INFORMATIONSSÄKERHET I INDUSTRIELLA STYRSYSTEM

FIE Teknisk Konferens 2014-04-23

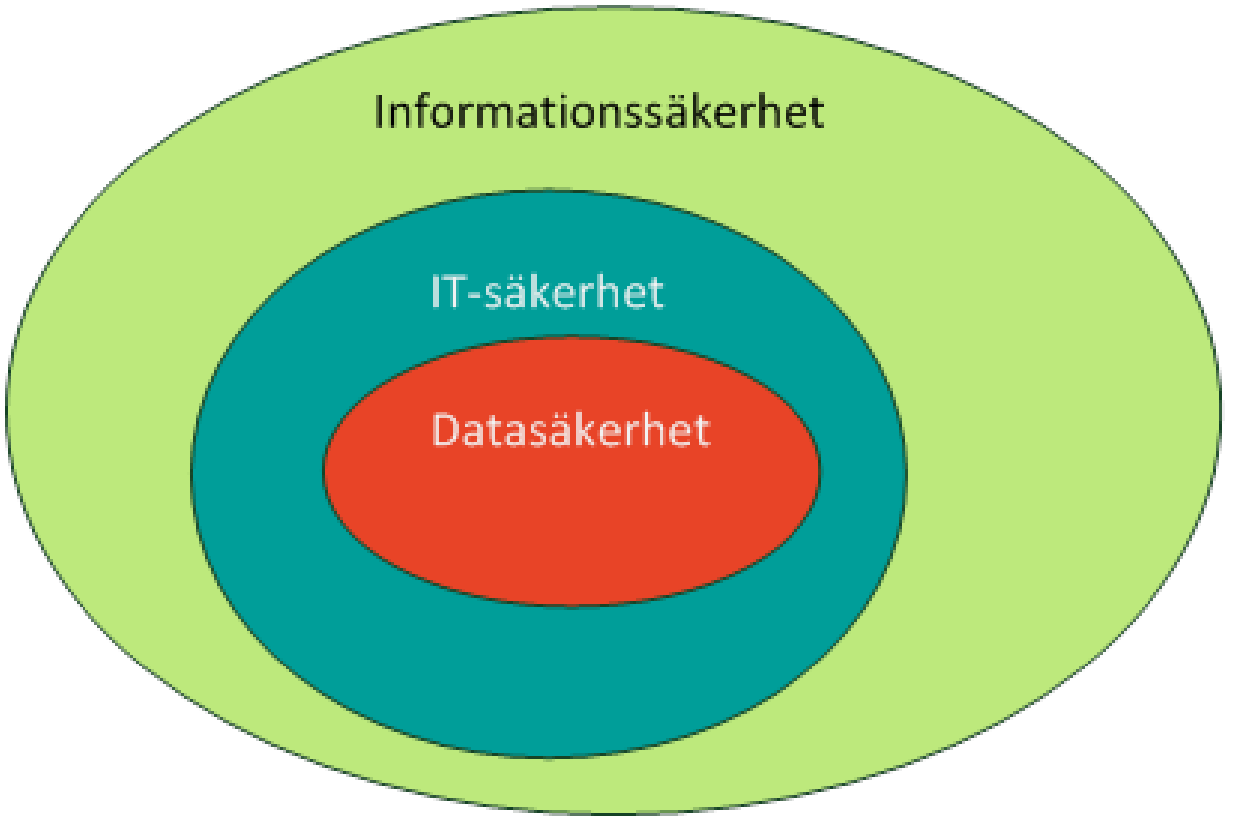
Rickard Svenningsson <rickard.svenningsson@sp.se>

SP Technical Research Institute of Sweden

RI.SE INSTITUTES

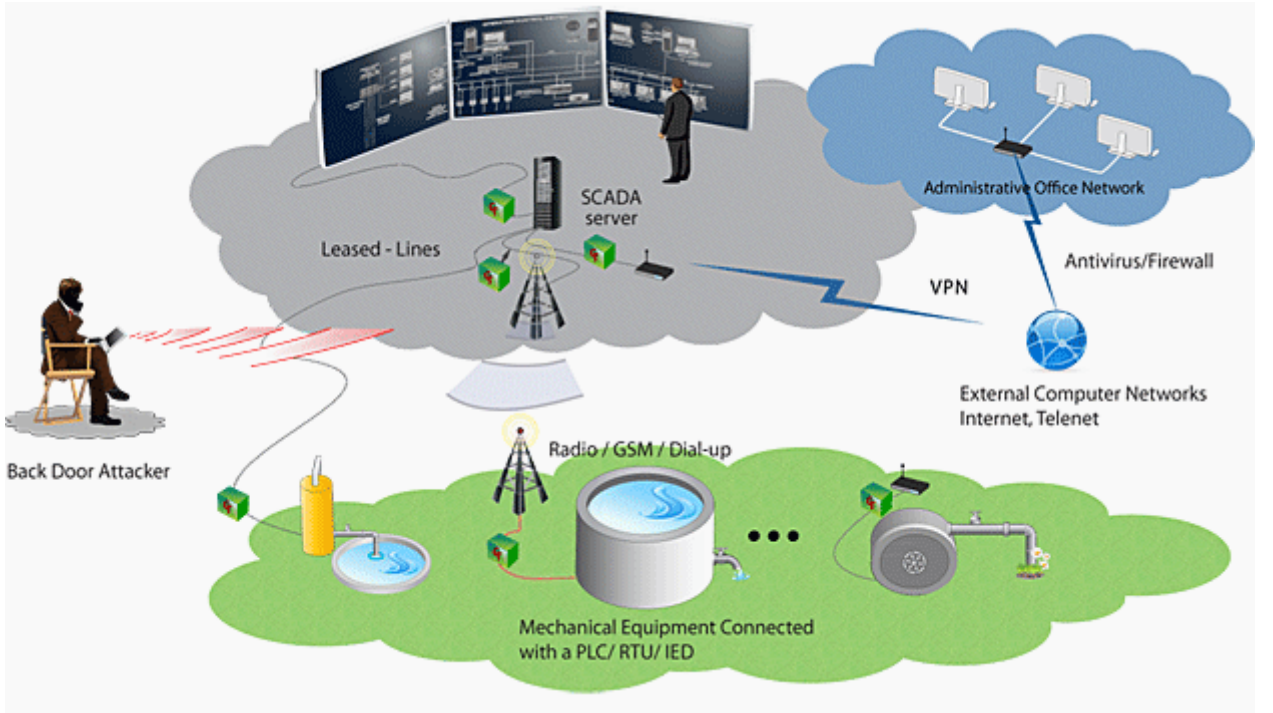
Terminologi

- SCADA (Supervisory Control And Data Acquisition)
  - Industriella styrsystem för styrning och övervakning av processer
- Datasäkerhet
  - Sekretess
  - Integritet
  - Tillgänglighet
  - …
- IT-säkerhet
  - Skydd av databehandlingsutrustning
  - Skalskydd (lås, larm mm)
  - Åtkomststyrning
  - …
- Informationssäkerhet
  - Rutiner och riktlinjer
  - Informationsklassificering
  - …



Industriella Styrsystem

Funktionssäkerhetskritiska industriella kontrollsystem (ICS), t.ex. SCADA, kopplas i allt större utsträckning upp mot kontorsdatanät och internet. Vi behöver alltså hantera data- och IT-säkerhetsaspekter integrerat med funktionssäkerhetsaspekter för sådana system.



Bildkälla: www.cryptango.com

ICS nu och förr

- Förr
  - Skräddarsydd hårdvara, ofta reläbaserat för hög driftsäkerhet
  - Kompletta lösningar från få leverantörer
  - Skräddarsydda kommunikationsprotokoll för ändamålet
  - Livslängd 15 – 20 år

- Nu
  - Ofta COTS-baserat med generella komponenter från stora tillverkare
  - Kommunikation via IP-nätverk (TCP/IP, UDP/IP, …)
    - Gamla kommunikationsprotokoll inbäddade
  - I högre utsträckning mjukvarukonfigurerat för ändamålet

Effekter av moderniseringen

- Sårbarheter upptäcks i större omfattning då fler delar samma källkod
- IT-avdelningen äger i större utsträckning även ICS-nätet
- Har man rätt kompetens för ICS hos IT, då ICS-nätet har andra krav och förutsättningar?
  - Realtidskrav på kommunikation
  - Säkerhetstestning är riskabelt
  - Tillgänglighet är kritiskt
  - Uppdateringar görs sällan då det kräver omfattande testning först (men nätverks-COTS kräver uppdateringar!)
  - Antivirus är oftast inte lämpligt i SCADA-komponenter (minimalt med program för realtidsdeterminism)
  - Outsourcing blir riskabelt

Tillgångar i det industriella styrsystemet

- Fysiska tillgångar, t.ex.
  - Kontrollsystem
  - Nätverkskomponenter
  - Byggnader
  - **Det som kontrolleras av styrsystemet (!)**

- Logiska tillgångar, t.ex.
  - IP
  - Algoritmer
  - Rutiner och vägledning
  - Processkunskap

- Mänskliga tillgångar, t.ex.
  - Specifik kunskap

Hot

- Safety - stokastiska hot
  - Förutsägbara felmoder
  - God tillgång till empiriskt data, t.ex. IEC TR 62380 eller MIL HDBK 217F för komponenter
  - Täcker in miljörelaterade hot (översvämning, brand osv.)

- Security – antagonistiska hot + stokastiska hot
  - Kända sårbarheter sprids snabbt på Internet (ex. pastebin)– svårt att hinna patcha
  - Empiriskt data svårtillgängligt – företag skyltar ogärna med att/hur de blir angripna
  - Motiverad, oförutsägbar och intelligent motståndare
  - Täcker också in miljörelaterade hot (översvämning, brand osv.) – kom ihåg ***tillgänglighet*** !

Antagonistiska hot

- Vem?
  - Insiders
  - Aktivister (”Hacktivister”)
  - Konkurrenter (länder, företag, individer)
  - Terrorister
  - Organiserad brottslighet
- Varför?
  - Status
  - Utmaning
  - Politiskt motiv
  - Roligt
  - Hämnd
  - Pengar
- Hur?
  - Social ingenjörskonst
    - Intrång i privatlivet
    - Bedrägeri
  - Hacking
    - Intrång i system
    - Personifiering
    - Systemattack (DDOS etc.)
  - Skadlig kod
    - Virus
    - Maskar
    - Trojaner
    - Bakdörrar

Skrämselpropaganda / Exempel

- Senast nu i April: Sårbarhet i OpenSSL (Heartbleed)
  - December 2011 till april 2014
  - Detta är ett problem ! Det tar lång tid att uppdatera alla SCADA-system för att lösa problemet.

- Givet i sammanhanget: STUXNET (2010)
  - Attack mot Siemens styrsystem
  - Specifikt inriktad på att förstöra anrikningsanläggningar i Iran
  - Okänt för allmänheten vem som skapade masken