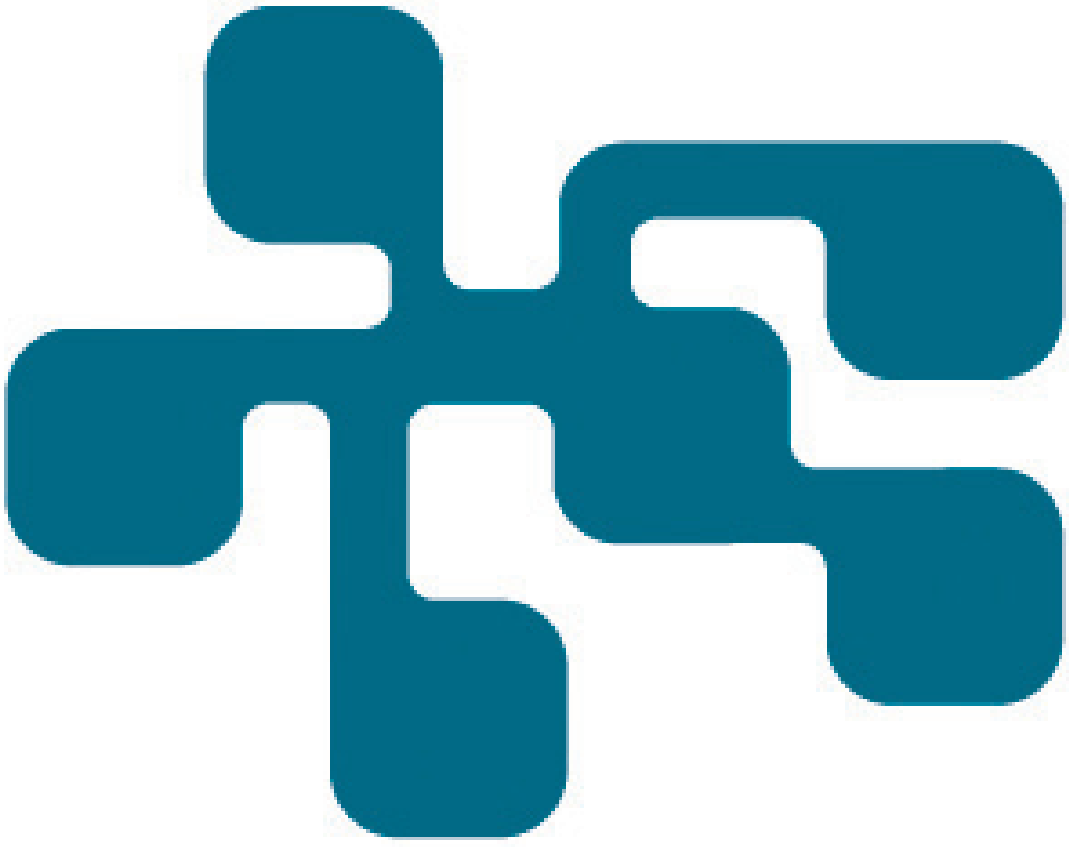
NCS3 - Beroenden till industriella informations- och styrsystem

En förstudie

Vidar Hedtjärn Swaling, Karin Mossberg Sonnek

FOI
MSB



FOI-R--4280--SE
MSB 2015-1075
ISSN 1650-1942

Juni 2016

Vidar Hedtjärn Swaling, Karin Mossberg Sonnek

NCS3 – Beroenden till industriella informations- och styrsystem

En förstudie

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet

Titel	NCS3 Förstudie – Beroenden till industriella informations- och styrsystem
Title	NCS3 Feasibility study - Dependencies to Industrial Information and Control Systems
Rapportnr/Report no	4280
Månad/Month	Juni
Utgivningsår/Year	2016
Antal sidor/Pages	48
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	
Projektnr/Project no	E13550
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Idag styrs de flesta viktiga samhällsfunktioner mer eller mindre autonomt med hjälp av ICS – industriella informations- och styrsystem. Komplexiteten i dessa system gör dem sårbara för såväl mänskligt felhandlande som olika slags latenta fel. Det har också blivit vanligt att koppla ihop ICS med IT-system av olika slag för att uppnå högre effektivitet. Eftersom IT-systemen ofta har kopplingar mot Internet ger detta en möjlighet att komma åt, och i värsta fall störa eller slå ut styrsystemen.

Oavsett orsak vill man inte att ett fel i ICS ska leda till allvarliga konsekvenser för samhället. Därför vill MSB (Myndigheten för samhällsskydd och beredskap) sätta upp ett ramverk för analys av samhällsviktiga verksamheters beroenden till ICS. Syftet med denna studie är att lägga grunden till ett ramverk för identifiering och analys av sådana beroenden.

Målet är att kartlägga vilka krav ICS ställer på begrepp och metoder som används inom beroendeanalyser. I förlängningen ska detta bidra till att analyser av samhällsviktiga verksamheters beroenden till ICS kan göras mer systematiskt, utan att viktiga aspekter förbises, försummas eller missförstås.

Studien utgår från följande problemställningar:

- Hur och var hittar man dessa beroenden? Vilka är de praktisk/tekniska utmaningar som kan förväntas vid tillämpning av metoder för beroendeanalys, när de system som ska analyseras involverar ICS?
- Hur ska man förstå dessa beroenden? Hur långt räcker befintliga begrepp och modeller?

Slutsatserna är att själva identifieringen av beroendena (beroendekartläggningen, eller systemanalysen), är möjlig att göra, men att den försvåras av flera skäl – dels eftersom ICS finns ”överallt” i verksamheterna, dels eftersom de interna beroendena ofta är komplexa (hög redundans, flera funktioner för samma

apparatur, latenta och systematiska fel, svårt att bryta ner systemen i moduler, stark koppling till fysiska processer och i vissa fall till IT-system.). Om syftet med beroendeanalysen är att identifiera sårbarheter, vilket det ofta är, ska man vara medveten om att förhållandet mellan de ”funktionella” beroendena och sårbarheterna kan bli mer komplext och oförutsägbart. För att hitta de kritiska beroendena måste man ha en helhetssyn och en genuin förståelse för systemens funktionalitet och flöden på många olika nivåer.

Utifrån de försök som har gjorts här antas att en god ansats kräver att man för det första kan dela upp analysen i olika steg, där man för varje steg har möjlighet att byta metod eller anpassa den, för det andra tydligt kan ange vad syftet med analysen är, och för det tredje med tydlighet kan avgränsa den verksamhet man analyserar.

Summary

Most of today´s critical infrastructures are more or less autonomously controlled by ICS – Industrial Information and Control Systems. The complexity of these systems makes them vulnerable to human errors as well as different kinds of latent faults. Many times, and increasingly, these systems are also connected to IT systems to gain higher efficiency. Since these systems have connections to the Internet there may be an opportunity for intrusions, interruptions or even severe damage to ICS.

Regardless of the source, failed ICS should not lead to severe societal consequences. That is why MSB (Swedish Civil Contingencies Agency) wants to set up a framework for analysis of critical infrastructure's dependencies to ICS. The aim of this study is to create the basis of a framework for identification and analysis of such dependencies.

This is done by investigating what ICS requires from concepts and methods that are used in the realm of dependency analyses. In the long term this will contribute to analyses of critical infrastructures dependencies to ICS being carried out more systematically, without important aspects being overlooked, neglected or misinterpreted.

The study is guided by the following questions:

- How are these dependencies to be found and where? What are the practical/technical challenges to be expected in application of methods for dependency analyses, when the systems to be analysed involve ICS?
- How are these dependencies interpreted and conceived? What is the potential of existing concepts and models?

The conclusions are that the very identification of dependencies (the mapping or systems analysis), is feasible, but nevertheless complicated because ICS are found anywhere in society and the internal dependencies are typically very complex (highly redundant, several functions for the same equipment, latent and systematic

failures, difficult to break down systems in modules, strong connections to physical processes and in some cases IT). If the purpose of the analysis is to identify vulnerabilities, which is often the case, it should be noticed that the relation between the functional dependencies and the vulnerabilities become more complex and less predictable. To find the critical dependencies a holistic approach is probably the most appropriate, as well as a genuine understanding of the systems functionality and flows at many different levels.

Based on the attempts made in this report a convenient approach is assumed to be one where, firstly, the analysis is split in different stages, where at each stage it is possible to shift or adjust the method chosen, secondly, where the aim is clearly specified, and finally, where the analysed object is clearly defined.

Förord

Denna rapport är baserad på FOI Memo 5588:2 *NCS3 Förstudie – Beroenden till industriella informations och styrsystem*. Memot togs fram på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) hösten 2015 som ett led i myndighetens program för ökad säkerhet i industriella informations- och styrsystem (NCS3 är ett samarbete mellan FOI och MSB som en del av detta program).

I framtagandet av rapporten har dialog förts med FOI-medarbetare med expertis inom beroendeanalys (i första hand Johan Lindgren vid avdelningen för försvarsanalys) respektive ICS (i första hand Lars Westerdahl vid avdelningen för ledningssystem vid FOI Linköping). Avstämningar kring projektets inriktning har återkommande gjorts med MSB:s Kristina Blomqvist och Anders Östgaard, bägge verksamma inom programmet för ökad säkerhet i industriella informations- och styrsystem.

Innehållsförteckning

1 Inledning

Idag styrs de flesta viktiga samhällsfunktioner (elproduktion, dricksvattenproduktion, transporter, mm.) mer eller mindre autonomt med hjälp av så kallade *industriella informations- och styrsystem*, även betecknade ICS (Industrial Control Systems). Dessa system kan till exempel lägga om växlarna på en järnvägsräls, ändra belastningen i en transformatorstation, eller slå av och på motorer som öppnar en dammlucka. Komplexiteten i dessa system gör dem sårbara för såväl mänskligt felhandlande som olika slags latenta fel. Det har också blivit vanligt att ICS kopplas ihop med en verksamhets administrativa IT-system. Eftersom dessa system ofta har kopplingar mot Internet finns det en möjlighet att komma åt, och i värsta fall störa eller slå ut, de industriella informations- och styrsystemen.

Oavsett orsak vill man inte att ett fel i ICS ska leda till allvarliga konsekvenser för samhället. Därför vill MSB (Myndigheten för samhällsskydd och beredskap) sätta upp ett ramverk för analys av samhällsviktiga verksamheters beroenden till ICS. Vad som ingår i att bygga ett sådant ramverk är oklart, inte minst som både samhällsviktig verksamhet och ICS är ganska diffusa begrepp. Även beroendeanalyser är ett svårtillgängligt område, med metoder som ofta leder till svårvaliderade och svårtillämpade modeller, och som i många avseenden behöver tid för mognad.

För att någorlunda avgränsa ett sådant ramverksprojekt är det viktigt att förutsättningarna undersöks i små steg. Det första steget tas i denna studie. Tanken är att vi här ska undersöka dels vad beroendeanalyser är eller kan vara, dels vilka krav ICS ställer på begrepp och metoder som används inom beroendeanalyser. I förlängningen ska detta bidra till att analyser av samhällsviktiga verksamheters beroenden till ICS kan göras mer systematiskt, och utan att viktiga aspekter förbises, försummas eller missförstås.

1.1 Syfte och problemställning

Syftet med denna förstudie är att *lägga grunden till* ett ramverk för identifiering och analys av samhällsviktiga verksamheters beroende till ICS.

LUCRAM[1] ger följande beskrivning av ett ”Ramverk för beskrivning och kartläggning av beroenden”: [9]

Ramverk [- - -] ger stöd till en beroendeanalys genom att beskriva aspekter av beroenden som bör tas hänsyn till vid en kartläggning, [samt] viss vägledning till

[1] Lund University Centre for Risk Assessment and Management.

hur en beroendeanalys faktiskt bör genomföras, oftast med ett visst begränsat analysstöd (t.ex. visualisering av beroenden).

Som framgår av LUCRAM:s beskrivning sönderfaller begreppet beroendeanalys i två delar, en som rör *beroendena i sig*, dvs. aspekter av beroenden som bör tas hänsyn till vid en kartläggning, och en som rör *analysen* av beroendena, dvs. hur de ska tolkas och vad de implicerar i olika avseenden. Vår studie kan därmed sägas utgå från följande problemställningar:

- Hur hittar man dessa beroenden? Var dyker de upp? Vilka är de praktisk/tekniska utmaningarna som kan förväntas vid tillämpning av metoder för beroendeanalys, när de system som ska analyseras involverar ICS?
- Hur ska man förstå dessa beroenden? Hur långt räcker befintliga begrepp och modeller?

1.2 Ansats och genomförande

Studien av de b*egreppsliga utmaningarna* görs med utgångspunkt i litteratur om beroendeanalyser och ICS samt i den begreppsapparat som används i MSB/KBM:s (KBM – Krisberedskapsmyndigheten, nuv. MSB) modell för beroendeanalys av samhällskritisk verksamhet (Modellen presenteras i skriften *Faller en – faller då alla?* [4]). Möjligheten att tillämpa vissa centrala begrepp på olika systemnivåer och för olika typer av system diskuteras och idén är att något därigenom ska kunna sägas om de generella förutsättningarna för en beroendeanalys.

Som utgångspunkt för undersökningen av de praktisk/tekniska utmaningarna används MSB/KBM:s modell tillämpad på exempelsystemet ”spårbunden trafik” som kartlagts i rapporten *NCS3 – Informations- och styrsystem inom spårbunden trafik* [5]. MSB/KBM:s beroendeanalysmetod har valts eftersom den

1. avser beroenden till samhällsviktig verksamhet, och
2. för att den är framtagen för att kunna användas i en risk- och sårbarhetskontext (i samverkan med vägledningar avseende skydd av samhällsviktig verksamhet, säkerhet i industriella informations- och styrsystem, etc.) och därmed erbjuder en relevant begreppslig plattform.

De frågor vi ställer oss är: Genom att tillämpa MSB/KBM:s beroendeanalysmetod på en kritisk infrastruktur, framkommer det någonting då som inte framkommer i begreppsanalysen? Kommer man tillräckligt djupt i beroendestrukturerna? Erfar vi något problem med själva metoden (tillvägagångssättet, arbetsgången) eller med empirin (det faktiska systemet)?

1.2.1 Avgränsningar

Fokus kommer att ligga på systemsäkerhet snarare än på vad som normalt hänförs till kategorin informations- och cybersäkerhet, dvs. på ICS snarare än IT. Inom IT-säkerhet talar man om förmågan att upprätthålla *konfidentialitet, korrekthet, tillgänglighet och spårbarhet*. I denna studie ska vi fokusera på systemberoenden och systemrisker, dvs. i huvudsak tillgänglighetsaspekten. De traditionella ”cyberhoten”, ofta med en antagonist implicerad, kommer endast att beröras i den mån de har bäring på systemberoenden eller dessas tolkning i termer av sårbarheter eller annat, eller i avseenden då det är viktigt att upprätthålla en tematisk gräns mellan ICS och IT.

Vidare gäller följande:

- Studien fokuserar på samhällsviktiga verksamheters beroende till ICS, inte spridningseffekter vid störningar inom dessa system, eller deras beroenden av andra verksamheter/system.
- Studien i den tillämpade delen (avsnitt 4.4) kommer endast att omfatta *beroendeanalysen* i MSB/KBM:s modell, inte spridningsanalysen.
- Underlaget för den applicering av MSB/KBM:s modell för beroendeanalys är begränsat och utgörs av den skriftliga rapport som tidigare tagits fram inom ramen för NCS3 och som behandlar informations- och styrsystem inom spårbunden trafik [5]. Studiens omfattning tillåter inte identifiering och test av fler modeller och exempelsystem.

1.2.2 Målgrupp

Studien vänder sig i första hand till personer med anknytning till MSB:s program för ökad säkerhet i industriella informations- och styrsystem, inklusive NCS3.[2]

Studien bör också kunna vara intressant för personer med ett allmänt intresse av kris- och riskhantering och samhällets beroende av tekniska system.

[2] Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Centrumet är ett samarbete mellan FOI och MSB.

2 Bakgrund

Nedan ges definitioner och teknisk bakgrund till denna studies huvudsakliga studieobjekt – samhällsviktig verksamhet och ICS.

2.1 Samhällsviktig verksamhet

I MSB:s *Handlingsplan för skydd av samhällsviktig verksamhet* [6] definieras samhällsviktig verksamhet via begreppet samhällsviktig funktion enligt följande:

Samhällsviktig funktion är ett *”[s]amlingsbegrepp för de verksamheter som upprätthåller en viss samhällsviktig funktionalitet. Varje sådan funktion ingår i en av [elva] samhällssektorer och upprätthålls således av en eller flera samhällsviktiga verksamheter.”*

De elva samhällssektorer inom vilka viktiga samhällsfunktioner kan identifieras är:

- Energiförsörjning
- Finansiella tjänster
- Handel och industri
- Hälso- och sjukvård samt omsorg
- Information och kommunikation
- Kommunalteknisk försörjning
- Livsmedel
- Offentlig förvaltning – ledning
- Skydd och säkerhet
- Socialförsäkringar
- Transporter

Samhällsviktig verksamhet ur ett krisberedskapsperspektiv definieras som verksamhet som uppfyller ett eller båda av följande villkor: [6]

- ”Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.”
- ”Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.”

2.2 Industriella informations- och styrsystem

ICS är en allmän term som omfattar flera typer av system för styrning, inklusive kontroll- och processövervakningssystem (SCADA – *Supervisory Control And Data Acquisition*), distribuerade styrsystem (DCS – *Distributed Control Systems*) och så kallade PLC:er (*Programmable Logic Controllers*).[3] Dessa system är vanligt förekommande inom kritisk infrastruktur såsom el, vatten och avlopp, transport och livsmedelsförsörjning, samt inom industrisektorer som olja-gas, kemisk industri, läkemedel, massa-papper och fordonstillverkning. Systemen är synnerligen kritiska för drift av infrastrukturer eftersom dessa är sammanlänkade på ett svåröverskådligt sätt.

ICS designades ursprungligen för att uppfylla högt ställda krav på prestanda, tillförlitlighet och flexibilitet. I regel var systemen fysiskt separerade från omgivande nätverk och baserade på patentskyddad hårdvara, mjukvara och kommunikationsprotokoll som inkluderade grundläggande möjligheter till felsökning och åtgärd, men som saknade de förutsättningar för säker kommunikation som ofta krävs i dagens system. Säkerhet inom ICS handlade i första hand om möjligheten att hindra fysisk åtkomst av nätverk och manöverpaneler. Internetbaserade tekniker började sitt intåg i ICS-designer under sent 90-tal. Dessa förändringar exponerade systemen för nya slags hot och höjde avsevärt sannolikheten för allvarliga incidenter. [13]

I MSB:s *Vägledning till ökad säkerhet i industriella informations- och styrsystem* [7] tillåts ICS omfatta all automation som kontrolleras eller stöds med hjälp av informationsteknik. De ingående teknikerna har vissa särdrag som kan vara värda att uppmärksamma: [13]

- SCADA avser i första hand system som är i hög grad distribuerade och som används för övervakning av anläggningar med stor geografisk spridning (typiskt tusentals kvadratkilometer) där central övervakning är kritisk för driften. SCADA används typiskt i system för vattendistribution, övervakning av rör- och transportledningar inom olja-gas, elkraftnät, och järnvägsnät.
- DCS används för att styra industriella processer inom i synnerhet processindustrin, dvs. elkraftproduktion, oljeraffinaderier, kemi-, livsmedels- och fordonsindustrin. DCS är en integrerad arkitektur med en övervakningsdel för styrning av flera delsystem som vart och ett ansvarar för detaljerna i en lokal process.

[3] Andra vanliga, mer eller mindre överlappande, benämningar är processkontrollsystem, processautomation, process-it, tekniska IT-system, anläggnings-IT, distribuerade kontrollsystem och inbyggda realtidssystem (RTE). Ibland finns det också branschspecifika lösningar eller benämningar.

- PLC:er är styrdatorer, oftast fast installerade, som finns i stor omfattning inom i stort sett alla industriella processer. PLC:er ingår som den mest processnära styrutrustningen i SCADA och DCS såväl som i styrutrustning i småskalig processindustri.

DCS- eller PLC-styrda delsystem ligger vanligtvis inom en rumsligt avgränsad anläggning och kommunikationen sker över lokala nätverk (LAN). Systemen är normalt mer tillförlitliga och kommunicerar med högre hastighet än de fjärrkommunikationssystem som används inom SCADA. SCADA-system är å andra sidan designade för att klara just de utmaningar som långväga kommunikation över flera olika media (radioteknik, trådlösa nätverk, fiber, kopparkabel, telefonnät [7]) innebär, i form av fördröjningar och dataförluster. DCS och PLC utnyttjar i allmänhet också i högre grad slutna reglerkretsar eftersom styrning av industriella processer är mer komplicerad än styrning av distributionsprocesser. Utförliga beskrivningar av typiska SCADA-, DCS- och PLC-arkitekturer återfinns i NIST 8009-32 *Guide to Industrial Control Systems (ICS) Security*. [13]

2.2.1 Cyberfysiska system

Begreppet ”cyberfysiska system” används ibland synonymt med ICS men definieras sällan. Det tycks kunna syfta på styrsystemen, dvs. ICS, såväl som hela konfigurationen med ett styrt och ett styrande/övervakande system, dvs. ICS samt den fysiska processen. I standarden ISO/IEC 27032 *Information technology – Security techniques – Guidelines for cybersecurity* [3] definieras inte “cyberfysiska system”, men väl begreppet “cyberspace” [cyberrymden]: “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.” [3, sid. 4]

Ett cyberfysiskt system skulle såtillvida kunna förstås som något som rör sig över gränsen mellan cyberrymden och den fysiska världen (jfr [14], sid. 5: ”en cyber-händelse innefattar både informationslagret och den verkliga världen”).[4]

På grund av oklarheterna kring begreppet ”cyberfysiska system” och dess tendens att implicera kopplingar mellan processer och IT, kommer vi att hålla oss till begreppet ICS. System som faller under begreppet ICS kan förvisso involvera IT, men denna koppling är inte förutsatt.

[4] En snabb genomgång av olika användningar av begreppet ”cyber” återfinns i kapitel 4 i Axell, E. et al. (2013) [1].

2.2.2 Skillnad mellan ICS och IT

ICS involverar i allt högre utsträckning IT-lösningar för att stödja sammankoppling och fjärråtkomst. Förutom strikt styrning och kontroll av den fysiska industriprocessen kommunicerar processnäten ofta med administrativa system för att öka effektiviteten i verksamheten. [7] ICS designas och implementeras dessutom med standardiserade datorer (pc-plattformar etc.), operativsystem, nätverk och protokoll, vilket gör att de alltmer liknar rena IT-system. [13]

Detta ger nya möjligheter, men gör samtidigt ICS långt mindre isolerat från den omgivande världen, vilket i sin tur skapar behov av att skydda systemen. Samtidigt som säkerhetslösningar har designats för att hantera säkerhetsproblem i typiska IT-system, så måste särskild försiktighet iakttas när de introduceras i ICS-miljö. I vissa fall behövs lösningar som är skräddarsydda för just ICS. Följande sammanställning omfattar saker som måste tillmätas särskild vikt när man skapar säkerhet för ICS: [13, sid. 3-3–3-6]

- I ett typiskt IT-system förekommer ingen fysisk interaktion med omgivningen medan ICS kan ha mycket komplex samverkan med fysiska processer, vilket i sin tur innebär att händelser i ”cyberdomänen” kan resultera i fysiska händelser. Detta medför bl.a. höga krav på tester i särskilda testmiljöer för komponenter som ska integreras i ett ICS.
- Till skillnad från IT handlar ICS om ”safety” snarare än ”security”. Det är människors liv och hälsa som står på spel snarare än datas konfidentialitet och integritet.
- I vissa IT-system är informationen som lagras och processas centralt mer kritisk än den distribuerade informationen. I ett ICS är det ytterst viktigt att skydda klienterna ute i systemets periferi (PLC:er mm.) eftersom de är närmast processerna. De centrala delarna av systemet kan fortfarande vara kritiska eftersom de kommunicerar med och kan påverka alla övriga noder i systemet.
- Till skillnad från IT är ICS ofta specialdesignade för en viss uppgift och bygger på lösningar som är unika för en viss installation. Detta betyder att olika ICS har olika brister ur ett sårbarhetsperspektiv. Detta betyder också att underhåll och support ofta bara kan utföras av ett fåtal aktörer, ibland bara den som levererade systemet.
- ICS är generellt tidskritiska och tolererar inte alltför stora taktvariationer (jitter) eller fördröjningar. Hög hastighet (throughput) är dock normalt inte avgörande för ICS. Det omvända gäller för IT-system – de klarar ofta avvikelser men kräver höga hastigheter.

- ICS är i allmänhet realtidssystem som inte tolererar oplanerade avbrott. Ofta kan de inte startas och stoppas utan att produktionen påverkas. De höga kraven på tillgänglighet, tillförlitlighet och underhållsmöjlighet (RAM – *Reliability, Availability, Maintenence*) innebär att typiska IT-strategier som t.ex. återstart inte är acceptabla. En del ICS utnyttjar redundanta komponenter i samtidig drift för att säkerställa kontinuitet.
- Typiska IT-komponenter är lokala och lätta att komma åt, medan ICS-komponenter kan vara isolerade, avlägset placerade och på andra sätt svåra att fysiskt komma åt.

Samtidigt som skillnaderna är stora kan det i många fall vara svårt att i praktiken skilja ICS från IT eftersom de ofta är starkt integrerade. Därmed kommer det att öppnas nya kontaktvägar och nya felkällor och sårbarheter uppstår. Dessa måste en beroendeanalys kunna ta hänsyn till.

3 Beroendeanalyser

Enligt MSB (2015) är beroendeanalysområdet relativt eftersatt, samtidigt som samhället genomgår och har genomgått en rad förändringar i form av: [9]

- ökad specialisering
- ökad institutionell fragmentering
- ökade beroenden mellan system, funktioner, etc.
- ökad komplexitet
- ökade beroenden av, och krav på, samhällets infrastrukturservice

Dessa förändringar ställer allt högre krav på genomförandet av beroendeanalyser, detta för att motverka storskaliga spridningseffekter.

Vad är då en beroendeanalys?

Tittar man på hur LUCRAM, MSB/KBM och andra har definierat eller tolkat beroendeanalyser är det tydligt att begreppet har två komponenter. För det första har vi själva *beroendet*, dvs. först måste beroendena identifieras, pekas ut, i en systemkartläggning. För det andra har vi *analysen* – beroendena ska analyseras, dvs. man måste förstå dem och värdera dem, för att sedan kunna dra slutsatser utifrån dem.

En metod för beroendeanalys måste således tillhandahålla frågor med vars hjälp beroendena kan bli synliga. Utöver detta måste en metod innehålla begrepp som kopplar dessa beroenden till andra viktiga aspekter som t.ex. sårbarhet, funktion och redundans.

Enligt LUCRAM är syftet med beroendeanalyserna (dvs. kartläggning och analys) att:

1. *Reducera en verksamhets eller funktions sårbarhet*, t.ex. genom investeringar i stötdämpare för speciellt kritiska beroenden (alternativa system, försörjning, etc.). Detta är huvudfokus i t.ex. kontinuitetsplanering. [9]
2. Aggregera informationen genom att *identifiera verksamheter som många andra är beroende av*, och som därför bör göras mer robusta. Berörs i t.ex. MSB:s projekt ”Faller en faller alla?” och ”Strategi för skydd av samhällsviktig verksamhet”. [9]

Det första syftet handlar alltså om att göra en verksamhet mindre sårbar genom att minska dess beroende av andra verksamheter. Fokus ligger på den enskilda verksamheten och dess beroenden ”bakåt” i försörjningskedjan. Det andra syftet handlar snarare om att i ett system av verksamheter fokusera på de mest kritiska.

Det andra syftet *förutsätter* det första eftersom beroendekartläggningen för var och en av verksamheterna måste vara gjord innan informationen aggregeras. De två syftena är därmed kopplade till vad som med KBM:s terminologi kallas ”beroendekedjor” (bakåtsyftande beroenden), respektive spridningskedjor (framåtsyftande beroenden). Dessa behandlas vidare i avsnitt 3.3 och kapitel 4.

Dessa syften ger ingen förklaring till vad ett beroende är eller hur man hittar ett beroende. I avsnitt 4 går vi igenom KBM:s metod för identifiering och analys av beroenden, och vi frågar oss – kan metoden hjälpa oss att hitta och analysera väsentliga beroenden mellan samhällsviktig verksamhet och ICS?

3.1 Beroenden till ICS – vad säger ”Vägledningen”?

Enligt MSB:s *Vägledning till ökad säkerhet i industriella informations och styrsystem* utgör samhällsviktiga verksamheters beroenden till industriella informations- och styrsystem ”potentiella sårbarheter som måste identifieras och analyseras”. Vidare innebär analyser av beroenden att man ”systematiskt går igenom en verksamhets eller ett systems olika komponenter och ställer frågor kring vad som behövs för att de ska fungera, dvs. kunna leverera till nästa instans i systemet så att den samhällsviktiga verksamhetens behov slutligen tillgodoses.” I MSB:s vägledning påpekas också att det finns potentiella utmaningar med att analysera verksamheters beroenden till industriella informations- och styrsystem som har att göra dels med dessa systems utbredning och komplexitet, dvs. att de finns överallt i samhället och dessutom är svåra att analysera i detalj. [7] En tänkbar svårighet som vi ska studera vidare i kapitel 5 är också det faktum att beroendekedjorna ofta går över två mycket olika domäner, den fysiska och den virtuella.

I vägledningen finns vidare en kort rekommendation om hur en systemkartläggning ska göras för att den ska kunna ligga till grund för en beroendeanalys (se rekommendation nr 3 – *Underhåll processer för systemkartläggningar och riskhantering i industriella informations- och styrsystem*, sid. 36).

3.2 Beroendeanalys i ett krisberedskapsperspektiv

KBM fick 2006 ett regeringsuppdrag som syftade till att stärka samhällets krisberedskapsförmåga genom att analysera beroenden mellan olika samhällsviktiga verksamheter. Projektet hade flera delmål, ett av dessa mål var att utveckla en metod för att genomföra beroendeanalyser. Projektet slutrapporterades i december 2008. I slutrapporteringen återfinns en

handlingsplan som bland annat föreslår en ökad användning av beroendeanalyser i myndigheters och andra aktörers risk- och sårbarhetsanalyser.

LUCRAM påpekar att det finns ett behov av att kunna aggregera information om beroenden från flera samhällsviktiga sektorer/funktioner/verksamheter för att kunna skapa helhetsbilder tvärsektoriellt eller sektoriellt på kommunal, regional och nationell nivå. [9]

Sammantaget kan beroendeanalyser ge en helhetsbild som bidrar till att:

- Förstå spridningseffekter i samhället, både i förebyggande och operativt syfte.
- Ge stöd till enskilda verksamheter/funktioner att förstå sin roll i helheten, dvs. vad/vem man påverkar direkt och indirekt och vad man själv beror av.
- Identifiera behov av större kunskap om andra verksamheters förmågor.
- Identifiera samhällsviktig verksamhet – *vissa verksamheter kan visa sig vara samhällsviktiga först efter en beroendeanalys.*
- Prioritera mellan samhällsviktiga verksamheter (de verksamheter som ger upphov till stora spridningseffekter bör prioriteras).

Dessa helhetsbilder bör användas för att stödja sektorer, samhällsfunktioner, samhällsviktig verksamhet, kommuner och regioner i åtgärdsprioriteringar genom en insikt i högre ordningens beroenden. [9]

I KBM:s *Faller en faller då alla…* påpekas också att beroendeanalyser ger förutsättningar för att göra en aggregerad analys av risker, sårbarheter och förmågor (lokalt, regionalt, nationellt, mm.), och att de därmed generellt kan fördjupa och höja kvaliteten på RSA:er och förmågeanalyser. [4]

3.3 Exempel på metoder för beroendeanalys

På uppdrag av MSB har LUCRAM publicerat skriften *Översikt över metoder för komplex beroendeanalys på sektoriell & tvärsektoriell nivå* [9]. Syftet med uppdraget var bl.a. att genomföra en inventering av befintliga metoder för beroendeanalys på sektoriell och tvärsektoriell nivå. De metoder som identifierades delades in i ett antal kategorier baserat på kriterier som systemnivå, tidsperspektiv, scenarioberoende resp. all hazard, förebyggande resp. operativ, typ av data, typ av beroenden, mognadsgrad och modellkomplexitet (t.ex. linjär/olinjär). Sammanställningen är mycket generell men skulle kunna vara utgångspunkt för en analys av vilka *slags* metoder som lämpar sig för analys av beroenden till ICS. Nedan ges sammanfattningar av olika kategorier av metoder tillsammans med LUCRAM:s omdöme av hur tillämpbar respektive

metodkategori är för ”komplex beroendeanalys på sektoriell och tvärsektoriell nivå”.

Ramverk för beskrivning och kartläggning av beroenden: Kategorin ”Ramverk för beskrivning och kartläggning” syftar till att stötta en beroendeanalys genom att beskriva aspekter av beroenden som bör tas hänsyn till vid en kartläggning. Ramverk kan även ge viss vägledning till hur en beroendeanalys faktiskt bör genomföras, oftast med ett visst begränsat analysstöd, t.ex. visualisering av beroenden. Till denna kategori räknar LUCRAM *KBM:s beroendehjul* (se vidare kapitel 4) samt Rinaldis ramverk.[5] Ramverksbeskrivningar ger oftast en relativt enkel och greppbar översikt över olika typer av beroenden och beroendeförhållanden. Dessa typer av metoder ger dock inget analysstöd eller simuleringsstöd och lämpar sig därmed inte för analys av mer komplexa beroendeförhållanden.

Empiriska metoder: Empiriska metoder analyserar beroenden utifrån inträffade händelser. Genom att upprätta en databas över inträffade händelser kan en karaktärisering göras av de konsekvenser som uppstår vid en händelse eller olycka på grund av beroenden. Sådan kunskap kan användas som underlag för att komplettera expertbedömningar. Metoderna kan även ge stöd till att kvantifiera styrkan på beroenden mellan sektorer samt informera prediktiva beroendemodeller, men eftersom metoderna är empiriska kan inte fenomen som ännu inte inträffat fångas in. De empiriska metoderna ger en begränsad bild av beroenden, och validiteten beror till stor del på vilka källor som använts för den empiriska analysen. Till viss del kan slutsatser generaliseras till liknande, framtida, händelser. Metoden uppfyller inte krav för analys av mer komplexa beroendeförhållanden och fångar främst beroenden på samhällsfunktionsnivå.

Agentbaserade metoder: Styrkan med de agentbaserade metoderna är framförallt att systemets funktion modelleras utifrån enklare regelstrukturer på agentnivå (bottom-up). Därmed kan systemaspekter studeras utan att systemet måste förstås i sin helhet. Varje agent interagerar med andra agenter i sin omgivning baserat på en uppsättning regler, som till exempel kan baseras på hur verkliga individer agerar. Varje enskild applikation av agentbaserad modellering har *ett särskilt fokus*, då modellerna annars fort blir för omfattande. Merparten av de agentbaserade modellerna avser fånga en hög nationalekonomisk nivå. Eftersom

[5] Rinaldi et al. [11] är ett ofta citerat ramverk för att beskriva beroenden mellan infrastrukturer. I ramverket föreslås olika dimensioner som man bör ta hänsyn till vid en beroendeanalys, t.ex. typ av spridningseffekt, hur snabbt en effekt sprids, grad av spatial upplösning, första och högre ordningens beroenden etc. Ramverket är tänkt att underlätta vid identifiering, förståelse och analys av kritiska beroenden genom att visa på viktiga karakteristika som bör fångas in i beroendeanalyser. Ramverket ger dock inget metodstöd för den konkreta kartläggningen av beroenden.

det krävs tydliga agenter för att metoden ska vara applicerbar är den oftast endast applicerbar på komponentnivå.

Systemdynamikmetoder: Systemdynamikmetoder kan sägas vara tillämpad system-/reglerteori och använder informationen från olika diagram (feedback loops, stocks och flows) för att skapa matematiska beskrivningar (ekvationer) av förhållanden mellan olika variabler i systemet för att därefter kunna simulera hur systemet beter sig vid störningar och förändringar. Metoderna lämpar sig för beslutsfattande på systemövergripande nivå snarare än för analys av komponenters beteenden (exempelvis förändringar i en infrastrukturs topologi). Metoderna kräver omfattande datainsamling, relativt hög nivå av kunskap för användande och modellvalideringen är resurskrävande.

Infrastrukturbaserade metoder: Inom forskningslitteraturen finns det en hel del metoder inom området modellering av beroenden mellan komponenter och system för tekniska infrastrukturer. Här modelleras ofta infrastrukturer och beroenden mellan infrastrukturer med hjälp av nätverksteori. I sin enklaste form modelleras dessa nätverk endast med hjälp av två komponenttyper: noder och länkar (som kopplar ihop och beskriver ett samband mellan noderna). I dessa fall används inga eller mycket enkla funktionella modeller som beskriver hur nätverket reagerar på systemnivå och effekten av beroenden vid störningar i form av att noder och/eller länkar tas bort, så kallade *topologiska modeller*. I mer avancerade metoder tas hänsyn till fysiska/funktionella aspekter av nätverket som på ett mer realistiskt sätt beskriver hur nätverket reagerar på störningar eller för att analysera effekterna av komponentbortfall på systemnivå. I hög grad utgör modellerna ”ett-till-ett”-representationer av det verkliga systemet vilket innebär att det relativt enkelt går att identifiera kritiska komponenter och utvärdera effekterna av åtgärder. Dock kan datainsamlingen och modelleringen bli väldigt omfattande, vilket ofta sätter begränsningar för antalet modellerade infrastrukturer samt detaljeringsgrad. Dessutom behöver analytikern relativt god domänskunskap om samtliga modellerade infrastrukturer. Det är relativt enkelt att koppla analysresultat till en beslutkontext och åtgärder för att förbättra systemet. Metoderna kräver dock omfattande sektorsspecifik indata både angående system och beroenden mellan systemen. Till viss del finns denna data tillgänglig avseende specifika infrastrukturer, dock oftast ej för beroenden *mellan* infrastrukturer. Vidare mäter dessa metoder systemkonsekvenser vilket inte nödvändigtvis är likvärdigt med samhällskonsekvenser, exempelvis kan en systemkonsekvens vara mängden icke-levererad el vilket inte nödvändigtvis behöver representera samhällskonsekvenser särskilt väl. Fördelen är att mer komplexa system och beroendeanalyser kan genomföras, där effekterna av komponentfel kan studeras för sammankopplade system.

Flödesbaserade metoder: Gemensamt för flödesbaserade metoder är att istället för att beskriva beroenden direkt mellan olika funktioner/aktörer beskrivs funktioners/aktörers beroende av och påverkan på flöden (t.ex. produkter,

tjänster, människor och resurser). Flödena kan därmed sägas förmedla beroenden mellan funktioner/aktörer. Resultaten från flödesbaserade metoder kan användas till att identifiera kritiska funktioner/aktörer och flöden utifrån ett holistiskt beroendeperspektiv samt kopplas till förmågebedömningar och risk- och sårbarhetsanalyser. Det är även möjligt att sammanfoga metoderna med infrastrukturbaserade metoder. Indata är främst baserad på expertbedömningar då datainsamling i annat fall blir omfattande.

Hybridmetoder: Genom att kombinera olika metoder kan styrkor hos respektive metod utnyttjas, samtidigt som svagheter till viss del kan minimeras. Resultatet från hybridmodeller kan oftast användas för att undersöka och belysa längre beroendekedjor, t.ex. att gå från komponentnivå i en infrastruktur till samhällsnivå. De flesta hybridmetoder kräver i stort omfattande datainsamling och aggregering av data från flera olika typer av datakällor. Metoderna resulterar ofta i en relativt avancerad analysmetod som kräver omfattande kunskap inom flera domäner.

4 KBM:s beroendeanalys

KBM fick 2006 ett regeringsuppdrag som syftade till att stärka samhällets krisberedskapsförmåga genom att analysera beroenden mellan olika samhällsviktiga verksamheter. Det så kallade ”beroendeprojektet” hade flera delmål, varav ett var att utveckla en metod för att genomföra beroendeanalyser. Metoden, som i sin slutversion publicerades 2008, användes inom beroendeprojektet för ta fram av beroende- och konsekvensanalyser inom nio olika samhällssektorer.

I denna studie används KBM:s metod för beroendeanalys som testmetod. Denna test skall ses som ett komplement till den teoretiska analysen (se avsnitt 1.3).

4.1 Syfte och nytta med beroendeanalysen

Metoden syftar till att identifiera och analysera kritiska beroendeförhållanden i samhället, främst med inriktning att kartlägga beroenden mellan samhällsviktiga verksamheter. Ett delsyfte är att personer inom de verksamheter som identifieras som samhällsviktiga själva ska få en förståelse för vilka andra verksamheter de är beroende av och vilka verksamheter som är beroende av deras verksamhet. Ytterligare ett delsyfte är att på en övergripande nivå (kommunal, regional eller nationell) kunna ställa samman en aggregerad bild av de beroenden som finns i samhället. De analyser som har gjorts med metoden i KBM:s regi har i huvudsak varit på den övergripande nivån och inte gått in på detaljer (exempelvis enskilda system och personalkategorier). Ett undantag utgör delar av de mer specifika sektorstudierna där metoden användes för att identifiera mer detaljerade och specifika beroenden.

KBM räknar i ett antal punkter upp vad en beroendeanalys kan användas till: [4]

- Öka förståelsen för verksamheters förmåga och därmed åstadkomma en bättre kontinuitetsplanering.
- Ge förutsättningar för att göra en aggregerad analys av risker, sårbarheter och förmågor.
- Ge underlag för prioritering av åtgärder, resursallokering, inriktning av studier/forskning, mm.
- Vara en del av operativt beslutsstöd.
- Underlätta samverkan mellan aktörer i krishanteringssystemet.

KBM skriver också att en beroendeanalys kan fördjupa och höja kvaliteten på RSA:er och förmågeanalyser. [4]

Om man gör en beroendeanalys av någon av ovan nämnda anledningar så behöver man utöver beroendeanalysen ytterligare kunskap och analys. Beroendeanalysen i sig är inte tillräcklig för att göra exempelvis en risk- och sårbarhets- eller en förmågeanalys.

Fokus i metoden ligger på att identifiera beroenden och att värdera dessa utifrån specifika kriterier, inte på att analysera dem, även om KBM skriver att ”kritiska beroenden kan betraktas som sårbarheter som varje verksamhet bör känna till och kunna hantera”. [4, sid. 20] Det stämmer visserligen till viss del, ett beroende som efter värderingen kan sägas vara kritiskt för en verksamhet kan innebära en sårbarhet, men beroendet säger ingenting om hur stor sårbarheten är, där behövs ytterligare analys.

De beroenden som sorteras vidare till den del av metoden där de värderas är beroenden till externa aktörer, regelverk, kapital och information. Detta beror gissningsvis på att ett av delsyftena med KBM:s beroendeanalys är att skapa en riskbild på samhällsnivå av hur olika samhällsviktiga verksamheter är beroende av varandra. De interna beroendena kan också tolkas som att de ligger under den undersökta verksamhetens egen kontroll och därmed inte är lika intressanta att kartlägga ur ett beroendeperspektiv. Om en verksamhet vill använda beroendeanalysen som underlag till en risk- och sårbarhetsanalys så bör dock även interna beroenden beaktas.

Analysen kan identifiera vilka andra verksamheter en specifik verksamhet är beroende av för att fungera, och även hur störningar hos en levererande verksamhet sprids. Det är det första användningsområdet som ska studeras här.

4.2 Viktiga begrepp

Det finns några centrala begrepp i KBM:s beroendeanalys och dessa definieras enligt: [4, sid. 14f]

Beroende	Att en verksamhet är beroende av en annan förklaras med att den har behov av den levererande verksamhetens varor eller tjänster. Beroenden delas in i (för den analyserade verksamheten) interna respektive externa.
Samhällsviktig verksamhet	En verksamhet är samhällsviktig om den uppfyller minst ett av villkoren: 1. Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.

	2. Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.
Kritiskt beroende	Ett kritiskt beroende är ett beroende som är avgörande för att samhällsviktiga verksamheter ska kunna fungera. Det karaktäriseras av att en störning i en levererande verksamhet snabbt och varaktigt försämrar funktionen hos den beroende verksamheten.
Stötdämpare	En stötdämpare innebär att den beroende verksamheten kan tillgodose behovet av en viss vara eller tjänst på något alternativt sätt om den ordinarie levererande verksamheten drabbas av en störning. Stötdämpare som har använts i den här studien är redundans, substitut och adaptivitet.
Uthållighet	Med uthållighet menas att verksamheten under en viss tid kan klara sig trots att den levererande verksamheten inte fungerar eller fungerar med en lägre kapacitet. Uthålligheten beror till stor del på vilka stötdämpare den beroende verksamheten har.

4.3 Övergripande metod

KBM:s beroendeanalys består av tre steg som beskrivs i Tabell 1:

1. Urval och beskrivning
2. Identifiering och värdering av externa beroenden
3. Aggregerad analys

Tabell 1: Stegen i KBM:s beroendeanalys. [4, sid. 23]

Steg	Föreslagna användare	Hjälpmedel
1) Urval och beskrivning	**Kommuner, län, myndigheter, företag**	**Kriterier för urval av samhällsviktig verksamhet**
Verksamheter, som är viktiga för att en kommun, län, myndighet eller företag ska fungera på ett acceptabelt sätt, väljs ut.		
Varje verksamhets uppgift beskrivs utifrån vad den ska leverera, i vilken omfattning och till vem.		
2) Identifiering och värdering av externa beroenden	**Enskilda verksamheter**	**Beroendehjulet**
De behov en verksamhet har för att kunna upprätthålla verksamheten enligt beskrivningen identifieras.		
Utifrån de identifierade behoven lyfts de behov fram som innebär ett beroende av en extern verksamhet eller resurs.		
De externa beroendenas styrka värderas utifrån konsekvenser, stötdämpare och uthållighet.		
3) Aggregerad analys	**Kommuner, län, myndigheter, företag**	**Matrisen**
Det material som tagits fram för varje verksamhet samlas in och sammanställs.		
Beroenden mellan samtliga verksamheter visualiseras i form av spridningskedjor, beroendekedjor och fokuskedjor.		

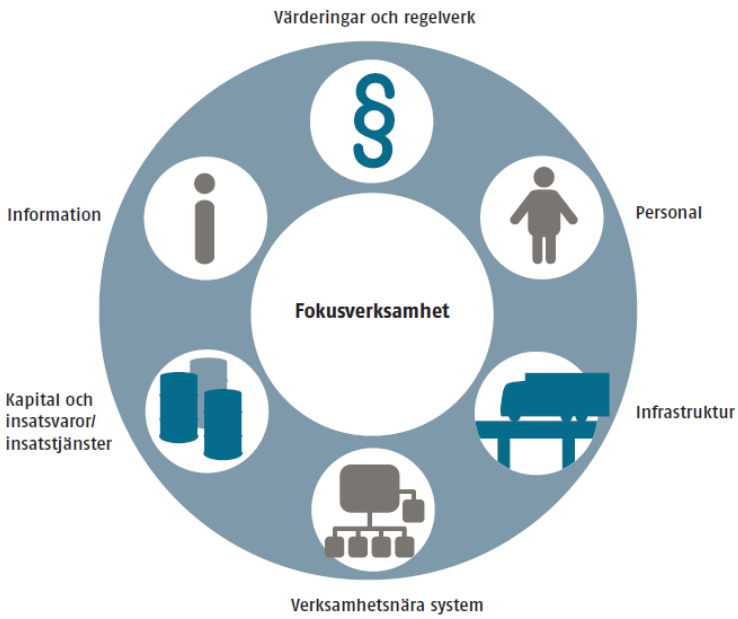
Redan i den översiktliga beskrivningen ser man att metoden i sin ursprungliga form inte ger stöd för att identifiera beroenden mellan samhällsviktiga verksamheter och ICS-system. Detta dels därför att metoden syftar till att

identifiera beroenden mellan verksamheter på en aggregerad nivå, dels eftersom den fokuserar på externa beroenden och många av de ICS-system som kan innebära sårbarheter finns inom verksamheten. Det hindrar dock inte att man kan plocka ut delar av metoden (i steg 2) och applicera dem på en mer detaljerad nivå och då även ta hänsyn till interna beroenden.

4.3.1 Identifiering och värdering av externa beroenden

I steg 1 (se Tabell 1) identifieras de verksamheter som ska analyseras vidare och i steg 2 analyserar verksamheterna själva sina behov och beroenden. Syftet med analysen i steg 2 är att identifiera och värdera verksamhetens externa beroenden enligt KBM [4, sid. 23].

4.4 Identifiering av externa beroenden



Figur 1: Beroendehjulet. [4, sid. 24]

För att identifiera externa beroenden kan man ta hjälp av beroendehjulet (Figur 1). Man sätter då verksamheten i mitten och går systematiskt igenom kategorierna som finns runt om; Värderingar och regelverk, Personal, Infrastruktur, Verksamhetsnära system, Kapital och Insatsvaror/-tjänster och

Information. För varje kategori svarar man på frågan ”Vilket behov har vår verksamhet av verksamheter och resurser inom denna kategori för att fungera?”. Detta kan verksamheten göra själv eller så kan man anlita en extern part som exempelvis kan använda hjulet som ett stöd under intervjuer med nyckelpersoner. ”Beroendehjulet” kan även användas som ett hjälpmedel under diskussioner kring en verksamhets beroenden. Här är det viktigt att man tidigare (i steg 1) har beskrivit vilken uppgift verksamheten har, vad den ska leverera, i vilken omfattning och till vem, och att man utgår från den beskrivningen då man besvarar frågan.

Slutligen väljs de behov som innebär att verksamheten har ett beroende av en extern verksamhet eller resurs ut för vidare analys. KBM ger inga motiv till varför man väljer bort att studera interna beroenden. En användare bör själv fundera om det är lämpligt eller inte för det syfte man har med analysen.

Värt att notera är att en av de kategorier man undersöker med beroendehjulet är just verksamhetsnära system som inkluderar exempelvis ICS. En möjlig utvidgning av hur man använder beroendehjulet för att identifiera beroenden mellan den studerade verksamheten och ICS, som inte är direkt kopplade till verksamheten, är att i ett iterativt förfarande:

1. Identifiera vilka beroende det finns mellan den studerade verksamheten och verksamheter och/eller resurser inom olika kategorier.
2. För varje identifierad verksamhet och resurs göra en ny analys där verksamheten/resursen sätts i centrum av beroendehjulet för att sedan identifiera vilka ICS-system som verksamheten/resursen är beroende av inom olika kategorier.

Problemet med en sådan ansats är att analysen snabbt växer och blir väldigt stor. Man måste i så fall bestämma sig för vilka beroenden som ska prioriteras för en fortsatt analys. Se vidare exemplet sist i detta avsnitt.

4.4.1 Värdering av externa beroenden

Efter att ha identifierat externa beroenden så ska dessa enligt KBM (2008) värderas utifrån *verksamhetens förmåga att hantera en störning i en annan verksamhet* som den är beroende av. [4, sid. 25]

Till hjälp i värderingen görs en bedömning av konsekvenser, stötdämpare och uthållighet enligt:

- *Konsekvenser*: Vad händer med den egna verksamheten om en verksamhet man är beroende av inte fungerar?

- *Stötdämpare*: Finns det alternativa sätt att uppfylla behovet utan den verksamhet man är beroende av?
- *Uthållighet*: Hur länge klarar sig verksamheten utan den verksamhet som den är beroende av?

Enligt KBM (2008) så är ett kritiskt beroende ”ett beroende som är avgörande för att samhällsviktiga verksamheter ska kunna fungera. Det karaktäriseras av att en störning av en levererande verksamhet snabbt och varaktigt försämrar funktionen hos en beroende verksamhet. Sådana funktionsnedsättningar kan inträffa om den beroende verksamheten saknar stötdämpare och därmed uthållighet.” [4, sid. 13]

Värderingen av det externa beroendet görs enligt skalan ”kritiskt beroende”, ”tydligt beroende” och ”svagt eller osäkert beroende”.

- *Kritiskt beroende*: Verksamheten har inga stötdämpare och en mycket begränsad uthållighet vilket gör att verksamheten relativt omgående drabbas av funktionsnedsättningar.
- *Tydligt beroende*: Verksamheten har vissa stötdämpare och en viss uthållighet vilket gör att verksamheten kan fortsätta under en begränsad tid. Hur allvarligt ett tydligt beroende är kan variera mellan olika kriser. Vid en viss kris kan beroendet uppgraderas till kritiskt för att vid en annan graderas ner till inget beroende.
- *Svagt eller osäkert beroende*: Verksamheten kan få svårigheter under vissa specifika förutsättningar men kan i de flesta fall hantera störningen väl.

Observera att värderingen inte säger något om sannolikheten för att den verksamheten ska utsättas för en störning. Att ett beroende klassas som kritiskt behöver därför inte innebära en sårbarhet. Detta illustreras ytterligare av exemplet i Tabell 2.

Tabell 2: Exempel över en beroendeanalys av hur verksamheten vid ett kärnkraftverk är beroende av kylvatten.

KBM:s värderingskriterier		Bedömning
Konsekvenser	Vad händer med den egna verksamheten om en verksamhet man är beroende av inte fungerar?	Om kylvattnet försvinner eller överstiger (säg) 25 grader så måste kärnkraftverket stänga ner sin energiproduktion.
Stötdämpare	Finns det alternativa sätt att uppfylla behovet utan den verksamhet man är beroende av?	Nej
Uthållighet	Hur länge klarar sig verksamheten utan den verksamhet som den är beroende av?	Ingen alls

I exemplet i Tabell 2 är beroendet mellan kärnkraftverket och kylvattnet kritiskt enligt KBM:s sätt att se det. Men för att säga att det kritiska beroendet innebär en sårbarhet (som eventuellt ska åtgärdas) så måste man även väga in om kylvattenförsörjningen kan störas ut. Antag att kärnkraftverket ligger långt norrut, att det har ett djupvattenintag och att temperaturen på havsvattnet tidigare aldrig har varit högre än 15 grader de allra varmaste sommarperioderna. Det är då inte troligt att kylvattnet kan bli för varmt, men det tar man inte hänsyn till då man identifierar kritiska beroenden enligt KBM:s metod. Ett ytterligare exempel, som är draget till sin spets, är att de allra flesta verksamheter är kritiskt beroende av gravitationen. Försvinner gravitationen skulle det vara omöjligt att bedriva sjukvård, sophämtning eller att transportera gods längs järnvägen. Alla dessa verksamheter har med rätta ett kritiskt beroende till gravitationen, men att kalla detta för en sårbarhet skulle nog inte många gå med på.

4.5 Tillämpning – spårbunden trafik

Nedan visas ett försök att tillämpa metoden på verksamheten spårbunden trafik med hjälp av beroendehjulet.

I centrum av hjulet	Identifierad verksamhet/resurs
Spårbunden trafik	Infrastruktur: spårnätet
	Verksamhetsnära system: *tågledningssystem*
	Kapital och insatsvaror: …
	Information: Information till passagerare via tågpersonal och på perronger
	Värderingar och regelverk: Transportstyrelsens föreskrifter och regler
	Personal: Eldriftledare
	… (listan kan göras hur lång som helst)
Tågledningssystem	Verksamhetsnära system: AoK (Ansökan om kapacitet)
	Verksamhetsnära system: SpecTra (stödsystem för specialtransporter)
	Verksamhetsnära system: Servrar, etc.
	Personal: *Tågklarerare*
Tågklarerare	Verksamhetsnära system: Mobiltelefoner
	Verksamhetsnära system: Lås på dörrar

I just detta fall går det att identifiera hundratals verksamheter/resurser inom varje kategori. Om det överhuvudtaget är görbart är det troligen inte effektivt i relation till vad analysen ger. Det måste finnas kriterier för vilka verksamheter/resurser som ska tas med och på vilken aggregeringsnivå.

En fråga som dyker upp är om ska man titta på normaltillståndet när man identifierar beroenden. Under en intervju inom studien spårbunden trafik [5] berättade en respondent att om det blir brist på personal (av någon anledning) så måste man ringa in extrapersonal. Alla som arbetar inom organisationen har inte fast telefon så man är beroende av att mobiltelefonerna fungerar. Dessutom, för att personalen ska kunna komma till sina arbetsplatser, måste passersystemen fungera. Här har vi alltså identifierat två beroenden som finns vid personalbrist (mobiler och passersystem). Men om personalbristen bara uppstår under en extraordinär händelse, ska dessa beroenden i så fall finnas med i analysen?

Ett motsvarande exempel är att om ett styrsystem som är uppkopplat mot Internet skulle utsättas för en IT-attack utifrån, så är man beroende av såväl personal som kan gå in och patcha (uppdatera) systemen och av personal som kan sköta styrsystemet manuellt. Dessa behövs dock inte i normaltillståndet. I detta fall är det alltså helt avgörande att man skiljer normaltillståndet från ett där systemet utsätts för press – beroendet är alltså i någon mening villkorat. I de beroende- och konsekvensstudier som KBM genomförde inom ramen för ”Beroendeprojektet” användes scenarier för att studera beroenden och konsekvenser vid en specifik händelse. Denna ansats ger beroendeanalysen en kontext att förhålla sig till som kan vara relevant.

5 DIGREL – erfarenheter från kärnkraftsområdet

DIGREL är ett projekt som drivs av NEA (The Nuclear Energy Agency), en organisation inom OECD (Organisationen för ekonomiskt samarbete och utveckling), som syftar till att skapa förutsättningar för modellering av s.k. Digital I&C (Instrumentation and Control) i PSA (Probabilistic Safety Assessment[6]). PSA är en metod för kvantifiering av haverisekvenser, systemotillgängligheter etc. i kärnkraftverk som bygger på felträds- och händelseträdsmetodik, dvs. en metod där ingående komponenter och dessas *beroenden* modelleras hierarkiskt med avseende på olika systemfunktioner. PSA skulle med LUCRAM:s terminologi räknas till kategorin infrastrukturbaserade metoder.

Kärnkraftverk byggs idag med ett starkt inslag av digitala komponenter i de system som ska styra och övervaka reaktorskyddssystemet och andra säkerhetskritiska system såväl som vanliga driftsystem. Utvecklingen går alltså *från analog till digital I&C*. Just dessa komponenter har visat sig vara svåra att modellera i PSA, särskilt eftersom de till stor del involverar mjukvara:

The task of incorporating a reliability model of a digital I&C based RPS [reaktorskyddssystem] into a traditional PSA model meets a number of challenges due to the specific features of digital I&C, e.g. features such as functional dependencies, signal exchange and communication, fail-safe design [- - -]. This requires both new modelling approaches and new fault tree structures, which are to be incorporated within the existing PSA model structure. Another challenge due to the complexity and number of components within a digital I&C RPS is to keep the PSA model comprehensive at a reasonable size.

I DIGREL var uppgiften att skapa en taxonomi för modellering av de komponenter som ingår i digital I&C. Projektet redovisas i en OECD/NEA-rapport [10] och i en NKS-rapport [1], Båda från 2015. (Innehållet i dessa är inte identiskt varför båda används som referenser i denna studie.)

Ansatsen inom DIGREL är intressant av två skäl.

- I&C och ICS är olika tekniska termer för ungefär samma sak – båda avser styrsystem i någon mening. Det är också så att bägge har erfarit en utveckling mot ett allt starkare inslag av mjukvara. Skillnaden är att I&C används i extremt säkerhetskritiska sammanhang och därmed i princip

[6] Förkortningen PSA används även på svenska och brukar då uttydas *Probabilistiska säkerhetsanalyser*. I USA används i regel PRA (*Probabilistic Risk Assessment*) som synonym till PSA.

aldrig har kopplingar mot Internet (däremot används en hel del moderna plattformar och mjukvara). [12]

- För att kunna etablera en taxonomi för modellering av mjukvara i PSA måste man först fundera på vilka fel som kan inträffa, vilka beroenden komponenterna ingår i, vilka systemgränser och abstraktionsnivåer som är relevanta (för att få rätt upplösning utan att analysen blir för komplex), samt varifrån man hämtar information/data om felen. [10] Dessa aspekter är relevanta även i en analys av ICS.

Inom DIGREL har man alltså, eftersom den styrs av syftet som är att bygga en PSA-modell, gjort ett slags *beroendeorienterad problematisering* av en teknik som starkt påminner om ICS, vilket gör projektets resultat högst relevanta för våra syften. Frågan är – vilka karaktäristika hos I&C måste man enligt DIGREL ta i beaktande vid beroendeanalyser? Många av de svårigheter som uppstår vid modellering av I&C har sin grund i att tekniken innehåller ett starkt inslag av mjukvara. Nedan följer en sammanställning:

- Mjukvarufel (“failures”) orsakas generellt av systematiska felkällor (“faults”), dvs. i första hand designfel, och inte av slumpfel (”random errors”). Detta betyder bl.a. att s.k. CCF (Common Cause Failures) dominerar.
- Latenta fel, i första hand de som klassas som ”non-fatal, plausible behavior” har stor betydelse för systemsäkerheten. Sådana fel innebär att styrutrustningen ger felaktig output, men att ett övervakningssystem eller en operatör inte kan avgöra om I&C-enheten (eller någon ingående modul) har felat eller inte. Sådana fel kan bli synliga antingen först efter lång tid, eller om driftförutsättningarna plötsligt ändras, t.ex. om reaktorn måste snabbstoppas.
- I&C-enheter har ofta många samtidiga attribut och kan vara programmerade att ändra beteende utifrån driftläge. Detta ökar rimligen betydelsen av latenta fel (se ovan) och försvårar modellering av beroenden, inte minst som data för flera felmoder[7] kan behöva samlas in för en och samma komponent, samtidigt som det kan finnas ett beroende mellan dessa data.
- I&C sitter ofta i högredundanta system samtidigt som sannolikheten att ett kritiskt fel upptäcks är stor. Detta betyder att latenta fel ofta modelleras som s.k. CCF (Common Cause Failures) dvs. som ett teoretiskt beroende där felsannolikheten bestäms av en matematisk modell (mer eller mindre influerad av empiri). Ofta används

[7] En ”felmod” avser ett sätt som något kan fela på. Typiska felmoder för en pump som normalt är i drift är ”obefogat stopp”, medan en standby-pump snarare har felmoden ”utebliven start.

konservativa så kallade screeningvärden för att se om en säkert överskattad felbenägenhet har någon påverkan på systemet. Om påverkan är liten betyder det i regel att just den komponentgruppen kan anses försumbar och kanske inte behöver modelleras alls. Att hitta alla tänkbara CCF:er kräver, om det ens är möjligt, stor systemkännedom, vilket betyder att modelleringen ofta är starkt förenklad. Detta gör det i sin tur svårare att tolka en anläggnings riskprofil.

- Det är generellt svårt att hitta data för mjukvara. I många fall får man förlita sig på data från leverantören och tester som gjorts under designprocessen. (Jfr [15, sid. 1].)

Ett problem som också hanteras inom DIGREL är vilken abstraktionsnivå man ska välja när man modellerar. Den taxonomi som utvecklas i DIGREL bygger på en hierarkisk definition av fem nivåer: [10, s. 44]

1. *System level*: Hela I&C-systemet, t.ex. reaktorskyddssystemet eller andra enheter som har definierats som system och som svarar för en uppsättning säkerhetsfunktioner.
2. *Division level*: Fysiskt separerade delar av ett system.
3. *I&C unit level*: Element inom en ”division” som implementerar specifika funktioner som är avgörande för funktionaliteten hos det övergripande I&C-systemet. Kategorier på denna nivå definieras utifrån deras generiska funktion, t.ex. datainhämtning, -bearbetning och -kommunikation.
4. *I&C unit modules level*: Motsvarar grupper av hårdvaruelement såsom I/O-kort, moderkort, kretskort, etc. och mjukvaruelement som utför väldefinierade specialfunktioner såsom operativsystem, applikationer, programvara, etc.
5. *Basic component level*: Hårdvara såsom resistorer, CPU:er, RAM-minnen, och kretsar på ett kretskort. På denna abstraktionsnivå antas mjukvara vara en svart låda för fortsatta analyser (se nedan).

I den taxonomi som utvecklas i DIGREL skiljer man mellan hård- och mjukvarurelaterade felmoder på nivå 4 och 5, men inte på de övre tre nivåerna. [10, sid. 110]

En av projektets rekommendationer är att man bör modellera på så hög abstraktionsnivå som möjligt så länge det finns relevanta data och alla beroenden finns representerade. När det gäller mjukvara innebär detta att man i praktiken bör stanna på modulnivå (nivå 4). [1, sid. 38] På nivån under (”Basic component level”) skulle det handla om att modellera kodsträngar, och att analysera dessa ur ett tillförlitlighetsperspektiv framstår inte som meningsfullt. [1, sid. 30] Ofta är

innanmätet i kommersiell mjukvara (s.k. COTS – Commercial-off-the-shelf) helt och hållet otillgängligt för slutanvändaren. [1, sid. 38]

6 Diskussion – ICS ur ett beroendeperspektiv

Utifrån de systemkaraktäristika och beroendeanalysmetoder som har redovisats, samt tillämpningen av KBM-metoden och erfarenheterna från DIGREL, ska vi i detta avsnitt diskutera vilka aspekter som man måste ta särskild hänsyn till, alternativt undersöka vidare, om man ska bygga ett ramverk för analys av beroenden mellan samhällsviktig verksamhet och ICS. Finns några principiella skillnader som måste hanteras av ett ramverk? Vad gäller för kartläggning respektive analys (värdering) av beroendena? Frågan är för det första om det är skillnader i själva systemen, i strukturer, topologi, utbredning, mm., för det andra om det är skillnader i funktioner, felmoder och annat som har bäring på risk, sårbarhet och andra tillämpningar av beroendeanalysen.

På en mycket övergripande nivå kanske det räcker att identifiera en samhällsviktig verksamhet utifrån någon lista (t.ex. i *Vägledning för samhällsviktig verksamhet* [8]) och sedan fråga en ”expert” om denna verksamhet är beroende av ICS. Ska kartläggningen göras på flera nivåer, med hög upplösning eller i syfte att göra en kvantitativ analys, måste man troligen involvera många experter med god systemkännedom på olika nivåer. Ett problem enligt flera källor är att dessa system finns ”överallt” och att de ingår i mycket svåröverskådliga beroendekomplex. Detta ”vet” vi redan på förhand kommer att bli en utmaning vid en beroendeanalys. Saken kompliceras ytterligare av att ICS numera innehåller mycket IT vilket öppnar upp kontaktvägar mot nya felkällor.

I kapitel 5 listades några typiska egenheter som troligen kommer att påverka beroendeanalysen. En av dem förtjänar särskild uppmärksamhet. Det gäller fel som i DIGREL förknippas med ”non-fatal, plausible behavior”. I en typisk ICS-konfiguration är processen funktionellt beroende av styrning på flera nivåer. Styrningen är i sin tur beroende av feedback från processen om att allt är som det ska. Normalt omhändertas säkerhetskritiska fel direkt, antingen genom att processen automatiskt går in i felsäkert läge (fail-safe mode), eller genom att någon nivå i styrsystemet upptäcker avvikelsen och vidtar åtgärd (larmar, kopplar in ett redundant reservsystem e dyl.). Fel som faller i kategorin ”non-fatal, plausible behavior” avser fall där processen får felaktig input, men där detta inte upptäcks annat än via dess konsekvenser (kanske efter lång tid genom att någon utrustning går sönder), i samband med test och underhåll eller då driftförutsättningarna mer eller mindre drastiskt ändras (i värsta fall för att något exceptionellt har inträffat).

Problemet uppstår med andra ord när någon nivå i systemet, t.ex. en PLC, ger felaktig output men där detta inte påverkar processen på något omedelbart negativt sätt (”non-fatal”) och heller inte upptäcks på andra nivåer i systemet eftersom processen liksom den felande enheten ser ut att fungera normalt

(”plausible behavior”). Sannolikheten för att ett sådant fel ska kunna inträffa i verkligheten, och dessutom få konsekvenser, är beroende av systemets felhanteringslogik, dvs. huruvida felindikering uteblir eller någon enhet ger felaktig information om att allt är normalt. Försvårande faktorer i moderna system med starkt inslag av mjukvara är

- att enheterna kan ha många olika attribut, där vissa är relevanta under normal drift och andra under exceptionella förhållanden.
- kommunikationen mellan systemen (både styr- och feedback-signalen) kan gå över nätverk (”administrativ IT” [7] e dyl.) som har anslutningar mot Internet.

Det senare ger möjlighet för en eventuell ”angripare” att introducera fel och/eller falska feedback-signaler i systemet. Sådana fel kan ha mer eller mindre allvarliga konsekvenser beroende på hur säkerhetskritiska systemen är. Ett exempel på en verklig händelse är fallet Stuxnet. [7]

En poäng här är att det tycks råda ett asymmetriskt förhållande mellan funktionella beroenden och sårbarheter. Om man bara tar fasta på uppenbara funktionella beroenden, typiskt de som går från högre till lägre nivåer i systemhierarkin, fångar man upp en delmängd av sårbarheterna, men kanske inte alla. En process kan nämligen störas ut även via de feedbacksignaler som styrningen behöver för sin korrekta funktion. Det finns sårbarheter som inte följer det funktionella beroendet utan snarast går i motsatt riktning. Tolkningen av beroenden i termer av sårbarheter är därmed inte trivial när man har att göra med ICS.

Förekomsten av latenta fel innebär också att det kan vara nödvändigt att använda sig av något scenario för att beroendet, och motsvarande sårbarhet, ska bli synligt i analysen eftersom det kanske är först vid ändrat driftläge som vissa fel uppenbaras.

En av studiens problemställningar handlade om huruvida ICS ställer några särskilda krav på beroendeanalyser. Med utgångspunkt i det nyss förda resonemanget verkar det uppenbart att man måste ha en helhetssyn och en genuin förståelse för hur dessa system interagerar och hur informationen flödar i dem för att man inte ska missa viktiga förhållanden i beroendeanalysen. Vilka förhållanden som är viktiga bestäms vidare av beroendeanalysens syfte eftersom syftet styr hur beroendet tolkas (i termer av t.ex. funktioner eller sårbarheter). Man måste också förstå att det finns vissa beroenden som är svåra att modellera, att systemen kommunicerar med varandra på ett sätt som kanske inte alltid är transparent, samt att många ICS har kopplingar till Internet vilket gör att antagonistiska hot blir relevanta. I detta sammanhang utgör systemets redundans, som normalt är hög, en viktig motkraft som måste analyseras noggrant, om möjligt genom explicit modellering och annars genom CCF-modellering.

Den stora frågan var och är dock om fel i ICS kan äventyra samhällsviktiga verksamheter. Vad är det i så fall frågan om för fel? Sådant är svårt att avgöra utan att göra ett långtgående modelleringsexperiment. I ett nästa skede bör man ta fram exempel på system, och utifrån den sammanställning av olika analysmetoder som gjorts i denna rapport, göra en ansats att analysera dem (t.ex. i workshopform). Det är fortfarande oklart hur nära dessa system man kommer. Tillämpar man KBM:s metod med utgångspunkt i en samhällsviktig verksamhet ska man vara beredd på att analysen växer mycket snabbt. Kanske blir den oöverskådlig innan man på allvar har lyckats kartlägga de beroenden till ICS som finns? Utifrån de försök som har gjorts här antas att en god ansats kräver att man för det första kan dela upp analysen i olika steg, där man för varje steg har möjlighet att byta metod eller anpassa den (eventuellt är det något slags hybridmetod i LUCRAM:s bemärkelse som är det bästa alternativet), för det andra att man tydligt kan ange vad syftet med analysen är (kvantitativ, kvalitativ, sårbarhetsanalys, systemkartläggning, etc.), och för det tredje att man med tydlighet kan avgränsa den verksamhet man analyserar.

6.1 Vad ska ett ramverk innehålla?

Man kan också fråga sig vilka element som ska ingå i ett ramverk. Med hänvisning till vad som beskrivits i avsnitt 1.1 behöver ett ramverk beskriva ”aspekter av beroenden som bör tas hänsyn till vid en kartläggning, samt viss vägledning till hur en beroendeanalys faktiskt bör genomföras”. Några förslag på vad som skulle kunna ingå är:

- Metodstöd – en förteckning över vilka metoder som kan vara lämpliga och hur de används.
- Viktig kunskap om systemen med avseende på beroenden och vad bör man se upp med.
- Syften och goda exempel.
- Typiska system och en sammanställning över felmoder och felmekanismer.
- Referenser.

Ramverket bör också ge vägledning ifråga om vad som ska skyddas, vad som ska levereras, samt vilka säkerhetskrav som gäller. Viktiga förutsättningar för en beroendeanalys är att man skaffar sig kunskaper om systemets betingelser, användning, driftkrav mm., samt att man noga anger syftet och de utmaningar och fallgropar som är knutna till just det syftet.

7 Slutsatser

De generella insikterna från denna studie är att själva identifieringen av beroendena (beroendekartläggningen, eller systemanalysen om man så vill), är möjlig att göra, men att den försvåras av flera skäl – dels eftersom ICS finns ”överallt” i verksamheterna, dels eftersom de interna beroendena ofta är komplexa (hög redundans, flera funktioner för samma apparatur, latenta och systematiska fel, svårt att bryta ner systemen i moduler, stark koppling till fysiska processer och i vissa fall till IT-system.). Om syftet med beroendeanalysen är att identifiera sårbarheter, vilket det ofta är, ska man vara medveten om att förhållandet mellan de ”funktionella” beroendena och sårbarheterna kan bli mer komplext och oförutsägbart. För att hitta de kritiska beroendena måste man ha en helhetssyn och en genuin förståelse för systemens funktionalitet och flöden på många olika nivåer.

Nedan sammanfattas några av de viktigaste utmaningarna som framkommit i studien samt förslag på frågor att gå vidare med:

1. Common Cause Failures (CCF) tenderar att dominera riskbilden i system med komplexa beroenden, hög redundans och starkt inslag av mjukvara (eftersom mjukvarufel i regel är systematiska). Vad finns det generellt för principer för modellering av CCF i de relevanta verksamheterna/funktionerna? Om modelleringen är starkt förenklad blir riskprofilen hos en anläggning eller funktion svårare att tolka och använda.
2. Mjukvarubaserade system kan inte utan vidare brytas ner i komponenter. Man bör välja den högsta möjliga abstraktionsnivån med hänsyn till syftet med beroendeanalysen (valet av abstraktionsnivå måste i vissa fall ställas mot möjligheten att samla in data, etc.).
3. Latenta fel, i första hand de som klassas som ”non-fatal plausible behavior” har stor betydelse för systemsäkerheten i t.ex. kärnkraftverk. Sådana fel kan bli synliga antingen först efter lång tid, eller om driftförutsättningarna plötsligt ändras. Hur stor betydelse har detta i system som stödjer samhällsviktig verksamhet? Finns det kulturer och principer som motverkar dem? (t.ex. beträffande fail-safe-lösningar, redundanser, testprogram, utbildning, etc.). I vilken grad är det realistiskt att ta höjd för antagonistiska attacker mot/via ICS i t.ex. en riskanalys?
4. Det är generellt svårt att hitta data om mjukvarufel. I många fall får man förlita sig på data från leverantören. Applicering av sådana data kräver i regel att modellen är mycket detaljerad. Vilka data finns att tillgå för de verksamheter som är relevanta med avseende på samhällsviktig verksamhet?

5. Skyddar man rätt saker? I ett ICS är det ytterst viktigt att skydda klienterna ute i systemets periferi (PLC:er mm.) eftersom dessa är närmast processerna. I ett IT-system är det ofta de centrala delarna som är mest kritiska. Kan säkerhetsfilosofier från de olika världarna (ICS och IT) kombineras på ett bra sätt?

Vidare är det viktigt att noggrannare undersöka vilka metoder som är framkomliga när det gäller samhällsviktig verksamhet och ICS. En workshop för att komma ytterligare en bit på vägen skulle kunna ta sin utgångspunkt i denna rapports sammanställning av metoder tillsammans med några väl valda fallstudier. Utifrån de försök som har gjorts här antas att en god ansats kräver att man för det första kan dela upp analysen i olika steg, där man för varje steg har möjlighet att byta metod eller anpassa den, för det andra tydligt kan ange vad syftet med analysen är, och för det tredje med tydlighet kan avgränsa den verksamhet man analyserar.

8 Referenser

1. Authén, S., m fl. (2015). *Guidelines for reliability analysis of digital systems in a PSA context – Final report*. NKS-330, ISBN 978-87-7893-411-6.
2. Axell, E. m fl. (2013). *Robust kommunikation, cybersäkerhet och artificiell intelligens för säkerhet i RPAS*. FOI Rapport 3825, ISSN 1650-1942.
3. ISO/IEC 27032 (2012), *Information technology – Security techniques – Guidelines for cybersecurity*. International Standard, ISO/IEC 27032:2012(E).
4. Krisberedskapsmyndigheten (2009). *Faller en faller då alla? En slutredovisning från KBM:s arbete med samhällskritiska beroenden*. Tillgänglig på www.msb.se.
5. Mossberg Sonnek, K. m fl. (2015). *NCS3 – Informations- och styrsystem inom spårbunden trafik – en kartläggning*. FOI-rapport 4029, MSB 2014-1131.
6. MSB (2013). *Handlingsplan för skydd av samhällsviktig verksamhet*. ISBN: 978-91-7383-373-8.
7. MSB (2014). *Vägledning till ökad säkerhet i industriella informations och styrsystem*. MSB718, ISBN: 978-91-7383-462-9.
8. MSB (2014). *Vägledning för samhällsviktig verksamhet, Att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid*. MSB620, ISBN: 978-91-7383-392-9.
9. MSB (2015). *Översikt över metoder för komplex beroendeanalys på sektoriell & tvärsektoriell nivå*. ISBN 978-91-7383-593-0, MSB904.
10. OECD-NEA (2015), *Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis*. NEA/CSNI/R(2014)16.
11. Rinaldi, S., Peerenboom, J., and Kelly, T. (2001). ”Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies”, *IEEE Control System Magazine*, Vol. 21, nr 6, sid. 11-25.
12. Song m fl. (2012). “A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants”, *Nuclear Engineering Technology*, Vol. 44, No. 8, December 2012.

13. Stouffer, K. m fl. (2011). *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82.

14. Veibäck, E. m fl. (2014). *Informations- och cybersäkerhet i nationell risk- och förmågebedömning – diskussion och presentation av en tankemodell*. FOI Memo 5100.

15. Wahlström, B. (2015). *Differences Between Analog and Digital I&C*, 9th International Conference on Nuclear Plant Instrumentation, Control & Human–Machine Interface Technologies (NPIC & HMIT 2015), Charlotte, North Carolina, Feb. 23–26, 2015.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se