Skydda cyberfysiska system

Carl Önne

Enheten för säkerhet i cyberfysiska system

Avdelningen för cybersäkerhet och säkra kommunikationer

Myndigheten för samhällsskydd och beredskap

DHS Directed

Aurora Generator Test

March 4, 2007

Cyberfysiska system

- …datorbaserade system för interaktion med maskiner, fordon och annan utrustning inklusive sensorer som kan inhämta data från omgivningen.

Var finns de?

- Energi
  - Produktion & distribution
- Fastighetsautomation
  - Hissar, klimat mm
- Processindustrier, vatten & avlopp
  - Fjärrvärme, vattenrening, raffinaderier, pumpar mm
- Transport
  - Trafikljus, belysning, klaffbroar, flyg, tåg, intelligenta fordon
- Och vidare:
  - Medicinteknik, larm & övervakningssystem, hemmasystem mm

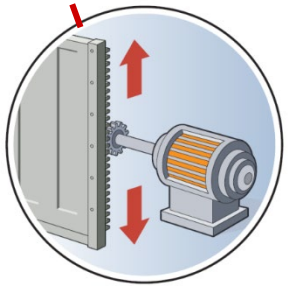
Styrdator som kan skicka elektriska signaler

Internet

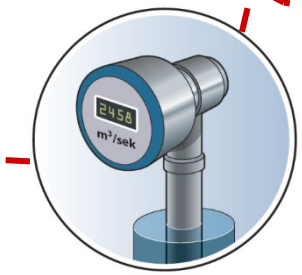
SCADA-system

Människa-maskin gränssnitt

Administrativa nätet



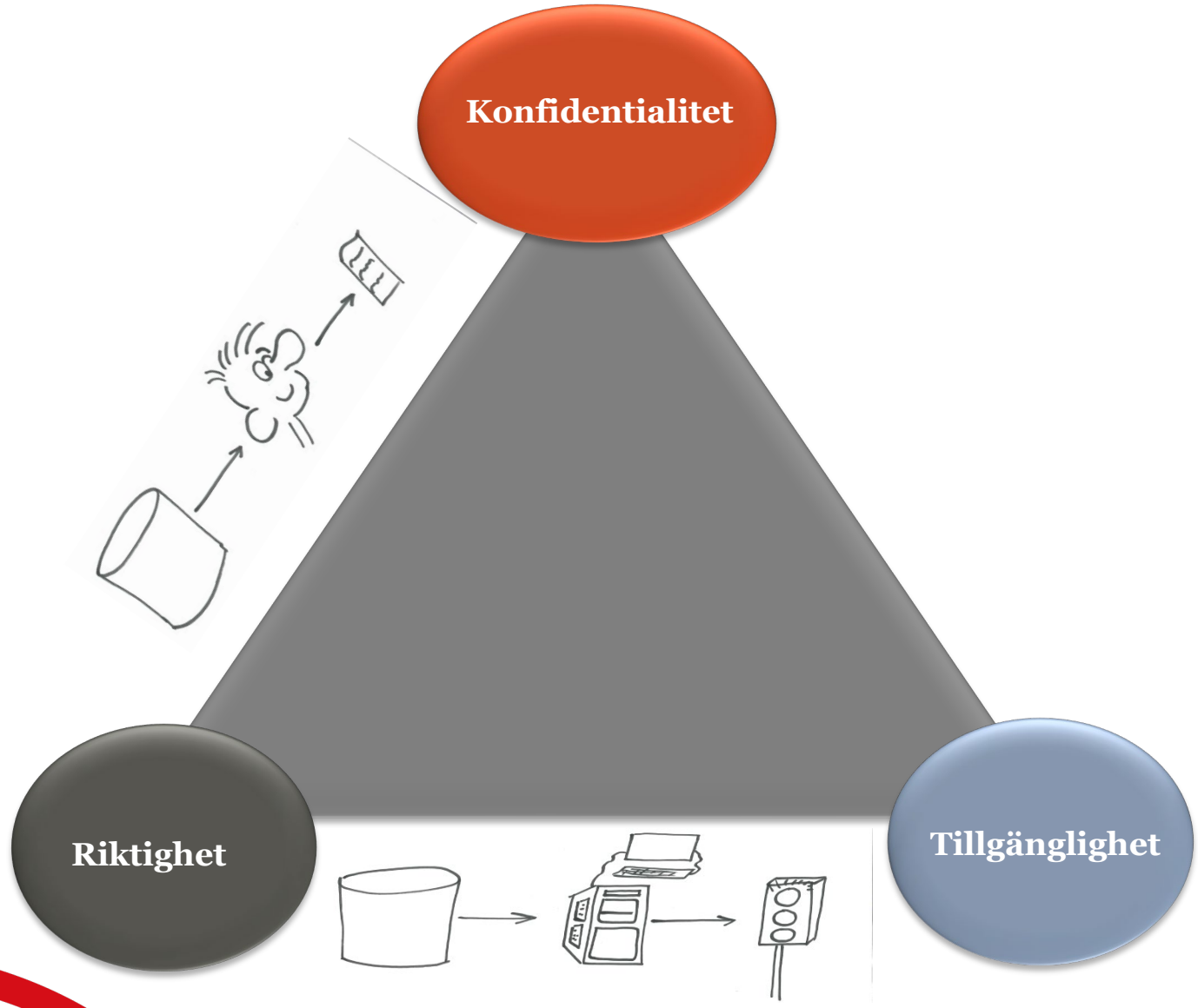
Något som kan påverka processen



Sensor som kan mäta tillståndet

Myndigheten för samhällsskydd och beredskap

KRT eller TRK?



	Administrativ IT	Informations- och styrsystem
Skydd och antivirus	Används nästan alltid	Svårt att få till
Systemens livslängd	3-5 år	Upp till 20 år
Outsourcing	Vanligt	Ovanligt
Patchhantering	Körs regelbundet	Genomförs sällan
Förändringshantering	Körs regelbundet	Utmanande beroende på legacy system
Realtidskrav	Ovanligt	Kritiskt
Tillgänglighet	Driftavbrott ofta acceptabelt	Korta avbrott kan få ödesdigra konsekvenser
Säkerhetskultur	Hög medvetenhet kring säkerhetsfrågor	Ofta låg medvetenhet kring säkerhetsfrågor
Fysisk säkerhet	Ofta bra	Mycket bra – men ofta är driftplatser obemannade

	Administrativ IT	Informations- och styrsystem	IoT
Skydd och antivirus	Används nästan alltid	Svårt att få till	Svårt att få till
Systemens livslängd	3-5 år	Upp till 20 år	1 till 10 år
Outsourcing	Vanligt	Ovanligt	
Patchhantering	Körs regelbundet	Genomförs sällan	Kan kanske inte göras
Förändringshantering	Körs regelbundet	Utmanande beroende på legacy system	
Realtidskrav	Ovanligt	Kritiskt	
Tillgänglighet	Driftavbrott ofta acceptabelt	Korta avbrott kan få ödesdigra konsekvenser	
Säkerhetskultur	Hög medvetenhet kring säkerhetsfrågor	Ofta låg medvetenhet kring säkerhetsfrågor	
Fysisk säkerhet	Ofta bra	Mycket bra – men ofta är driftplatser obemannade	Ofta exponerade

Hotbild

Myndigheten för samhällsskydd och beredskap

Vägledning

Myndigheten för samhällsskydd och beredskap

BAS5 (Tidigare SvK FOSS)

- Fem säkerhetsverktyg som underlättar för operatörer av industriella informations- och styrsystem
  1. Logginsamlingsserver
  2. Nätverksinspelningsserver
  3. Larmserver
  4. IDS-server
  5. Brandvägg för SCADA- och ICS-miljö (länk)

- Installations- och användarmanual för ovanstående

Myndigheten för samhällsskydd och beredskap

Utbildning, träning och övning

Nationell Cyber Range (NCR) i Linköping

Myndigheten för samhällsskydd och beredskap

Forskning, studier, test och experiment

Research Centre on Resilient Information and Control Systems (RICS) : 2015 - 2020

Center for Resilient Critical Infrastructures (CERCES) : 2015 - 2020

Använder Nationell Cyber Range

Resilient Internet of Things (RIOT) : 2019 – 2023

Myndigheten för samhällsskydd och beredskap

Elektromagnetiska – hot, störsändare och mikrovågsvapen

Hembygge, försäljning på nätet

Foto: Information Unlimited, https://www.amazing1.com/

Fordonsburen utrustning för att stoppa bilar genom att bestråla elektroniken.
Foto: Diehl Defence

Foto: FOI

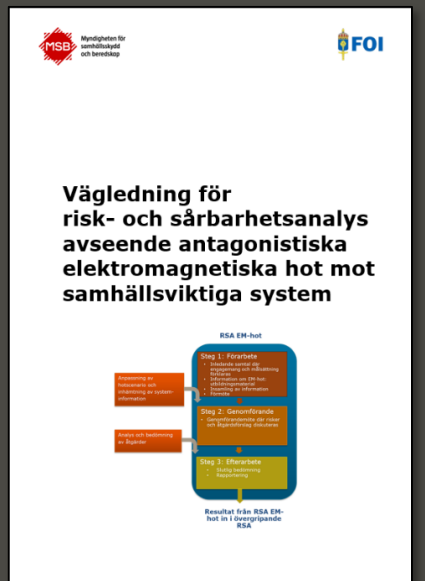
Foto: FOI

Foto: Necom-Telecom

Myndigheten för samhällsskydd och beredskap

En förlängning (del av) Cyberhotet

- Ökad integrerad användning av trådlös kommunikation inom system och mellan system
- System med kritiska beroenden
- Sårbara nyckelkomponenter



Myndigheten för samhällsskydd och beredskap

Tack!

https://www.msb.se/ICS

https://www.msb.se/elektromagnetiskahot

Myndigheten för samhällsskydd och beredskap