



Myndigheten för
samhällsskydd
och beredskap

Cyberfysiska system – vad är det?



Hej! På kommande sidor
kommer jag att beskriva för
dig vad cyberfysiska system är.



Maskiner, fordon och apparater som innehåller små och stora datorer är vanligt förekommande i samhället. Dessa datorer används för att styra och övervaka maskinerna, fordonen eller apparaterna antingen med eller utan en människas inblandning. Datorerna är också inkopplade i ett eller flera nätverk med sladdar eller trådlöst. Ett cyberfysiskt system är datorerna, nätverken och deras möjlighet att göra om styrsignaler till händelser i maskinen, fordonet eller apparaten de är kopplade till.

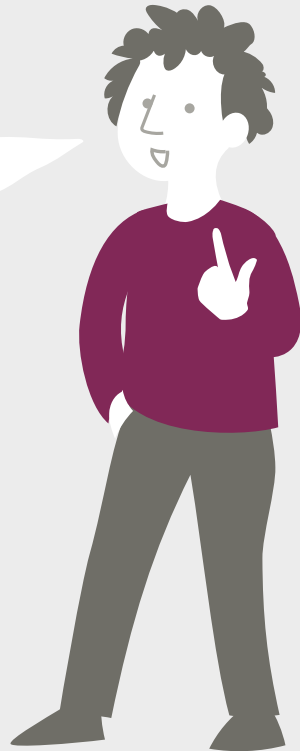
MSB beskriver cyberfysiska system som ”datorbaserade system för interaktion med maskiner, fordon och annan utrustning, inklusive sensorer som kan inhämta data från omgivningen”.

Låt oss titta närmare på vad det kan vara för typ av system och hur dessa kan styras.



MSB delar in cyberfysiska system i två delar, ICS och IoT.

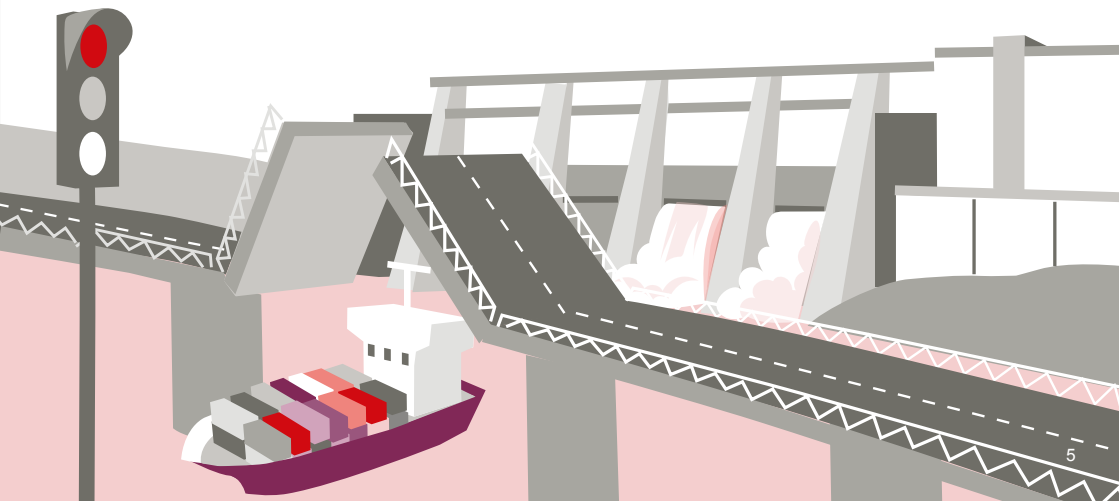
ICS betyder Industrial Control System och IoT är en förkortning av Internet of Things. Nu ska jag berätta vad det är för något.



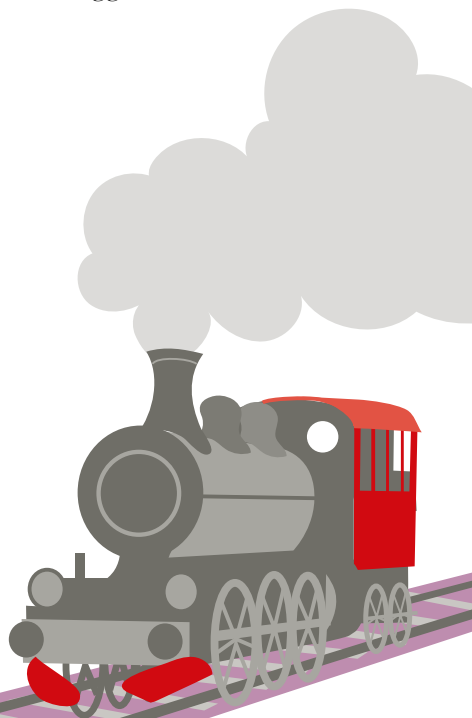
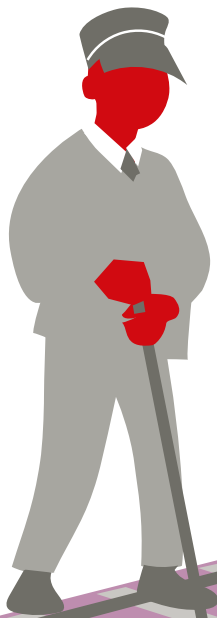
På svenska kan ICS översättas till industriella informations- och styrsystem. ICS kan vara datorsystem som finns inom till exempel vattenkraft i våra älvar, vattenrening i din kommun eller fjärrvärme till ditt hus. Det kan även vara datorsystem som finns inom transportsektorn för att lägga om växlar för tåg, öppna och stänga broar eller få trafikljus att slå om.

En process är ett slags flöde där det du lägger in i processen förändras så att det du får ut är det du ville att processen skulle göra. Det kan till exempel vara smutsigt vatten som går in i ett reningsverk. När reningsverkets processer har renat vattnet kan det släppas ut i naturen igen.

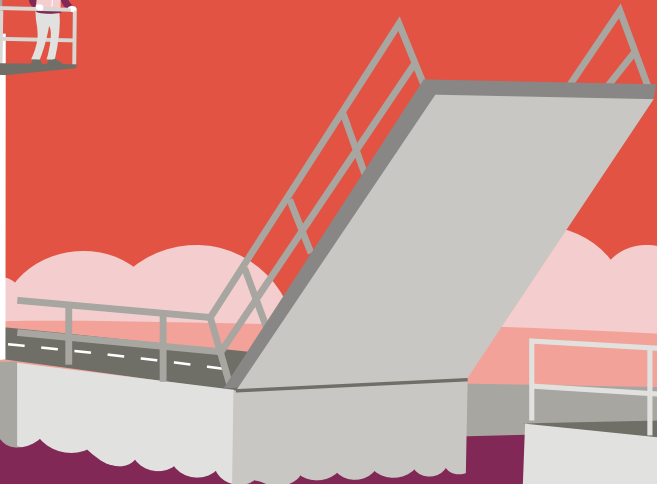
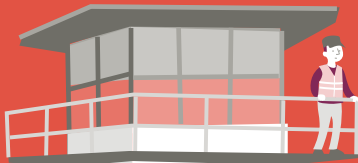
Som du förstår kontrolleras många processer som används inom bland annat samhällsviktig verksamhet med ICS.



De system som ICS kontrollerar var tidigare manuellt, elektriskt eller mekaniskt styrda. Det var till exempel när en människa som vred på en ratt för att öppna en lucka, slog om en strömbrytare eller drog i en spak för att lägga om en växel för tåget.



I takt med att samhället har blivit mer tekniskt utvecklat och datoriserat har små datorer skapats som öppnar luckan eller fäller spaken. De här små datorerna övervakades tidigare av människor i en central som var placerad direkt i närheten av luckan eller växeln.



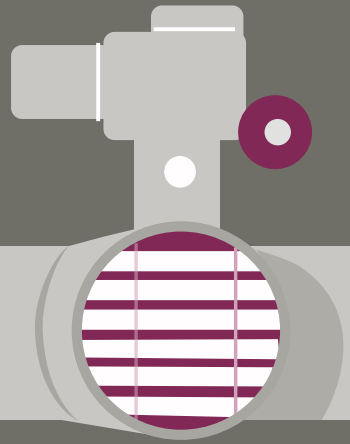
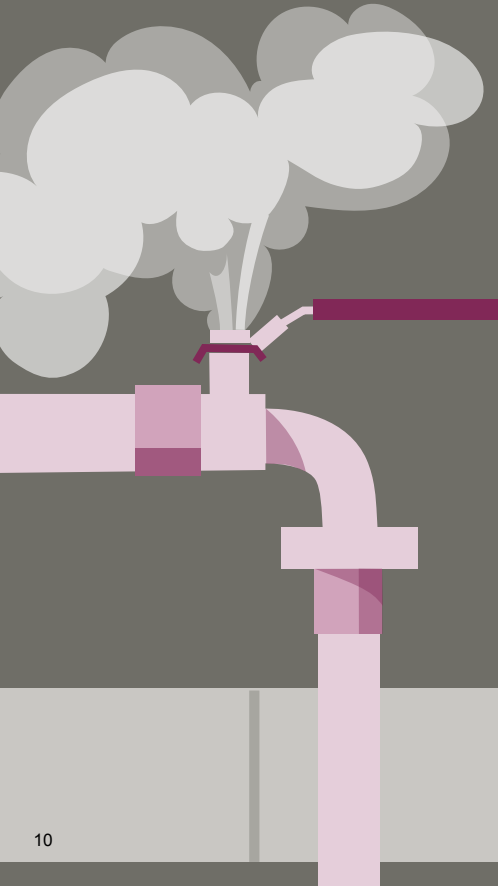
Men samhället utvecklas fort. Det innebär att människan kan övervaka och påverka luckan eller växeln på allt längre håll. Systemen kan även kopplas ihop i nätverk. De kan till och med kopplas upp mot internet!



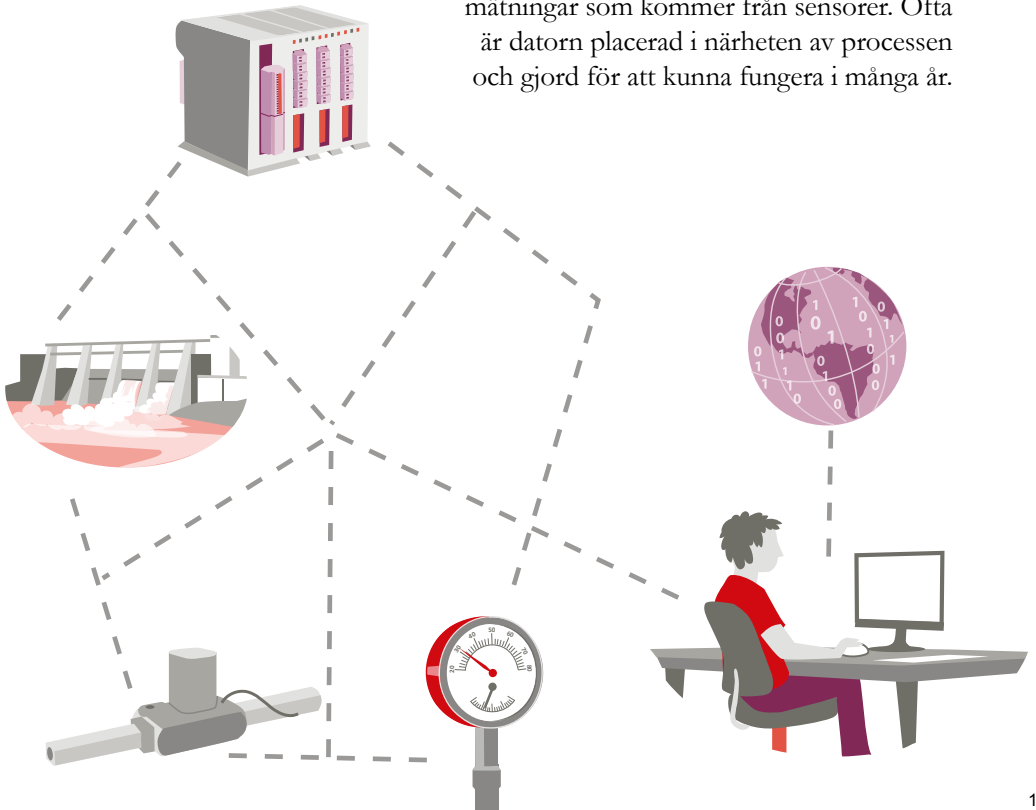
Det går att beskriva ICS som flera samverkande funktioner som påverkar en process. En sådan funktion kan vara sensorer som mäter processen, som till exempel temperatur och flöde.



En annan funktion kan vara ett ställdon (även kallad ”aktuator”) som påverkar processen. Exempel på ställdon är en ventil som kan styra tryck eller en motor som öppnar ett spjäll.



Ytterligare en funktion är en dator som har till uppgift att styra processen. Styrningen av ställdonen baseras på förutbestämda programmerade inställningar men även via mätningar som kommer från sensorer. Ofta är datorn placerad i närheten av processen och gjord för att kunna fungera i många år.

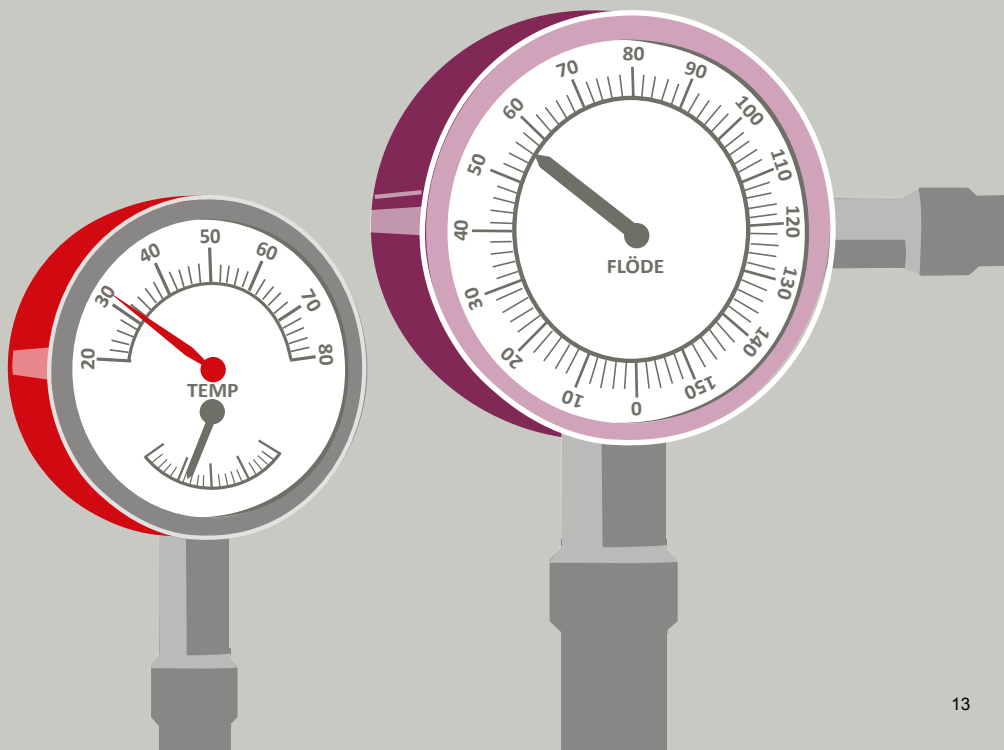


En dator behöver ett operativsystem för att fungera. Operativsystem behöver uppdateras ofta, annars blir det sårbart och kan då lättare angripas eller gå sönder. Ett operativsystem som inte uppdateras blir därför med tiden sårbart.

ICS-datorer är tänkta att användas i 15, 20, ja ända upp till 30 år. När såg du en så gammal dator senast? ICS-datorerna kan därför sedan länge ha passerat tillverkarens slutdatum, precis som mjölk som har passerat sitt utgångsdatum. För ett gammalt system som har passerat slutdatum finns det inte några nya versioner av datorns operativsystem och inte heller några säkerhetsuppdateringar. Det finns med andra ord inte någon support på systemet. Systemet blir fort sårbart och kan därför vara öppet för angrepp. Men i ICS-datorer som används så länge finns sårbarheterna kvar. Därför behöver ICS-datorerna skyddas extra noga. Ett sårbart operativsystem kan göra det möjligt för andra personer än de som ska komma åt operativsystemet att skada eller påverka operativsystemet.

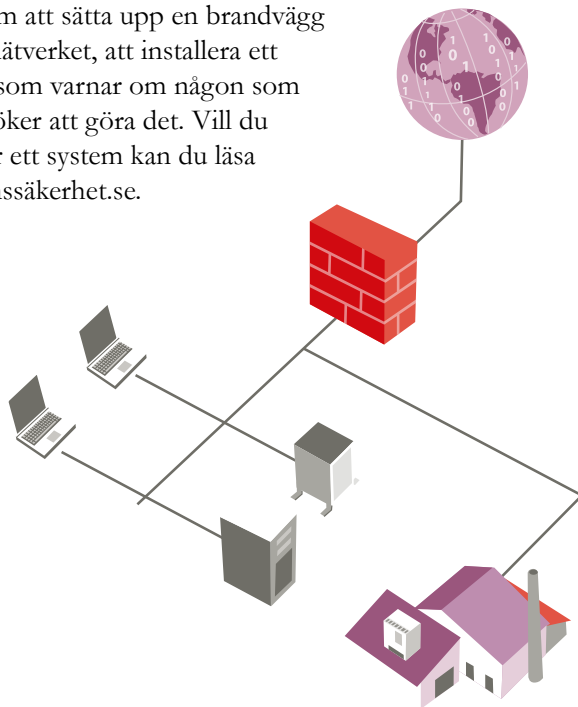


En process behöver övervakas för att säkerställa att ingenting blir fel. Men processen måste kunna påverkas för att förändra den eller korrigera den. Ökar behovet av leverans behöver ställningens inställningar ändras, till exempel för att öka tryck, minska temperatur eller öka hastighet.

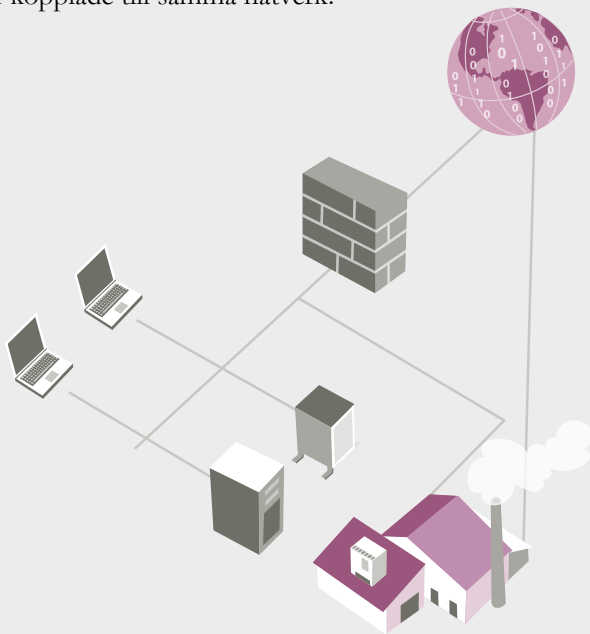


Genom att koppla ICS till datornätet för kontoret eller andra system är det möjligt att få ut mätvärden för att till exempel skapa fakturor till kunder eller för att samla statistik.

Om datornätet i sin tur är kopplat till internet kan vem som helst som har tillgång till internet komma åt ICS, om det inte skyddas på något sätt. Systemet kan skyddas på massor av olika sätt. Det kan ske genom att sätta upp en brandvägg i nätverket, att segmentera nätverket, att installera ett intrångsdetekteringssystem som varnar om någon som inte ska komma åt ICS försöker att göra det. Vill du veta mer om hur du skyddar ett system kan du läsa om det på www.informationssakerhet.se.



I dagens tekniskt utvecklade samhälle kan även sensorer, ställdon och datorer, det vill säga de delar som ingår i processen, också vara uppkopplade mot internet. Det innebär att varje enskild del kan ha en egen uppkoppling till internet. Om ICS dessutom är kopplad mot datornätet kan det innebära att kontorsdatorerna eller andra system blir åtkomliga från internet via ICS. Om inte denna uppkoppling skyddas blir det som en bakväg in i ICS men även till kontorsdatorerna. Detta är möjligt eftersom ICS och kontorsdatorerna är kopplade till samma nätverk.



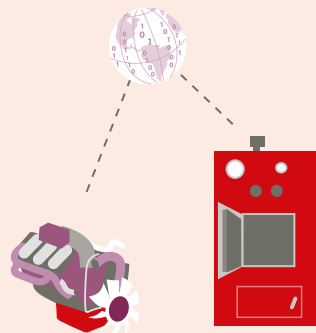
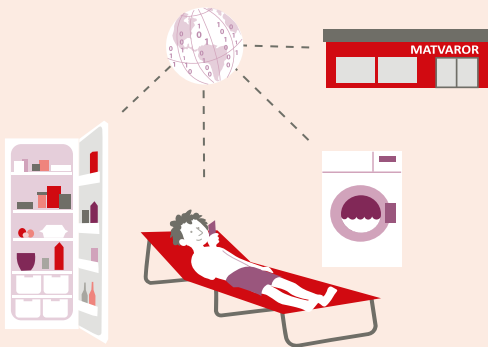
I det moderna samhället finns det allt fler cyberfysiska system i form av IoT. Det är en förkortning av Internet of Things, eller sakernas internet, som det heter på svenska. Sakernas internet består av små datorer som kopplas upp mot internet för att övervaka saker i vår vardag som till exempel hemlarm,

att tända och släcka
ljuset med hjälp av
mobiltelefonen

och att låsa och låsa upp
dörren hemma.

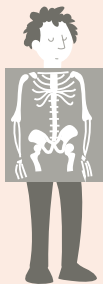


Att sköta tvättmaskinen ifrån Mallorca eller att kontrollera eller justera temperaturen eller vilka varor du har i kylen eller frysen hemma.

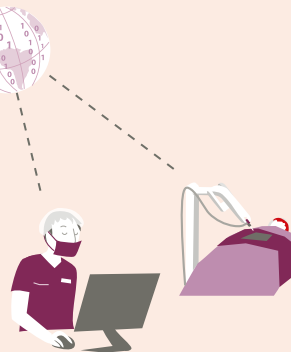


Men IoT kan även bestå i att övervaka en fastighetsventilation, reservkraftsystem, oljepannan,

till och med röntgenapparaten,



eller manövrera en robot som opererar en människa.



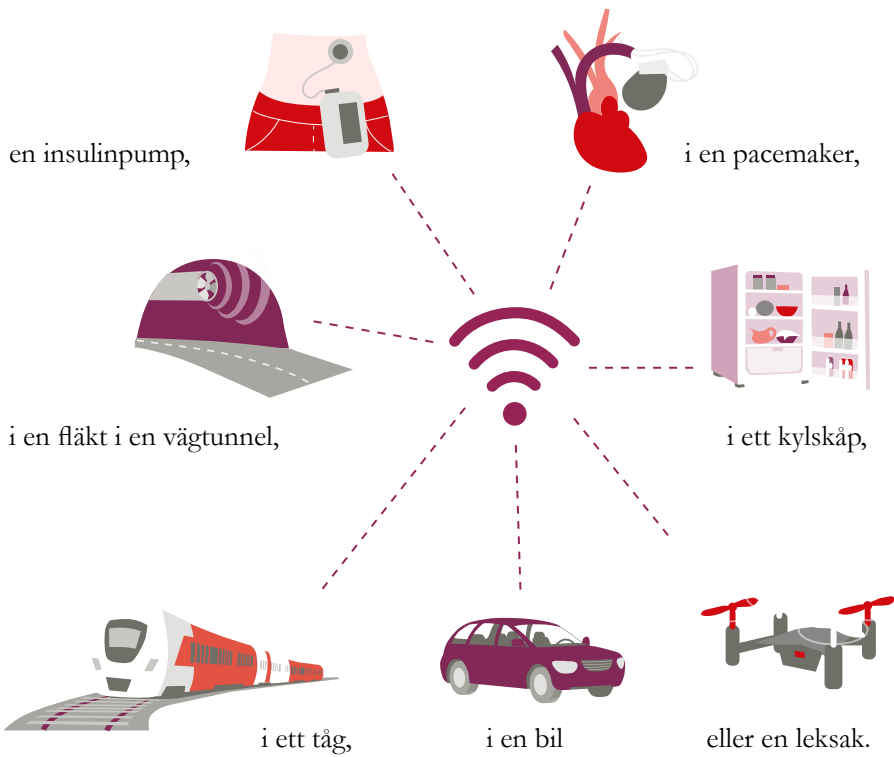
IoT kan även övervaka transporter genom självkörande fordon.



IoT kan också övervaka processer som sker mellan maskiner. Det brukar kallas för M2M. Det betyder Machine to Machine, det vill säga att maskiner talar med varandra och lär sig av varandra.



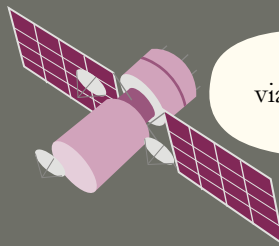
I dagens samhälle är det svårt att säga exakt var ett cyberfysiskt system finns eller var de kommer finnas i framtiden. Ett cyberfysiskt system kan finnas i



Det finns inte heller någon begränsning för varifrån signalen kommer som kan påverka det cyberfysiska systemet.

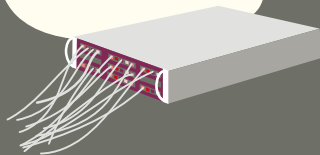


Den kan komma via
trådlöst nätverk,



via satellit,

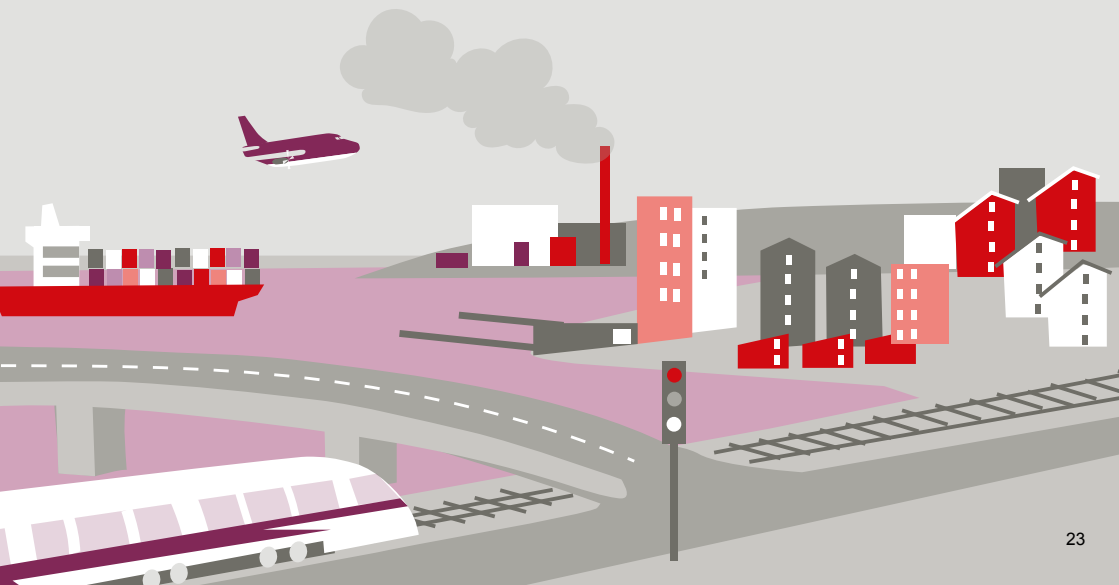
via ett trådbundet
nätverk,



eller optiska
signaler.



Som du förstår är cyberfysiska system viktiga system som finns i viktiga funktioner eller styr viktiga processer i vårt samhälle. Det innebär att vi behöver skydda dem så att inte obehöriga personer kan komma åt dem. Det är viktigt att det finns någon person som är ansvarig för cyberfysiska system. Att det finns någon som tar ansvar för systemet över hela dess livslängd. Det behöver finnas en systemägare till cyberfysiska system precis som till andra it-system. Cyberfysiska system är också it-system. Det måste finnas någon utpekad som ser till att det finns skydd och att det cyberfysiska systemet övervakas, kontrolleras och styrs på ett säkert sätt.





Myndigheten för
samhällsskydd
och beredskap

© **Myndigheten för samhällsskydd och beredskap (MSB)**

651 81 Karlstad Tel 0771-240 240 www.msb.se

Tryck: DanagårdLiTHO Produktion: Advant

Publ.nr MSB1449 – oktober 2019 ISBN 978-91-7383-974-7