SIEMENS

Security Integrated

Create Sustainable Value

Industrielle Security-funktioner til automatiseringssystemer

SIEMENS

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

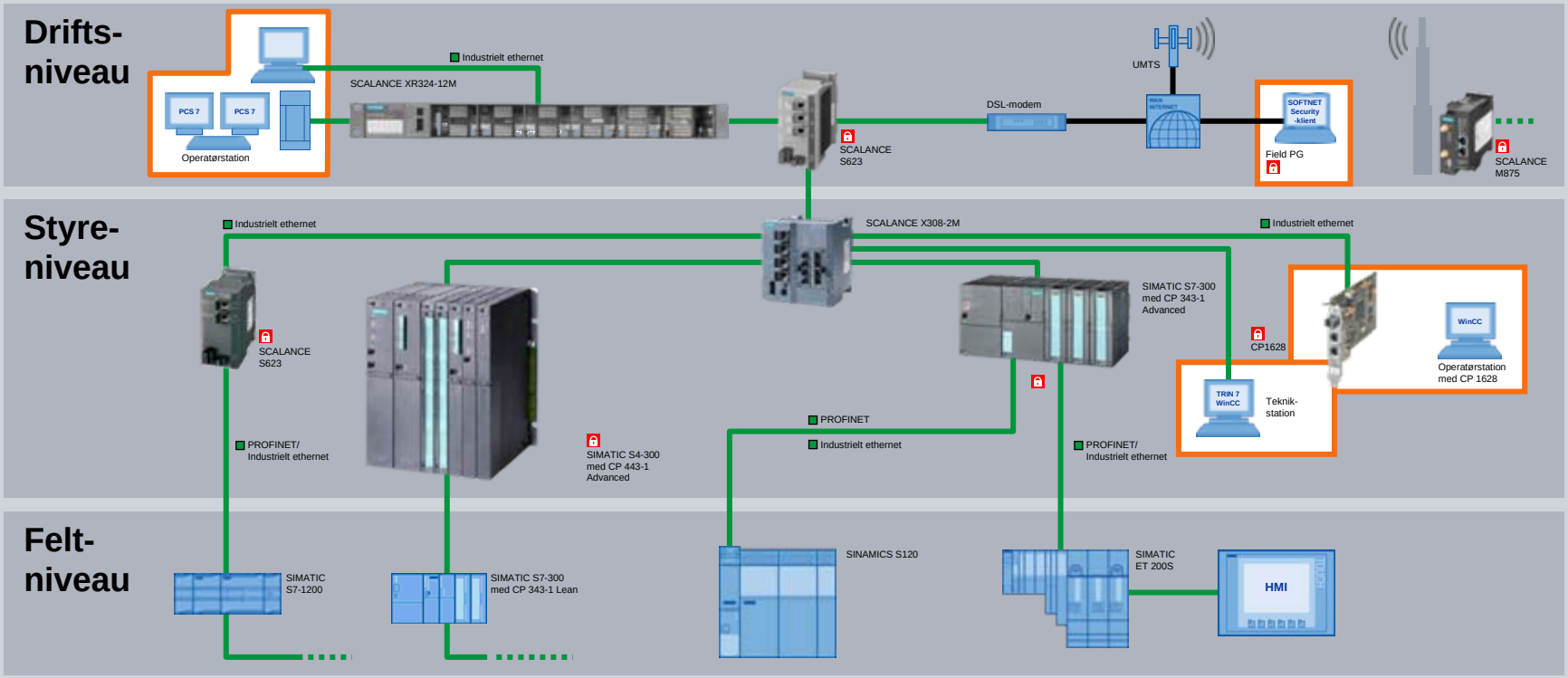
Kommunikation skal observeres ved hjælp af systemer til overvågning af netværksindtrængen og underopdeles intelligent af firewalls (cellebeskyttelseskoncept)

PC-baserede systemer - Security @ SCADA-niveau

- Virusscanner
- Whitelisting
- Deaktivering af tjenester
- VPN-klientsoftware
- Brugerstyring

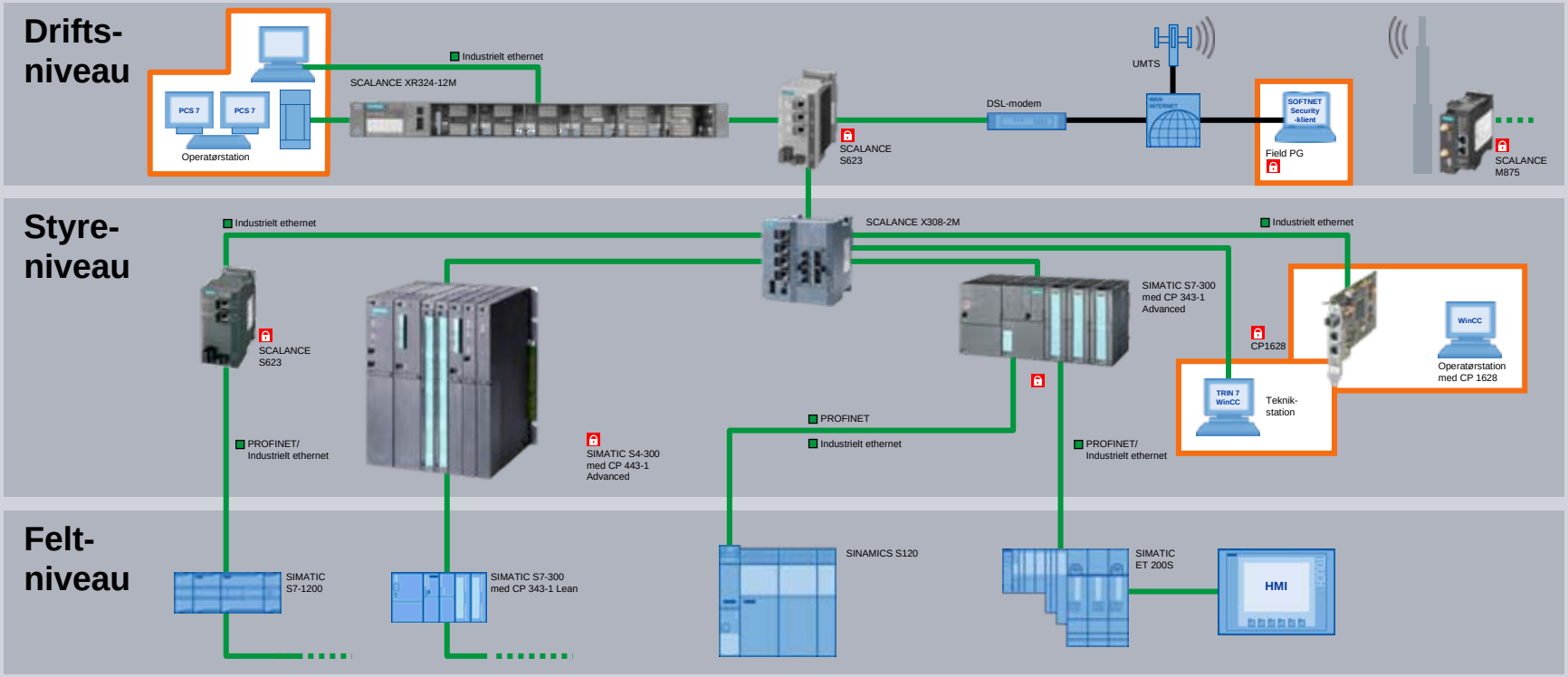
Virusscanner

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



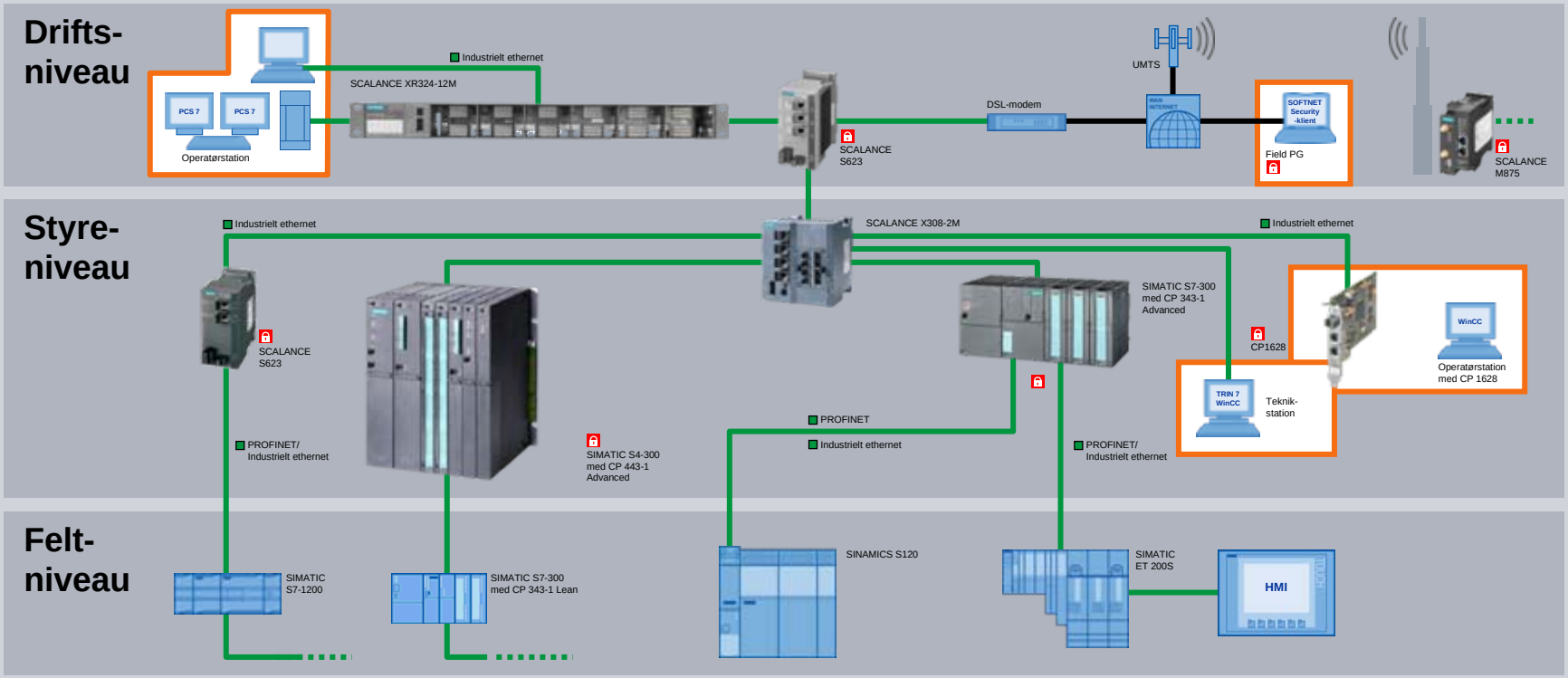
Whitelisting

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



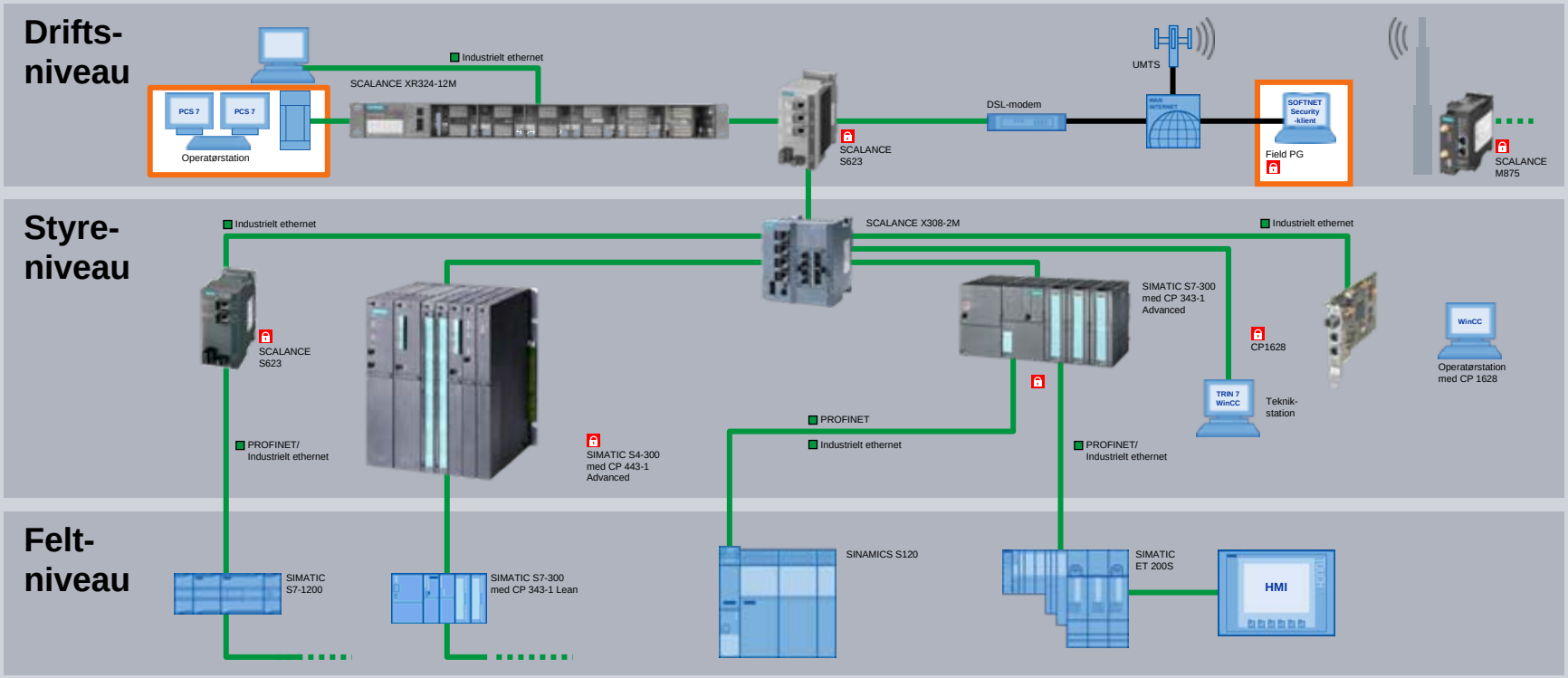
Deaktivering af tjenester

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



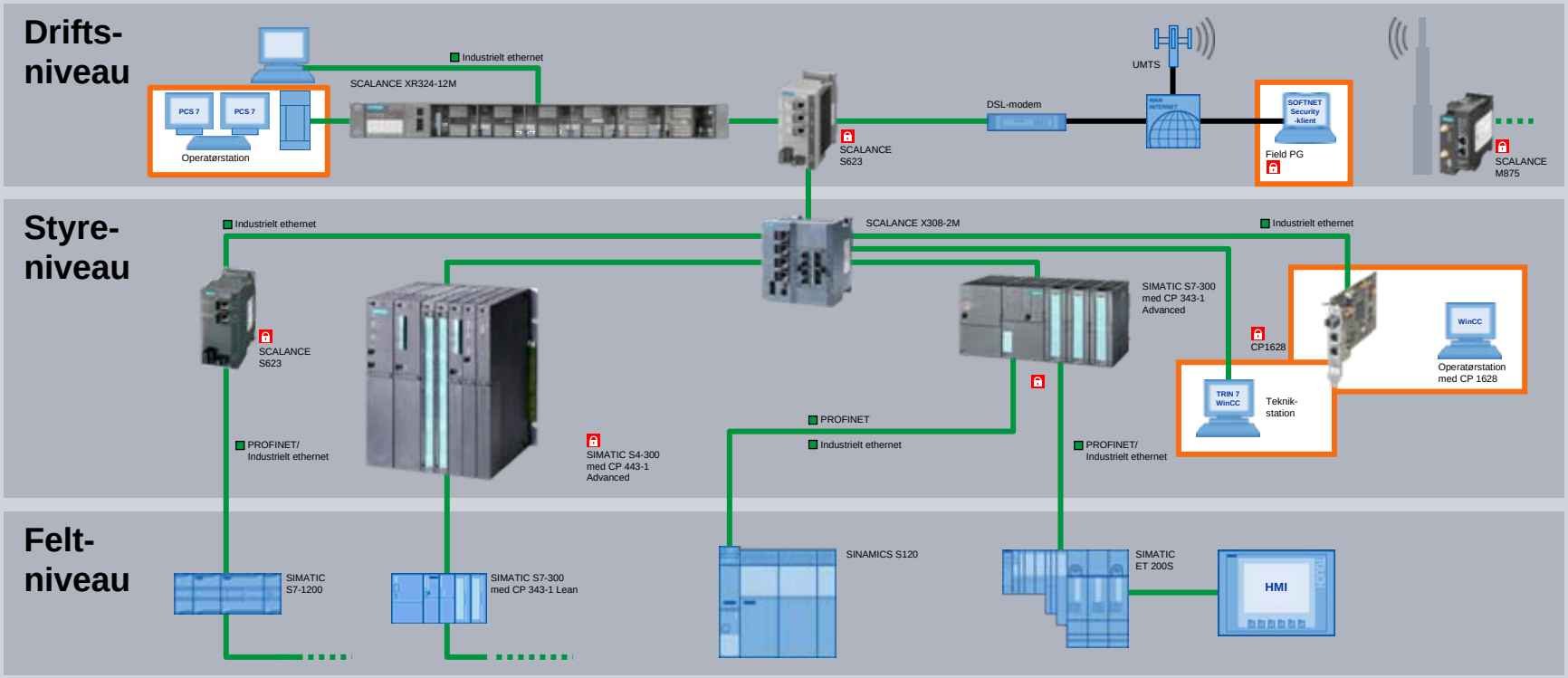
VPN-klientsoftware

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**



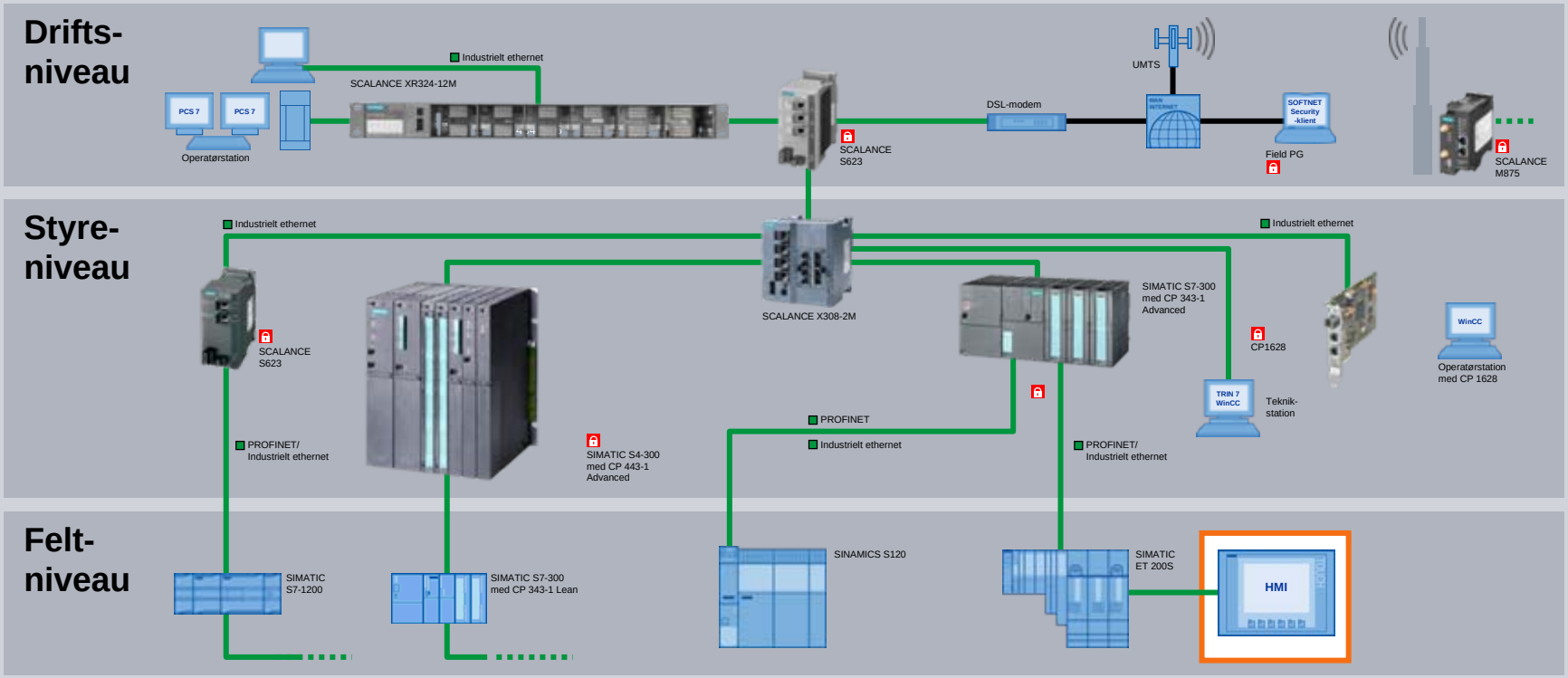
Controller/HMI Systems – Security @ the Controller/SCADA level

SIEMENS

- Brugerstyring
- Deaktivering af tjenester
- Deaktivering af hardware og porte
- IP Hardening
- Beskyttelse af adgangskode
- Beskyttelse af knowhow
- Kopibeskyttelse

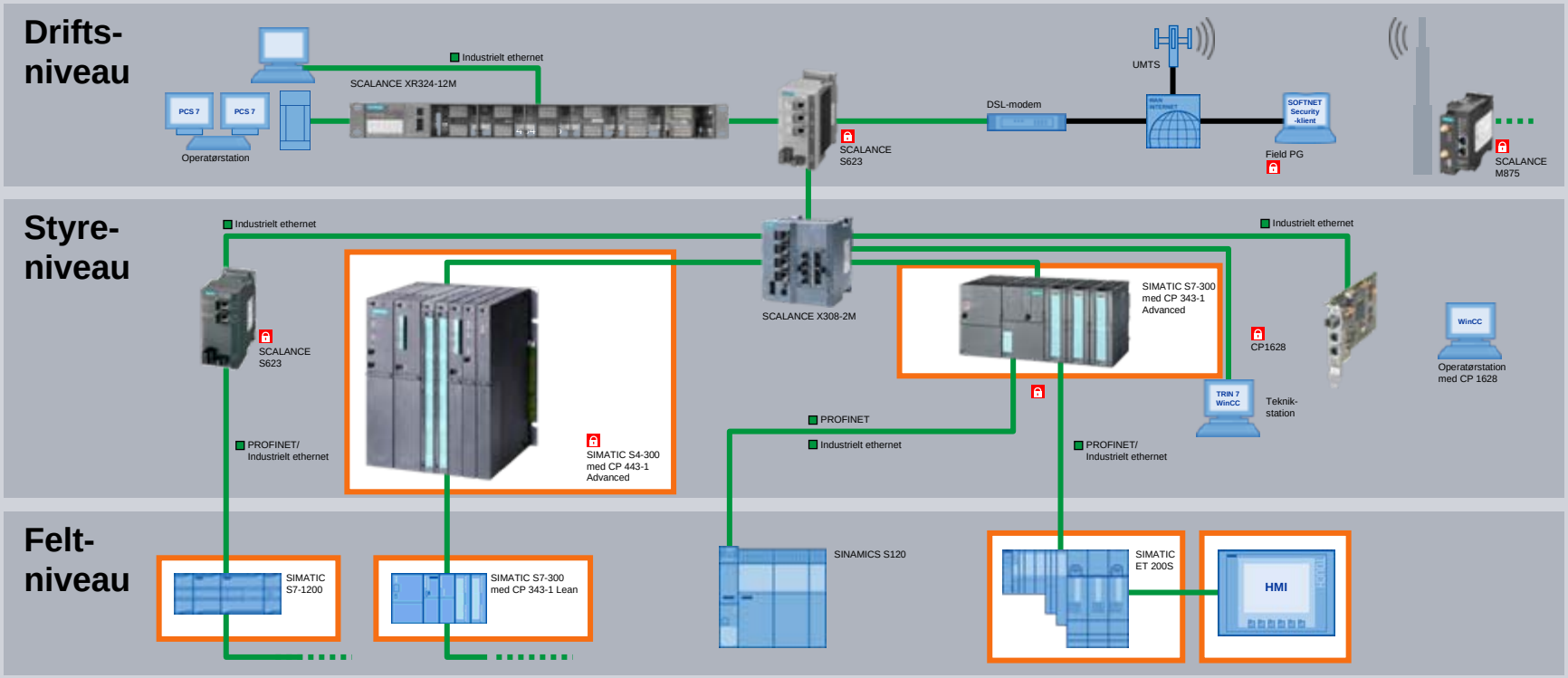
Brugerstyring

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



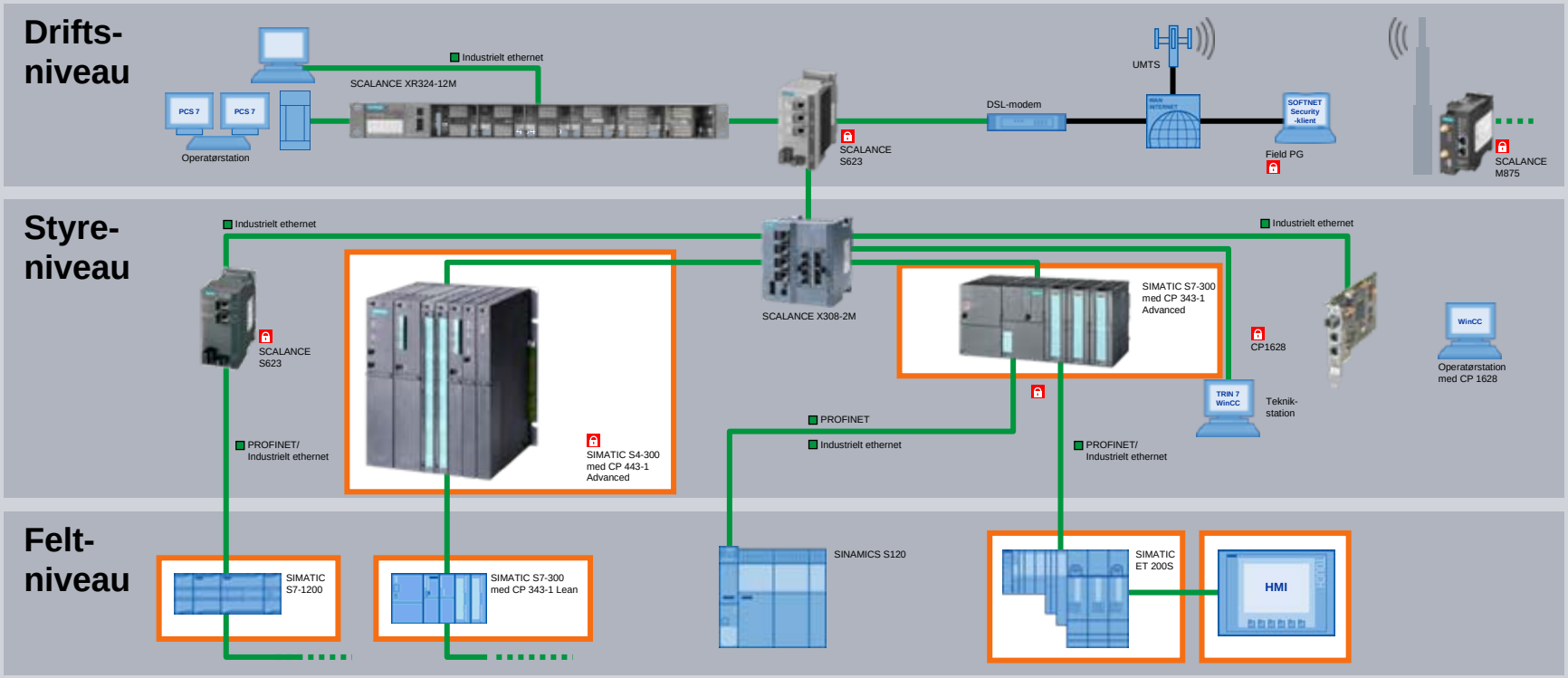
Deaktivering af tjenester

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



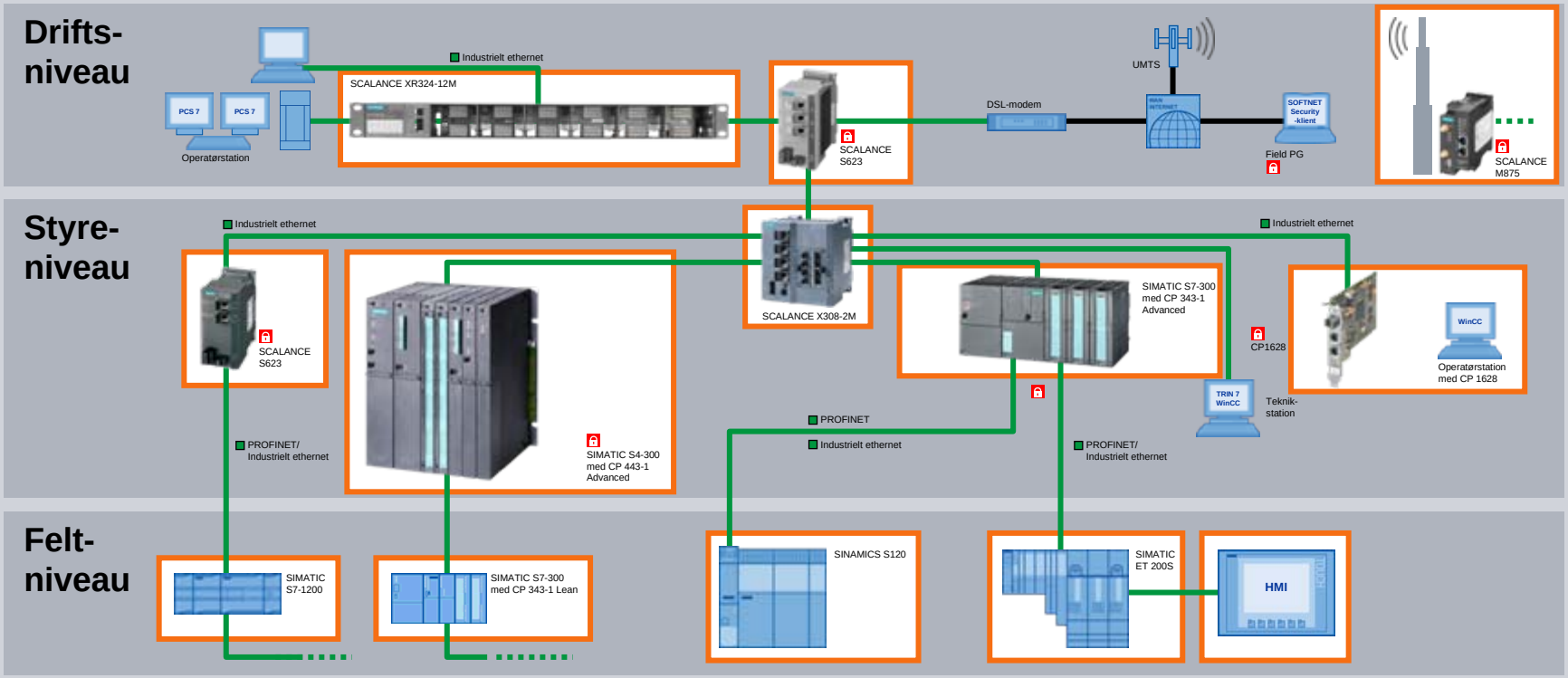
Deaktivering af hardware, porte og protokoller

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



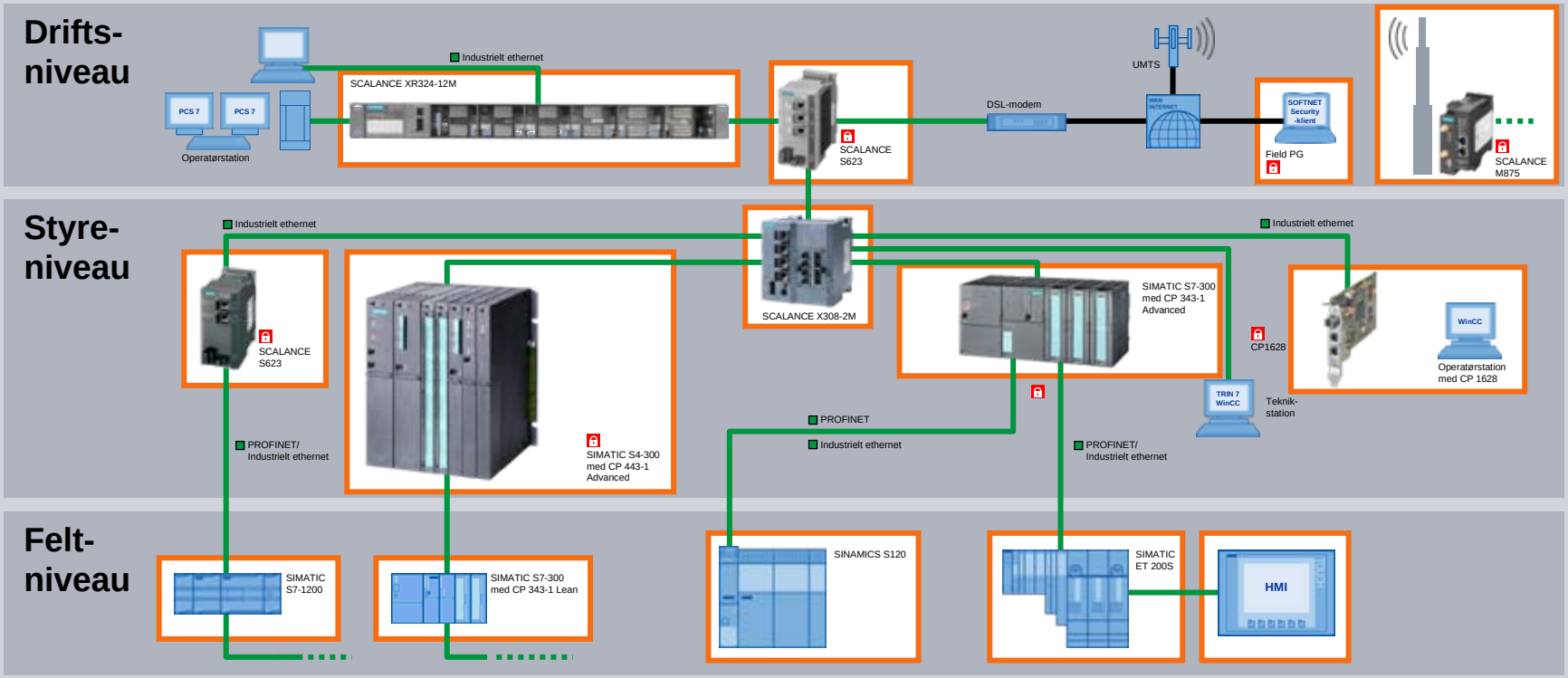
IP-Hardning

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



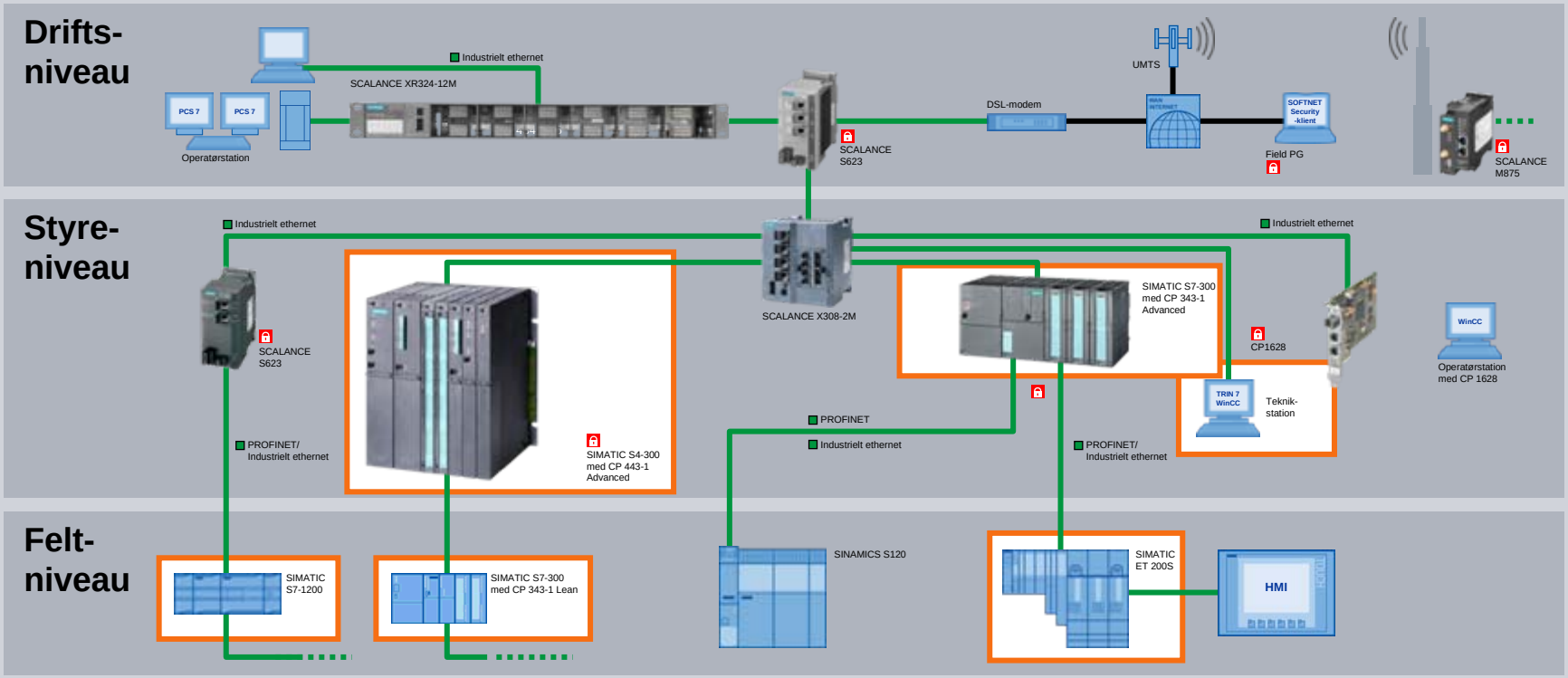
Beskyttelse af adgangskode

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



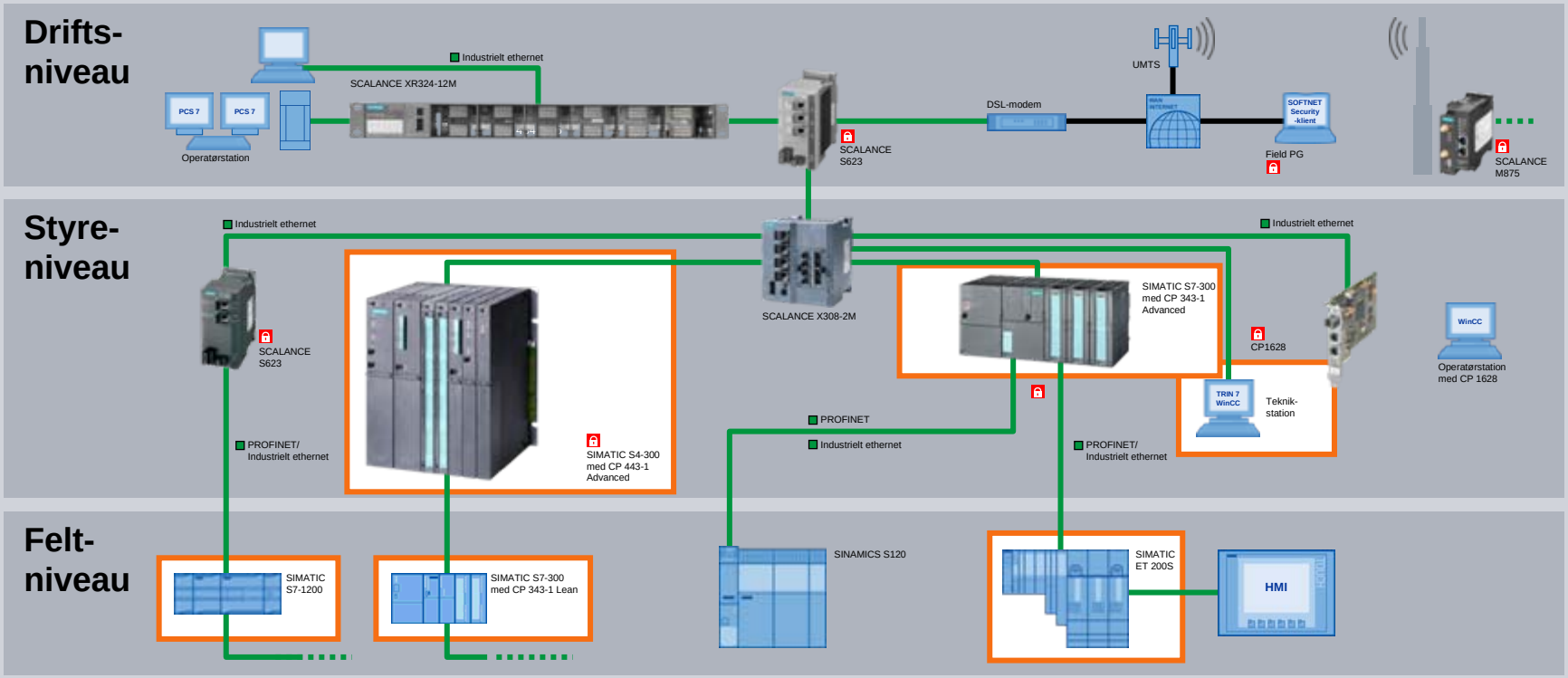
Beskyttelse af knowhow

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



Kopibeskyttelse

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

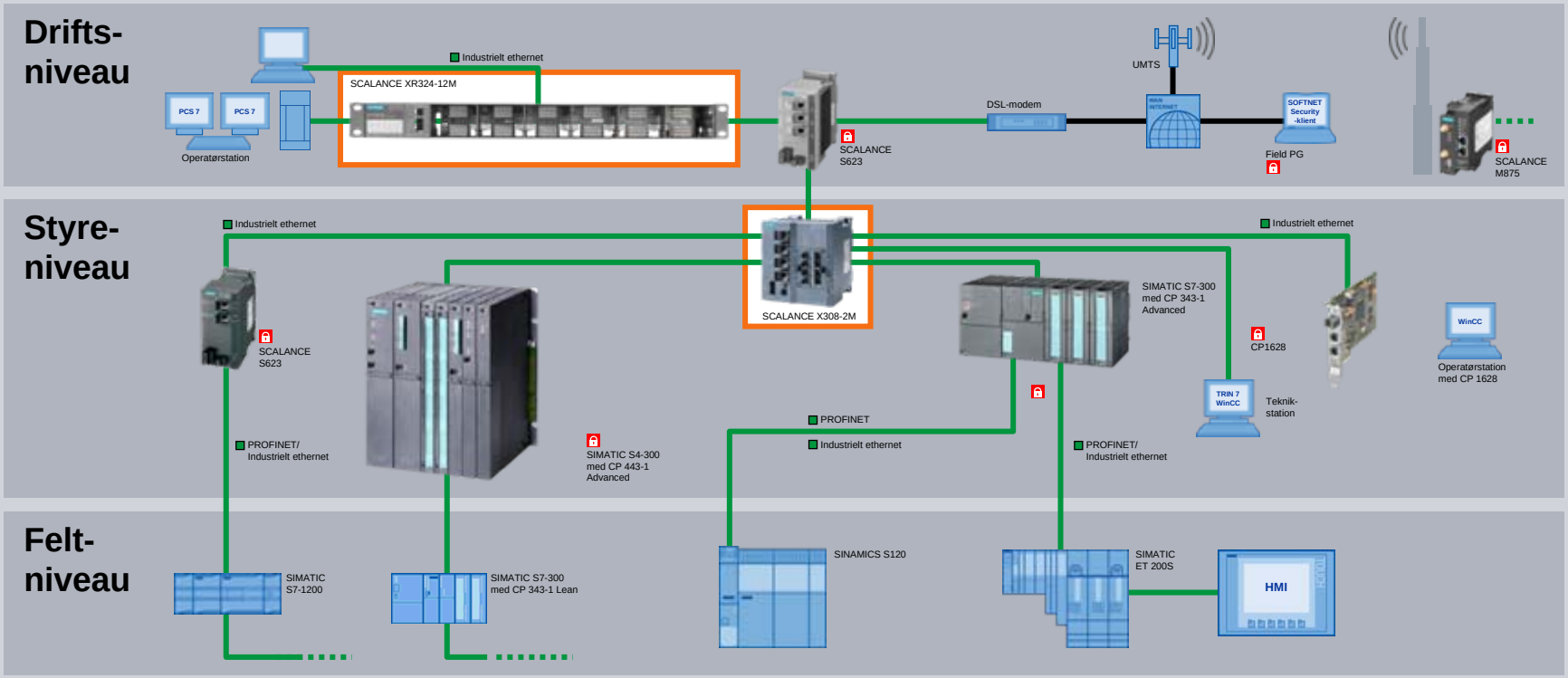


Kommunikationssystemer - Security @ feltniveau

- Virtuelle LAN (VLAN)
- Port-security og RADIUS-serverautenticitet
- Firewalls
- Virtuelle private netværk (VPN)

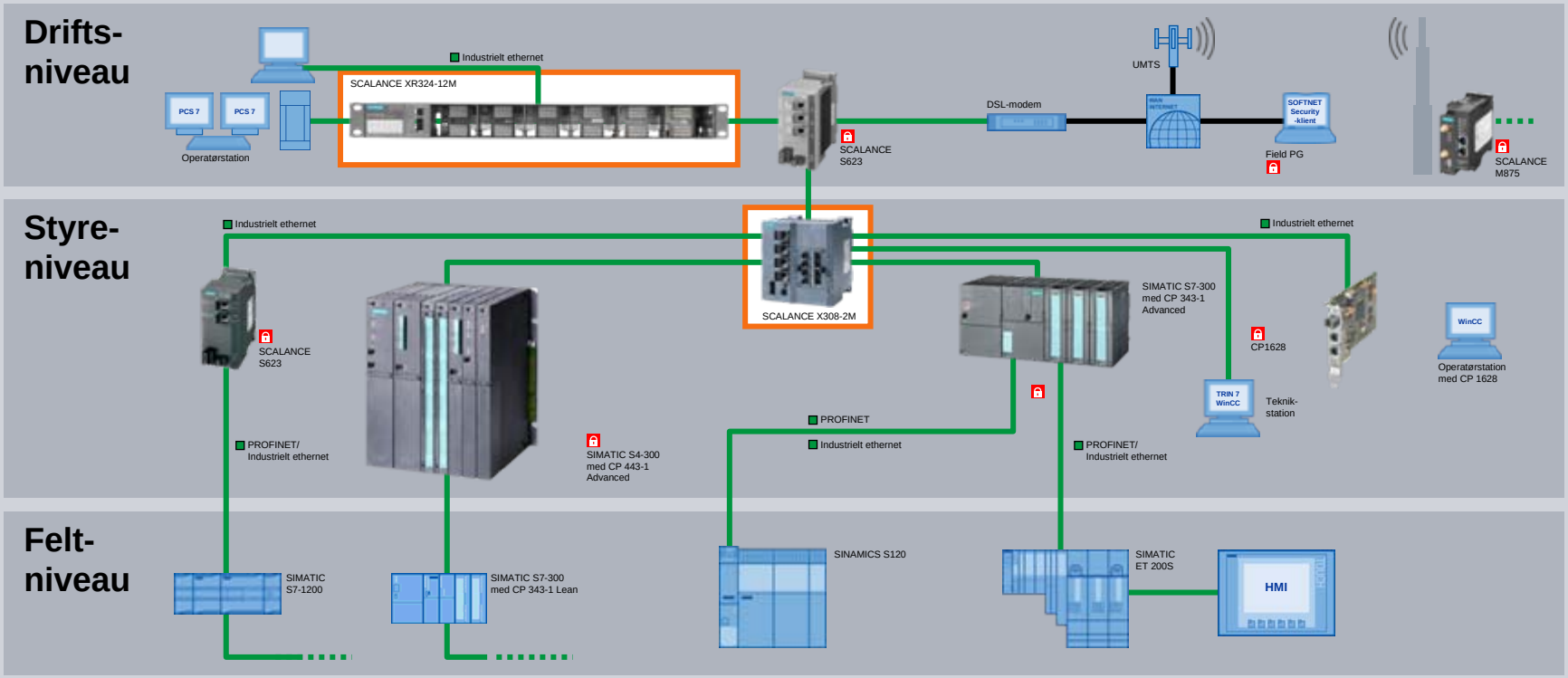
Virtuelle LAN

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



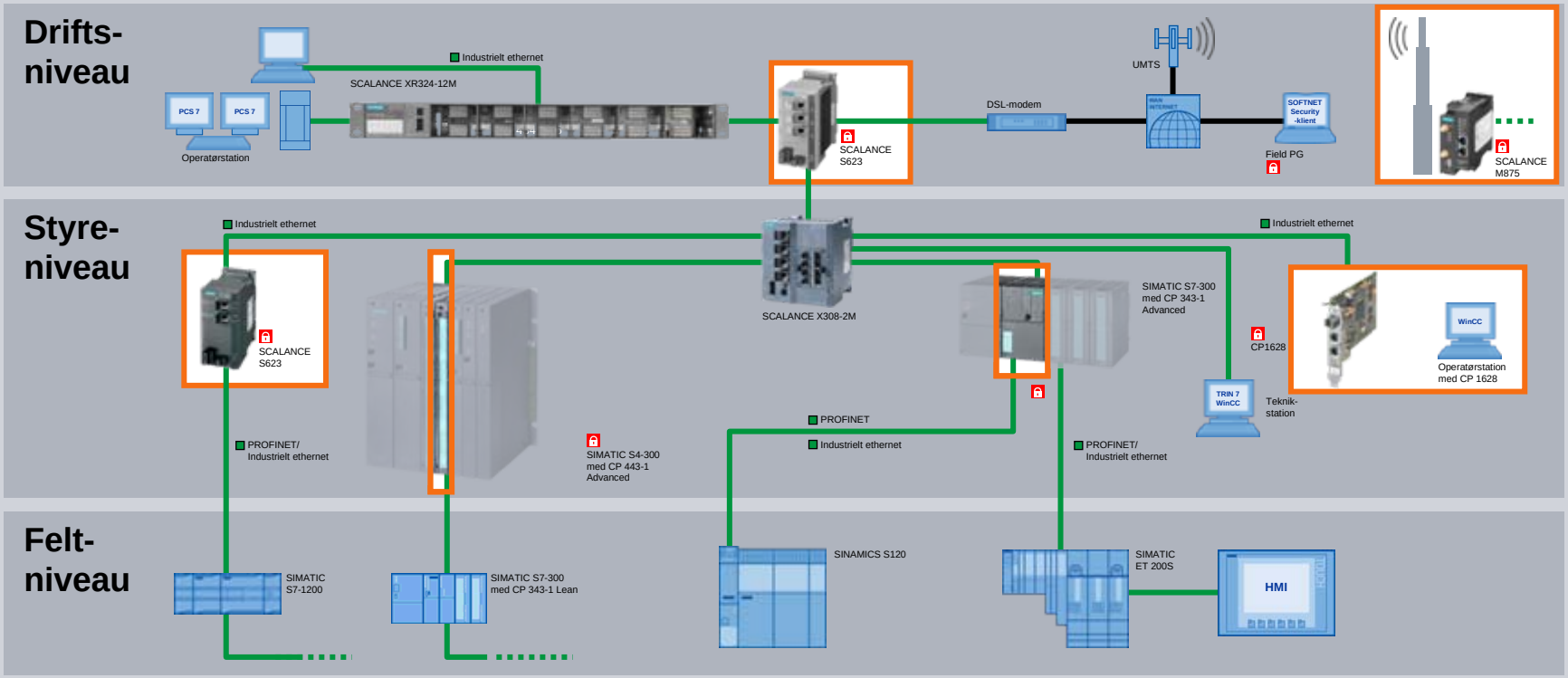
Port-security og RADIUS-serverautenticitet

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



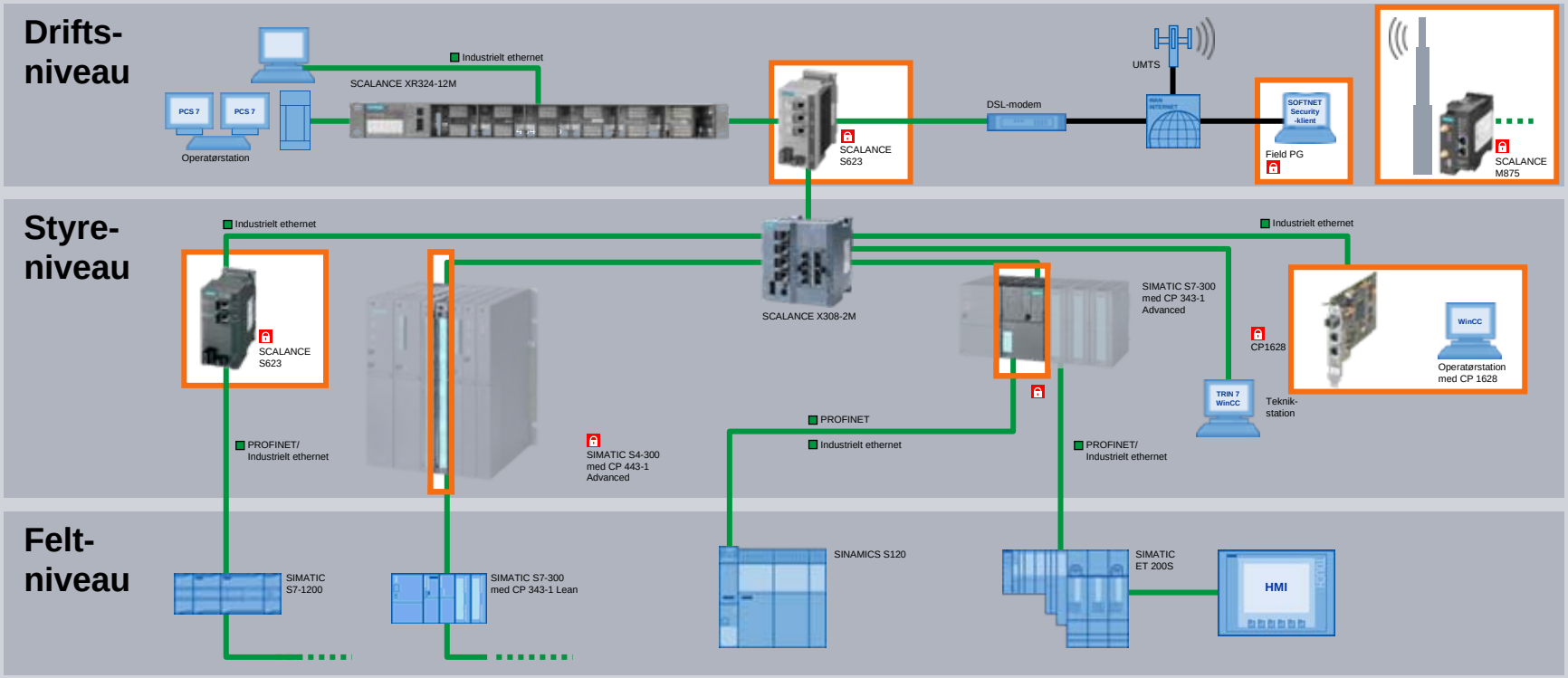
Firewalls

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



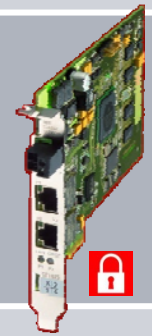
Produkter – industriel security

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



Produkter – Industriel security

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:

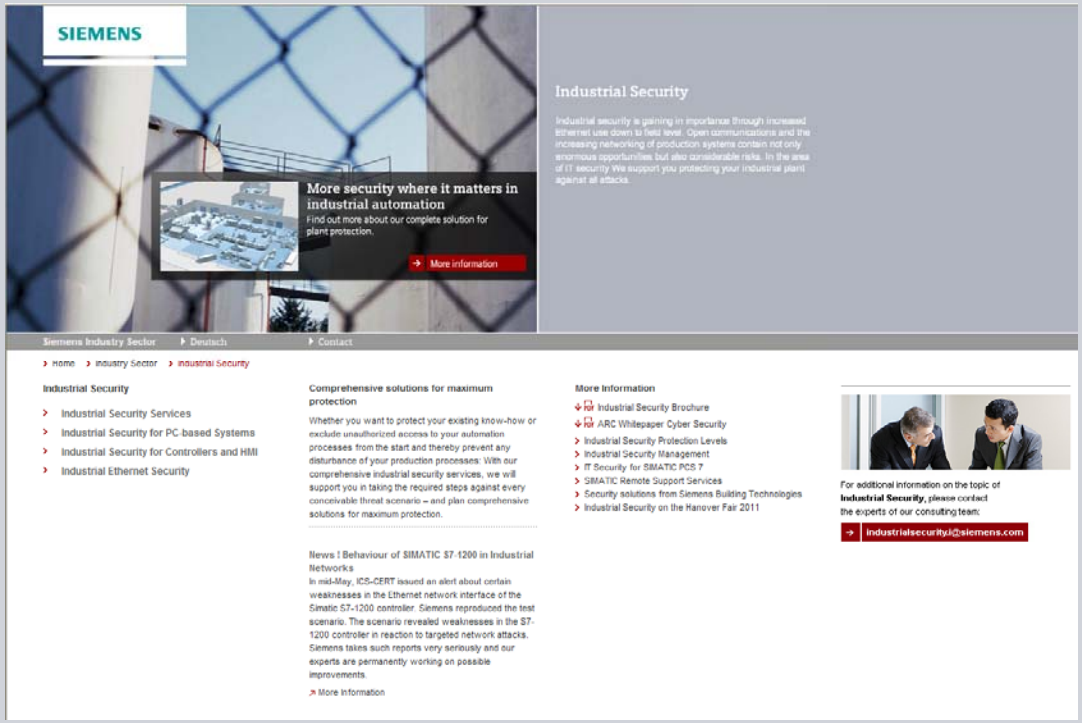
- Applications & Tools on the topic of "Industrial Security"

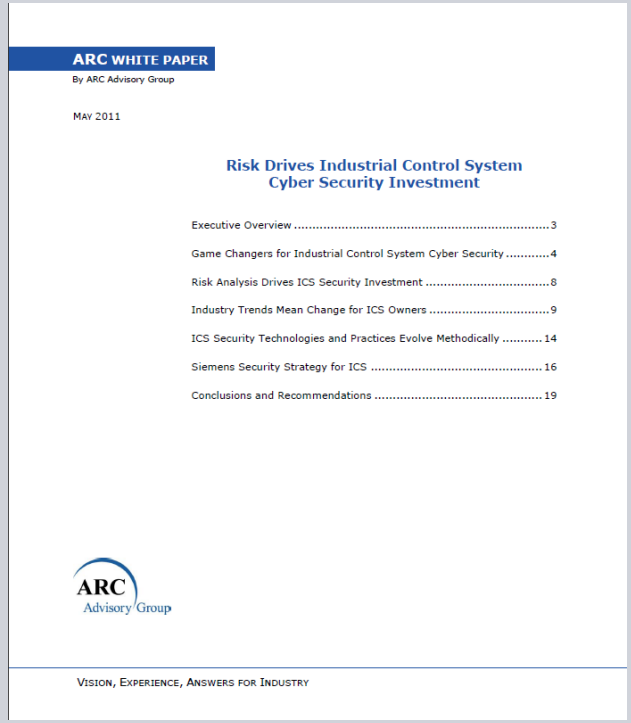
Information om emnet "Industrial Security" med fokus på:

- 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





Se her: WWW.siemens.com/industrial-security

Tak for opmærksomheden ☺

Security Integrated