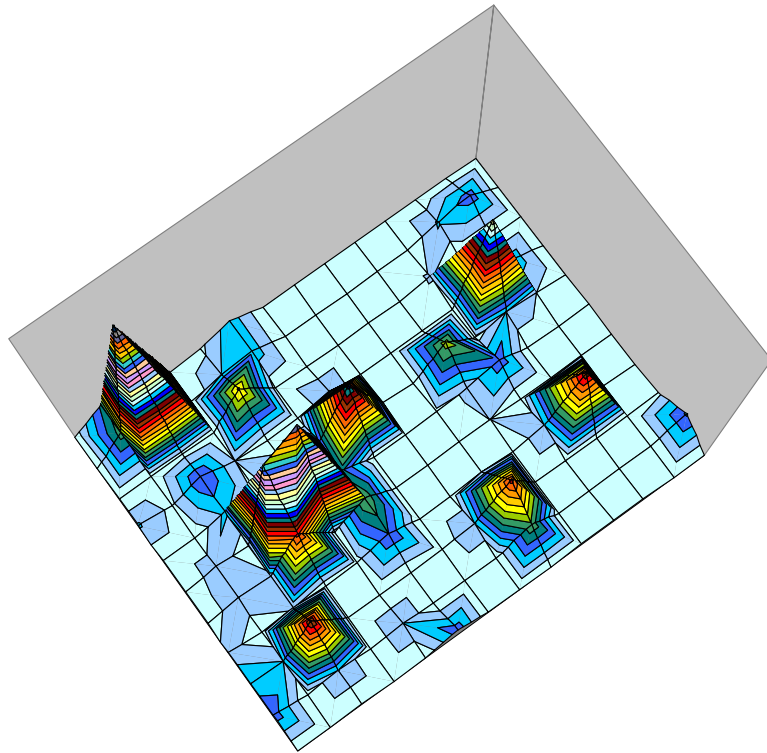


# SYSTEMTILLTRO



**Jan Andersson, Michael Malm, Ronny Thurén**



TOTALFÖRSVARETS FORSKNING SINSTITUT

Ledningssystem

Box 1165

581 11 Linköping

FOI-R--1121--SE

Oktober 2003

ISSN 1650-1942

**Vetenskaplig rapport**

Jan Andersson, Michael Malm, Ronny Thurén

## Systemtilltro

<b>Utgivare</b> Totalförsvarets Forskningsinstitut - FOI Ledningssystem Box 1165 581 11 Linköping	<b>Rapportnummer, ISRN</b> FOI-R--1121--SE	<b>Klassificering</b> Vetenskaplig rapport
	<b>Forskningsområde</b> 8. Människan i totalförsvaret	
	<b>Månad, år</b> Oktober 2003	<b>Projektnummer</b> E7044
	<b>Verksamhetsgren</b> 5. Uppdragsfinansierad verksamhet	
	<b>Delområde</b> 81 MSI med fysiologi	
<b>Författare/redaktör</b> Jan Andersson Michael Malm Ronny Thurén	<b>Projektledare</b> Ronny Thurén	
	<b>Godkänd av</b> Martin Rantzer	
	<b>Uppdragsgivare/kundbeteckning</b>	
	<b>Tekniskt och/eller vetenskapligt ansvarig</b>	
<b>Rapportens titel</b> Systemtilltro		
<b>Sammanfattning (högst 200 ord)</b> <p>I införandet av det nya nätverksbaserade försvaret (NBF) får frågan om tilltro mellan en operatör och systemet en allt större betydelse. Samverkan mellan användare och system är mycket viktigt om synergieffekter skall uppnås. I litteraturöversikten hittades många rapporter om studier av tilltro i relationer mellan människor som individer och mellan människa och maskin. Förutsägbarhet, pålitlighet, och övertygelse påverkar graden av tilltro. För att få en uppfattning om användbarheten av de olika modellerna i litteraturöversikten genomfördes empiriska studier. Soldater från två flygvapenförband och en grupp människor som utvecklar ett tekniskt avancerat system (ledningssystemet CETRIS som ska användas i korvett Visby) intervjuades. Flygvapenförbanden var de två svenska snabbinsatsförbanden, transportförbandet SWAFRAP C-130 och spaningsförbandet SWAFRAP AJS. C-130 intervjuades på sin hemmabas och AJS i samband med en internationell övning i Polen. Systemen var definierade som respektive flygvapenförband och ledningssystemet. Fyra av de elva faktorerna påvisades vara mer betydelsefulla än de övriga sju med avseende på tilltro till de valda systemen. Dessa fyra faktorer var förutsägbarhet, användbarhet, robusthet och ansvarstagande. En slutsats kan alltså vara att Totalförsvaret framförallt ska bearbeta dessa fyra faktorer eftersom det är de som påverkar systemtilltron mest påtagligt, med reservation för att de inte är signifikanta som enskilda faktorer.</p>		
<b>Nyckelord</b> tilltro, förutsägbarhet, användbarhet, robusthet, ansvarstagande		
<b>Övriga bibliografiska uppgifter</b>	<b>Språk</b> Svenska	
<b>ISSN</b> 1650-1942	<b>Antal sidor:</b> 54 s.	
<b>Distribution enligt missiv</b>	<b>Pris:</b> Enligt prislista	

<b>Issuing organization</b> FOI – Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping	<b>Report number, ISRN</b> FOI-R--1121--SE	<b>Report type</b> Scientific report
	<b>Programme Areas</b> 8. Human Systems	
	<b>Month year</b> October 2003	<b>Project no.</b> E7044
	<b>General Research Areas</b> 5. Commissioned Research	
	<b>Subcategories</b> 81 Human Factors and Physiology	
<b>Author/s (editor/s)</b> Jan Andersson Michael Malm Ronny Thurén	<b>Project manager</b> Ronny Thurén	
	<b>Approved by</b> Martin Rantzer	
	<b>Sponsoring agency</b>	
	<b>Scientifically and technically responsible</b>	
<b>Report title (In translation)</b> System trust		
<b>Abstract (not more than 200 words)</b> <p>When facing the new network-based warfare, in the spirit of RMA, the question of trust between an operator and the system takes on a more important significance. The interaction with the user is very important if advantages are to be gained. In the study of the literature on the subject, many reports were found on the study of trust in relations between individuals, and between humans and machines. Predictability, dependability and faith affect the degree of trust. To form an idea of the applicability of the theoretical models found in the literature, empirical studies were performed. Soldiers in two military air force units and a group of people working with the development of a technically advanced system (the real-time command, control, communications, computers, intelligence and interoperability system (C4I2) CETRIS that is to be used in the Swedish Visby Class corvette) were interviewed. The air force units were the two Swedish Air Force Rapid Reaction Units (SWAFRAP): the transport (C130) and the reconnaissance unit (AJS). C130 were interviewed at their home base and AJS at an international exercise in Poland. Four of the eleven factors were indicated as being more important regarding trust in the chosen systems than the other seven. These four factors were predictability, usefulness, robustness and responsibility. One conclusion could be that the Swedish Total Defence should study these four factors in particular, as they seem to have a more obvious effect on users' trust in a system.</p>		
<b>Keywords</b> trust, predictability, usefulness, robustness, responsibility		
<b>Further bibliographic information</b>	<b>Language</b> Swedish	
<b>ISSN</b> 1650-1942	<b>Pages</b> 54 p.	
	<b>Price acc. to pricelist</b>	

## Sida

6	1. Uppdraget
6	1.1 Övergripande mål för projektet
7	1.2 Bakgrund
7	1.2.1 Ny krigföring
7	1.2.2 Nätverksförsvar
8	1.2.3 Problemområde
9	1.3 Genomförandet
9	2. System-Systemtilltro
9	2.1 System
10	2.2 Systemdimensioner
10	2.3 Vald definition - för detta arbete
11	2.4 Tilltro / ”Trust”
11	2.4.1 Definitioner
11	2.4.2 Baseringsgrunder
12	2.4.3 Process
12	2.4.4 Parametrar
13	2.4.5 Olika former av systemtilltro som ett resultat av processen
14	3. Operatören
14	3.1 Personlig disposition
14	3.2 Inlärningsstil
15	3.3 Locus of Control
15	3.4 KASAM
15	3.5 Personlig erfarenhet
16	3.6 Stress
16	4. Sårbarhet
16	4.1 Tillit och sårbarhet.
17	4.2 Exempel 1: Människa - Människa
17	4.3 Exempel 2: Människa - System
18	5. Totalförsvaret - en unik miljö
18	6. Tilltro – i ett samarbete mellan två aktörer
18	6.1 Tilltro – människa-människa
19	6.1.1 Förutsägbarhet
19	6.1.2 Pålitlighet
20	6.1.3 Övertygelse
20	6.2 Tilltro – människa-maskin
20	6.2.1 Teoretiska modeller för tilltro
21	6.2.2 Mätning av Tilltro
22	6.2.3 Socialpsykologiska frågeställningar
23	6.2.4 Tilltro med avseende på argumenterande system
24	6.2.5 Tilltro till specifika råd från intelligenta system
24	6.2.6 Tilltro då informationstillförlitligheten varierar
25	7. Summering av litteraturstudien

---

26	<b>8. Metod</b>
26	<b>8.1 Datainsamlingsmetoder</b>
27	8.1.1 Enkät 1 (Hjulet)
27	8.1.2 Enkät 2
28	8.1.3 Instrumentval
28	<b>9. Fallstudier</b>
28	<b>9.1 Utvalda förbandssystem</b>
28	9.1.1 SWAFRAP C-130
29	9.1.2 SWAFRAP AJS 37
29	9.1.3 CETRIS, Korvett Visby
29	<b>9.2 Datainsamlingsprocedur</b>
30	<b>10. Analys av Enkät 1</b>
30	10.1 Beskrivning av resultaten från SWAFRAP AJS 37
32	10.2 Beskrivning av resultaten från SWAFRAP C-130
33	10.3 Beskrivning av resultaten från CETRIS, Korvett Visby
35	10.4 Sammanställning av resultaten från ”Hjulet”
36	<b>11. Analys av Enkät 2</b>
37	<b>12. Sammanställning av samtliga empiriska resultat</b>
38	12.1 Resultaten av empiriska nedslag i ljuset av teoretiska modeller
38	<b>13. Systemtilltro – i ett framtida NBF</b>
38	<b>13.1 Virtuella team och virtuella organisationer</b>
39	13.1.1 Skapa och vidmakthålla systemtilltro
39	13.1.2 Swift trust
39	13.1.3 Systemparametrar
40	13.1.4 Icke-rutin och övning
40	<b>13.2 Att sprida innovationer</b>
41	<b>14. En holistisk bild av systemtilltro</b>
42	14.1 Ingångsvärden
43	14.2 Processen
43	14.3 Bedömd förmåga
44	<b>15. Slutsatser</b>
45	<b>16. Förslag till vidare forskning</b>
	<b>Appendix</b>
46	1 Enkät Hjulet
47	2 Enkät Parametertest
48	3 Tabeller
51	<b>Referenser</b>

---

## 1. Uppdraget

Systemtilltro är ett projekt initierat inom området FOI's strategiska forskningskärnor. Projektet har drivits som en förstudie under ca 10 månader och bemannats av 11,6 personmånader. Uppgiften bestod i framförallt 3 deluppgifter.

1. Genomföra en litteraturöversikt med syfte att skapa en bild av fenomenet systemtilltro.
2. Genomföra studier på verksamma ”system” inom försvarsmaktens (FM) organisation.
3. Koppla litteraturen och de empiriska resultaten till ett framtida nätverksbaserat försvar (NBF).

Resultatet av deluppgifterna presenteras i denna forskningsrapport som i och med deluppgifternas karaktär blir relativt stor. För att underlätta läsarens möjlighet till översikt kan rapportens upplägg summeras enligt följande:

Kap 3, 4, 6 och 7 behandlar framför allt litteraturöversikten.

Kap 8-12 redovisar det empiriska arbetet.

Kap 13 handlar om systemtilltro i virtuella organisationer (i analogi till NBF).

Dessa kapitel anknyter till deluppgifterna ovan.

Initialt, i kap 1-2, diskuteras centrala aspekter för arbetet, bl.a. systemtilltro i en kontext med valda avgränsningar och syften. Kap 5 berör Totalförsvarets speciella verksamhet och problematiserar några aspekter som tydligt påverkar systemtilltro i denna miljö. I kap 14-16, slutligen, presenteras författarna egna försök till summerande hypoteser och slutsatser samt frågeställningar som inbjuder till vidare forskning.

### 1.1 Övergripande mål för projektet

I alla typer av system där en operatör eller deltagare på något sätt är beroende av andras eller andra enheters prestation eller uppförande skapas någon form av relation mellan operatören och systemet. Kvaliteten i denna relation utgörs bland annat av operatörens tilltro till systemet. Det kan vara hans/hennes förtroende för sina arbetskamraters förmåga att utföra sina delar av arbetsuppgifterna, tilltron till ett fordons prestanda eller driftsäkerhet eller en datoroperatörs tilltro till informationen han får via sin dator. Om man redan i skapandet av ett system kan ta hänsyn till vad operatören bygger sin tilltro till systemet på kommer mycket att vara vunnet för att erhålla ett effektivt system med avsedd funktion. Vidare kan ett systems gränssnitt vara mer eller mindre påverkande. Det framkommer i litteraturen (se kapitel 4) att ett gränssnitt kan vara mer eller mindre ”övertalande”. Hög tilltro är viktig för att underlätta samarbetet mellan operatören och systemet så att synergieffekter mellan operatör och system erhålls. I projektet kommer vi att söka de mekanismer som ligger bakom en användares tilltro till det system han eller hon har till sitt förfogande och vi måste därför förstå hur en operatör skapar sin systemtilltro.

Frågeställningar som är centrala i projektet är således:

1. Vad är systemtilltro?
2. Hur skapar man systemtilltro?
3. Hur bibehåller man systemtilltro?
4. Hur återskapar man systemtilltro?
5. Hur mäter man systemtilltro?
6. Hur påverkar tilltro respektive misstro systemets effektivitet?



Det empiriska arbetet kommer att fokusera på fråga 1 och fråga 5 i en FM miljö. De övriga frågorna kommer att diskuteras i någon mån och studeras i det fortsatta arbetet, d.v.s. i efterföljande studier.

## 1.2 Bakgrund

### 1.2.1 Ny krigföring



I de nya riktlinjerna för försvaret läggs stor vikt vid att snabbt och effektivt kunna inhämta, bearbeta och delge information. Genom att göra detta bättre än en tänkt motpart når man informationsöverlägsenhet. Den nya krigföringen (RMA) bygger enl Per Nilsson (Övlt Hkv Kri Led och sektC NBF) i princip på fyra hörnstenar:

- **Samverkande system av system;** Network Centric Warfare (NCW),
- **Överlägsen lägesuppfattning;** Dominant Battlespace Awareness (DBA),
- **Beslutsöverlägsenhet,**
- **Precisionsinsatser.**

### 1.2.2 Nätverksförsvar

Detta moderna, flexibla och rörliga försvar som enligt riksdagsbeslut skall skapas kan ses som en utveckling mot ett nätverksförsvar, vilket kan beskrivas utifrån en övergripande indelning av FM's förmågor i tre delar (Försvarsberedningens Rapport 2001-08-30):

- **information och omvärldsuppfattning**
- **ledning med beslutsstöd**
- **insats och verkan**

Genom att, med sensorer och andra informationskällor, skapa bilder av vad som händer i vår omgivning erhålls omvärldsuppfattning. När dessa byggs samman i nätverk kan man skapa en samlad lägesbild som, i nära realtid, kan spridas till staber, befattningshavare och andra som behöver den. Med grund i lägesbilden och domänkompetens skapar ledning med beslutsstöd möjligheter för snabba och relevanta beslut. I ett icke-hierarkiskt nätverk kan det skapas förutsättningar för ledningsfunktionen att verka från den mest lämpliga nivån beroende på situationen. Detta samlat möjliggör effektivare, graderad insats och verkan vid rätt tillfälle. När dessa tre förmågor byggs samman i ett nätverk kan synergieffekter erhållas.

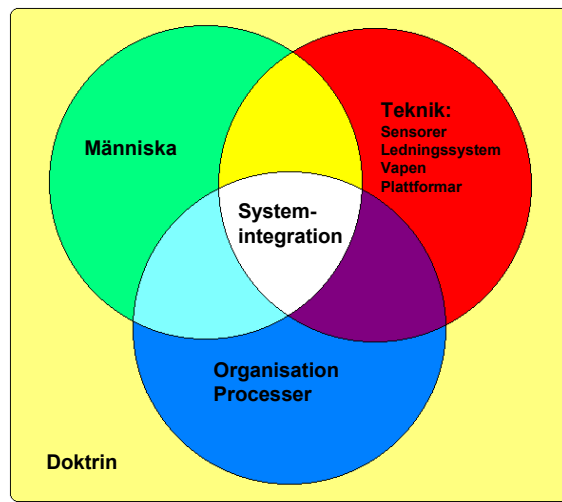
Nätverksförsvaret kan innebära att ett hierarkiskt arbetssätt överges, dvs. arbete och kommunikation sker horisontellt och i nätverk och organisationen blir därmed plattare. Avsikten är att uppnå ett bättre resursutnyttjande och ett mer gemensamt och integrerat agerande av stridskrafterna. Även förmågan till civil-militär samverkan kan förbättras genom att gemensamma resurser bättre nyttjas med utvecklingen av nätverksförsvaret bl.a. som stöd vid sjö- och flygräddning och miljöolyckor.

### 1.2.3 Problemområde

Ur detta perspektiv måste det anses nödvändigt att operatörer och beslutsfattare (användare) har tilltro till det system han eller hon använder. I ett system med stor lokal frihet (Brehmer, 2002) där beslutsfattaren, som samtidigt är genomförare, utgår ifrån information från tekniska system i större utsträckning än tidigare, krävs troligen att beslutsfattaren kan lita på informationen som han/hon får. Det innebär att beslutsfattaren i stor utsträckning är beroende av informationssystemet. Hur beroende en individ är utav ett system har visat sig påverka hur interaktionen med systemet ser ut. Systemtilltron skapar förutsättningar för människorna i systemet att vilja, kunna och våga agera. Det innebär att individen måste ha förtroende för det ”stora systemet”, samt för det ”lilla systemet”, dvs den egna delen. Systemtilltron är aldrig svart eller vit, antingen eller, utan något utmed en skala (Muir, 1994).

Enligt ovanstående resonemang, där operatörer och beslutsfattare i högre grad än tidigare, troligen kommer att inhämta information via stora system i nätverk och därigenom skaffa sig beslutsunderlag som kan grunda sig på ett mycket stort antal informationskällor, hamnar källan (inte nödvändigtvis geografiskt) långt från användaren. Han eller hon får svårare att bilda sig en uppfattning om informationens kvalitet. Rapporter, iakttagelser, sensordata o.s.v. får en anonym inramning och kanske inte ens framgår i sin ursprungliga form utan har fusionerats med andra data för att verifieras och öka i exakthet. En användare får inte möjlighet att värdera sin information på samma sätt som han/hon skulle göra med kännedom om källan. En aspekt på systemtilltro måste alltså vara att användaren har möjlighet att skapa sig en befogad tilltro till den information som man grundar sina beslut på!

Människan bör betraktas, inte bara som den av systemet servade beslutsfattaren utan också som en viktig nod i systemet! För att uppnå önskad systemeffekt (operativ förmåga) måste människan (beslutsfattare/operatörer), delsystemen, organisationsstrukturer och processer integreras utifrån ett förmågeperspektiv (se Figur 1).



Figur 1 illustrerar den ovan diskuterade integration som bör beaktas (Dahlbäck, 2001).

Detta innebär att operatörens förmåga påverkas av i vilken utsträckning han/hon har tilltro till ett system. I ett NBF är det sannolikt att operatören tvingas till interaktion med ”nätet”, vilket direkt ytterligare förstärker betydelsen av systemtilltro då operativ förmåga är av intresse. Dessa argument gör det än mer angeläget att systemtilltroaspekter studeras och beaktas i den unika miljö som Totalförsvaret agerar i.

### 1.3 Genomförandet

Då ”fenomet” systemtilltro inte är studerat inom ramen för FOI: s verksamhet tidigare är det svårt att uttala sig om hur systemtilltroproblematiken ”ser ut” inom Totalförsvaret. Vi valde därför att studera flera enheter i en och samma studie och att vägledas av resultat från tidigare forskning, framförallt teoretiska men också metodiska, vilket resulterade i en litteraturöversikt och ett empiriskt arbete. Både litteraturstudien och de empiriska resultaten redovisas i detta arbete. Inledningsvis presenteras litteraturöversikten för att a) illustrera hur forskningsvärlden har resonerat kring tilltroproblematiken i stort, och b) diskutera hur tidigare resultat kan relateras till vår, i vissa fall, unika verksamhet inom Totalförsvaret: ”komplexa system i dynamiska (extrema) situationer”. Därefter presenteras de explorativa empiriska studier vi genomfört. Resultat och slutsatser av dessa studier redovisas därefter. Slutligen diskuteras på vilket sätt som Totalförsvaret bör inrikta fortsatt verksamhet inom ramen för systemtilltro, speciellt med avseende på en NBF-inriktning.

De empiriska studierna genomfördes dels i förbandsmiljö på flygvapnets snabbinsatsförband; SWAFRAP C-130 och SWAFRAP AJS och dels i ett utvecklings- och utprovningsslab i Järfälla där ledningssystemet till kustkorvett Visby, Cetris utvecklas. Snabbinsatsförbanden valdes då där fanns erfarenhet av insatser i ”skarpa lägen”, dvs krigszoner i bl.a. Kosovo. Cetris valdes för att få tillfälle att studera ett system av stark teknisk karaktär. Närmare beskrivning av fallstudierna ges i kapitel 9.

## 2. System-Systemtilltro

Systemtilltro får anses vara ett begrepp med många dimensioner (Muir, 1987). Ett system kan ha olika utseende beroende på hur det definieras eller vem som gör det. Tilltron eller förtroendet får då även olika innebörd i olika situationer. Kontext, komplexitet, organisation, erfarenhet och förväntningar är exempel på faktorer som, i olika situationer, påverkar tilltron.

### 2.1 System

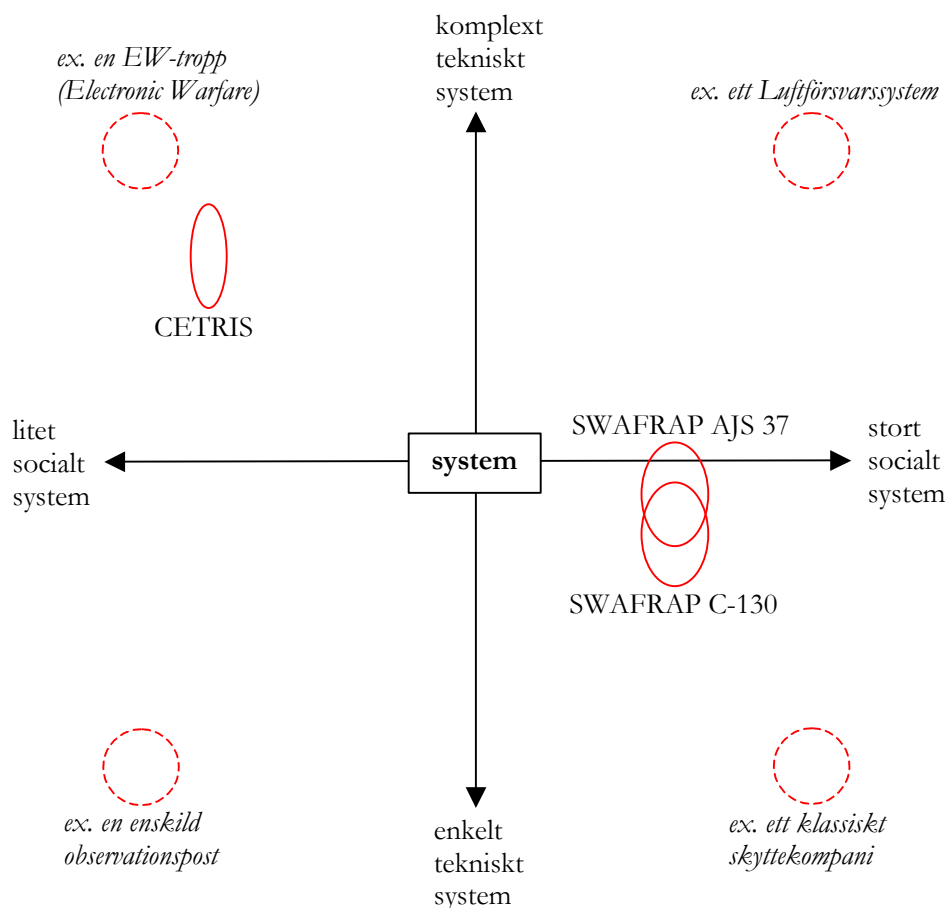
Nationalencyklopedins definition av system lyder: System (senlat. syste´ma, av grek. sy´stema 'helhet sammansatt av flera delar', av syni´stemi 'sammanställa'), samling element som hänger samman med varandra så att de bildar en ordnad helhet. System i denna allmänna bemärkelse uppträder i de mest skilda sammanhang såväl inom som utom vetenskapen. En människa kan således definiera ett system annorlunda än någon annan beroende på vilka element de uppfattar som viktiga, (t.ex. vilken roll de har eller vilken uppgiften är) trots att de verkar i samma miljö och har samma resurser till sitt förfogande. Det ligger alltså nära till hands att anta att systemet blir beroende av vilken uppgift det ska hjälpa människan att lösa.

En bilförare som kör sin bil kan betrakta bilen som sitt system vilket han samverkar med genom ratt, pedaler, reglage och instrument. I ett större perspektiv verkar han i ett system bestående av vägar, andra bilister, trafikregler, väderförhållanden, osv. Om vi säger att hans uppgift är att förflytta bilen framåt (eller bakåt) kan vi kanske begränsa systemet till bilen och föraren, medan om uppgiften är att ta sig från punkt A till punkt B, får systemet en annan omfattning och får betraktas ur det större perspektivet. På samma sätt skulle en pilot kunna betrakta sitt flygplan med dess besättning som ett system medan flygplanet ingår i ett förband som i förbandschefens ögon utgör systemet.

I ett nätverk med informationsvägar, kommunikationskanaler och beslutsstöd, baserat på någon form av IT-lösning kanske systemet beskrivs olika av olika operatörer beroende på hans eller hennes erfarenhet och kännedom i ämnet. Vilken uppfattning operatören har av systemet han verkar i måste vara grundläggande för tilltron till detsamma.

## 2.2 Systemdimensioner

I projektet har begreppet system getts ett brett avstamp; från den ensamme operatören vid en datorterminal till globala system av system (se Figur 2). I ett försök att illustrera detta ritas vi ett koordinatsystem där axlarna representerar mängden involverade operatörer respektive graden av komplexitet hos systemet. Illustrationen i två dimensioner valdes eftersom i synnerhet det tekniska och det sociala nätverket påverkas i ett framtida NBF.



Figur 2. Tvådimensionell illustration av system.

I fältstudierna har två system kunnat undersökas; dels ledningssystemet CETRIS i den 2:a kvadranten och dels Swafrap-förbanden i den 4:e. Det har varit viktigt att i dessa fältstudier definiera vad vi menar med systemet i varje enskilt fall så att alla försökspersoner får samma utgångsläge i sina tankegångar.

## 2.3 Vald definition - för detta arbete

Ett system är alltså en avgränsad summa av interagerande delar. Det innebär att ett och tillsynes samma system kan vara skilda ting för olika personer med olika uppgifter i olika organisationer. Det centrala i den valda utgångspunkten är att det är viktigt att poängtera vilket system som är fokus för den specifika frågeställningen. Det är centralt att den operatör som deltar i studien vet vilket avgränsat system han/hon ska uttala sig om. Vet inte operatören vilket system som avses då systemtilltro diskuteras blir validiteten i utslagorna låga.

## 2.4 Tilltro / ”Trust”

### 2.4.1 Definitioner.

Vi har under litteraturgenomgången funnit ett flertal definitioner av begreppet tilltro. I likhet med Shalit (1988) noterar vi att operatörens/operatörernas subjektiva upplevelse är avgörande vid fastställandet av systemtilltron. Med utgångspunkt från detta har vi valt att fokusera på kognitiva definitioner i huvudsak. Flera forskare har föreslagit en definition av ”trust”. Här följer några exempel:

**Fogg & Tseng** (1999) menar att tilltro är:

“a positive belief about the perceived reliability of, dependability of and confidence in a person, object or process.”

**Rotter** (1980) definierar tilltro som:

“a generalized expectancy held by an individual that the word, promise, oral or written statement of another individual or group can be relied upon.”

**Gambetta** (1988) uppfattar tilltro som:

“a calculated decision to cooperate with specific others, based on information about others personal qualities and social constraint.”

**Zucker** (1986) föreslår att tilltro är:

“a set of expectations shared by all those involved in an exchange.”

**McAllister** (1995) framhåller två former av tilltro:

“one grounded in cognitive judgments of another’s competence or reliability and another founded in affective bonds among individuals.”

**Sitkin and Roth** (1993) förutsätter att tilltro är:

“a belief in a persons competence to perform a specific task under specific circumstances.”

Ett försök, från vår sida, att formulera en definition på systemtilltro med utgångspunkt från Totalförsvarets speciella uppgift skulle kunna vara:

*” Tilltro är operatörens subjektiva bedömning av systemets förmåga att lösa sin uppgift även i ogynnsamma, extrema situationer”*

Detta innebär att tilltro är något som är individberoende samt avhängigt individens definition av systemet. Tilltron är tydligt kopplad till en förmåga, och för Totalförsvaret ofta i extrema situationer. Denna subjektiva tilltro kan dock basera sig på olika grunder för olika individer, vilket diskuteras nedan.

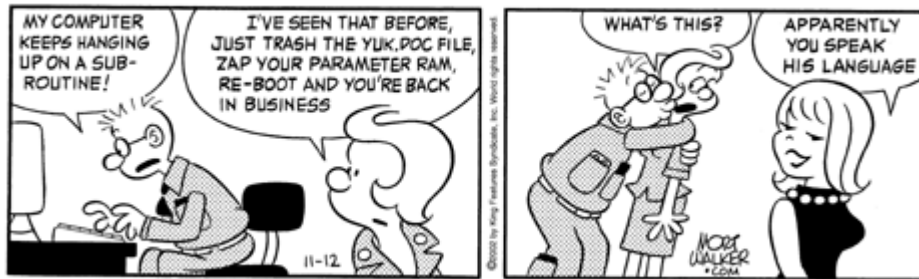
### 2.4.2 Baseringsgrunder

Flera forskare framhåller teorier om vad tilltron baseras på.

Sitkin (1995) lyfter fram tre källor till tilltro nämligen competence (sakkunskap), benevolence (välvilja) och values (värderingar). Lewicki och Bunker (1995a; 1995b) hävdar att tilltro är calculus based (beräknad), knowledge based (kunskaps-) och/eller identification based (identifieringsbaserad). Calculus based innebär att man gör en kalkyl av vad man kan vinna på ett givet agerande ställt mot vad det kan kosta om man misslyckas. Knowledge based innebär att man genom att ha kunskap kan avgöra om systemet är pålitligt. Kunskapen kan ha erhållits på flera olika sätt; exempelvis genom personlig erfarenhet eller genom överföring från någon annan. Identification based innebär att man kan identifiera sig med systemet, dess avsikter och värderingar, och genom denna identifiering utveckla en tilltro.

### 2.4.3 Process

Flera forskare pekar på att tillit utvecklas genom en process. Rempel et al (1985) hävdar att tilltro utvecklas över tiden i tre steg från predictability via dependability till faith. Processen är inte avslutad i och med man uppnått faith utan är dynamisk, dvs beroende på vad som inträffar kommer operatören att ompröva/ifrågasätta sin faith troligen genom att backa tillbaka först till dependability och sedan till predictability. Alla tre områdena är viktiga vid varje enskilt tillfälle men individen tycks fokusera på en av dem mer än de övriga beroende på var individen befinner sig i processen.



### 2.4.4 Parametrar

Vid litteraturgenomgången identifierades ett antal parametrar som olika forskare, utifrån olika aspekter på systemtilltro, funnit påverka operatörens uppfattning:

#### **Predictability (Förutsägbarhet)**

Predictability innebär att operatören kan förutsäga hur systemet kommer att agera och reagera vilket innebär att operatören har en viss kontroll vad avser framtiden. Olika typer av situationer och system torde kräva olika typer av tidshorisonter vad avser predictability.

#### **Capability (Förmåga)**

Capability syftar på systemets prestanda och därmed dess förmåga att verka i olika situationer.

#### **Intentionality (Avsikt)**

Intentionality avser de bakomliggande motiv som finns för systemet. Ett personpositionerings-system kan å ena sidan uppfattas som en säkerhetsåtgärd men å andra sidan som ett system för övervakning/ kontroll av individers agerande ("Storebror ser dig").

#### **Transference (Överlåtande)**

Transference avser överföring av systemtilltro från andra signifikanta delar av systemet. Beroende på operatörens uppfattning om dessa delar kommer han/hon uppfatta systemet på olika sätt.

#### **Robustness (Robusthet)**

Robustness handlar om systemets förmåga att "stå pall", dvs förmågan att fungera även om systemet är skadat och i krävande och ogynnsamma miljöer.

#### **Familiarity (Familiäritet)**

Familiarity syftar på operatörens förmåga att känna igen systemet givet andra system som han/hon har erfarenhet av.

**Understandability (Begriplighet)**

Understandability syftar på systemets förmåga att låta operatören förstå hur systemet "tänker" och arbetar.

**Usefulness (Användbarhet)**

Usefulness syftar på om man som operatör uppfattar systemet som användbart givet den uppgift man har. Man kan troligtvis ha tilltro till systemet i sig men baserat på den situation man befinner sig i och det uppdrag man har att genomföra kan bedömningen av systemet bli annorlunda.

**Honesty (Ärlighet)**

Honesty syftar på om systemet är ärligt eller om systemet "mörkar" eller har dolda avsikter.

**Reliability (Funktionssäkerhet)**

Reliability syftar på systemets förmåga att fungera utan att fel inträffar.

**Dependability (Tillförlitlighet)**

Dependability syftar på hur pålitligt operatören uppfattar systemet vilket bl.a. beror på funktionssäkerheten.

**Responsibility (Ansvar)**

Responsibility syftar på om systemet uppfattas som ansvarstagande och ansvarsfullt.

**Faith (Övertygelse)**

Faith syftar på operatörens vilja att bortse från eventuella tveksamheter. (Faith är troligen mer att betrakta som ett slutresultat än som en egen parameter.) Dock torde en operatör med hög grad av disposition för faith låta denna faktor påverka uppfattningen om systemet.

Ovanstående parametrar behöver noggrannare analyseras, definieras och jämföras i syfte att ta bort parametrar som beskriver samma eller närliggande saker. Det är intressant utifrån ett totalförsvarsperspektiv att studera vilka av dessa parametrar, eller faktorer, som påverkar tilltron hos befattningshavare i totalförsvarmiljöer. Avsikten är att utnyttja dessa a priori faktorer och mäta vilken betydelse de har för tilltron för "våra" operatörer (se metod och resultatdel för detaljer).

**2.4.5 Olika former av systemtilltro som ett resultat av processen**

Flores och Solimon (1998) samt Brenkert (1998) definierar olika former av tilltro. Dessa olika former kan man se som ett resultat av en process där ovanstående parametrar varit avgörande.

De olika former av tilltro man funnit är:

**Simple trust**

Simple trust innebär ett naivt förhållningssätt där operatören på olika sätt försöker undvika distrust.

**Blind trust**

Blind trust innebär en envishet och där man försöker att som operatör lura sig själv.

**Basic trust**

Basic trust innebär en grundläggande upplevelse av säkerhet och trygghet.

**Authentic trust**

Authentic trust är sådan tilltro som är reflekterad och där operatören förstår vad tilltron innebär och dess begränsningar.

**Articulated trust**

Articulated trust innebär en uttalad tilltro till systemet.

**Guarded trust**

Guarded trust innebär att tilltron måste skyddas av t.ex. regler och ev bestraffningar vid brott mot tilliten.

**Extended trust**

Extended trust innebär att operatörens tilltro till en del av systemet kan sprida sig och även inkludera andra delar av systemet.

### 3. Operatören

I centrum av systemtilltron står operatören enligt vår valda definition. Det är operatörens subjektiva bedömning av systemets förmåga att lösa sin uppgift även i ogynnsamma, extrema situationer, som avgör graden av systemtilltro. Nedan följer ett antal aspekter på operatören som torde påverka hans/hennes subjektiva bedömning. Det innebär att den process som skapar någon grad av tilltro även är påverkad av individuell karaktäristik.

#### 3.1 Personlig disposition

Flera forskare (exvis Kee och Knox (1970) samt Sitkin och Roth (1993)) påpekar att tilltro är en dispositiv egenskap, d.v.s. olika individer har olika utgångslägen i sin tilltro. Vissa människor tenderar att från början lita på ”andra” men ändrar sig i takt med att de ”andra” inte infriar förväntningarna. Andra människor startar med att inte lita på ”andra” och ändrar sig i takt med att de ”andra” visar sig vara tillförlitliga. Människor tycks alltså utgå från olika lägen på skalan och justerar sedan bedömningen i efterhand.

Francis Fukuyama (1995) drar i sin bok ”Trust” den dispositiva aspekten ett steg längre där han hävdar att kollektiv (organisationer, stater) påvisar dispositiva tendenser som får konsekvenser för samhällsutvecklingen. S.k. ”low-trust” länder där misstron är den initiala grundregeln har svårigheter att bygga bl.a. globala organisationer då det kräver samarbete och ”trust” gentemot främlingar. Fukuyama nämner bl.a. Sydkorea som ett ”low-trust” land. Som ett exempel på ett ”high-trust” land nämner han Japan som genom sin ”trust” förmår att bättre samarbeta med främlingar vilket är en förutsättning för stora globala organisationer och företag.

Den initiala förmågan och viljan att lita på och samarbeta med ”okända andra” påverkas alltså av den personliga dispositionen.

#### 3.2 Inlärningsstil

Var och en har sitt unika sätt att ta in information och omvandla den till kunskap.

Kolb (1984) beskriver hur vi, i princip, disponerar två olika sätt att ta in information, nämligen genom konkreta upplevelser eller abstrakt tänkande. Kolb menar att vi genom disposition och erfarenhet utvecklar dessa två sidor. Vissa personer utvecklar en preferens för endera av de två som kan vara olika stark och vissa utvecklar båda sätten någorlunda lika. Kolb menar vidare att vi i princip har två olika sätt att omvandla den information vi tagit in till kunskap, nämligen genom aktivt experimenterande eller genom reflekterande observation. Olika individer utvecklar olika metoder att omvandla information till kunskap liksom man även utvecklar förmågan att ta in information.

Den kombination av hur man tar in information och hur man omvandlar den till kunskap utgör inlärningsstilen. Olika inlärningsstilar kräver olika inlärningsituationer och inlärningshjälpmedel. Olika typer av beslutsstöd vad avser både utformning och funktion torde passa olika operatörer olika bra baserat på deras inlärningsstil.



### 3.3 Locus of Control

Locus of Control (LOC) (Rotter, 1980) beskriver var en individ uppfattar att det som påverkar honom eller henne är placerat; utanför eller inom individen. Ett yttre LOC innebär att en individ uppfattar att det som påverkar ligger utanför individen själv. Att det blir som det blir beror på faktorer som individen inte har kontroll över och inte kan påverka. Man uppfattar sig oftare än andra som offer för omständigheterna. Ett inre LOC innebär att en individ uppfattar händelser som ett resultat av egna förhållningssätt, beslut och ageranden. Man uppfattar sig oftare som ansvarig eller medansvarig till det som sker. Var och en har en tyngdpunkt åt antingen yttre eller åt inre LOC.

En yttre LOC torde försvåra för operatören att agera och utnyttja systemets potential framförallt i en hotfylld situation medan en inre LOC torde hjälpa individen att mobilisera sina resurser för att åstadkomma ett resultat. Det innebär att utvecklade system bör beakta att operatören bör uppleva att han/hon kan kontrollera systemet.

### 3.4 KASAM

KASAM betyder ”Känsla av sammanhang” (Antonovsky, 1991) och beskriver vad en individ måste göra för att kunna agera i olika situationer. Antonovsky hävdar att för att en individ skall agera krävs:

1. Att hon förstår den situation hon befinner sig i, dvs att situationen är begriplig.
2. Att hon upplever att situationen har med henne att göra, att hon berörs av situationen, dvs att situationen är meningsfull för henne.
3. Att hon kan göra något åt situationen, dvs att situationen är hanterbar.

En person som förstår den situation hon befinner sig i, uppfattar situationen meningsfull samt upplever att hon kan hantera den har en hög KASAM. Om hon inte förstår situationen, inte uppfattar den som meningsfull samt upplever att hon inte kan göra något åt den har hon en låg KASAM. En person kan även ha en rigid KASAM, dvs tror sig ha en hög KASAM men i själva verket kanske blundar för vital information, avgränsar eller avskärmar sig eller tillgriper någon annan form av psykologiskt försvar för att hantera situationen.

Ben Shalit berör i sin bok ”Stridens och Konflikts Psykologi” (1988) samma frågeställningar som Antonovsky. Terminologin och synsättet är likartat även om de närmar sig ämnet från skilda utgångspunkter (Shalit med konflikter som utgångspunkt och Antonovsky med hälsa som utgångspunkt).

### 3.5 Personlig erfarenhet

Kleins (1998) arbete med bl.a. brandmästare visar att den personliga erfarenheten är av stor betydelse för förmågan att hantera olika typer av situationer. Genom erfarenhet får operatören tillgång till ”mönster” och indikatorer på mönster som underlättar beslutsfattande även under svåra förhållanden. Den personliga erfarenheten möjliggör för operatören att värdera systemets förmåga i en given situation och därmed avgöra vilka beslut och åtgärder som kommer att fungera. Systemtilltro är relaterat till förmågan hos operatören att värdera ett system vars olika delar och funktion i en given situation är dynamisk, dvs delvis föränderlig beroende på bl.a. sammansättning och funktionsduglighet.

### 3.6 Stress

Operatörens stressbelastning påverkar dennes förmåga att värdera och utnyttja systemet. Befinner sig operatören långt ner i den sk ”stresskonen” är operatören att betrakta som instabil (i jämförelse med när han är högt uppe i stresskonen), dvs. den subjektiva bedömningen av systemet är mer eller mindre oförutsägbart. Operatören kan antingen välja att uppfatta systemet som en hjälp som han/hon sätter tilltro till eller som ett hinder som ytterligare belastar operatören och som därför kommer att betraktas med misstro. En operatör och ett system förväntas fungera även under starkt stressfyllda förhållanden. I dessa situationer är det av särskild vikt att operatören har tilltro till systemet.

Kapitel 3 har kortfattat redogjort hur individkaraktäristik påverkar operatörens tilltro till ett system. Detta förhindrar inte att tilltron påverkas av ytterligare miljöomständigheter och att bl.a. sårbarhet är en bidragande stressfaktor i detta sammanhang. Sårbarhet och dess relation till systemtilltro är problematiserad i litteraturen. Nästa kapitel innehåller en kort översikt och några exempel på hur sårbarhet kopplas till systemtilltroproblematiken.

## 4. Sårbarhet

### 4.1 Tillit och sårbarhet.

Tilltro som begrepp och i detta fall systemtilltro blir meningsfullt först när man är sårbar och måste agera under osäkerhet samt i riskfyllda situationer. Sårbarhet är en tydlig faktor inom totalförsvarets verksamhetsområden. Nedan diskuteras hur sårbarhet är relaterad till begreppet tilltro.

”In the absence of vulnerability, the concept of trust is not necessary” (Mishra, 1996)

Under trygga, säkra och riskfria förhållanden är systemtilltro inte en avgörande faktor. För projektet har det varit av särskilt intresse att studera tilltro i situationer som kännetecknas av osäkerhet, kaos, tvetydighet samt där operatören är sårbar. Den största delen av den tidigare forskningen är inte gjord utifrån det perspektivet, varför vi ser behovet av fortsatt forskning i den för Totalförsvaret unika miljön.

Operatörer och eller soldater uppvisar främst tre former av rädsla kopplat till sårbarhet i strid (Shalit, 1988). Dessa är rädsla att dö, att bli skadad samt rädsla att svika sina kamrater. Av dessa är rädslan att svika sina kamrater större än att själv bli skadad och att dö! (att dö kommer på tredje plats). Tilltron till ett system kan därför inte enbart begränsas till systemets förmåga att lösa sin uppgift samtidigt som det skyddar och säkrar mig. Den måste också beakta systemets förmåga att hjälpa mig så att jag inte sviker mina kamrater.

En närliggande aspekt berör robustheten i systemet:

”A managed system should be able to defend itself against, or resolve from, shocks, and it should be able to create and exploit opportunities” (Coyle, 1986)

Ett system bör alltså ha förmågan att fungera även om det är sönder, dvs. fungera genom ett antal olika reservsystem eller kompletterande system samt också kunna fungera i olika former av reservnivåer där systemets funktion är degraderat. Ett system bör även kunna vara självläkande, dvs. en skada på systemet ”läks” genom att systemet förmår bygga upp den skadade delen eller att systemet förmår ersätta den skadade delen med en ”frisk” del.

Det är alltså inte endast upplevd sårbarhet för egen eller andras person som påverkar tilltron utan även sårbarheten i de tekniska system som utnyttjas för att lösa en given uppgift. Nedan presenteras två exempel på hur ”svaga” system eller sårbarhet får konsekvenser för operatörers handlande.

## 4.2 Exempel 1: Människa - Människa

I en studie där man studerade hur domare påverkades av råd från rådgivare (advisors) fann man några intressanta resultat. Resultaten visar att rådgivarens självförtroende påverkade graden av tilltro hos domaren. Om rådgivaren uppvisade ett högt självförtroende ökade graden av tilltro. Det ska poängteras att denna studie genomfördes i ett sammanhang där rådgivaren var expert i större utsträckning än domaren. Det resulterade också i att domaren oftare tog det råd som rådgivaren gav om domaren hade en hög tilltro till rådgivaren.

Detta innebär att om en asymmetri i kunskap finns mellan parter (som i denna studie) påverkas den ”svagare” partens tilltro av hur självsäker ”experten” är. Dessutom påvisar denna studie att graden av tilltro står i direkt relation till handlande. Har domaren tilltro till rådgivaren är han/hon mer benägen att använda det råd som rådgivaren ger.

## 4.3 Exempel 2: Människa - System

På Vallviks Bruk, en processindustri utanför Söderhamn i Hälsingland, inträffade 1998 en olycka som, pga. oläsbara larm, nära kostade en operatör livet. I en sodapanna där restprodukter från pappersmasseframställningen eldas för brukets egna energibehov, uppstod en vattenläcka som ledde till en mycket kraftig explosion. Både pannan och sodahuset förstördes i explosionen. Innan olyckan inträffade hade det övervakande datorsystemet gett en så stor mängd larm i så hög hastighet att inget av dem gick att avläsa. Man fick ingen vägledning om vad som var fel och misstänkte att det var datorsystemet som krånglade. En operatör gick in i sodahuset för att kontrollera och hann precis ut igen innan explosionen inträffade. (Källa: Ny Teknik 011205)

Här litade man alltså inte längre på larmsystemet trots att det säkert gav korrekta larm för alla fel som uppstod i och kring sodapannan. Informationen tillförde ingen kunskap, varför man förlorade tilltron till systemet och måste skaffa sig en egen uppfattning om vad som hände. Detta belyser vikten av att informationen man får måste vara användbar och begriplig.

Detta exempel påvisar hur personalens uppgifter förändrades i och med att ny teknik involverades i deras vardag. En analogi till ett framtida NBF är inte avlägsen. En ny form av sårbarhet utvecklas då personalen är i händerna på tekniska system. Därmed inte sagt att de tekniska systemen inte är funktionella, exemplet talar om för oss att en ny form av sårbarhet existerar som vi måste beakta vid implementering av tekniska system.

Dessa exempel påvisar att tekniska system genererar nya problem, de gör individerna sårbara på ett nytt sätt. Poängen med dessa exempel är att illustrera att införandet av ny teknik alltid genererar ett nytt beteende. Hur detta beteende gestaltar sig beror troligen på i vilken grad operatörerna litar på systemen, dvs. en tilltroproblematik. Senare kommer en litteraturoversikt att redovisas vars syfte är att skapa en bild av hur tilltroproblematiken har behandlats i litteraturen men också att ge en vägledning för fortsatt arbete.

## 5. Totalförsvaret – en unik miljö

I detta arbete framkommer att systemtilltro skapas av och i en relation till ett system. Vi har också diskuterat vad ett system är i detta arbete. Vi påstår också att tidigare forskning kan vägleda vårt arbete med reservation för att Totalförsvarets miljö är unik, vilket ställer ökade krav på förståelse för systemtilltroproblematiken. Vad vi menar med unik miljö och dess relation till systemtilltro förtydligas nedan.

Totalförsvaret skall framförallt verka vid kriser och katastrofer samt konflikter och krig. Dessa situationer kännetecknas bl a av kaos, utsatthet, osäkerhet, komplexitet samt tvetydighet. Förhållandena och situationerna är dynamiska och skiftar ofta. Dessutom måste man utgå från att individen, hans/hennes kamrater och den utrustning och organisation han/hon disponerar kan bli skadad eller utslagen. Oavsett insats kommer stresspåslaget att vara stort och man kommer inte att agera som man skulle ha gjort under gynnsamma och trygga förhållanden. Behovet av och kravet på systemtilltro måste ses mot den bakgrunden. Kriser och katastrofer, konflikter och krig är extrema situationer som i många stycken ställer extrema krav på både operatörer och system. Operatörerna kommer alltså många gånger att befinna sig långt ner i stresskonen där deras fysiska, mentala och känslomässiga förmåga är mer eller mindre begränsad. Många viktiga beslut som skulle kräva en avspänd och trygg miljö kommer förmodligen att behöva tas under stark press. Systemen får då inte vara sådana att de ökar stresspåslaget och blir till en ”extra fiende” utan måste hjälpa operatören och istället medverka till en lägre stressnivå. Denna extrema miljö ställer systemtilltron på sin spets, i synnerhet i ett framtida NBF, där tilltron till systemet i hög grad beror av informationen från ett ”anonymt” tekniskt system istället för från en överordnad chef.



Denna i många fall unika miljö påverkar hur Totalförsvaret bör beakta systemtilltroproblematiken. Dock ska tidigare forskning utnyttjas för att vägleda detta arbete. Nedan följer en sammanfattning av en litteraturstudie som belyser dels inom vilka områden som tilltro problematiserats och vilka entydiga resultat man erhållit.

## 6. Tilltro – i ett samarbete mellan två aktörer

### 6.1 Tilltro – människa-människa

Upprinnelsen till begreppet systemtilltro kommer från forskningen som fokuserade på det engelska begreppet "TRUST" som "rakt" översatt står för tillit, tilltro och förtroende. Den forskning som bedrevs med början på det tidiga 60-talet (Deutsch, 1960) fokuserade uteslutande på relationen mellan individer. Vilka faktorer som är avgörande för att man upplever en annan individ som tillförlitlig var den dominerade pragmatiska frågeställningen. De teorier som växte fram under 60 och 70-talet med avseende på TRUST var byggstenar för vad vi idag kallar modeller för systemtilltro, som fokuserar mer på relationen människa-system.

Det visade sig att TRUST var en central aspekt som tydligt påverkade mellanmänniska relationer, allt från relationer mellan länder, mellan majoriteter och minoriteter, köpare och säljare, patienter och terapeuter, föräldrar och barn o.s.v. T.o.m. domare påverkas i högre grad av ett råd om tilltron till rådgivaren är hög (Sniezek & van Swol, 2001) och de är mer säkra på att informationen är korrekt.

“As distrust increases, the social fabric disintegrates” (Rotter, 1980)

På samma tydliga sätt fann man också att individer med ett högt tilltrokapital (individer som i större utsträckning litade på andra) inte var mer lättlurade eller naiva, vilket varit en enkel men felaktig uppfattning (Rotter, 1980). Man kunde visa att det inte var korrelerat med ökad naiv inställning. Individer som litade mer på sin sociala omgivning var inte lättare att lura. De var bra på att lita på dem som man faktiskt kunde lita på, d.v.s. de var selektiva. Vidare kunde man visa att individer som litade på andra var mindre benägna att ljuga och troligen mindre benägna att stjäla. Dessutom var de oftare benägna att ge andra en ”andra chans” och respekterade andras rätt i större utsträckning. Vidare söktes de (individer med högt tilltrokapital) oftare upp som vänner men de var även i mindre utsträckning olyckliga eller oroliga. Dessutom var de mer omtyckta av både individer med högt och lågt tilltrokapital. Detta var entydiga empiriska resultat. Litteraturen innehöll givetvis även en teoretisk diskussion om vad begreppet TRUST egentligen representerar och hur man kan mäta TRUST.

I mitten av 1980-talet började teoretiska modeller växa fram som lyfte fram tre viktiga dimensioner: förutsägbarhet (predictability), pålitlighet (dependability) och övertygelse (faith). Dessa dimensioner återkommer när vi diskuterar människa-maskin tilltro. De konvergerande resultaten, oavsett val av metod eller val av analys, indikerar att dessa dimensioner definierar begreppet TRUST (tilltro). Eftersom dessa tre dimensioner är begreppsplattformar för de modeller som förklarar människa-maskin relationen beskrivs dessa lite närmare nedan. Det ska dessutom noteras att översättningar av de engelska begreppen inte är enkla. Det de representerar i engelskan motsvarar inte till fullo de valda svenska begreppen. Det innebär att beskrivningarna av begreppen representerar de engelska och inte nödvändigtvis de svenska.

### 6.1.1 Förutsägbarhet

Tilltro bygger till viss del på tidigare erfarenheter av ett uppvisat beteende. Stabiliteten i hur man beter sig i givna sociala situationer, och hur ofta man befinner sig i dessa, skapar en förutsättning för hur väl man kan förutse hur en annan människa kommer att bete sig. Denna dimension kallas förutsägbarhet, och är en viktig aspekt för att tilltron ska vara stor.

### 6.1.2 Pålitlighet

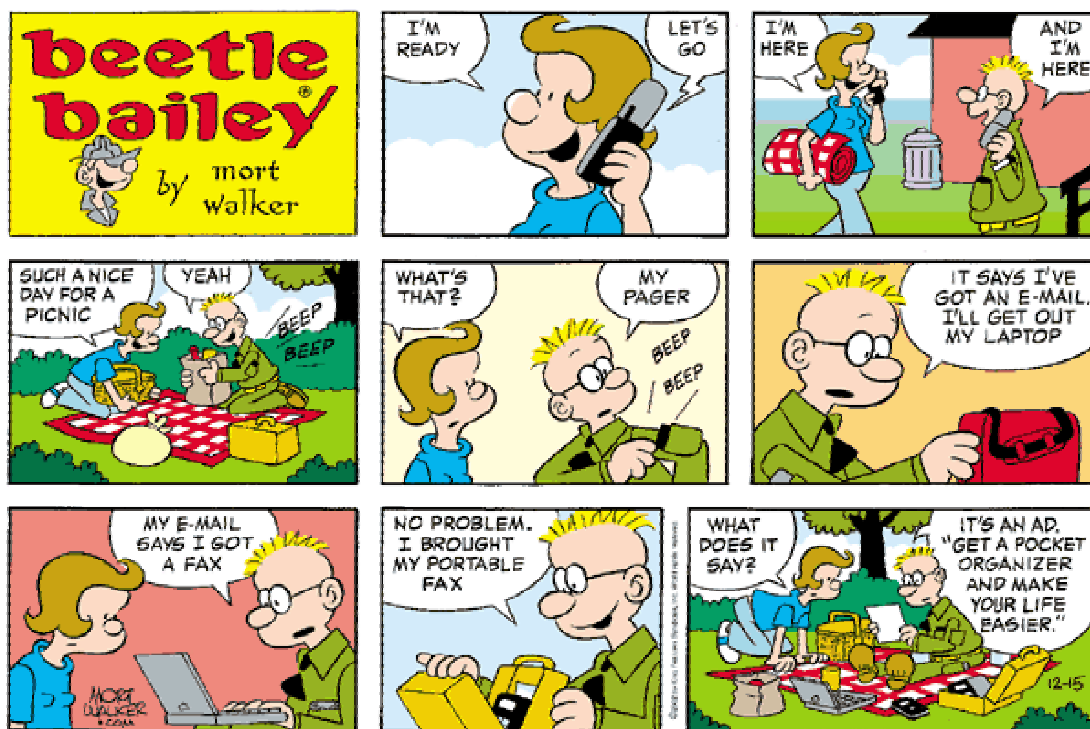
Om vi byter fokus, lämnar en individs specifika beteende eller handlingar, och närmar oss de mer genuina karaktärsdragen för en individ så är istället dimensionen pålitlighet av intresse. Karaktärsdrag som t.ex. om individen är en ärlig person som vi kan lita på, är ett typexempel på en aspekt som är avgörande för tilltro. Dessa genuina karaktärsdrag är inte desamma som beteendet i olika situationer även om uppfattningen om karaktärsdragen till stor del är baserad på tidigare erfarenheter, dock inte på summan av tidigare erfarenheter (Rempel et al., 1985).

Förutsägbarhet och pålitlighet är till stor del påverkade av historien. Den tredje dimensionen, övertygelse, har en tydligare framtidsinriktning.

### 6.1.3 Övertygelse

Begreppet tilltro kan inte uteslutande baseras på historien (det kan uppkomma helt nya extremt stressfulla situationer som relationen inte mött tidigare) utan också på slutsatser om en annan individs motiv och intentioner. Man menar att man går bortom historien och ”övertygelse-dimensionen” innehåller även en uppfattning om underliggande motiv och intentioner.

Dessa dimensioner är inte uteslutande, d.v.s. de står inte för unika aspekter av tilltro, utan snarare representerar de olika former av kognitiv abstraktion. Argumentet är att begreppen är olika baser som, ur olika perspektiv, utnyttjas för att skatta och bedöma hur en individ kommer att bete sig i framtiden. Vidare har man även utvecklat denna modell för olika aspekter av motiv: inre (intrinsic), yttre (extrinsic), och instrumentella (instrumental). Man har t.ex. kunnat visa hur dessa olika motiv korrelerar med tilltro och att människor upplever att det är inre motiv som styr individens egna handlingar medan yttre motiv, i större utsträckning, styr andra individers handlingar. Denna modell har i stor utsträckning påverkat studier av människa-maskin tilltro (Muir, 1987).



## 6.2 Tilltro – människa-maskin

### 6.2.1 Teoretiska modeller för tilltro

Litteraturoversikten med avseende på människa-maskin-tilltro resulterade i en heterogen bild. Två tydliga spår går att utläsa, ett spår med ett teoretiskt fokus och ett spår med ett tillämpat, empiriskt fokus. Tyvärr möts inte dessa i tillräckligt stor utsträckning vilket leder till att de empiriska fynden och de teoretiska modellerna ”står för sig själva” i någon mån. Det innebär att ett intressant resultat, t.ex. hur felaktig information (från systemet) påverkar i vilken grad operatören litar på ett tekniskt system, blir svårtolkat om resultatet inte kopplas till teoretiska modeller. Vi inleder översikten med en teoretisk modell för människa-maskin-interaktionen utifrån ett tilltropsperspektiv. Det finns dock flera modeller som är mer specifika t.ex. tilltro till beslutsstöd (Cohen, 2000). Därefter presenteras några nedslag i den empiriska bas som existerar idag.

När det gäller tilltro människa-maskin har Muir (1987; 1994) utvecklat en modell för att utifrån teoretiska resonemang generera empiriska studier. Syftet med modellen är att utifrån ett operatörsperspektiv förklara tilltro. För att förstå graden av tilltro i ett människa-maskin perspektiv förenar hon två modeller. En modell är den vi presenterat tidigare och en annan är Barber's modell från 1983 (Barber, 1983). Den första modellen beskriver tilltrobegreppet utifrån ett dynamiskt perspektiv, d.v.s. hur tilltro utvecklas och påverkas. Barber's modell däremot beskriver meningen med tilltrobegreppet, d.v.s. förväntningar utifrån a) uthålligheten i naturlagar, moral osv., b) teknisk kompetens, och c) anförtrott ansvar.

Detta innebär att individer, utifrån t.ex. naturlagens karaktär, skapar sig mentala modeller vilka i sin tur leder till hur individer förutsäger framtida händelser. Framtida händelser kan förutsägas utifrån t.ex. teknisk kompetens (min dator är pålitlig), eller anförtrott ansvar (piloten kommer att vara ansvarstagande i framtiden också). Den tekniska kompetensaspekten är speciellt intressant utifrån ett FM-perspektiv. Tre olika tekniska kompetenser är speciellt intressanta menar Barber (1983): expertkunskap, teknisk färdighet och rutiner. En operatör förväntar sig kanske att systemet ska utföra enkla rutiner men inte att sammanställa (teknisk färdighet) eller att tolka (expertstöd) data.

Detta innebär slutligen att en operatörs tilltro påverkas av vilka förväntningar han/hon har på systemet (Meanings of trust) och vilken historia han/hon har med systemet (Dynamics of trust). Den integrerade människa-maskin-modell för tilltro som växer fram genererar, menar Muir, en modell som dels beskriver det multidimensionella begreppet tilltro men samtidigt levererar mer eller mindre testbara frågor. Vidare finns det starka argument för att de teoretiska modellerna för människa-människa relationen med avseende på tilltro är tillämpningsbara på en människa-maskin relation menar Muir (1994).

Det svenska tilltrobegreppet är i detta arbete mest besläktat med det engelska begreppet 'trust'. Det finns även andra begrepp som t.ex. trovärdighet (Credibility) som inte betyder exakt samma sak (Fogg & Tseng, 1999). De menar att trovärdighet i större utsträckning fokuserar på: Tilltro till information = Trovärdighet. Detta arbete kommer inte att göra en särskilnad på dessa begrepp då det inte blir nödvändigt. Det är dock viktigt att förstå att det svenska tilltrobegreppet är svårt att översätta på ett korrekt sätt.

### 6.2.2 Mätning av tilltro

I denna litteratur framgår det att mätningen av tilltro är betydelsefull för att vi ska förstå förhållandet mellan tilltro och användandet av system (Bisantz & Seong, 2001; Jian, Bisantz, & Drury, 2000). Bisantz et al. startade med att studera 3 olika former av tilltro: människa-människa, människa-maskin och tilltro i allmänhet med avseende på automatiserade system. De fann att faktorerna som förklarar tilltro var liknande för de olika typerna av tilltro. De fann 12 faktorer av betydelse för tilltro, vilka vi återkommer till i de empiriska studier som presenteras nedan. Dessutom fann de att 'distrust' och 'trust' var motsatser och inte olika begrepp. Andra forskare har tydligare fokuserat på tilltro med avseende på människa-maskin interaktionen (Madsen & Gregor, 2000) med avseende på "intelligenta" system. De fann t.ex. att kognitiva och affektiva aspekter av tilltro kan mätas och att de starkaste indikatorerna för tilltro var de affektiva aspekterna (personligt fäst, övertygelse). Dessutom har Ashleigh och Stanton (2001) genom begreppsanalys funnit 13 faktorer som kan delas upp på tre huvudfaktorer; emotionella, kognitiva och handlingar.

Det innebär att det existerar instrument som kan mäta tilltro och att vi även här ser en tydlig överlappning mellan människa-människa resultat och människa-maskin resultat med avseende på

mätning av tilltro. Dessutom levererades ett flertal faktorer som är tydligt relaterade till begreppet tilltro. Dessa kommer att utnyttjas för att förklara hur operatörer i FM ser på ett idag implementerat system. Återigen framkommer det att affektiva aspekter är av större betydelse för tilltron än t.ex. systemets tekniska kompetens, vilket möjligtvis är förvånade.

### 6.2.3 Socialpsykologiska frågeställningar

Det är slående att människa-människa och människa-maskin jämförelser är så lika i många avseenden när det gäller tilltro. I litteraturen som fokuserar på denna problematik finner man t.ex. att interaktiva datorer uppfattas påvisa karaktärsdrag såsom mänsklighet, artighet, ärlighet, och inkongruens (Quintanar, Crowell, Pryor, & Adamopoulos, 1982). Då man manipulerade datorns responsstil förändrades operatörens uppfattning med avseende på egenskaperna mänsklighet och ärlighet. Det visade sig också att de datorer som var mest människolika upplevdes som minst ärliga. Quintanar et al. förklarar detta med att det finns en tendens att uppfatta mekaniska och automatiserade system som mer objektiva i någon mening. Vidare har Nass, Moon, Fogg, Reeves, & Dryer (1995) påvisat att man med enkla medel (de olika systemen uttryckte sig olika starkt, var olika säkra och hade olika namn) kan påvisa olika personligheter med system, dvs. att system kan uppfattas ha olika personligheter. De lät försökspersoner som antingen var dominanta eller undergivna interagera med dominanta eller undergivna system. De fann inte bara att försökspersonerna upplevde de olika systemen som olika personligheter utan också att försökspersonerna responderade som om de responderade till människor med dessa typer av personligheter. Det visade sig också att de föredrog de personligheter som liknade dem själva, dvs. en dominant person föredrog en dominant dator och att en undergiven försöksperson föredrog en undergiven dator. Det har också påvisats att försökspersoner som är beroende av datorn, som i ett lag där man är beroende av varandra, uppvisar samma effekter som om man skulle vara med i ett lag av människor. Försökspersonerna som var med i datorlag upplevde datorerna som mer lika dem själva, de var mer samarbetande och mer mottagliga för information (med högre kvalitet) från datorn. De tyckte även att deras dator var mer vänskaplig (Nass, Fogg, & Moon, 1996). Det har dessutom visat sig att elever på mellanstadiet som använder expertsystem i undervisningen tilldelar dessa system "lifelike" egenskaper - 'the persona effect'. Det innebär, menar Lester et al (1997), att de tilldelar systemet mänsklig karaktäristik som har positiva effekter på inlärningssituationen.

Dessa resultat är entydiga i den bemärkelsen att interaktionen mellan en individ och en dator enkelt kan upplevas på samma sätt som en interaktion med en annan människa. Med enkla medel kan en dator tillskrivas personlighet och andra mer mänskliga variabler. Det får dock till följd att datorerna tillskrivs kompetens som den inte har och att tilltroproblematiken ökar eftersom den kan uppfattas som t.ex. oärlig. Det leder oss in på nästa område som fokuserar mer i detalj på system som fungerar som beslutsstöd.





### 6.2.4 Tilltro med avseende på argumenterande system

Även inom detta specifika område finns tydliga likheter i resultat med avseende på interaktionen människa-människa och människa-maskin.

Resultaten från interaktionsstudier människa-människa tyder på att utseendet på den som kommunicerar påverkar hur information uppfattas. En attraktiv individ är mer övertygande än individer som inte är attraktiva. Det är de eftersom de kommunicerar på ett annorlunda sätt menar Chaiken (Chaiken, 1979). Detta ska också tolkas i ljuset av att vi, som individer, uppvisar affektion innan någon egentlig empiri existerar, dvs. att affekten föregår den kognitiva processen (Zajonc, 1980). Empirin är dock nödvändig för att ha en, i någon mån, korrekt uppfattning om den andra individen. Fogg (1998) visar t.ex. att datorer som använder en interaktiv teknik påverkar en individs attityder och beteende. Ett begrepp som används inom detta område är 'Captology'. Det innebär att tekniken på samma sätt som kommunicerande individer påverkar den som är involverad. Tekniska system kan alltså vara mer eller mindre övertygande vilket resulterar i en högre eller lägre grad av tilltro. Det har visat sig att system med en förklarande kapacitet ('explanatory capacity') leder till större tilltro och högre grad av korrekt hantering samt att de fungerar bättre som 'utbildare' (Miller & Larson, 1992). Det är alltså inte bara gränssnittet som är betydelsefullt (Egger, 2001).

Vidare har Ajzen och Fishbein, (1980) påvisat, utifrån en modell om "Reasoned Action", att våra attityder till generella företeelser eller skeenden inte påverkar vårt beteende på samma sätt som attityder till mer specifika ting. Detta återspeglas i människa-maskin litteraturen på ett uppenbart sätt. Man har dessutom kunnat påvisa att attityden till olika typer av system varierar. Det verkar som om attityden till system som håller ordning på information och kvantifiering av data upplevs mer positivt än system som är beslutsstödsbetonade (Kerber, 1983). Det interaktiva beteendet med avseende på datorer påvisades utifrån specifika attityder (se reasoned action) enligt Pancer, George & Gebotys (1992). Detta har även påvisats i studier med ledningssystemmiljöer (Fields, 2001).

Ovanstående resonemang innebär att tilltron till ett system påverkas innan det har haft en reell chans att visa vad det faktiskt kan prestera. Vid en implementering av ett "nytt" system får alltså marknadsföringen av systemet en betydelse. Vidare är det uppenbart att det är specifika attityder som ska bearbetas innan implementering sker. En operatör som får en uppfattning om att systemet kan stödja operatören på ett markant sätt kommer med större säkerhet att testa systemet med "öppna ögon". Det framkommer dock att tilltron måste vara



kalibrerad, d.v.s. att tilltron varken ska vara för stor eller för liten. Det visade t.ex. Masalonis (2001) då det, för flygledare, existerade en positiv korrelation med avseende på missade konflikter i luften och en hög grad av tilltro, dvs. de lätade för mycket på systemet. Flygledare skulle interagera med de flygplan som hade korsande flygbanor, varvid de fick hjälp av ett beslutsstöd. De flygledare som hade en för stor tilltro till "systemet" missade fler plan med korsande banor. Vidare ger de empiriska studierna en entydig bild av system med "förklarande kapacitet". System med förklarande kapacitet påvisar positiva effekter med avseende på tilltro. Det är dock svårt att avgöra hur central den förklarande kapaciteten är för olika typer av system. Det är möjligt att system med "intelligentare" funktioner bör innehålla denna kapacitet och att mindre intelligenta

inte behöver det. Det är fullt möjligt att det kan vara tvärtom, eller att alla typer av system måste innehålla denna kapacitet.

### 6.2.5 Tilltro till specifika råd från intelligenta system

Det visar sig att olika grad av expertis är betydelsefull med avseende på om man litar på ett 'intelligent' systems utsaga eller inte (Honaker, Hector, & Harrell, 1986). Honaker et al. påvisade att grupper med olika stor kunskap gjorde samma bedömning då de fick utsagor som innehöll inkorrekt information. De experiment-deltagare som hade stor ämneskunskap tyckte dock att de systemgenererade utsagorna (den information som de skulle bedöma) var mindre användbara och mindre lätta att förstå än vad de som ej var experter tyckte. Utsagorna var identiska för bägge grupper (det var bara märkningen som skiljde dem åt). Detta innebär att graden av expertis var betydelsefull när det gällde systemgenererad information men inte då det gällde expertgenererad information. Lerch och Prietula (1989) har visat på liknande resultat. De varierade källan på tre sätt (expertsystem, expert och amatör) och fann att försökspersonerna litade mer på rådet/utsagan från experten än från expertsystemet eller amatören (återigen var det bara märkningen som skiljde dem åt). Det var ingen skillnad i hur mycket de litade på expertsystemet och amatören. Det ska dock påpekas att andra forskare som gjort liknade studier (Andrews & Gutkin, 1991) inte fann dessa effekter. Det existerar vissa skillnader i detaljer i vilket råd/utsaga som försökspersonerna ska bedöma/använda. Dessa skillnader kan förklara de skilda resultaten. Det är dock viktigt att poängtera att bägge studierna använde sig av experter inom de områden som råden/utsagorna behandlade. Waern och Ramberg (1996) påvisade också att individer hade en högre tilltro till människor än till datorer. De använde sig av liknade utsagor som Lerch och Prietula (1989) men de som bedömde utsagorna/råden i denna studie var inte experter.

Dessa resultat är inte entydiga även om det verkar som om, i de flesta fall, tilltron till system inte är lika stor för råd/utsagor från expertsystem som om de kommer från experter. Det som skiljer dessa studier ifrån många övriga tilltrostudier är att de har studerat experter. Detta är intressant utifrån ett FM perspektiv eftersom FM personal är experter på sina olika områden. Det ska dock poängteras att denna diskrepans i grad av tilltro till olika källor inte var faktiska diskrepanser, utan endast en skillnad i varifrån experterna trodde att råden/utsagorna kom. Denna mänskliga "felhandling/felbedömning" verkar vara relaterad till grad av expertis. Dessa studier har dock inte fokuserat på hur försökspersonerna har använt råden/utsagorna och hur tillförlitligheten förändras över tiden då tillförlitligheten varierar.

### 6.2.6 Tilltro då informationstillförlitligheten varierar

Den övergripande frågeställningen för detta område är framförallt hur korrekt och inkorrekt information från ett expertsystem påverkar den direkta prestationen men också hur inkorrekt och korrekt information förändrar interaktionsbeteendet med systemet. Dessutom problematiseras distansen/avståndet mellan de aktörer som interagerar, vilket är av speciellt intresse i ett nätverk. Hanowski, Kantowitz och Kantowitz, (1994) har fokuserat på hur bilförare behandlar information från avancerade trafikguidesystem. De varierade, på samma sätt i bägge studierna, graden av korrekt information. Betingelserna varierade mellan 100% korrekt till 71 % och 43 % korrekt. Dessa betingelser varierade över två typer av miljöer, välkänd och ny. Det gör att förarna var experter i en miljö och mer amatörlika i en okänd miljö. Resultaten genererade att förarna presterade bäst då de fick information som var 100% korrekt. Då informationen var 71% korrekt accepterade förarna informationen och använde den, men när informationen endast var korrekt i 43% av fallen försämrades prestationen markant. Det var även så att förarna accepterade information oftare i en ickefamiljär miljö, dvs. då man var i större behov utav stöd eftersom man inte var expert längre. I en studie genomförd med experter på sitt område framkom att tilltron påtagligt förändrades då expertsystemet uppvisade fel. Dessa operatörers beteende, då de

upptäckt att systemet inte uppförde sig korrekt, resulterade i att de övergick till manuell kontroll istället för automatiserad kontroll. Det innebar att tilltron minskade kraftigt men att prestationen inte föll. Tilltron för systemet tilltog dock över tiden men med en låg hastighet (Lee, 1991). Detta går att förklara menar Lee eftersom systemets ”tekniska kompetens” och ”förväntningarna att naturlagarna fortsätter gälla” (Barber, 1983; Muir, 1987) har påverkats på ett tydligt sätt. Dock har olika ”prediktionssystem” (egen och andras flygväg presenteras på skärm) för piloter testats i simulatören. Man finner att prestationerna försämras när graden av otillförlitlig information ökar (Wickens, Gempler, & Morphew, 2000).

Om man lämnar problematiken med tillförlitlig information från ett system och istället betraktar tillförlitligheten i operatörens utsagor påvisas intressanta resultat i ljuset av ett nätverksbaserat försvar. Moon (1998) varierade avståndet mellan ett frågande system och individen som skickar iväg svar. I ett fall skulle ”svaret” skickas till nästa rum med hjälp av systemet, i ett fall skulle det skickas ca en svensk mil och i ett fall skulle svaret skickas flera hundra mil. Resultaten visar att den svarande individen blir mindre ärlig om det upplevda avståndet ökar. Vidare konstateras att operatören blir mer påverkad ju närmare det upplevda systemet är.

Dessa resultat ger ett entydigt svar med avseende på hur tilltron påverkas av felaktig information från ett expertsystem och hur dynamiken i tilltro ser ut över tiden. Dessutom verkar det vara viktigt, igen, om de som studeras är experter eller inte eftersom beteendet som experten uppvisar skiljer sig ifrån den mindre kunnige. Utifrån dessa resultat påvisas att expertkunskap är centralt med avseende på hur tilltro till informationen från ett expertsystem uppstår. I dessa studier uppstår inga negativa bieffekter av expertis, som i fallet där råd/utsagor behandlas av experter.



## 7. Summering av litteraturstudien

Det framgår i litteraturoversikten att många faktorer påverkar en individs tilltro till ett system. Det framkom entydigt att tilltroproblematiken som gäller för människa-människa även gäller för människa-system/dator interaktionen. De teoretiska modeller som presenterades bygger på modeller från människa-människa teorier. Förutsägbarhet, pålitlighet, och övertygelse påverkar graden av tilltro. Det innebär att systemtilltro påverkas dels av en historia med det specifika systemet men också av en föreställning om i vilken grad systemet är att lita på i framtiden. Denna framtida tilltro kan inte förutsägas med ”generella attityder” utan med ”specifika attityder”. Det verkar också som om system med en förklarande kapacitet, i större utsträckning uppvisar bättre förutsättningar för att skapa en hög grad av tilltro, men att tilltron även är påverkad av föreställningen om systemet innan systemets har testats. Systemtilltron måste dock vara kalibrerad, dvs. även en övertro på ett system bör undvikas. System uppfattas även som mänskliga och försökspersoner agerade på olika sätt beroende på vilken personlighet som de uppfattade att systemet hade, dvs. försökspersonerna interagerade med system som om de var mänskliga. Det framkom dock att vi inte värderar t.ex. råd från intelligenta system på samma sätt som vi värderar råd från intelligenta mänskliga individer. Visar det sig att informationen från ett system inte är tillförlitligt krävs en lång tid av interaktion för att återuppbygga den tilltro som en

operatör initialt hade. Slutligen har studierna visat hur man bör mäta systemtilltro och vilka faktorer som är mer eller mindre avgörande för att skapa en kalibrerad systemtilltro.

Med hjälp av litteraturöversikten och med hänsyn till den unika miljö, som beskrivs i kap 5 ovan, som FM's personal ska verka inom, framträder några centrala aspekter som bör poängteras om systemtilltroproblematiken ska beaktas:

1. De system FM vill utnyttja bör marknadsföras på ett sätt som förhindrar att tilltroproblematik existerar innan operatören mött systemet.
2. Systemtilltron måste vara kalibrerad, dvs. användaren måste känna till både kapacitet och begränsningar.
3. Operatören kommer att interagera med systemet som om det var en mänsklig part med avseende på tillförlitlighet, dvs. systemet tillskrivs en personlighet.
4. Kan systemet förklara sig ökar tilltron. Detta verkar dock variera med hur "intelligent" systemet är.
5. Det är möjligt att med hjälp av systemets inneboende egenskaper påverka tilltron, dvs. att systemet kan ha en mer eller mindre övertygande argumentation – vilket påverkar tilltron.
6. Att t.o.m. yttre faktorer, som reella avstånd, påverkar hur en inkommande information uppfattas eller hur en utgående information presenteras.
7. Tilltro är beroende av sårbarheten, dvs. tilltroproblematiken ökar när sårbarheten ökar.

Dessa iakttagelser bör inte övertolkas eftersom resultaten inte är genererade i studier med experter i extrema miljöer, dvs. FM's verklighet. Det ska ändå poängteras att dessa iakttagelser t.o.m. kan vara mer betydande, eftersom miljöbetingelserna för FM's personal är extrema (se iakttagelse 7).

Detta arbete kommer dock inte att kunna leverera några entydiga svar på alla beskrivna och diskuterade frågor. Syftet med litteraturöversikten var att ta reda på vad den inomvetenskapliga litteraturen har att "erbjuda" som vägledare för totalförvarsrelaterad forskning. Den resterande delen av detta arbete kommer att fokusera på det empiriska arbete som genomförts inom ramen för projekt Systemtilltro.

## 8. Metod

### 8.1 Datainsamling

De empiriska nedslag, som genomfördes inom ramen för projektet, är i första hand påverkade av en explorativ ansats. Det innebär att vi samlade in data på olika sätt och att vi närmade oss olika vapengrenar och system på olika nivåer. Denna datainsamling kommer att redovisas först. Därefter kommer resultaten av studierna att presenteras.

Studien genomfördes som ett antal undersökningar och intervjuer med personer som har stark koppling till en organisation eller enhet som vi definierar som systemet. Varje person ombads fylla i två blanketter som närmare förklaras nedan. Den ena blanketten gav försökspersonen möjlighet att själv bedöma vad som påverkat hans eller hennes tilltro samt gradera detta medan den andra anger några parametrar som genom litteraturstudierna antas påverka tilltron till ett system. Vi kallar den förstnämnda ”hjulet” och den andra ”parametertest”. Hjulet är en metod utvecklad av Ben Shalit vid FOA under 70-talet.

#### 8.1.1 Enkät 1 (Hjulet)

En explorativ enkät användes. Den kallas Hjulet (se appendix 1) eftersom det är en rund tårtliknande cirkel med 12 delar som presenteras på ett A4 papper. Operatörernas uppgift i denna enkät var att skriva ner de faktorer som påverkar deras tilltro till ett givet system. Här alstras ett stort antal företeelser, påståenden eller känslor som intervjuobjektet själv tycker påverkar hans eller hennes tilltro. Denna enkät besvarades först så att operatörernas egeninitierade faktorer inte påverkades av de forskningslitteraturgenererade faktorerna. När ett valfritt antal ”tårtbitar” var ifyllda skulle varje genererad faktor värderas. Detta innebär att varje genererad faktor skulle rangordnas från 1-12 beroende på hur många faktorer som de skrivit ner. När detta var avklarat av samtliga skulle de även ge faktorn ett positivt/negativt tecken beroende på hur de uppfattade denna faktor i det givna systemet. Slutligen skulle de markera i vilken grad (skala 1-4) de själva kan påverka faktorn i sin roll som operatör.

Med hjälp av dessa data genomfördes en kvalitativ analys. Varje enskild operatörsgenererad faktor skrevs ut på en liten lapp som därefter samlades ihop i en bunt. Med hjälp av denna bunt försökte vi kategorisera de faktorer som genererats. Vi försökte, med hjälp samtliga lappar, hitta ett förklarande mönster, dvs. generera en hanterbar mängd faktorer som beskrev vad operatörerna upplevde vara betydelsefullt. Därefter beräknades också ett värde baserat på antalet ”lappar” och vilket värde respektive lapp hade. Det innebär att en faktors slutgiltiga värde påverkades av hur många som tyckte att en faktor var viktig men också i vilken grad faktorn var betydelsefull. Lapparna sorterades också under de faktorer som gavs i parametertestet (se nedan). På så sätt kunde varje faktor från Hjulet sorteras in i en matris och presenteras i tredimensionella kartor där antal och värdering bestämmer topografin.

#### 8.1.2 Enkät 2 (Parametertest)

Denna enkät var teoretiskt driven, dvs. innehöll elva av de faktorer som forskningslitteraturen påvisat är betydelsefulla utifrån ett tilltroperspektiv (se appendix 2). Enkäten var utformad på följande vis. En initial fråga behandlade operatörens uppfattning av tilltro med avseende på ett givet system (systemet kan variera mellan operatörsgupper). Därefter följde elva frågor med formuleringen ***”I vilken utsträckning påverkar faktor X din tilltro till systemet.”*** Detta genomfördes med avsikt att få reda på vilka av de i litteraturen ”viktiga faktorerna” som var mest betydelsefulla för operatörers tilltro i ett totalförsvssystem. Deltagarnas instruktioner var att på

en skala 1-7 markera hur central en faktor var för deras totala systemtilltro. Med hjälp av dessa enkäter genomfördes kvantitativa analyser, dvs. regressionsanalyser.

De givna faktorer som deltagarna ombads gradera var:

Förutsägbarhet	Begriplighet	Ansvarstagande
Förmåga	Användbarhet	Välmening
Robusthet	Driftsäkerhet	Kontrollerbarhet
Familjäritet	Pålitlighet	

Dessa parametrar har också använts för att skapa en gemensam bild för de faktorer som försökspersonerna genererat i Hjulet (se kapitel 9).

### 8.1.3 Instrumentval

Syftet med de olika instrumenten var att studera om resultaten med avseende på tilltro varierade som en effekt av hur man ställer frågan. Om samma mönster i datamängden erhålls, oavsett val av instrument, ökar tillförlitligheten. Visar det sig att datamönstret varierar som en effekt av instrumentval blir eventuella slutsatser inte lika entydiga, utan bör betraktas med en större skepsis.

## 9. Fallstudier

### 9.1 Utvalda förbandssystem

De valda systemen var SWAFRAP C-130, SWAFRAP AJS 37 och CETRIS, Korvett Visby. Operatörer i dessa förbandssystem tillfrågades om sin tilltro till systemet, där systemet var definierat olika för respektive förband. Dessa intervjuresultat samt en kort beskrivning av respektive förband redovisas nedan. Dessutom hade de olika operatörerna, som ingick i studien, olika roller i de olika systemen. I t.ex. SWAFRAP C-130 ingick bl.a. flygmekaniker, navigatörer, flygförare, och ledningspersonal. Argumentet för den stora variationen i system och roller var återigen den breda explorativa ansatsen. Den risk som uppstår i och med detta arbetssätt är att de involverades olika uppfattningar/åsikter varierar i så stor utsträckning att det endast uppstår "en massa brus", dvs. att resultaten blir svåra att tolka. Fördelen är dock att vi skapar oss en "rikare" bild av olika försvarsgrenar och systemnivåer för att få en uppfattning om hur lika eller olika de är i uppfattningen om tilltro.

#### 9.1.1 SWAFRAP C-130

Enligt regeringsbeslut skall Sverige, från den 1 januari 2001, ha ett antal förband i beredskap för snabba insatser inom ramen för EU, VEU, FN eller Nato. För flygvapnets del innebär detta att två sammansatta snabbinsatsförband; Swedish Air Force Rapid Reaction Unit (SWAFRAP) C-130 och SWAFRAP AJS, skall vara berett att med 30 dagars varsel kunna delta i en s.k. Peace Support Operation (PSO) i Europa eller dess närhet.

**SWAFRAP C-130** är ett transportförband baserat på F7 i Såtenäs som omfattar 65 personer och förfogar över fyra stycken TP 84 Hercules. Svenska försvaret förfogar totalt över åtta st TP 84, samtliga baserade på F7. I intervjuerna



träffade vi personal ur divisionen, dvs flygande personal, underhållskompaniet och förbandets ledning, totalt 19 personer vid två olika tillfällen. Systemet utgörs här av förbandet SWAFRAP C-130 i sin helhet.

### 9.1.2 SWAFRAP AJS 37



**SWAFRAP AJS** är det andra av flygets snabbinsatsförband som utgörs av ett spaningsförband baserat på F21 i Luleå och omfattar 219 personer. I förbandet ingår flygplan AJS 37 anpassade för spaning som successivt

kommer att uppgraderas till JAS 39.

Intervjuerna genomfördes då förbandet deltog i Nato/PFF-övningen ”Strong Resolve” i Polen i mars 2002. I övningen deltog ca 115 man ur SWAFRAP AJS varav 58 st kunde intervjuas.

Även här definierades systemet som hela förbandet, SWAFRAP AJS.

### 9.1.3 CETRIS, Korvett Visby

Korvett Visby är ett s.k. ”multi-purpose”-fartyg med hög förmåga och avancerad teknik som utvecklas i samarbete mellan FM, FMV, FOI samt svenska universitet och högskolor. Projektet leds av FMV. Kännetecknande för Korvett Visby är smygteknik, som rönt stor internationell uppmärksamhet, samt förmåga att utföra flexibla och mångsidiga uppgifter såsom ytstrid, ubåtsjakt och minröjning. För att klara detta kommer fartyget att utrustas med ett avancerat luftförsvar och ett kraftfullt ledningssystem. Ledningssystemet i Visby, betecknat **CETRIS**, utvecklas i samarbete med SaabTech Systems i Järfälla och utvärderas i provmiljö av representanter från PTK (Provturskommando Visby, FM), FMV och SaabTech Systems. Intervjuerna kunde genomföras med 13 personer fördelade på alla dessa tre kategorier. Systemet utgjordes här av ledningssystemet CETRIS som är av stark teknisk karaktär och betraktades ur en operatörs synvinkel.



## 9.2 Datainsamlingsprocedur

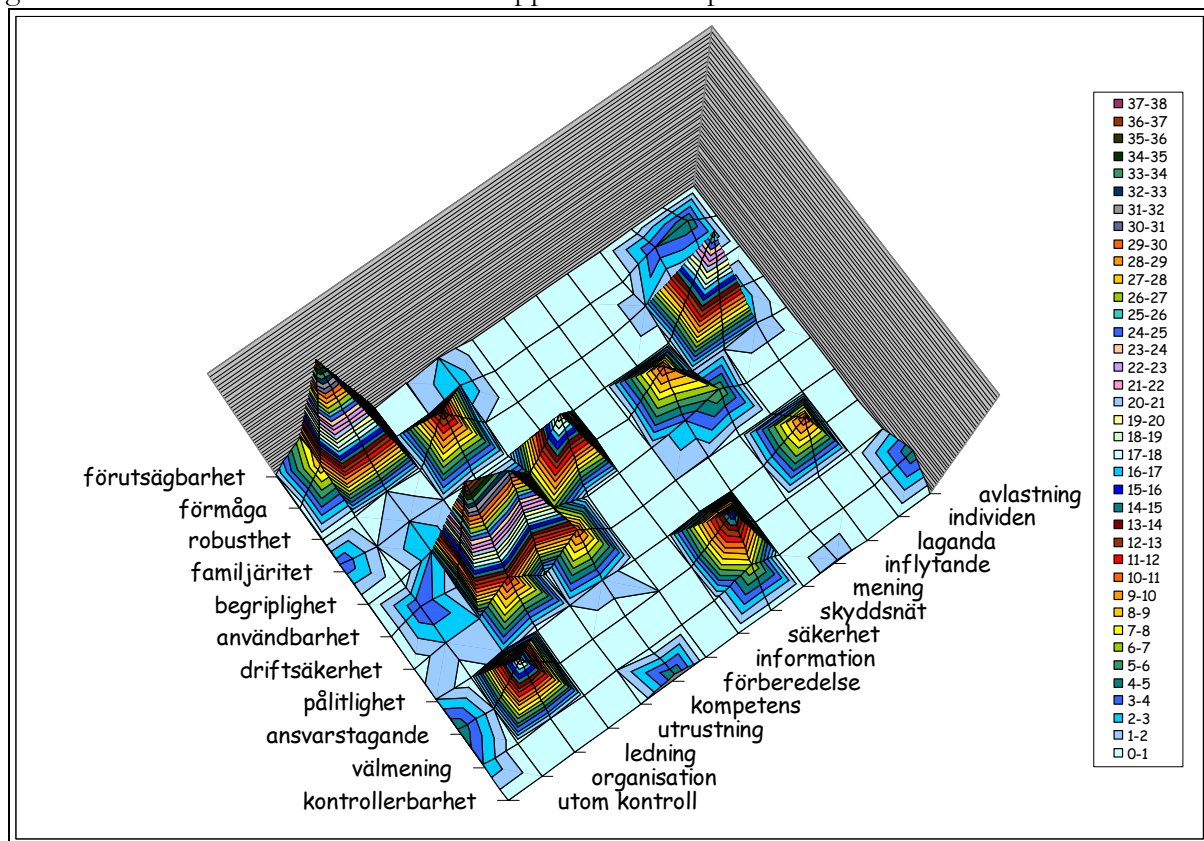
Varje datainsamlingstillfälle inleddes med att vi presenterade syftet med projektet i korta ordalag. Vidare gick presentationen in på att diskutera en given definition på systemtilltro eftersom detta varierade mellan förbanden. Avsikten med definitionspresentationen var att samtliga deltagare skulle ha en uppfattning om vad begreppet representerade för dem. Det var dock centralt för oss att inte påverka deltagarnas uppfattning om tilltro i något avseendegenom att t.ex. diskutera problem eller resultat. Därefter delades enkät 1 ut. Tillvägagångssättet för dess ifyllnad presenterades fortlöpande. Det innebär att samtliga närvarande slutförde steg 1 innan steg 2 påbörjades. När samtliga deltagare slutfört steg 3 och 4 delades enkät 2 ut. Innan enkät 2 fylldes i diskuterades, kort, de olika föreslagna faktorernas innebörd. Därefter fick deltagarna ställa eventuella frågor. När deltagarna fyllt i enkät 2 tackade vi för deras hjälp och avslutade ’mötet’.

## 10. Analys av Enkät 1

Samtliga deltagares egengenererade faktorer (som påverkar deras tilltro till respektive system) skrevs ut på lappar. Därefter sorterades dessa lappar (varje förbandssystem för sig) utifrån den enkla principen att försöka ”hitta ett mönster”. Först samlades lappar ihop som var lika, dvs. alla som var relaterade till en och samma gemensamma nämnare utan att ”den gemensamma nämnaren” var explicit uttryckt. Det var givetvis så att det fanns naturliga begrepp som var ”uppenbara” direkt som t.ex. faktorer som berörde ledning i ett av förbanden. Det var dock lika vanligt att kategorierna växte fram i sorteringsarbetet, som t.ex. skyddsnet. Förbandens olika ”högar” av egenproducerade faktorer genererade olika många gemensamma kategorier. Dessa kommer att redovisas nedan var för sig. (Samtliga uträknade värden finns redovisade i tabellform i appendix 3, tabell 2 - 7.) Därefter avslutas analysen av enkät 1 med en summerad analys.

### 10.1 Beskrivning av resultaten från SWAFRAP AJS 37

Deltagarna genererade 384 faktorer. Varje faktor var dessutom värderad (se ovan). Sorteringen/kategoriseringen resulterade i 14 kategorier. Figur 3 illustrerar vilka kategorier som genererades samt vilket värde som förknippades med respektive faktor.



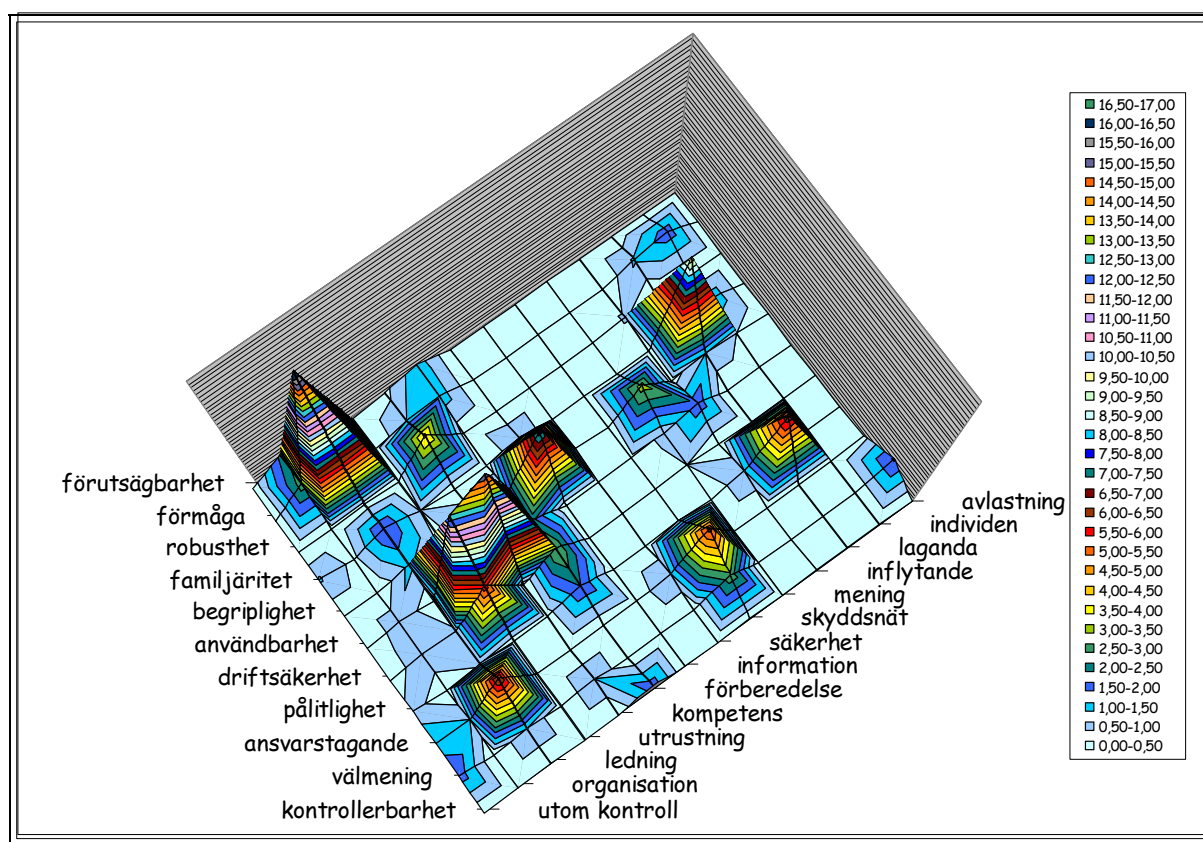
Figur 3. Illustrerar en matris med genererade "ovägda" faktorer för deltagarna från AJS 37.

Med hjälp av dessa data genererades följande resultat. Mycket är likt SWAFRAP C130, som ni finner nedan. Det som avviker är att ytterliggare en faktor, laganda, träder fram i SWAFRAP AJS 37. När det gäller de teoretiska faktorerna "träffas" åtta faktorer, där **Familjäritet** ingår som en betydande faktor och **Förutsägbarhet** inte gör det (jmf SWAFRAP C 130). Resultaten kan sammanfattas på följande sätt.



1. Den upplevda faktorn **Förberedelse** träffar den teoretiska faktorn **Driftsäkerhet**.
2. Den upplevda faktorn **Information** träffar den teoretiska faktorn **Begriplighet**.
3. Den upplevda faktorn **Skyddsnet** träffar den teoretiska faktorn **Ansvarstagande**.
4. Den upplevda faktorn **Kompetens** träffar den teoretiska faktorn **Användbarhet** och i viss mån **Robusthet**.
5. Den upplevda faktorn **Utrustning** träffar den teoretiska faktorn **Användbarhet** och i viss mån **Driftsäkerhet**.
6. Den upplevda faktorn **Ledning** träffar den teoretiska faktorn **Förmåga** och i viss mån **Ansvarstagande**.
7. Den upplevda faktorn **Organisation** träffar i viss mån den teoretiska faktorn **Förmåga**.
8. Den upplevda faktorn **Laganda** träffar den teoretiska faktorn **Familjäritet** och i viss mån **Pålitlighet**.

När vi skapar samma matris med ”vägda” faktorer (viktighet och antal) genereras en något annorlunda bild.

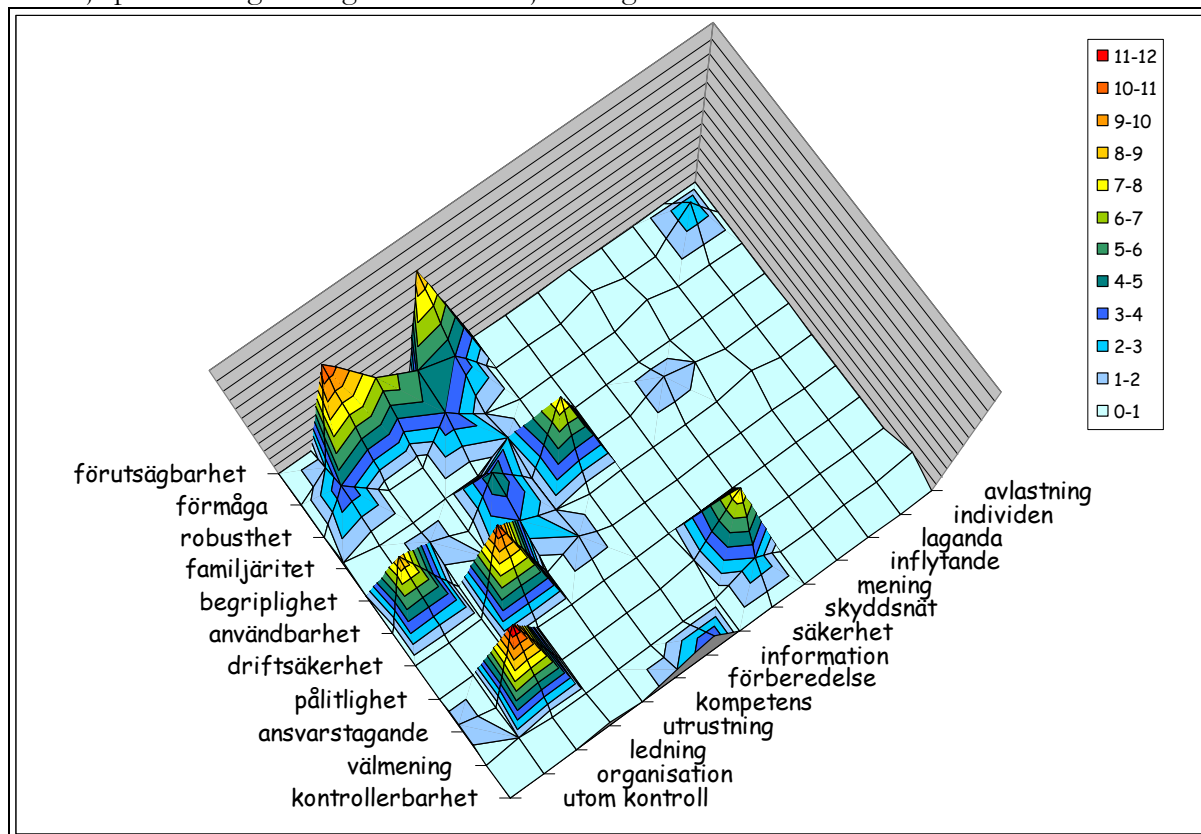


Figur 4. Illustrerar en matris med ”vägda” faktorer (se text för detaljer) för AJS 37.

Sex av de åtta upplevda faktorerna träder fram. **Förberedelse** och **Organisation** försvinner eftersom de hade för ”låg” vikt enligt befattningshavare. När det gäller de sex som återstår genereras ett identiskt mönster. Detta innebär, sammantaget att **Användbar Kompetens** och **Användbar Utrustning** är mycket centralt för AJS förbandet och att **Ledningens Förmåga** och **Ledningens Ansvarstagande** är det också. Det är på samma sätt för AJS förbandet att **Skyddsnetet** är viktigt och att **Informationen** är begriplig/tydlig. Det som avviker i jämförelse med C130 är att **Lagandan** är central för systemtilltro. De vill vara familjära med pålitliga lagmedlemmar – vilket är viktigt.

## 10.2 Beskrivning av resultaten från SWAFRAP C-130

Deltagarna genererade 138 stycken faktorer. Varje faktor var dessutom värderad (se ovan). Sorteringen/kategoriseringen ”resulterade” i 14 kategorier. Kategorierna, som var ett resultat av bearbetningen för AJS 37, användes igen. Detta tillvägagångssätt valdes eftersom jämförelsen mellan dessa förband var central. Risken är att man går miste om information som skulle träda fram om inte denna a priori kategorisering användes. Fördelarna bedömdes vara större än nackdelarna. Figur 3 illustrerar vilka centrala kategorier som genererades samt vilket värde som förknippades med respektive faktor (de faktorer som omnämns mindre än tio gånger är borttagna ur den efterföljande analysen eftersom antalet ”träffar” är för lågt som underlag för slutsatser). Med hjälp av samtliga data genererades följande figur.



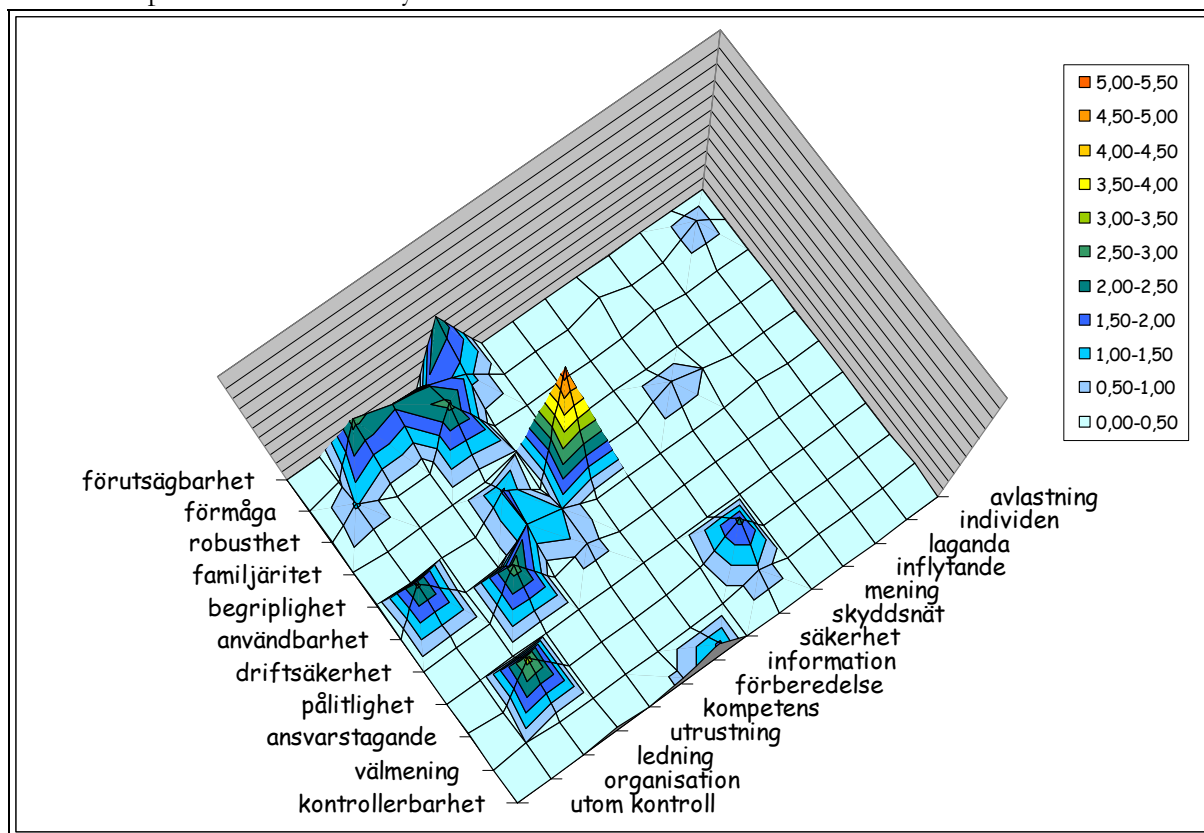
Figur 5. Illustrerar en matris över det antal faktorer som C130 deltagarna genererade och de teoretiska faktorerna.

Figuren påvisar att sju övergripande faktorer omnämndes av ett flertal av befattningshavarna. Innehållet i dessa sju ställdes därefter i relation till de teoretiskt drivna faktorerna. Det resulterade i att sju av de elva teoretiska faktorerna fick ett betydande antal träffar. För att kunna skapa denna matris studerades återigen ”lapparna”, dvs. vad befattningshavaren uttryckt på ”lappen” jämfördes med de teoretiska faktorerna. Denna bild resulterar i följande tolkning:

1. Den upplevda faktorn **Förberedelse** träffar den teoretiska faktorn **Förutsägbarhet** och i viss mån **Förmåga**.
2. Den upplevda faktorn **Information** träffar den teoretiska faktorn **Begriplighet** och i viss mån **Kontrollerbarhet**.
3. Den upplevda faktorn **Skyddsnät** träffar den teoretiska faktorn **Ansvarstagande**.
4. Den upplevda faktorn **Kompetens** träffar flera teoretiska faktorer likvärdigt (**Förmåga**, **Robusthet**, **Begriplighet** och **Användbarhet**).
5. Den upplevda faktorn **Utrustning** träffar den teoretiska faktorn **Driftsäkerhet** och **Förmåga**.
6. Den upplevda faktorn **Ledning** träffar den teoretiska faktorn **Ansvarstagande** och **Förmåga**.

## 7. Den upplevda faktorn **Organisation** träffar den teoretiska faktorn **Användbarhet**.

När vi skapar samma matris med ”vägda” faktorer (viktighet och antal) genereras, i detta fall, exakt samma utfall. Befattningshavarna uttrycker faktorer som ligger nära verksamheten, dvs. konkreta aspekter som är av betydelse för deras tilltro.

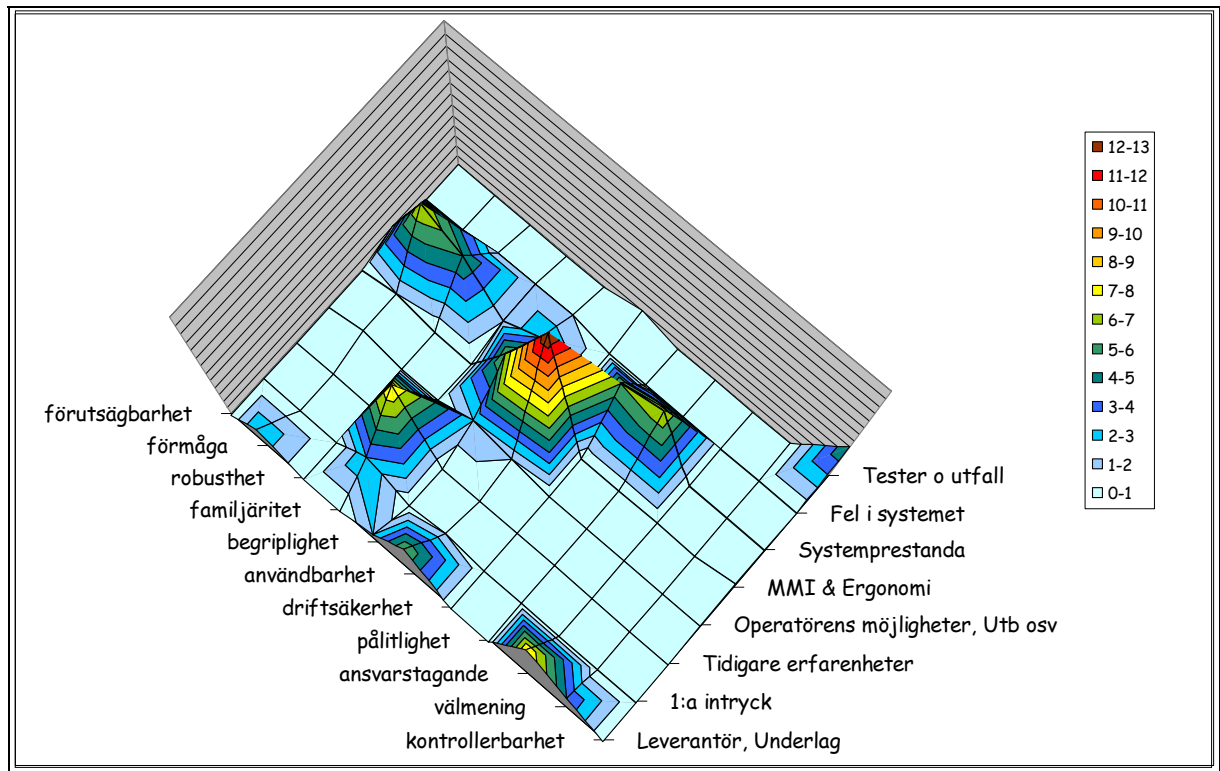


Figur 6. Illustrerar en matris med ”vägda” faktorer (se text för detaljer) för C130.

För SWAFRAP C130 bör det lyftas fram att faktorn **Ledning** är intressant eftersom den kraftigt markerar ansvarstagande och förmåga, dvs. ledningen måste uppvisa ett ansvarstagande och en förmåga. Vidare är det viktigt att informationen måste vara begriplig och att skyddsnetet måste fungera. Det innebär att faktorer som rätt kompetens, utrustning och förberedelse är betydelsefulla men även att andra faktorer, som inte på samma sätt kan relateras till den direkta uppgiften (skyddsnet, tydlig information och ett tydligt ansvarstagande från ledning), också är viktiga.

### 10.3 Beskrivning av resultaten från CETRIS, Korvett Visby

Deltagarna genererade 99 stycken faktorer. Varje faktor var dessutom värderad (se ovan). Sorteringen/kategoriseringen resulterade i kategorier. Figur 7 illustrerar vilka kategorier som genererades samt vilket värde som förknippades med respektive faktor.



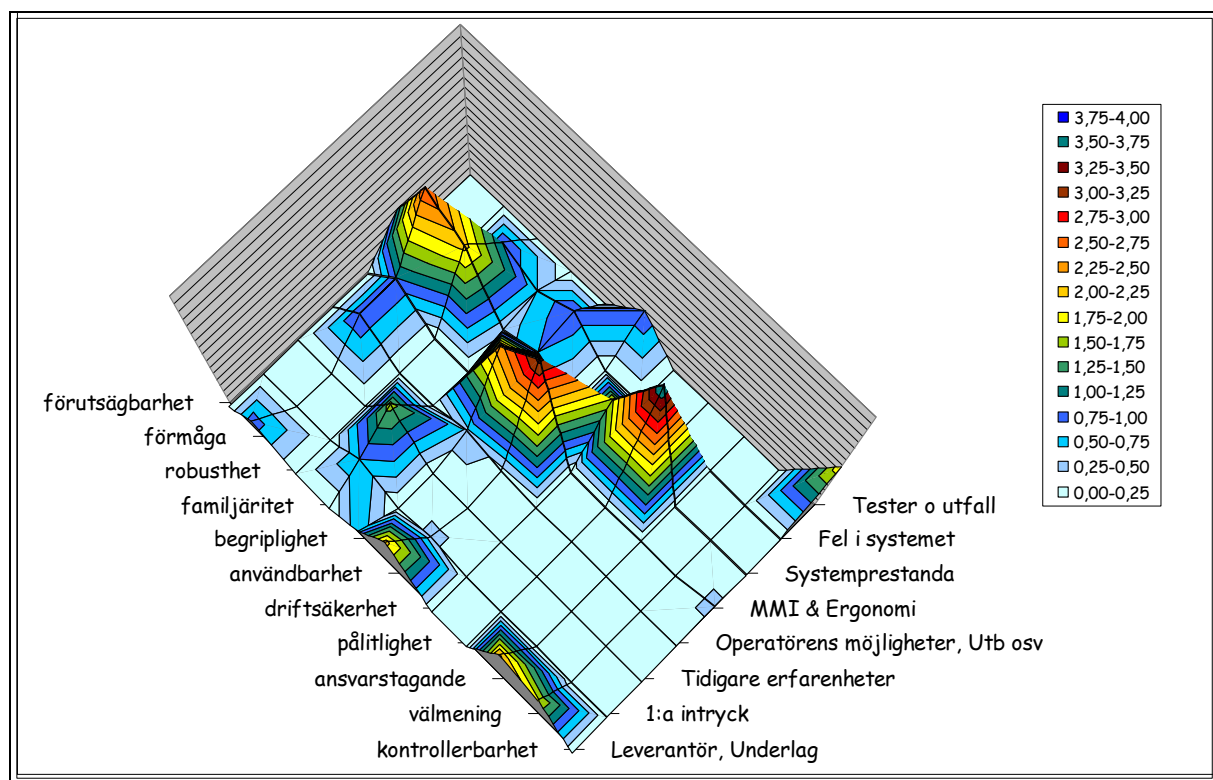
Figur 7. Illustrerar en matris över resultaten från CETRIS.

Med hjälp av dessa data genererades följande mönster. Tre upplevda faktorer träder fram och sju teoretiska faktorer.

1. Den upplevda faktorn **Leverantör/Underlag** träffar de teoretiska faktorerna **Användbarhet** och **Ansvarstagande**.
2. Den upplevda faktorn **MMI/Ergonomi** träffar den teoretiska faktorn **Användbarhet** och **Begriplighet**.
3. Den upplevda faktorn **Systemprestanda** träffar de teoretiska faktorerna **Förmåga**, **Robusthet**, **Driftsäkerhet** och **Pålitlighet**.



Vid en analys där även betydelsen/vikten påverkar det slutgiltiga värdet för varje faktor genereras ett identiskt mönster.



Figur 8. Resultaten från CETRIS med vägda faktorer.

Detta ger att "bilden" från befattningshavare inom Korvett Visby, som utvecklar ett ledningssystem, uppger andra faktorer som är av betydelse för systemtilltron än vad befattningshavare inom SWFRAP C130 och SWAFRAP AJS 37 uppger. Det är dock inte märkligt eftersom de bedömer tilltron till ett ledningssystem under utveckling och inte tilltron till ett aktivt förband. Vid ledningssystemutveckling lyfter befattningshavarna fram två faktorer som inte direkt har med teknisk prestanda (**systemprestanda**) att göra. Systemet ska ha hög **Användbarhet** utifrån ett **MMI/Ergonomi** perspektiv men leverantörens "attityd" är viktig. Det verkar som att **Leverantör/Underlag** ska vara användbar och vara ansvarstagande.

#### 10.4 Sammanställning av resultaten från "Hjulet".

Vid en första analys av hjulet ser man att likheterna mellan två operativa förband är många (C130 och AJS). Det gemensamma är att deras egengenererade faktorer av vikt är desamma (förutom Laganda). Faktorerna Skyddsnät, Ledning och Information uppvisar identiska mönster, viktiga faktorer som inte alla direkt kan kopplas till de uppgifter förbandet ska utföra (eftersom det framförallt handlar om ledningens ansvarstagande och inte förmåga).

Det som avviker är vilka teoretiska faktorer som påverkas av de egengenererade faktorerna. C130 markerar ofta förmåga där AJS 37 endast markerar förmåga med avseende på ledning och organisation. En viss skillnad med avseende på förberedelse finns (central faktor för båda). C130 trycker på förutsägbarhet och AJS trycker på driftsäkerhet. En spekulativ tolkning är att C130 inte upplever förberedelsebehovet tillgodosett när AJS 37 däremot upplever att de är förberedda men har en insikt om att driftsäkerheten är betydelsefull. Annars lyfts "naturliga" aspekter ofta fram, som rätt och användbar kompetens och utrustning. Resultaten avviker i betydande grad i relation till deltagarna från Korvett Visby, CETRIS (Ledningssystem). Det är inte konstigt eftersom de bedömer tilltron till ett tekniskt system. Det som framkommer är att två faktorer **Leverantör/Underlag** och **MMI/Ergonomi** lyfts fram tillsammans med **Systemprestanda**. **Ansvartagande** och **Användbarhet** är de faktorer som är betydelsefulla.

Dessa analyser är grundade på utsagor från befattningshavare i olika roller i olika system. Det gör att vi bör vara försiktiga med avseende på giltigheten i slutsatserna. Dessa brister försöker vi motverka, i någon mån, genom analysen av enkät 2. Får vi ett resultat som pekar åt samma håll i nästa enkät ökar reliabiliteten för data.

## 11. Analys av Enkät 2

Enkät 2 innehöll tolv frågor. Fråga 1 (övergripande tilltro till systemet) användes som kriterium i regressionsanalysen. En analys genomfördes för samtliga deltagare eftersom det endast var 56 operatörer totalt som besvarade denna enkät. Det innebär att resultatet måste begrundas i ljuset av att det var operatörer i olika roller, i olika förband, och på olika systemnivåer, som genomförde skattningarna.

Den övergripande (samtliga involverade operatörer för samtliga utvalda system) regressionsanalysen resulterade i att  $R=0.83$ ,  $R^2=0.69$ , och att  $F=3.84$ ,  $p<0.05$ , vilket innebär att de faktorer som var utvecklade för att fånga systemtilltro kan förklara 69 % av variansen. De statistiska termerna betyder att vi med 95 % sannolikhet har en modell som är statistiskt säkerställd, dvs. de elva faktorerna förklarar större delen av den varians som svaret på fråga 1 resulterade i (kriteriumvariabeln). Vidare påvisades att framförallt fyra faktorer var betydelsefulla med avseende på tilltro och att de sju övriga inte var betydelsefulla (se Tabell 1 för standardiserade betavikter) för dessa operatörer.

Tabell 1. Standardiserade betavikter, t-värden och signifikansnivå i fallande ordning (utifrån betavikternas storlek).

Faktor	Stand. Betavikt	T-värde	Signifikansnivå
Förutsägbarhet	0.337	1.723	0,101
Användbarhet	0.277	1.229	0.234
Robusthet	0.276	1.249	0.227
Ansvarstagande	0.256	0.956	0.347
Driftsäkerhet	-0.173	-0.495	0.626
Familjaritet	0.146	0.662	0.516
Förmåga	0.061	0.205	0.840
Välmening	0.059	0.345	0.734
Pålitlighet	-0.055	-0.174	0.864
Begriplighet	-0.053	-0.247	0.808
Kontroll	-0.031	-0.141	0.889

De fyra faktorerna var Förutsägbarhet, Användbarhet, Robusthet och Ansvarstagande. Ingen av dessa faktorer var signifikant i sig själv, dock var samtliga vikter relativt stora. Vidare visade det sig att de sju övriga var avsevärt mindre betydelsefulla för systemtilltro. Det innebär att om Totalförsvaret vill öka tilltron ska de framförallt bearbeta dessa fyra faktorer eftersom dessa tycks påverka systemtilltron mest, med reservation för att de inte är signifikanta som enskilda faktorer.

## 12. Sammanställning av samtliga empiriska resultat

De fyra faktorerna i analysen av enkät 2 är även intressanta utifrån de teoretiska modeller som beskrevs inledningsvis. Robusthet representerar någon form av pålitlig teknisk kompetens i Muir's modell från (1987). Detta återkommer vi till i diskussionen. Förutsägbarhet är central också enligt tidigare teoretiska modeller. Begreppet förutsägbarhet är ett nyckelbegrepp för de flesta teorierna för tilltro. Ansvarstagande kan möjligtvis kopplas ihop med övertygelse (faith) och anförtrott ansvar (Barber, 1983). Framförallt när det visar sig att det är värdet av ledningens och skyddsnetzets ansvarstagande som påverkar tilltron. Har befattningshavaren ett förtroende för ledningen och det skyddsnetz som omgärdar befattningshavaren ökar tilltron till systemet. Användbarhet är möjligtvis svårt att hantera teoretiskt dock uppvisar samtliga befattningshavare att faktorn är betydelsefull i realiteten. Det framkommer i Kompetens, Utrustning och MMI/Ergonomi faktorerna i synnerhet, dvs. att det är viktigt att dessa faktorer är användbara. En möjlig tolkning är att FM befattningshavare befinner sig i en situation/miljö som innehåller kunskaper/tekniska system som i realiteten inte är användbara fullt ut. En annan tolkning är att användbarheten är tillgodosedd och att befattningshavarna ändock insett att användbarheten är central för tilltron till system. Dessa analyser har visat följande:

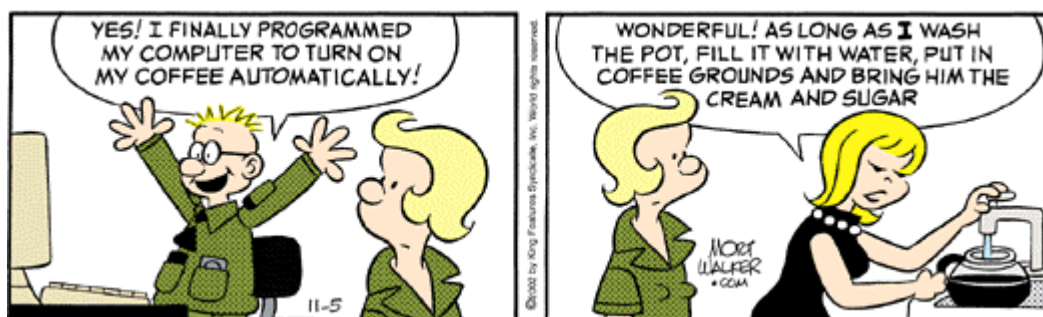
1. Flertalet viktiga faktorer är gemensamma för tilltron till systemet på en gemensam systemnivå. Likheterna mellan C130 och AJS 37 är stora i detta avseende.
2. Avvikelserna är särskilt påtagliga med avseende på var de egengenererade faktorerna ”landar” i termer av teoretiska faktorer.
3. Förutsägbarhet, pålitlighet, och övertygelse är teoretiska storheter vilket återkommer i dessa data (förutsägbarhet, ansvarstagande, robusthet, systemprestanda).
4. Användbarhet är en viktig faktor som inte enkelt placeras in i de teoretiska modellerna men enligt deltagarna är central för systemtilltro.
5. Lagandan, skyddsnetzets och informationens karaktär är avgörande för tilltron utifrån deltagarnas uppfattning.

Det är dock viktigt att poängtera att slutsatserna ska tolkas med försiktighet. Det beror på följande aspekter. De olika deltagargrupperna bestod av befattningshavare med olika roller. De tillfrågades om uppfattningar av systemtilltro med olika fokus, på teknisk systemnivå och förband/systemnivå. Slutsatserna ska därför tolkas som indikationer, inte säkerställda fakta. Dock samvarierar resultaten mellan enkäterna och mellan de olika grupper av operatörer som deltagit. Dessutom har data samlats in i olika miljöer, dvs. på hemmaplan och på internationell mark. Likheterna är ändock stora mellan C130 och AJS 37. Att lagandan är mer central för ett förband som befinner sig i Polen är inte anmärkningsvärt i sig. Det poängterar dock att de flesta av faktorerna är stabila men att specifika variabler kan variera med avseende på miljö. Ytterligare en aspekt bör beaktas för att inte en övertolkning ska ske. Deltagarna befann sig inte i en ”extremt sårbar” situation (se tidigare diskussion om sårbarhet). Även om de resultat som dessa datainsamlingar resulterat i är tydliga så är det inte uteslutet att andra faktorer är mer kritiska då en operatör befinner sig i en livshotande situation.



## 12.1 Resultaten av empiriska nedslag i ljuset av teoretiska modeller

Ett resultat av det empiriska arbetet är bl.a. att deltagande personal har gett indikationer på vad de upplever påverkar deras tilltro till ett givet system. Totalförsvaret och FM har därmed fått en fingervisning om vilka faktorer som bör beaktas om personalen ska känna högre grad av tilltro. Vidare har det framkommit att de teoretiska modeller som används för att förklara begreppet tilltro (trust) även fungerar i en unik totalförsvarmiljö. Förutsägbarhet och pålitlighet (Dynamics of trust) är mer baserade på historia än vad övertygelse är (jmf med engelskans begrepp (faith) som är mer framtidsinriktat). Våra frågor uttryckte dock inte en framtidsaspekt, vilket kan förklara denna skillnad. När det gäller "meaning of trust" är resultaten också rimliga. Framförallt aspekterna "teknisk kompetens" (robusthet och systemprestanda) och "anförtrott ansvar" (ansvarstagande). Den faktor som är svårare att förstå utifrån de teoretiska modellerna är "användbarhet" och "begriplighet" om inte dessa begrepp även ska inkluderas i systemprestanda, dvs. ett systems prestanda är betingat av i vilken utsträckning operatören upplever att det går att använda.



## 13. Systemtilltro – i ett framtida NBF

Den tredje uppgiften, att koppla litteraturen och empiriska resultat till ett framtida NBF, diskuteras nedan. Ett totalförsvaret baserat på nätverk med ökad lokal frihet skapar nya förutsättningar och likheten med en virtuell organisation ökar. Nedan följer därför en kortfattad redogörelse för vilken problematik som föreligger i virtuella organisationer (läs NBF) med avseende på systemtilltro.

### 13.1 Virtuella team och virtuella organisationer



Systemtilltro i globala virtuella organisationer och i globala virtuella team utgör ett särskilt komplext problem som både har likheter och olikheter med traditionella face-to-face team och organisationer.

Kristof et al (1995) definierar ett globalt virtuellt team som **"a temporary, culturally diverse, geographically dispersed, electronically communicating work group"**. Samma definition skulle även kunna gälla en global virtuell organisation.



### 13.1.1 Skapa och vidmakthålla systemtilltro

Det traditionella sättet att bygga tilltro existerar inte i virtuella team och organisationer. Eftersom medlemmarna inte träffar eller känner varandra finns inte de traditionella ledtrådarna för att bilda sig en uppfattning av de övriga medlemmarnas tillförlitlighet. Dessutom kännetecknas globala virtuella system av en teknologisk komplexitet som gör systemet svårt att överblicka och kontrollera.

I stället för att utveckla tilltro importerar eller övertar man tilltro från andra håll som man är mer bekant med. Tilltron utgår från förväntningarna på en roll i stället för att utgå från en relation med en annan individ. De olika rollerna (befattningarna) i systemet måste vara tydliga och väl definierade. Tilltro erhålls om rollerna är tydliga och rollinnehavaren lever upp till förväntningarna.

När teamet eller organisationen etablerats vidmakthålls tilltron av ett "highly active, proactive enthusiastic, generative style of action" (Meyerson, Weick, & Kramer, 1996). Detta innebär kortfattat att tilltroproblematiken förändras då totalförsvaret går emot en organisation som närmar sig en virtuell organisation. "Swift trust" är ett begrepp som utvecklats för att problematisera tilltro i just virtuella organisationer.

### 13.1.2 Swift trust

Mayerson, Weick och Kramer (1996) har skapat begreppet "swift trust" för att fokusera på den speciella typ av tilltro som gäller för temporära virtuella team och organisationer där "nu eller aldrig" tycks gälla för tilltron till systemet. Man kanske också skulle kunna kalla det för instant trust för att markera dess krav på att etablera tilltro antingen snabbt eller aldrig. "Swift trust" används dock främst för temporära virtuella team och organisationer som bildas för att lösa en gemensam uppgift med ett klar slut(tid)punkt, dvs. team och organisationer av projektform. Dessa team och organisationer består av medlemmar med olika kompetens, som har en ringa tidigare erfarenhet av att arbeta med varandra, och där det inte är troligt att de kommer att arbeta tillsammans någon mer gång. I dessa grupper finns inte den tid till förfogande som skulle krävas för att etablera tilltro för systemet på traditionell väg. Trots detta kräver denna typ av grupper tilltro för att kunna fungera.

Tilltron skapas genom en kombination av rollbaserad tilltro och en förväntan på att medlemmarna kan bidra till det gemensamma uppdraget. Infriade förväntningar på de övriga medlemmarnas bidrag, kompetens, professionalism och engagemang skapar tilltro till systemet. I en virtuell organisation är alltså de enskilda medlemmarnas förmåga av yttersta vikt. Att vara specialist eller mästare inom sitt område tycks vara en förutsättning för framgång då man i en virtuell organisation inte på samma sätt kan kompensera för medlemmars eventuella oförmåga. I en liknande projektbaserad (task force) tillvaro blir också tilltron till det egna närmaste systemet extra viktig då det stora systemet som man för tillfället ingår i, och som när uppdraget är genomfört kommer att upplösas, är att betrakta som en idé som inte låter sig fullt ut överblickas eller testas.

### 13.1.3 Systemparametrar

Parametrarna förutsägbarhet, användbarhet, robusthet och ansvarstagande identifierades som tidigare nämnts som betydelsefulla för operatörens systemtilltro. Virtuella team och organisationer är till sin karaktär temporära, dvs. de skapas, utför sitt uppdrag och därefter upplöses de. Varje virtuell organisation är därför att betrakta som ny och unik (medlemmarna kommer inte någon mer gång i exakt samma konstellation ta sig an exakt samma uppgift under

samma omständigheter). Detta ställer operatören inför annorlunda svårigheter när han skall avgöra systemets förutsägbarhet, användbarhet, robusthet och ansvarstagande. Tiden som står till förfogande för att öva systemet blir därför särskilt viktig samt operatörernas erfarenhet av att verka i virtuella organisationer och därmed förmågan att fånga upp de tecken och indikationer som kan tala om för en erfaren operatör vad, hur mycket och när han kan lita på systemet.

### 13.1.4 Icke-rutin och övning

Virtuella organisationer skapas oftast för att hantera uppgifter och situationer som inte är av rutinkaraktär utan som är svåra och annorlunda. Det innebär att dessa operatörer och system ofta kommer att hamna i nya situationer och genomföra uppdrag man inte tidigare genomfört, att jämföra med exempelvis traditionella flottiljöövningar inom Flygvapnet som kan betraktas som rutin för en erfaren operatör. Tilltron till systemet kommer därför också att baseras på systemets förmåga att fungera under nya och okända förhållanden (Aha, det fungerar även här!).

## 13.2 Att sprida innovationer

Systemtilltro är inte bara avgörande för operatörens beredskap att använda ett givet system. Det är också avgörande då ett nytt system skall introduceras och tas i bruk. Inom forskningsområdet ”Diffusion of Innovations” studerar man hur nya innovationer, idéer, fortplantar sig i organisationer. Man har funnit (Rogers, 1995) fem variabler som styr och påverkar införandet (rate of adoption) av en innovation. De fem variablerna är:

1. Hur man uppfattar egenskaperna hos innovationen.
  - Hur stor relativ fördel denna innovation har över befintligt system.
  - Om innovationen är kompatibel med befintligt system.
  - Om innovationen är komplex eller enkel till sin natur.
  - Om innovationen låter sig testas.
  - Om man kan observera resultatet av innovationen i förväg.
2. Hur man tar beslut om innovationen
  - Individens tar beslutet att bejaka eller förkasta innovationen.
  - Kollektivet tar beslutet att bejaka eller förkasta innovationen (konsensus).
  - Ett fåtal individer bestämmer över massan om att bejaka eller förkasta innovationen.
3. Kommunikationskanaler.

Införandet av en innovation påverkas av vilka typer av kommunikationskanaler som står till förfogande. Masskommunikation når många snabbt men tilltron till informationen är svårbedömd. Opinionsledarskap, dvs. ledarskap utövat av de individer som många och framförallt nyckelpersoner har tillit till är effektivare. De flesta budskap tycks, för att nå ut, förutsätta opinionsledare som tolkar, förmedlar och godkänner budskapet.
4. Det sociala systemets natur, dvs. normer, organisationsform etc.

Olika sociala system har olika kulturer. Kulturer grundar sig på vissa antaganden om hur verkligheten är beskaffad och hur vi bäst kan förhålla oss och agera får att nå våra syften. Antaganden som utgår från att verkligheten i grunden är statisk, att världen fungerar på ett mekaniskt vis och att kontroll är grunden för ledning kommer att få en bevarande funktion och därmed vara hindrande för idéer som strider mot det ”normala”. Olika organisationsformer tycks också vara förknippade med vissa antaganden. Så kan vi exempelvis se nätverksorganisationer som ett resultat av ett synsätt på verkligheten inspirerat av ekologi mer än mekanik.

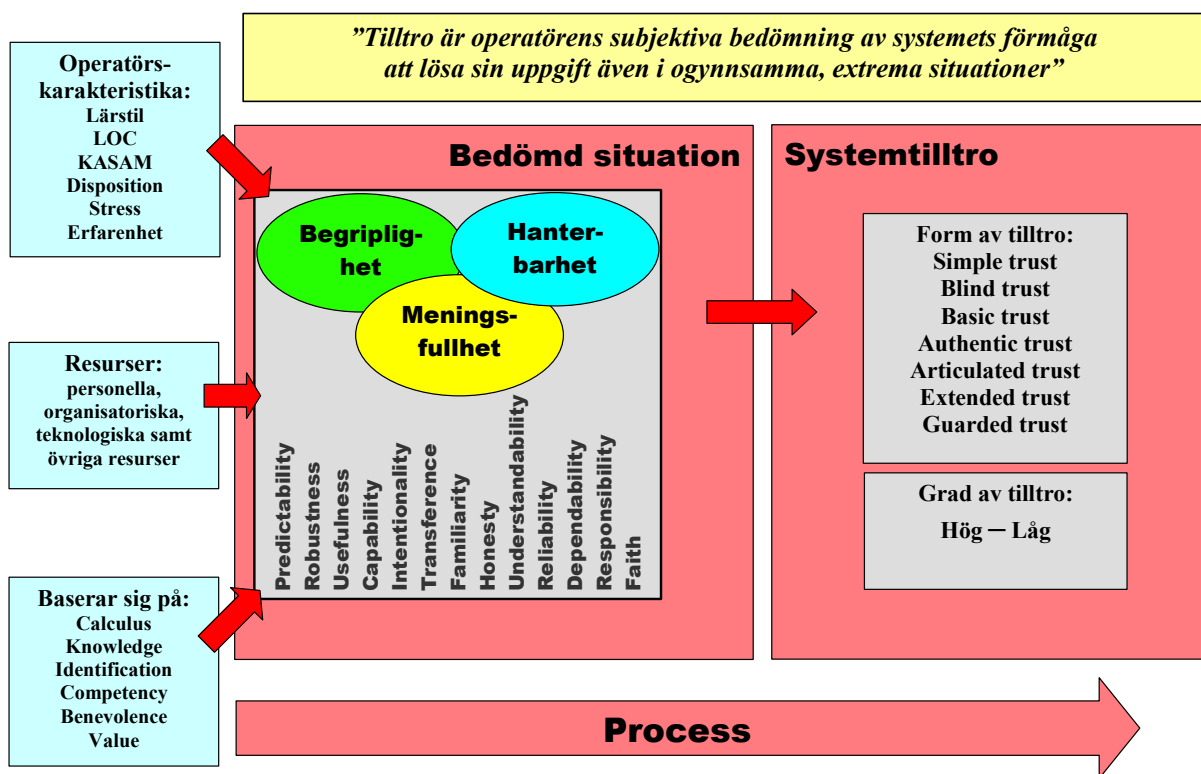
### 5. Förändringsagenternas förmåga att sälja innovationen.

Förändringsagenternas förmåga påverkas av flera faktorer. Förändringsagenter som har beslutsmyndighet inom sin organisation, dvs. de som själva har rätt att fatta beslut har större trovärdighet än de som inte har det. De förändringsagenter som uppfattas som kompetenta inom området, dvs. de som uppfattas som experter har större förmåga än de som inte uppfattas som kompetenta. De förändringsagenter som har en informell makt, dvs. är opinionsledare har större förmåga än de som inte har det. De förändringsagenter som bäst förstår sina klienters behov och situationens krav har större förmåga än de som inte gör det.

Kapitel 13 har försökt att beskriva två aspekter som ytterligare påvisar hur tilltroproblematiken accentueras av en förändring mot NBF; virtuella organisationer samt problematiken med innovationer. I ett försök att förenkla denna komplexa bild av systemtilltro, med allt från individkaraktäristik till uppgiftens svårighetsgrad och individuell förmåga, har vi en modell för hur detta skulle kunna gestalta sig. Denna modell kallar vi en holistisk bild av systemtilltro.

## 14. En holistisk bild av systemtilltro

Den holistiska bilden är en ansats att sammanfoga de olika delarna vi funnit ha betydelse för att skapa systemtilltro. Ansatsen är ett försök som är öppet för omprövning, dvs. inte slutgiltigt och definitivt. Den holistiska bilden är avsedd att tjäna som en karta att använda vid reflexion över systemtilltro och dess påverkan på systemet. Den centrala frågeställningen är huruvida den bedömda förmågan, och tilltron till denna förmåga, förmår att hantera den bedömda situation som du antingen befinner dig i eller som du förväntas ta dig an.



Figur 9. Ansats till holistisk bild av Systemtilltro.

## 14.1 Ingångsvärden

Vi har lyft fram tre områden som var och en för sig tycks vara väsentliga för uppbyggnaden av systemtilltro.

Det första området kallar vi **operatörskaraktäristika**, dvs. det som påverkar operatörens förmåga att bedöma vilken tilltro som är relevant samt överhuvudtaget det som skapar förutsättningar för operatören att känna tilltro till ett system. Här har vi;

- Operatörens inlärningsstil
- Locus of Control
- KASAM
- Disposition
- Stress

samt operatörens erfarenhetsnivå i termer av novis eller mästare.

Det andra kallar vi för **resurser** och innefattar allt det som operatören disponerar för att lösa uppgiften;

- personella
- organisatoriska
- teknologiska
- övriga resurser

**Personella resurser** inkluderar antal människor men även kompetens i form av kunskaper, färdigheter och attityder.

**Organisatoriska resurser** inkluderar exvis organisationsform, normer, värderingar, ledning, ledarskap etc. Ledarskapet påverkar systemtilltron! Vid övningen Strong Resolve framgick i intervjuer och hjuletanalyser att ledarskapet starkt påverkade tilltron till systemet. Då ledarskapet inte kan påverka den utrustning m.m. man disponerar i sig torde ledarskapet påverka systemtilltron genom påverkan av individernas uppfattning om sig själva och sin uppgift. En väsentlig dimension i ledarskapet är trovärdighet. Rolf Hedquist skriver i en rapport från Styrelsen för psykologiskt försvar (2002) att tillit förutsätter trovärdighet. Enligt Hedquist konstitueras trovärdighet av ledarens extroversion, självkontroll, konsekvens, kunskap, sociala kompetens, karaktär, prestige, identifikation och karisma.

**Teknologiska resurser** omfattar den teknik och teknologi som står till operatörens förfogande.

**Övriga resurser** är vad som för övrigt står till operatörens förfogande för lösandet av uppgiften.

Det tredje området utgör **baseringsgrunder** för operatörernas uppfattning och bedömning av tilltron. Shapiro, Sheppard och Cheraskin (1992) samt Lewicki och Bunker (1995a; 1995b) tar upp vad de kallar för;

- ”calculative-”,
- ”knowledge-” och
- ”identification” baserad tilltro.

Sitkin (1995) tar dessutom upp;

- ”competency-”,
- ”benevolence-” och
- ”value” baserad tilltro.

En skiljelinje går mellan tilltro som baserar sig på egen erfarenhet och tilltro som på något sätt är överförd och övertagen. En hypotes skulle kunna vara att man kan skapa systemtilltro genom överföring men att den förr eller senare måste verifieras genom egen personlig erfarenhet, framförallt om systemtilltron är avsedd för extrema situationer med stor sårbarhet.

Med de tre ingångsvärdena (operatörskaraktäristika, resurser samt baseringsgrunder) skapas, i en process, operatörens bedömning av systemet utifrån ett tilltrosperspektiv.

## 14.2 Processen

Processen för att skapa en bedömning av systemet ur ett systemtilltroperspektiv är parallell och följer det mönster som beskrivits av bl.a. Shalit (1988) samt Antonovsky (1991). Operatören måste bygga upp ett sammanhang och en helhet av systemet, dvs göra systemet:

- Begripligt (att jag förstår systemet),
- Meningsfullt (att jag vill använda systemet) samt
- Hanterbart (att jag kan använda systemet) i den situation jag befinner mig.

Situationen, eller kontexten, är central. De situationer som Totalförsvaret avses kunna hantera är ju situationer som kännetecknas av stor osäkerhet, komplexitet, föränderlighet samt tvetydighet. Många situationer kommer också att vara extrema och livshotande. Lewicki och Bunker (1995a; 1995b) hävdar också att tilltron är något som skapas i definierade steg och beskriver en sekventiell process. Viktiga parametrar för att kunna bedöma systemet är de parametrar som är identifierade i litteraturstudien och som i sin helhet är presenterade i rapporten. (Vissa av dessa parametrar var med avsikt borttagna ur enkäten då vi gjorde bedömningen att de antingen inte passade i denna typ av enkätundersökning eller då vi antog att de definitionsmässigt låg så nära en annan parameter att det skulle skapa förvirring hos de intervjuade.) Processen består av flera ”loopar” och mynnar ut i olika typer av tilltro med olika karakteristika samt styrkor och svagheter.

Ett problem är hur man definierar systemet. Detta framgick ganska klart vid övningen ”Strong Resolve” – Systemet är mitt system! Det framgick med stor tydlighet att när vi bad operatörer berätta om systemet så gjorde man det i första hand utifrån sitt eget system. Tillhörde man Flyg Underhållskompaniet (FU) så var SWAFRAP just FU. Det ”stora systemet” kom i andra hand. Detta torde innebära att man, för att kunna verka i det ”stora systemet”, måste vara väl integrerad i sitt ”lilla system”. Ju bättre integrerad man var desto lättare att tänka i det ”stora systemets banor”. (Jfr NBF).

### Olika typer av systemtilltro som resultat av processen

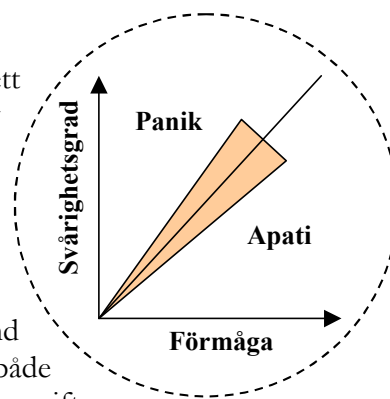
Processen resulterar i olika former av tilltro beskrivna av bl.a. Flores och Solomon (1998) samt Brenkert (1998). Eftersom tilltro blir viktigare ju sårbarare man är får de olika typerna av tilltro olika konsekvenser vad avser operatörens bedömda förmåga och vilja att utföra uppgiften.

## 14.3 Bedömd förmåga

Den bedömda förmågan är operatörens subjektiva bedömning av systemet utifrån ett situationsuppfattnings- och systemtilltroperspektiv.

### Förmåga kontra svårighetsgrad

Flera forskare lyfter fram situationsfaktorer som viktiga i ett tilltroperspektiv. Kee och Knox (1970) framhåller t.ex. graden av kontroll i en given situation som en situationsfaktor som påverkar tilltron. Robert och Marilyn Kriegel (1984) har utarbetat en modell där man ställer bedömd förmåga mot bedömd svårighetsgrad. Om bedömd svårighetsgrad överstiger bedömd förmåga hamnar man i ett område som de kallar för panikzonen. Om istället den bedömda förmågan överstiger bedömd svårighetsgrad hamnar man i vad de kallar för apatizonen. I både panik- och apatizonen blir min verkliga förmåga att lösa uppgiften långsiktigt degraderad. Om jag däremot befinner mig i en bra avvägning mellan bedömd



svårighetsgrad och bedömd förmåga kommer jag att långsiktigt kunna prestera bäst. Dock måste man ta i beaktande att även om jag befinner mig i en balanserad situation kommer jag att behöva ”dra mig ur” för att vila och återhämta mig. Vilken tilltro till systemet, samt vilken bedömning av situationen, som objektivt sett är korrekt är i sammanhanget ointressant då vi i slutändan ändå måste utgå från operatörens subjektiva bedömning varvid vi landar i den föreslagna definitionen:

**”Tilltro är operatörens subjektiva bedömning av systemets förmåga att lösa sin uppgift även i ogynnsamma, extrema situationer”**

## 15. Slutsatser

Följande slutsatser har vi funnit för de tre separata uppgifterna (se kap 1).

I deluppgift 1, som avser litteraturöversikten, framgår att ett flertal områden är problematiserade utifrån ett tilltroperspektiv. Här framkom med tydlighet hur utformningen av system påverkar tilltron och att individers förhållningssätt gentemot system i många stycken liknar de förhållningssätt som individer har gentemot andra individer. En problematik som inte belyses i tillräcklig utsträckning är då sårbarheten är hög, och då i synnerhet när den egna personen eller personer i den nära omgivningen är utsatta, eftersom totalförsvaret verkar i extrema situationer/miljöer (se kapitel 7 för utförligare diskussion).

I deluppgift 2 framkommer att de teoretiska modeller som existerar med avseende på tilltro går att tillämpa på totalförvarsinriktad verksamhet. Vidare framgår vilka faktorer som är av speciell vikt för de studerade förbanden. Dessa avviker i viss mån inbördes och speciellt då systemdefinitionen varierar (se kapitel 12 för utförligare diskussion).

I deluppgift 3 framkommer att det dessutom existerar unik problematik för organisationer som närmar sig karaktären av en virtuell organisation. Vidare är implementeringen av system/innovationer i dessa nya organisationsformer central för en välkalibrerad systemtilltro. Deluppgiften avslutas med en modell som försöker beskriva de faktorer som är av betydelse för en individs systemtilltro (se kapitel 13 och 14 för utförligare diskussion).

Slutsatsen är att systemtilltro är problematiserad i litteraturen även om vissa totalförsvarsbegränsningar existerar då den unika miljö som totalförsvaret verkar inom inte problematiseras tillräckligt. Litteraturen kan ändå ligga till grund för de unika frågeställningar som totalförsvaret har med avseende på tilltro. Slutsatsen är också att vi funnit några intressanta faktorer som är av betydelse för de studerade förbanden. Faktorer som totalförsvaret bör beakta i sin strävan att öka operativ förmåga. Slutsatsen är dessutom att tilltroproblematiken sprider sig över en rad områden, allt från individkaraktäristik till situationsanalys och bedömd svårighet och förmåga. Detta resulterar i en förenklad modell med avsikt endast att ge läsaren en bild av hur komplext tilltrobegreppet är och hur det kan relateras till en rad områden.

## 16. Förslag till fortsatt forskning

### Idéer om fortsatt forskning i projekt Systemtilltro 2003

Under arbetet i projektet har idéer om vilka aspekter som vi skulle vilja studera närmare efter hand vuxit fram. Dels djupare studier som kunde verifiera de resultat vi ser skönjas redan nu, men även att styra in studierna på sådana områden som är särskilt intressanta ur ett NBF-perspektiv.

Kortfattat kan dessa idéer redovisas som följer:

- Genomföra fältstudier med personer som deltagit i extrema situationer. Hur påverkar sårbarheten tilltron?
- Undersöka större, sociala, tekniska nätverk för att närma oss NBF-perspektivet.
- Verifiera redan gjorda studier genom större och mer riktade underlag.
- Hur påverkar de funna parametrarna en operatörs handlande?
- Hur påverkar avståndsuppfattningen i ett nätverk en operatörs handlande?
- Identifikationsprocesser. Djupare studier av socialisering av icke-mänskliga system.
- Kan tilltron till ett system kalibreras för att undvika att operatören initialt har för hög eller låg tilltro till systemet?
- Ett stridsvärdesbegrepp för systemtilltro bör kunna utvecklas.

Med redan vunna kunskaper och genomtänkta studier skulle flera av dessa aspekter kunna undersökas och ge djupare och mer NBF-inriktad kunskap om begreppet systemtilltro.



## Appendix 1

## Hjulet

Nyckelord: \_\_\_\_\_

Blanketten som användes för att generera egeninitierade faktorer.



## Appendix 2

## Parametertest

# SystemTilltro

Hur stort förtroende har du för \_\_\_\_\_?

**1**         **7**  
Litet  Stort

Skatta din upplevelse (1-7) av systemet vad avser systemets:

	<b>1</b> <small>Liten</small>	<b>7</b> <small>Stor</small>	<b>Irrelevant</b>
<b>Förutsägbarhet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Förmåga</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Robusthet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Familjaritet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Begriplighet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Användbarhet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Driftssäkerhet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Pålitlighet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Ansvarstagande</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Välmening</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>
<b>Kontrollerbarhet</b>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		<input type="checkbox"/>

Blanketten som användes vid parametertesten.

## Appendix 3

## Tabeller

	utom kontroll	organisation	ledning	utrustning	kompetens	förberedelse	information	säkerhet	skyddsnät	mening	inflytande	laganda	individen	avlastning
förutsägbarhet	1	7	1		1	2								
förmåga		9	37	1	1	3						4	5	
robusthet			1		14	1					2			
familjäritet	4	1	2	1			1					27	3	
begriplighet			3	1	1	6	20	1		11	1	1	2	
användbarhet		4	1	38	32	6			1	3	6			
driftsäkerhet		2	2	12		11			1	1				
pålitlighet	2		2		1	2			1		1	11		
ansvarstagande	5	1	19				1	1	16					1
välmening	3		1		1				7					5
kontrollerbarhet						5					2			

Tabell 2. SWAFRAP AJS. Värden från analys av hjulet.

	utom kontroll	organisation	ledning	utrustning	kompetens	förberedelse	information	säkerhet	skyddsnät	mening	inflytande	laganda	individen	avlastning
förutsägbarhet	0,14	2,13	0,33		0,33	1,33								
förmåga		2,79	16,70	0,11	1,00	1,29						1,07	1,79	
robusthet			0,20		4,08	0,17					0,57			
familjäritet	1,07	0,33	2,00	0,50			1,00					9,85	1,29	
begriplighet			1,13	0,33	1,00	1,64	7,69	0,50		3,27	0,25	1,00	0,50	
användbarhet		0,84	0,17	13,01	15,52	2,12			0,33	0,56	1,80			
driftsäkerhet		1,00	0,57	5,76		3,03			0,33	0,50				
pålitlighet	0,80		0,57		0,20	2,00			0,50		1,00	6,37		
ansvarstagande	1,32	1,00	6,56				0,20	1,00	5,69					0,33
välmening	1,80		1,00		1,00				2,88					2,08
kontrollerbarhet						1,79					0,50			

Tabell 3. SWAFRAP AJS. Normaliserade värden från analys av hjulet.

	utom kontroll	organisation	ledning	utrustning	kompetens	förberedelse	information	säkerhet	skyddsnät	mening	inflytande	laganda	individen	avlastning
förutsägbarhet						9								
förmåga		2	11	7	5	4				1			3	
robusthet		4			4	1					1			
familjäritet	1					2								
begriplighet	1		2		5	1	8			2	1			
användbarhet		9		1	3	1						1		
driftsäkerhet				11		2								
pålitlighet														
ansvarstagande	2		12					1	8					
välmening		1							3					1
kontrollerbarhet				1		2	4							

Tabell 4. SWAFRAP C130. Värden från analys av hjulet.

	utom kontroll	organisation	ledning	utrustning	kompetens	förberedelse	information	säkerhet	skyddsnät	mening	inflytande	laganda	individen	avlastning
förutsägbarhet						2,45								
förmåga		0,36	2,69	2,13	1,92	1,23				0,50			0,90	
robusthet		1,07			2,67	0,13					0,25			
familjäritet	0,14					0,44								
begriplighet	0,14		0,21		1,56	0,13	5,33			1,00	0,50			
användbarhet		2,61		0,10	1,50	1,00						0,25		
driftsäkerhet				2,81		0,80								
pålitlighet														
ansvarstagande	0,50		3,20					0,33	2,13					
välmening		0,50							0,90					0,14
kontrollerbarhet				0,50		0,67	1,60							

Tabell 5. SWAFRAP C130. Normaliserade värden från analys av hjulet.

	Leverantör, Underlag	1:a intryck	Tidigare erfarenheter	Operatörens möjligheter, Utb osv	MMI & Ergonomi	Systemprestanda	Fel i systemet	Tester o utfall
förutsägbarhet						1		
förmåga	3			1	1	7		
robusthet						5	1	
familjäritet		3	8			1	1	
begriplighet	2			2	6	3	1	
användbarhet	6	1		1	13			1
driftsäkerhet						6		
pålitlighet						7		
ansvarstagande	8							
välmening	4							
kontrollerbarhet					1			5

Tabell 6. CETRIS. Värden från analys av hjulet.

	Leverantör, Underlag	1:a intryck	Tidigare erfarenheter	Operatörens möjligheter, Utb osv	MMI & Ergonomi	Systemprestanda	Fel i systemet	Tester o utfall
förutsägbarhet						1,00		
förmåga	0,90			1,00	1,00	2,72		
robusthet						2,08	1,00	
familjäritet		0,75	1,60			0,33	0,50	
begriplighet	0,67			0,44	2,40	0,75	1,00	
användbarhet	2,12	0,33		0,14	3,31			1,00
driftsäkerhet						1,71		
pålitlighet						3,77		
ansvarstagande	2,29							
välmening	1,78							
kontrollerbarhet					0,33			1,92

Tabell 7. CETRIS. Normaliserade värden från analys av hjulet.

---

**Referenser**

- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
- Andrews, L. W., & Gutkin, T. B. (1991). The Effects of Human Versus Computer Authorship on Computers' Perceptions of Psychological Reports. *Computers in Human Behaviour*, 7, 311-317.
- Antonovsky, A. (1991). *Hälsans mysterium*. Stockholm: Natur och Kultur.
- Ashleigh, M. J., & Stanton, N. A. (2001). Trust: Key Elements in Human Supervisory Control Domains. *Cognition, Technology & Work*, 3(2), 92-100.
- Barber, B. (1983). *The logic and limits of trust*. NJ: Rutgers University Press.
- Bisantz, A. M., & Seong, Y. (2001). Assessment of Operator Trust in and Utilization of Automated Decision-Aids under Different Framing Conditions. *International Journal of Industrial Ergonomics*, 28(2), 85-97.
- Brehmer, B. (2002). *Ledning i NBF*. Stockholm: Krigsvetenskapliga Institutionen, FHS.
- Brenkert, G. G. (1998). Trust, Morality and International Business. *Business Ethics Quarterly*, 8(2), 293-317.
- Chaiken, S. (1979). Communicator Physical Attractiveness and Persuasion. *Journal of Personality and Social Psychology*, 37(8), 1387-1397.
- Cohen, M. S. (2000). *A Situation Specific Model of Trust in Decision Aids*. Paper presented at the International Conference on Human Performance, Situation Awareness & Automation, Savannah, Ga.
- Coyle, R. G. (1986). *System Dynamics Modelling: a Practical Approach*. London: Chapman and Hall.
- Dahlbäck, G. (2001). Faktorer av betydelse vid utformning av det nya svenska försvaret samt vid genomförande av operationer med framtidens insatsstyrkor. Förslag till aktiviteter. Linköping.
- Deutsch, M. (1960). The Effect of Motivational Orientation upon Trust and Suspicion. *Human Relations*, 13, 123-139.
- Egger, F. N. (2001, 27-29 June). *Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness*. Paper presented at the Affective Human Factors Design, Singapore.
- Fields, G. S. (2001). *The Effect of External Safeguards on Human-Information System Thrust in an Information Warfare Environment*. Unpublished Master's thesis.
- Flores, F., & Solomon, R. C. (1998). Creating trust. *Business Ethics Quarterly*, 8(2), 205-232.
- Fogg, B. J. (1998, April). *Persuasive Computers: Perspectives and Research Directions*. Paper presented at the CHI '98, New York.
- Fogg, B. J., & Tseng, H. (1999, May). *The Elements of Computer Credibility*. Paper presented at the CHI '99, Pittsburgh.
- Fukuyama, F. (1995). *Trust - The social virtues and the creation of prosperity*. New York: Simon & Schuster.
- Gambetta, D. (1988). Can we trust? In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213-238). New York: Basil Blackwell.
- Hanowski, R. J., Kantowitz, S. C., & Kantowitz, B. H. (1994). *Driver Acceptance of Unreliable Route Guidance Information*. Paper presented at the Human Factors and Ergonomics Society 38th Annual Meeting.
- Hedquist, R. (2002). *Trovärdighet - en förutsättning för förtroende* (No. 182). Stockholm: The National Board of Psychological Defence (SPF).

- Honaker, L. M., Hector, V. S., & Harrell, T. H. (1986). Perceived Validity of Computer- Versus Clinician-Generated MMPI Reports. *Computers in Human Behaviour*, 2, 77-83.
- Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an Empirically Determined Scale of Trust in Automated Systems. *Int Journal of Cognitive Ergonomics*, 4(1), 53-71.
- Kee, H. W., & Knox, R. E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. *Journal of Conflict Resolution*, 14(3), 357-366.
- Kerber, K. W. (1983). Attitudes towards specific uses of the computer Quantitative, decisionmaking and record-keeping applications. *Behaviour and Information Technology*, 2(2), 197-209.
- Klein, G. (1998). *Sources of power : how people make decisions*. Cambridge, Mass.: MIT Press.
- Kolb, D. A. (1984). *Experiential Learning: Experience as the source of learning and development*. Englewood Cliffs, N. J.: Prentice-Hall.
- Kriegel, R. J., & Kriegel, M. H. (1984). *The C-Zone: Peak Performance Under Pressure*. Doubleday.
- Kristof, A. L., Brown, K. G., Jr, H. P. S., & Smith, K. A. (1995). The virtual team: A case study and inductive model. In M. M. Beyerlein, D. A. Johnson & S. T. Beyerlein (Eds.), *Advances in interdisciplinary studies of work teams: Knowledge work in teams* (Vol. 2, pp. 229-253). Greenwich, CT: JAI Press.
- Lee, J. D. (1991). *The Dynamics of Trust in a Supervisory Control Simulation*. Paper presented at the Human Factors Society 35th Annual Meeting.
- Lerch, F. J., & Prietula, M. J. (1989). How do we trust machine advice?
- Lester, J. C., Converse, S. A., Kahler, S. E., Barlow, S. T., Stone, B. A., & Bhogal, R. S. (1997). *The Persona Effect: Affective Impact of Animated Pedagogical Agents*. Paper presented at the CHI '97, New York.
- Lewicki, R. J., & Bunker, B. B. (1995a). Developing and Maintaining Trust in Work Relationships. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 114-139). Thousand Oaks, CA: Sage.
- Lewicki, R. J., & Bunker, B. B. (1995b). Trust in relationships: A model of development and decline. In B. B. Bunker, J. Z. Rubin & Associates (Eds.), *Conflict, cooperation and justice* (pp. 133-173). San Francisco: Jossey-bass.
- Madsen, M., & Gregor, S. (2000). Measuring Human-Computer Trust.
- Masalonis, A. J. (2001). *Effects of situation-specific reliability on trust and usage of automated decision aids (decision support)*.
- McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, 38, 24-59.
- Meyerson, D., Weick, K. E., & Kramer, R. M. (1996). Swift trust and temporary groups. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in Organizations: Frontiers of Theory and Research* (pp. 166-195). London: Sage Publications.
- Miller, C. A., & Larson, R. (1992, Nov 15-18). *An Explanatory and "Argumentative" Interface for a Model-Based Diagnostic System*. Paper presented at the UIST '92.
- Mishra, A. K. (1996). Organizational responses to crisis: The centrality of trust. In R. M. Kramer & T. R. Tyler (Eds.), *Trust in organizations: Frontiers of theory and research* (pp. 261-287). Thousand Oaks, CA: Sage.
- Moon, Y. (1998). *The Effects of Distance in Local versus Remote Human-Computer Interaction*. Paper presented at the CHI '98, New York.
- Muir, B. M. (1987). Trust between humans and machines, and the design of decision aids. *Int Journal of Man-Machine Studies*, 27, 527-539.
- Muir, B. M. (1994). Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. *Journal of Ergonomics*, 37(11), 1905-1922.
- Nass, C., Fogg, B. J., & Moon, Y. (1996). Can computers be teammates? *Int J Human-Computer Studies*, 45, 669-678.
- Nass, C., Moon, Y., Fogg, B. J., Reeves, B., & Dryer, D. C. (1995). Can computer personalities be human personalities? *Int J Human-Computer Studies*, 43, 223-239.

- 
- Pancer, S. M., George, M., & Gebotys, R. J. (1992). Understanding and Predicting Attitudes Towards Computers. *Computers in Human Behaviour*, 8, 211-222.
- Quintanar, L. R., Crowell, C. R., Pryor, J. B., & Adamopoulos, J. (1982). Human-computer interaction: A preliminary psychological analysis. *Behaviour Research Methods & Instrumentation*, 14(2), 210-220.
- Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in Close Relationships. *Journal of Personality and Social Psychology*, 49(1), 95-112.
- Rogers, E. M. (1995). *Diffusion of Innovations* (4 ed.). New York: Free Press.
- Rotter, J. B. (1980). Interpersonal Trust, Trustworthiness and Gullibility. *American Psychologist*, 35(1), 1-7.
- Shalit, B. (1988). *The psychology of conflict and combat*. New York: Praeger Publishers.
- Shapiro, D. L., Sheppard, B. H., & Cheraskin, L. (1992). Business on a handshake. *Negotiation Journal*, 89(4), 365-377.
- Sitkin, S. B. (1995). On the positive effects of legalization on trust. *Research on Negotiation in Organizations*, 5, 185-217.
- Sitkin, S. B., & Roth, N. L. (1993). Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, 4, 367-392.
- Snizek, J. A., & van Swol, L. M. (2001). Trust, Confidence and Expertise in a Judge-Advisor System. *Organ Behav Hum Decis Process*, 84(2), 288-307.
- Waern, Y., & Ramberg, R. (1996). People's Perception of Human and Computer Advice. *Computers in Human Behaviour*, 12(1), 17-27.
- Wickens, C. D., Gempler, K., & Morphew, M. E. (2000). Workload and Reliability of Predictor Displays in Aircraft Traffic Avoidance. *Transportation Human Factors*, 2(2), 99-126.
- Zajonc, R. B. (1980). Feeling and Thinking, Preferences Need no Inferences. *American Psychologist*, 35(2), 151-175.
- Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840-1920. In B. M. Staw & L. L. Cummings (Eds.), *Research in Organizational Behaviour* (Vol. 8, pp. 53-111). Greenwich, CT: JAI Press.

