

Prosjekt: Utvikling av «Factory Control System» med tilhørende sikkerhetssystem.

De fleste moderne automatiserte anlegg i dag, som har en viss størrelse og omfang, de er jo en del av et nettverk og de styres skjermbaserte systemer (HMI). Det er godt mulig å integrere inn i hverandre veldig mange tekniske systemer, slik at alle sammen kan styres og kontrolleres fra en felles «app».

Disse systemene har tradisjonelt hatt ett forholdsvis lavt sikkerhetsnivå, ved at disse systemene i liten grad har vært utsatt for cyberangrep. Dette har nå endret seg ganske radikalt.

Først så har det nå etter hvert blitt vanlig å koble de automatiserte anleggene opp mot Internett.

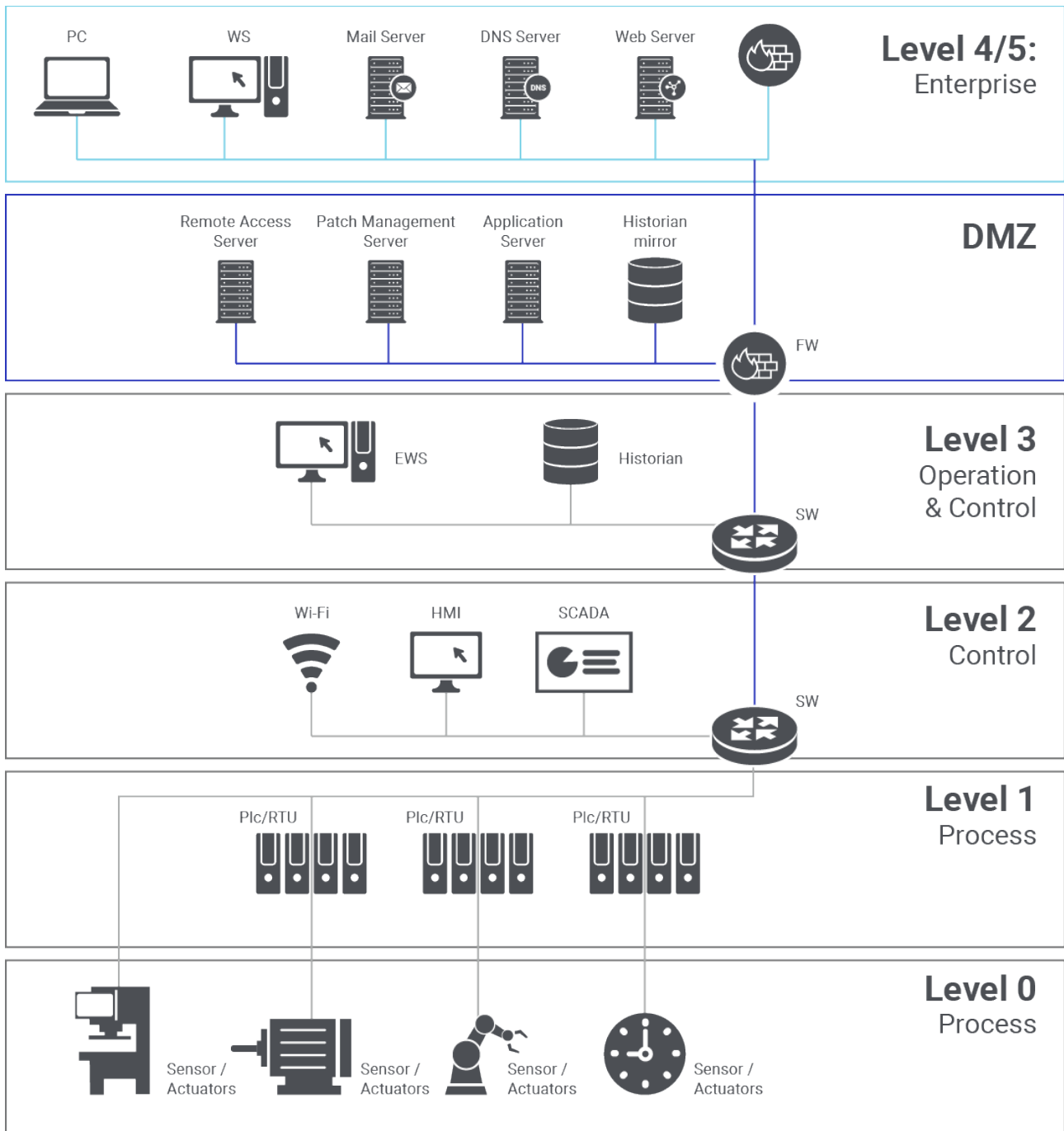
Dernest så har antallet gjennomførte angrep mot automatiserte anlegg økt nokså radikalt gjennom de siste årene. Mange av disse angrepene har også være «vellykket» for hackerne ved at de har klart å trenge inn i og å ødelegge store tekniske anlegg.

Blant de mest kjente angrepene er angrepet mot Norsk Hydro i 2019 og angrepet mot Colonial Pipeline i 2021. Hackerne klarte i begge tilfellene å ta kontroll over de tekniske driftssystemene og ødelegge dem fullstendig. I begge tilfeller så ble servere og PC'er kryptert av hackerne og det ble krevd løsepenger for å kunne gi tilgang til en krypteringsnøkkel for å låse opp systemene. Norsk Hydro betalte ikke.

Et noenlunde komplett «Factory Control System» kan jo for eksempel inneholde disse funksjonene:

- Styring av ventilasjonsanlegg.
- Styring av varmpumpe.
- Styring av reguleringsløyfe.
- Styring av sekvensstyring med bormaskin.
- Styring av pneumatikk.
- Styring av hydraulikk.
- Styring av industrirobot.
- Overvåkning av prosess via web-camera.
- Alt sammen ut i fra en felles «app».
- Fjernstyring fra Internett.
- VPN – Virtual Private Network
- Risikovurdering og sikkerhetstiltak.
- Innhold fra siste års eksamen for VG3 automatisering.

Det finnes en internasjonal referansemodell for organisering av IKT delen av automatiserte anlegg og for risikovurdering og oppbygging av sikkerhetssystemer for automatiserte systemer som heter «Purdue modellen». Denne modellen er beskrevet på den figuren som følger på neste side.



I forhold til «de tradisjonelle automasjonsfaget» så jobber man jo for en stor del på de to laveste nivåene i denne modellen. Er vi klar for litt «dybdeløring» der vi også ser på dette med å bygge opp et slikt komplett automasjonssystem inklusive en tilpasset sikkerhetsløsning?

- Klarer vi å ha på plass et komplett «Factory Control System» innen sommeren?
- Hvor mange PLS'er og systemer klarer vi å integrere inn i dette?
- Klarer vi å utarbeide gode nok sikkerhetsløsninger?