

Skydda cyberfysiska system

Carl Örne

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



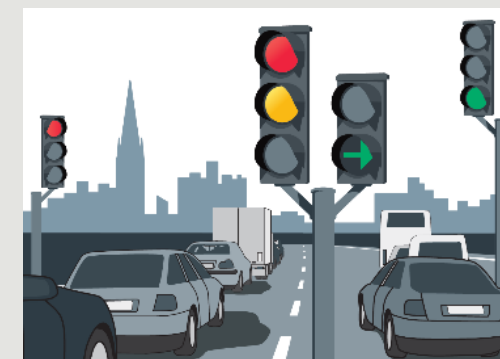
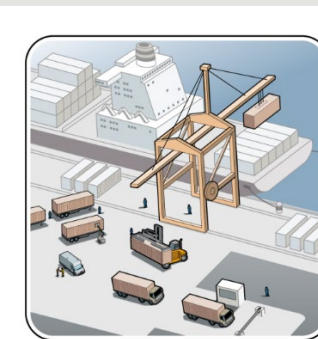
Cyberfysiska system

- ...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



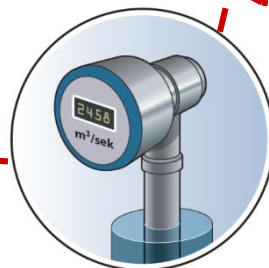
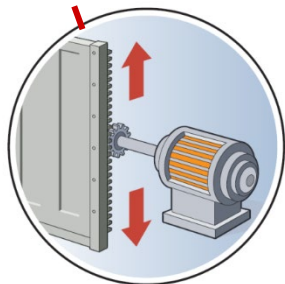
Styrdator som kan skicka elektriska signaler



Internet

SCADA-system

Människa-maskin gränssnitt

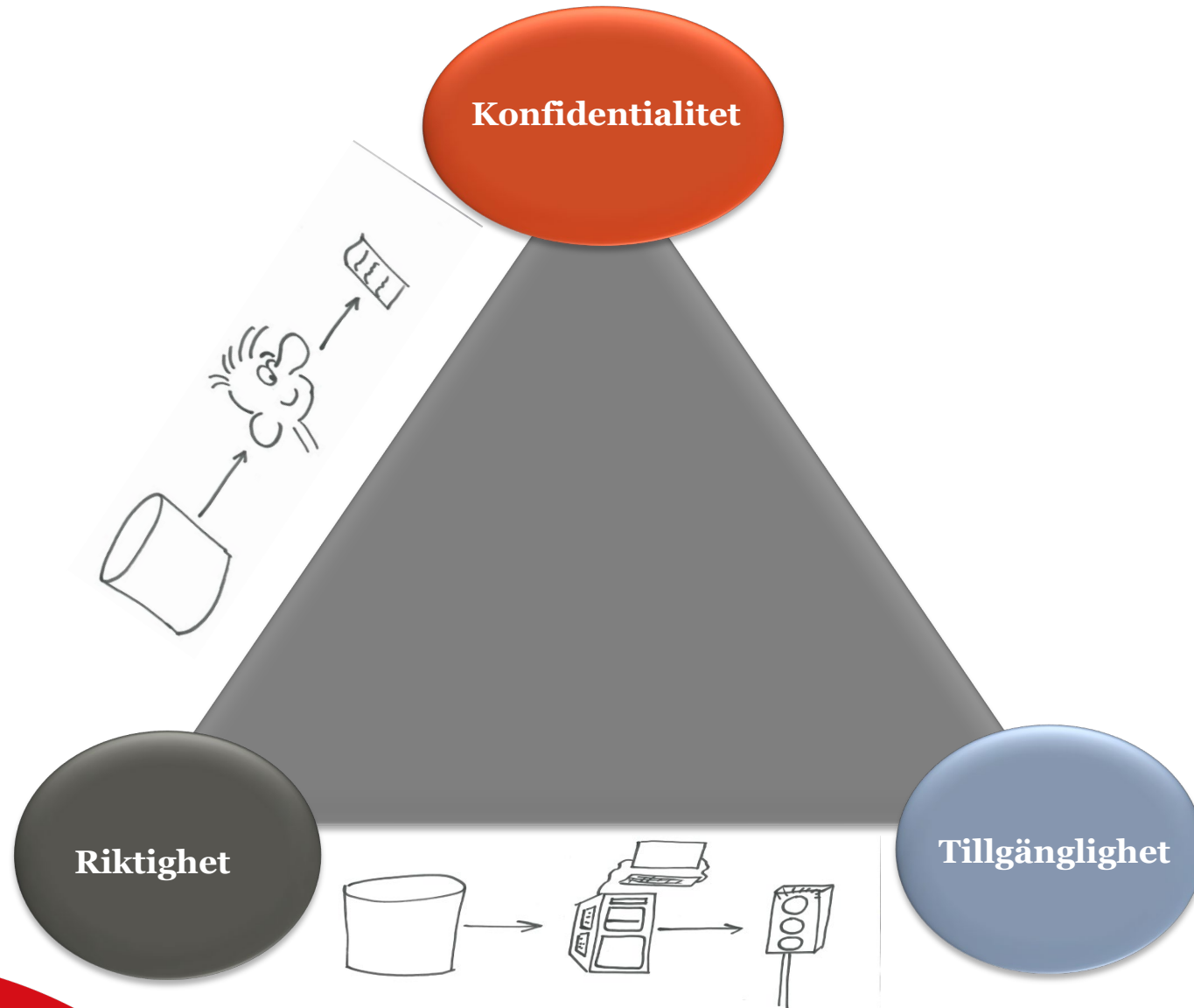


Något som kan påverka processen

Sensor som kan mäta tillståndet

Administrativa nätet

KRT eller TRK?



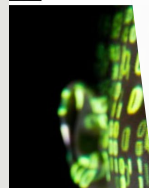
	Administrativ IT	Informations- och styrsystem
Skydd och antivirus	Används nästan alltid	Svårt att få till
Systemens livslängd	3-5 år	Upp till 20 år
Outsourcing	Vanligt	Ovanligt
Patchhantering	Körs regelbundet	Genomförs sällan
Förändringshantering	Körs regelbundet	Utmanande beroende på legacy system
Realtidskrav	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

An alarm into US

Paul Szoldra, Task



Alert (TA18-106A)

Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

Original release date: April 16, 2018 | Last revised: April 20, 2018

Print

Tweet

Send

Share

Russian 'Trojan' malware critical in since 20

Systems Affected

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

Overview

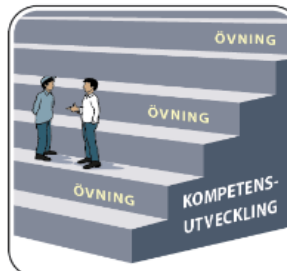
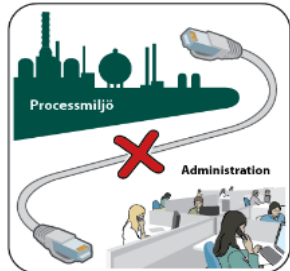
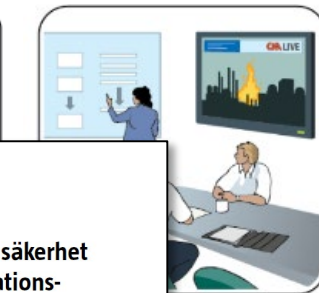
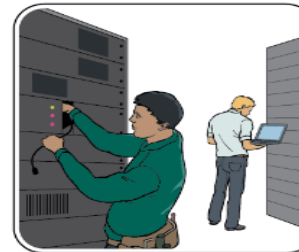
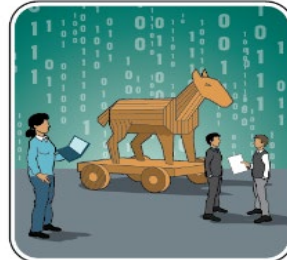
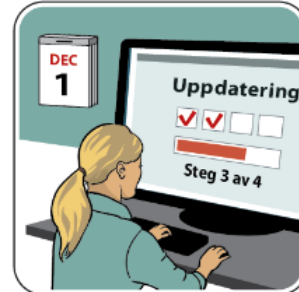
Update: On April 19, 2018, an industry partner notified NCCIC and the FBI of malicious cyber activity that aligns with the techniques,

"In the worst case, lives lost»

Dagbladet found over 2500 Norwegian management systems on-line. These are used for example in defense, health, oil industry and public transport.

RUSSIAN HACKING ATTACKS COULD 'FLOOD US CITIES WITH SEWAGE' AND CAUSE DEADLY EXPLOSIONS

Vägledning



MSB Myndigheten för samhällsskydd och beredskap

Vägledning till ökad säkerhet i industriella informations- och styrsystem

The collage includes several images: a control room with multiple monitors, a power plant with large turbines, a close-up of a control panel, and an industrial facility with tall chimneys.

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



NCS3 - Regelverk och krav inom området industriella informations- och styrsystem

En uppdatering av utvecklingen sedan december 2012

KARIN MOSSBERG SONNEK, FREDRIK LINDGREN

FOI
MSB

NCS3 - Industriella protokoll i Sverige

En översikt över protokoll inom industriella informations- och styrsystem i kritisk infrastruktur

Björn Lindahl

FOI
MSB

NCS3 - Virtualisering inom industriella informations- och styrsystem

En översikt

AMUND GUDMUNDSON HUNSTAD
CHRISTINA DAHL

FOI

NCS3 - Kryptografiska funktioner inom industriella informations- och styrsystem

ESSI, DAVID LINDAHL, LARS WESTERDAHL

FOI
MSB

NCS3 - Industriella informations- och styrsystem inom fastighetsautomation

En förstudie

KARIN MOSSBERG SONNEK, FREDRIK LINDGREN

FOI

NCS3 - Beroenden till industriella informations- och styrsystem

En förstudie

Karin Mossberg Sonnek

FOI

NCS3: Internetanslutna styrsystem i Sverige

En studie av Censys och Shodan

HANNES HOLM

ERSSON,
VER

FOI
MSB

NCS3 - Översikt över arbetet med cyberfysiska system på kommunal nivå

ERSSON,
VER

FOI
MSB

NCS3 - Molntjänster inom industriella informations- och styrsystem

En översikt av säkerhetsaspekter

AMUND GUDMUNDSON HUNSTAD
MARTIN KARRESAND

FOI
MSB

NCS3 Studie – Standardserie ISA/IEC 62443

Användning och erfarenheter bland svenska ICS-aktörer

AR HEDTJÄRN SWALING, ANN-SORE STENÉRUS DOVER

FOI

NCS3 Studie – IoT-relaterade risker och strategier

Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem

FOI

Monitorerings- och övervakningssystem

Prisering och översikt av IDS-teknik inom IIS

ESAND

FOI
MSB

FOI-R-4197-SE
MSB 2015:2
ISSN 1650-1942

FOI-R-4415-SE
MSB 2016:5134
ISSN 1650-1942

Mars 2017

FOI-R-4597-SE
MSB 2017:1620
ISSN 1650-1942

Juni 2018

Utbildning, träning och övning

Nationell Cyber Range (NCR) i Linköping



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



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

En förlängning (del av) Cyberhotet

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

MSB Myndigheten för samhällsskydd och beredskap FOI

Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktiga system



Bilderna: MSB/FAU och Bilderna: Peter Hansson/FAU/FAU/FAU


MSB Myndigheten för samhällsskydd och beredskap FOI

Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktiga system



MSB Myndigheten för samhällsskydd och beredskap FOI

Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktiga system



Vägledning
för skydd mot avsiktliga EM-hot

En säker värld för en säkrare värld



FORTIFIKATIONSVERKET

MSB Myndigheten för samhällsskydd och beredskap

Tack!

<https://www.msb.se/ICS>

<https://www.msb.se/elektromagnetiskahot>



Myndigheten för
samhällsskydd
och beredskap