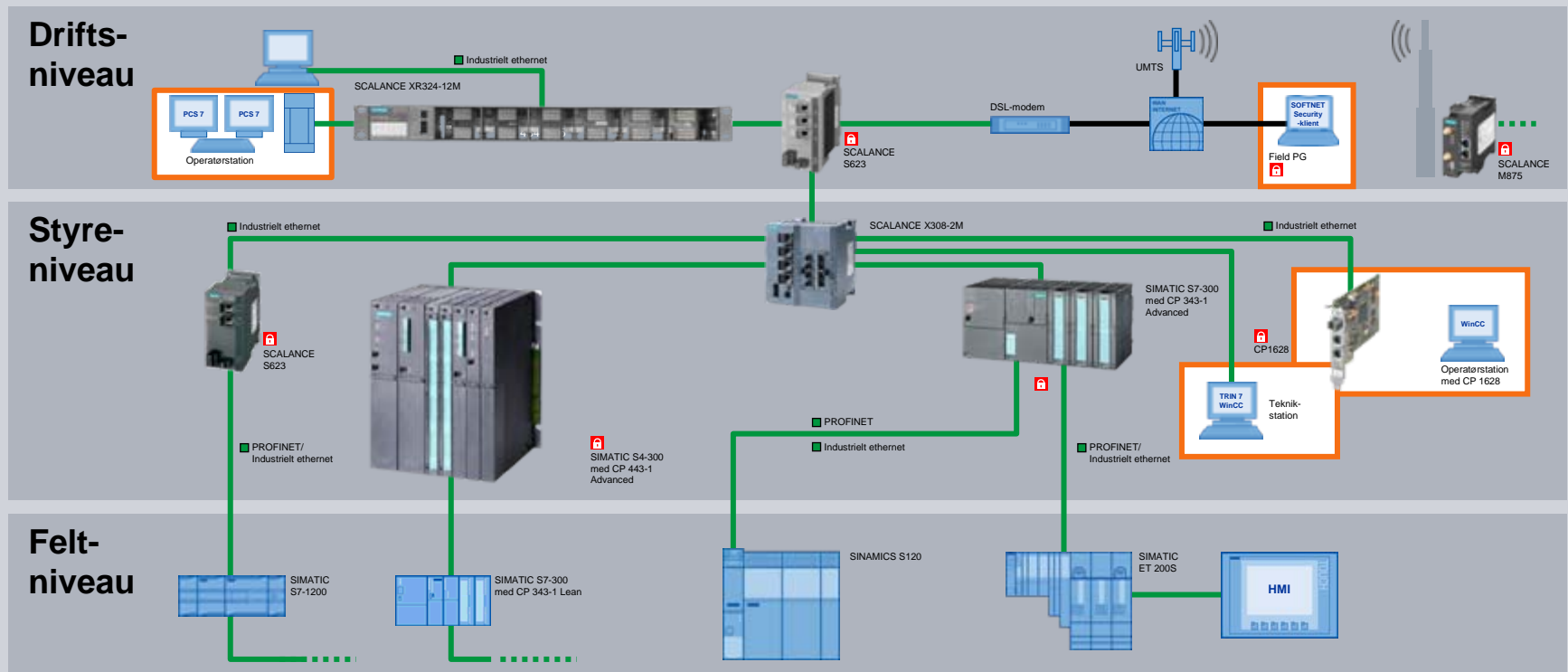
## VPN-klientsoftware

Brug af VPN-klientsoftware som **SOFTNET Security-klient** til tilslutning af en pc til sikre automatiseringsceller



## Brugerstyring

Central brugerstyring af anlægget til teknik- og operatørstationer til identificering af brugere og tildeling af adgangsrettigheder ved hjælp af SIMATIC-logon





# Controller/HMI Systems – Security @ the Controller/SCADA level

**SIEMENS**

**Brugerstyring**

**Deaktivering af tjenester**

**Deaktivering af hardware og porte**

**IP Hardening**

**Beskyttelse af adgangskode**

**Beskyttelse af knowhow**

**Kopibeskyttelse**

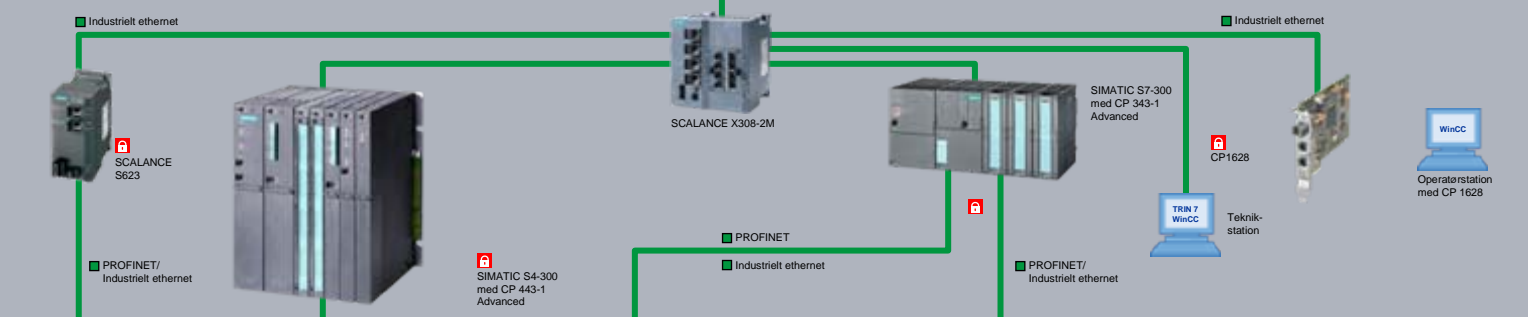
## Brugerstyring

Central brugerstyring af anlægget til **HMI-systemer** til identificering af brugere og tildeling af adgangsrettigheder ved hjælp af **SIMATIC-logon**

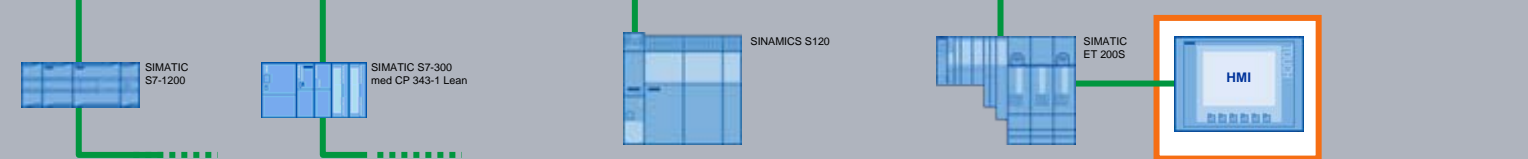
### Drifts-niveau



### Styre-niveau



### Felt-niveau



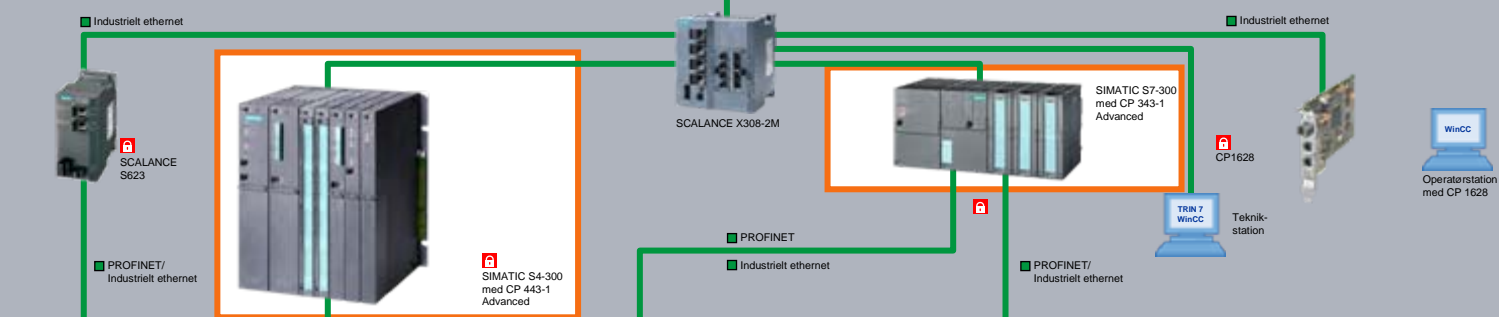
## Deaktivering af tjenester

Deaktivering af ubenyttede tjenester som webservere på PLC'er, perifere systemer og HMI-systemer

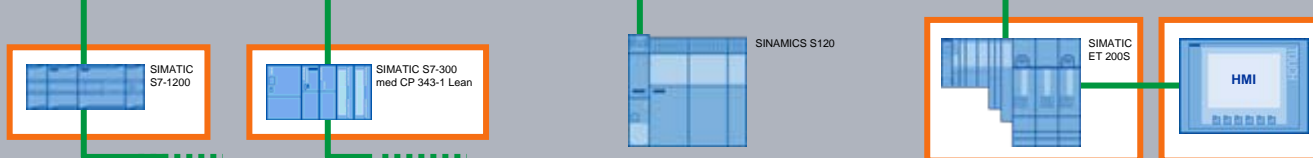
### Drifts-niveau



### Styre-niveau

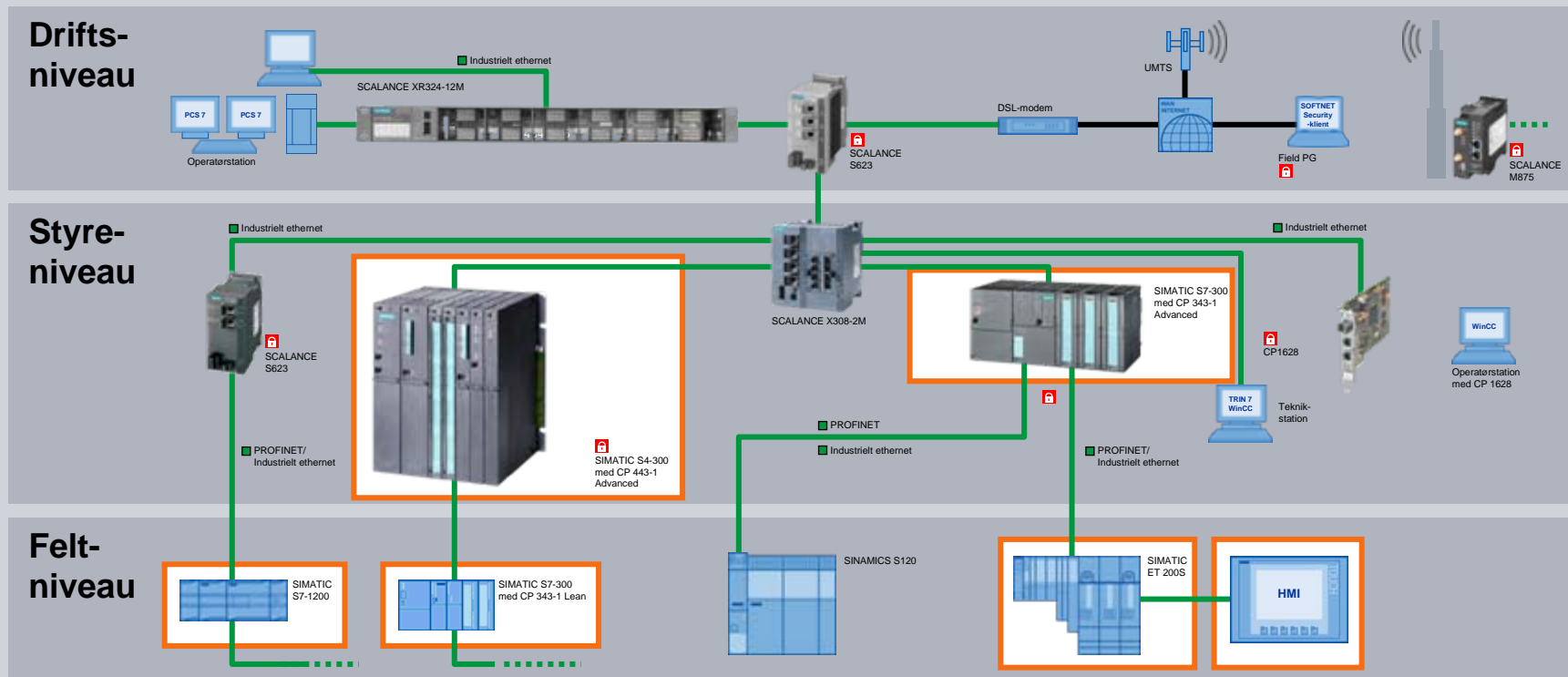


### Felt-niveau



## Deaktivering af hardware, porte og protokoller

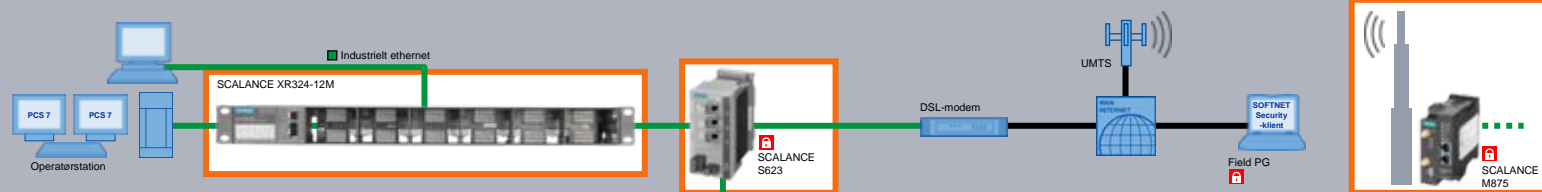
Deaktivering af ubenyttede RJ45-stik, TCP/UDP-porte og protokoller som **SNMP** på PLC'er, perifere systemer og HMI-systemer



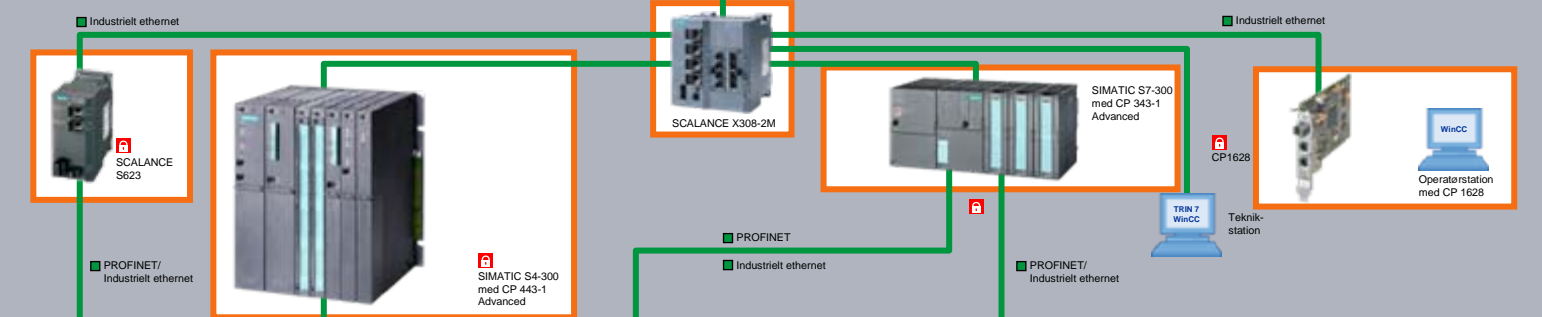
## IP-Hardning

Produkter fra Siemens Industry Automation & Drive Technologies er hærkede, så de kan modstå kommunikationsoverload og fejlbehæftede netværkstelegrammer

### Drifts-niveau



### Styre-niveau

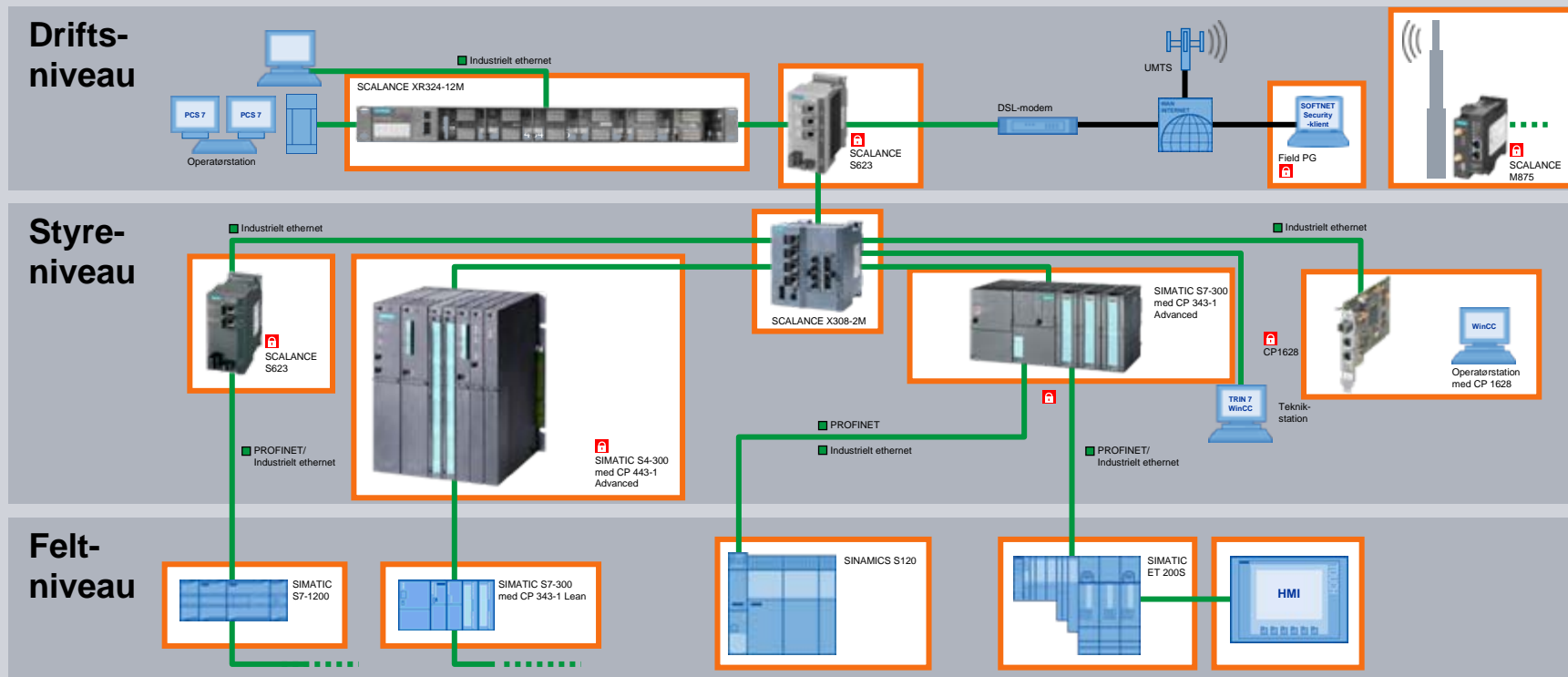


### Felt-niveau



## Beskyttelse af adgangskode

Brug adgangskoder til at få adgang til enheder via webservere eller konfigurationsværktøjer



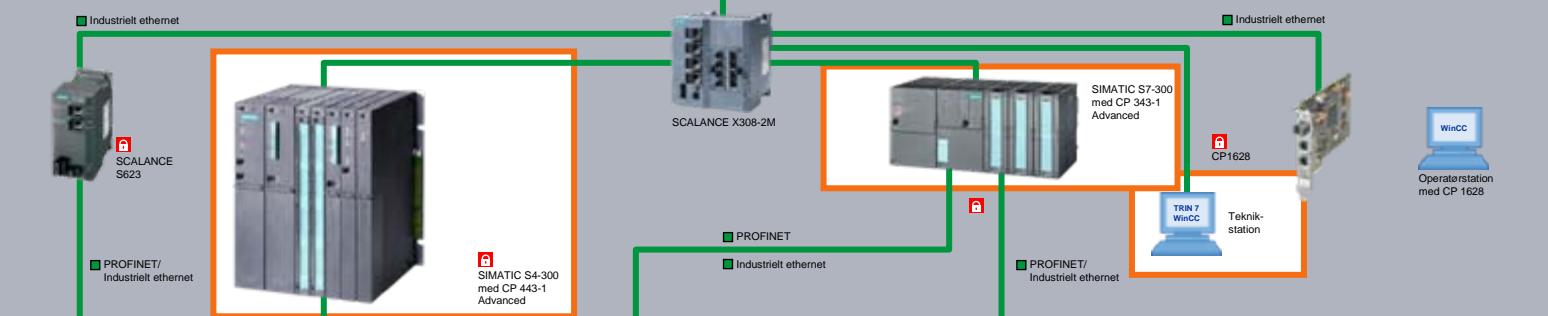
## Beskyttelse af knowhow

Programblokke med SIMATIC STEP 7 og SIMOTION SCOUT samt SINUMERIK kan beskyttes med adgangskoder

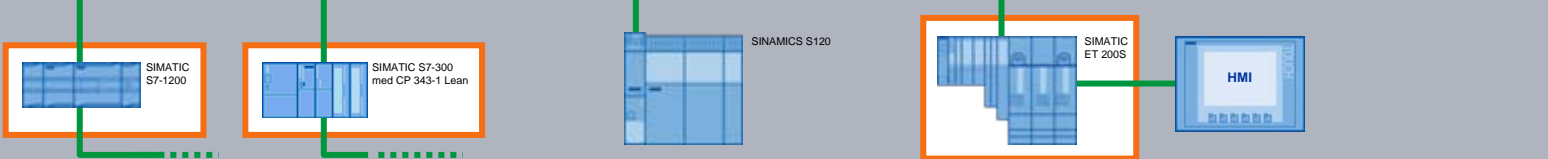
### Drifts-niveau



### Styre-niveau



### Felt-niveau



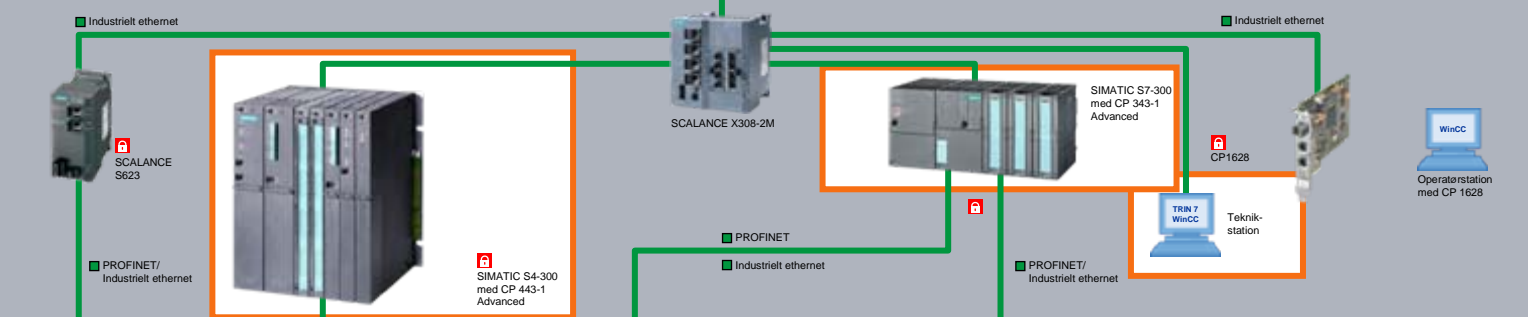
## Kopibeskyttelse

SIMATIC S7-programmer kan bindes til en bestemt PLC eller et serienummer for Micro Memory Card for at forebygge kopiering

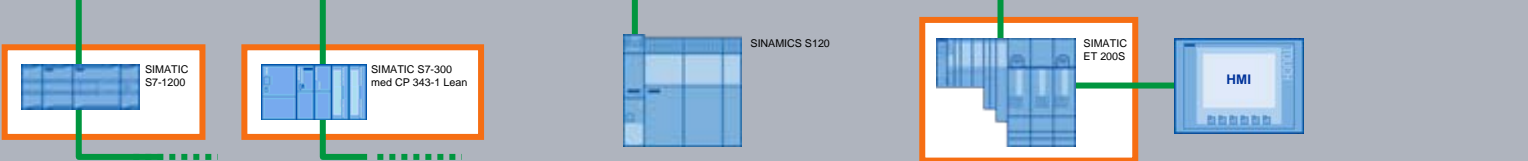
### Drifts-niveau



### Styre-niveau



### Felt-niveau





## Kommunikationssystemer - Security @ feltniveau

**Virtuelle LAN (VLAN)**

**Port-security og RADIUS-serverautenticitet**

**Firewalls**

**Virtuelle private netværk (VPN)**

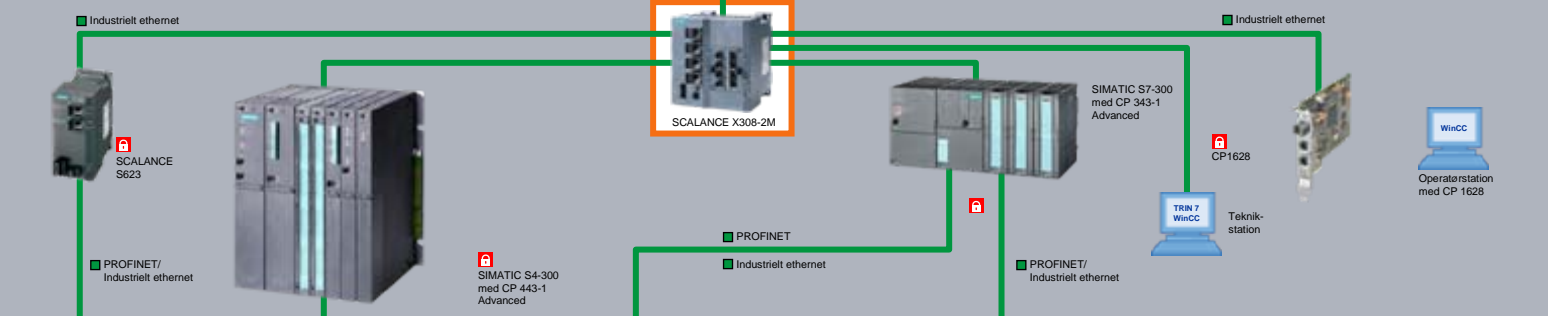
## Virtuelle LAN

Brug af **VLAN** til at underopdele enterprise og plant netværk i logiske netværkssegmenter for at undgå uønsket tværgående trafik

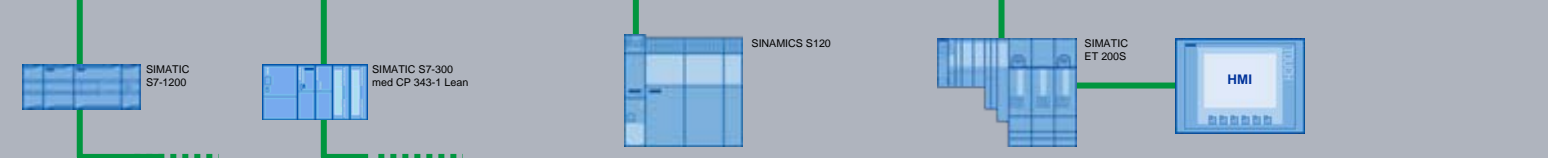
### Drifts-niveau



### Styre-niveau



### Felt-niveau



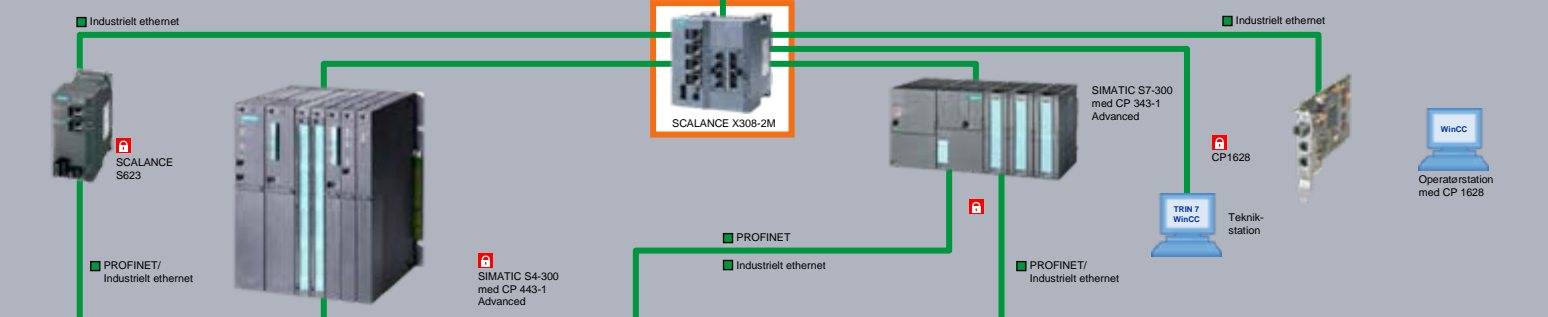
## Port-security og RADIUS-serverautenticitet

Aktivering af port-security og RADIUS-serverautenticitet, så kun foruddefinerede enheder kan forbindes til et industrielt ethernetnetværk baseret på SCALANCE X

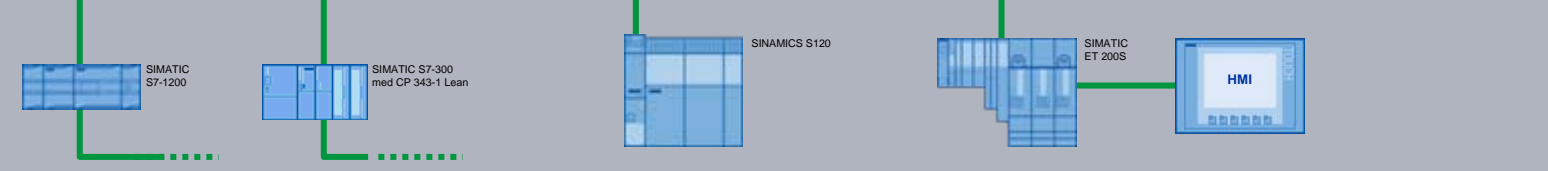
### Drifts-niveau



### Styre-niveau

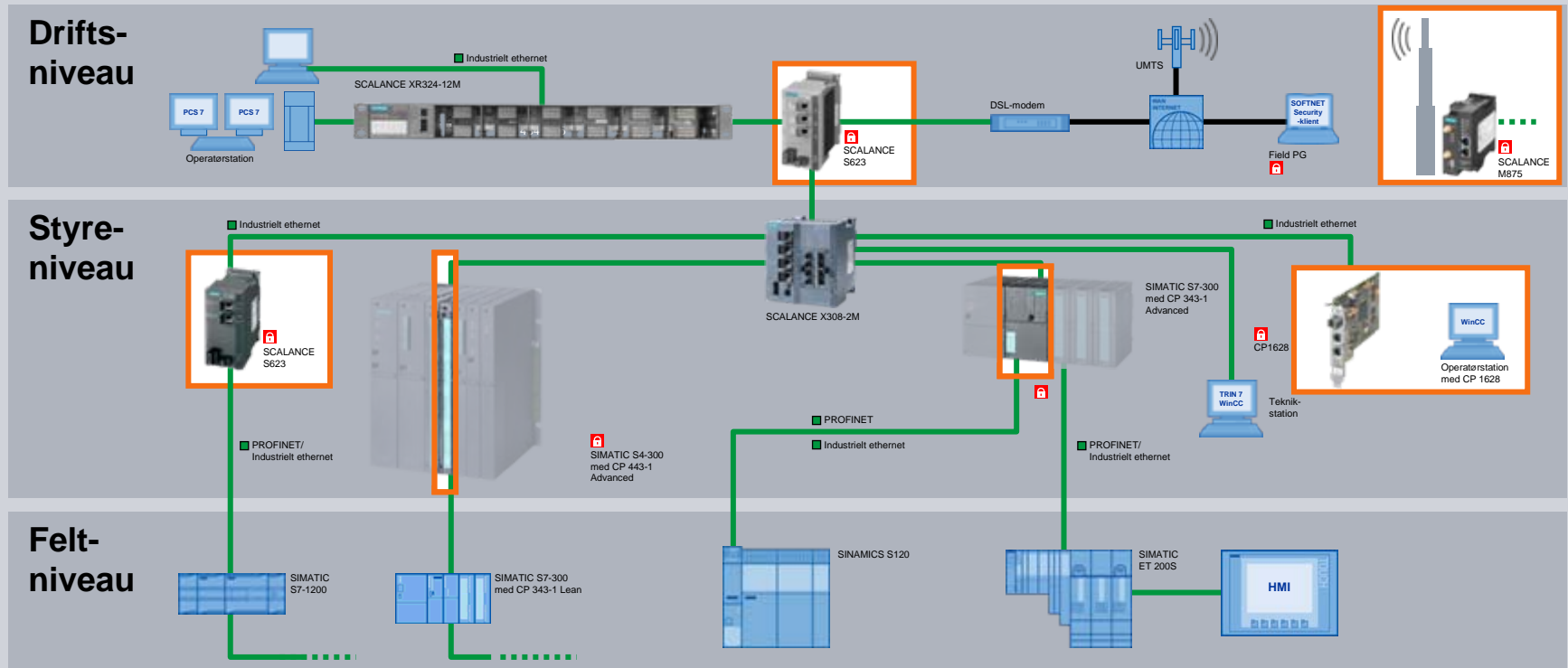


### Felt-niveau



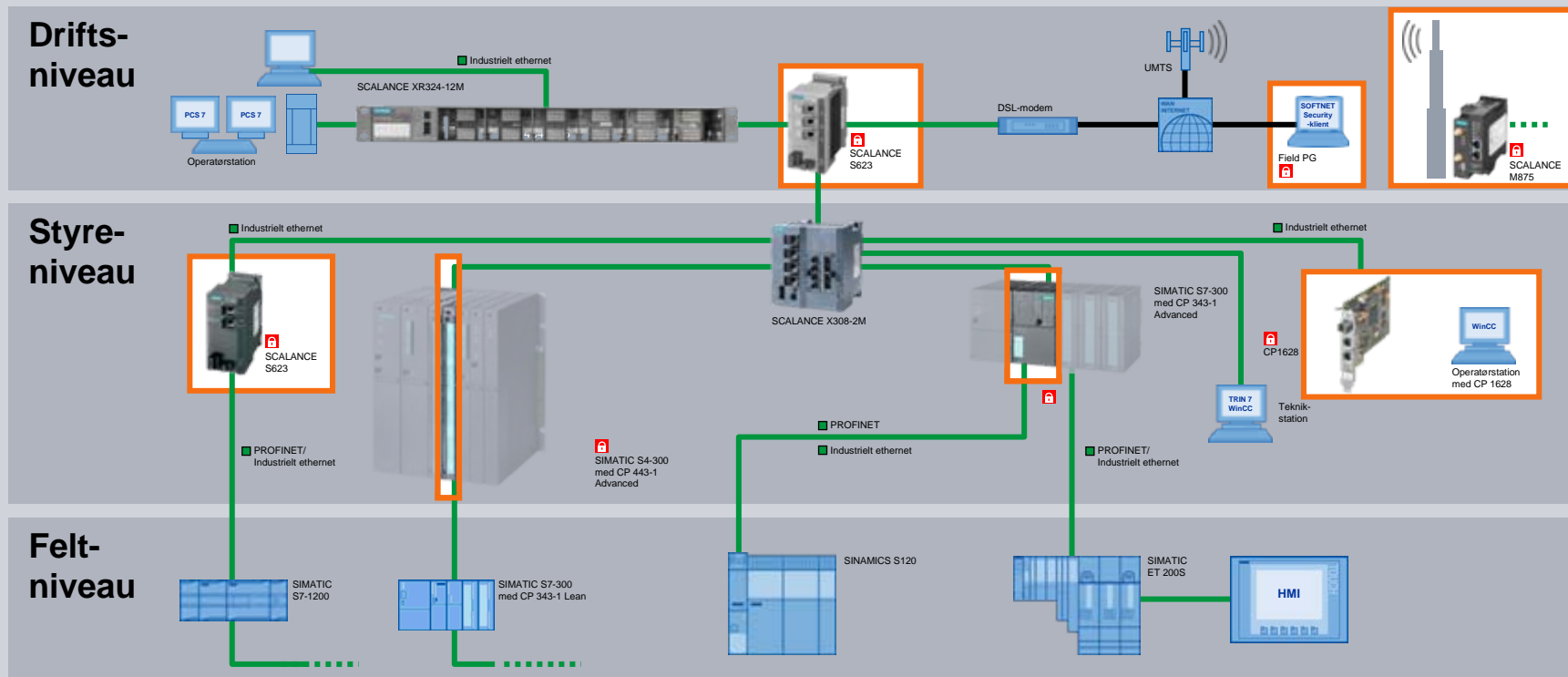
## Firewalls

Underopdeling af anlægsnetværket i sikre automatiseringsceller efter **cellebeskyttelseskonceptet**; brug **SCALANCE S** eller **security-integrerede komponenter**; SINUMERIK har en ekstra intern firewall



## Virtuelle private netværk

Anvendelse af VPN for at tillade sikker kommunikation mellem automatiseringsceller og fjernadgang; brug **SCALANCE S** eller **security-integrerede** komponenter





### CP 343-1 Advanced og CP 443-1 Advanced – S7-300 og S7-400 kommunikationsprocessorer med security-funktioner

- Opfølgningssamlinger, avancerede CP'er med security
  - firewall og VPN til internt cellebeskyttelseskoncept
  - 100 % kompatibel med aktuelle avancerede CP'er
- Omkostningsbesparelser gennem security-merværdifunktion
- Omkostningsbesparelser gennem to separate interface og indbygget router
- Fuld integrering i STEP 7



### CP 1628 – Kommunikationsprocessor med security til pc'er

- Den omfattende pålidelige beskyttelse (firewall, VPN) til pc'er uden specialistviden til operativsystemer
- Omkostningsbesparelser gennem security-merværdifunktion





### Security-modul SCALANCE S og Softnet Security-klient

- Udvidelse af SCALANCE S-produktlinjen
  - yderligere security-funktioner til cellebeskyttelse
  - DMZ-port til en sikrer forbindelse af et DSL-modem eller som et serviceinterface
- Softnet Security-klient (64 bit-version)



### SCALANCE M873 og M875 – hurtig UMTS-router med eller uden VPN

- UMTS-router
  - til klassiske teleservice- og telekontrolformål
  - til yderligere formål som videotransmission
  - variant med yderligere VPN-funktion og togadgang
- Anvendes med Siemens' remote service



## Mere Security information

Generel oversigt:

- [Applications & Tools on the topic of "Industrial Security"](#)

Information om emnet "Industrial Security" med fokus på:

- [Microsoft Security Updates](#)
- [Virus Protection](#)
- [Whitelisting Protection Mechanisms](#)
- [Firewall](#)
- [Virtual Private Network \(VPN\)](#)
- [Access Control](#)
- [Remote Access via Internet, Gateways](#)
- [Stuxnet](#)

Se her: <http://support.automation.siemens.com/WW/view/en/50203404>



## Endnu mere Security information

**SIEMENS**

### Industrial Security

Industrial security is gaining in importance. Through increased internet use down to field level, open communications and the increasing networking of production systems contain not only enormous opportunities, but also considerable risks. In the area of IT security we support you protecting your industrial plants against all attacks.

**More security where it matters in industrial automation**  
Find out more about our complete solution for plant protection.  
[More information](#)

Siemens Industry Sector | [Dienstleistungen](#) | [Contact](#)

[Home](#) | [Industry Sector](#) | [Industrial Security](#)

#### Industrial Security

- > Industrial Security Services
- > Industrial Security for PC-based Systems
- > Industrial Security for Controllers and HMI
- > Industrial Ethernet Security

**Comprehensive solutions for maximum protection**

Whether you want to protect your existing know-how or exclude unauthorized access to your automation processes from the start and thereby prevent any disturbance of your production processes: With our comprehensive industrial security services, we will support you in taking the required steps against every conceivable threat scenario – and plan comprehensive solutions for maximum protection.

**More Information**

- > Industrial Security Brochure
- > ARC Whitepaper Cyber Security
- > Industrial Security Protection Levels
- > Industrial Security Management
- > IT Security for SIMATIC PCS 7
- > SIMATIC Remote Support Services
- > Security solutions from Siemens Building Technologies
- > Industrial Security on the Hannover Fair 2011

**News: Behaviour of SIMATIC S7-1200 in Industrial Networks**

In mid-May, ICS-CERT issued an alert about certain weaknesses in the Ethernet network interface of the Simatic S7-1200 controller. Siemens reproduced the test scenario. The scenario revealed weaknesses in the S7-1200 controller in reaction to targeted network attacks. Siemens takes such reports very seriously and our experts are permanently working on possible improvements.

[More Information](#)

For additional information on the topic of **Industrial Security**, please contact the experts of our consulting team:  
[industrialsecurity@siemens.com](mailto:industrialsecurity@siemens.com)

**ARC WHITE PAPER**  
By ARC Advisory Group

MAY 2011

### Risk Drives Industrial Control System Cyber Security Investment

Executive Overview ..... 3

Game Changers for Industrial Control System Cyber Security ..... 4

Risk Analysis Drives ICS Security Investment ..... 8

Industry Trends Mean Change for ICS Owners ..... 9

ICS Security Technologies and Practices Evolve Methodically ..... 14

Siemens Security Strategy for ICS ..... 16

Conclusions and Recommendations ..... 19

**ARC Advisory Group**

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY

Se her: [WWW.siemens.com/industrial-security](http://WWW.siemens.com/industrial-security)



# Tak for opmærksomheden 😊

Security Integrated