

ISO 27000 for Dummies



Ulf Dellborg

Säkerhetsbakgrund

- Flygförare FV
- Flygsäkerhet Viggen FMV
- Signalsystem Adtranz
- Kunsult IT++
 - Projektledning
 - Krav
 - Arkitektur
 - Säkerhet

ISO 27000.....



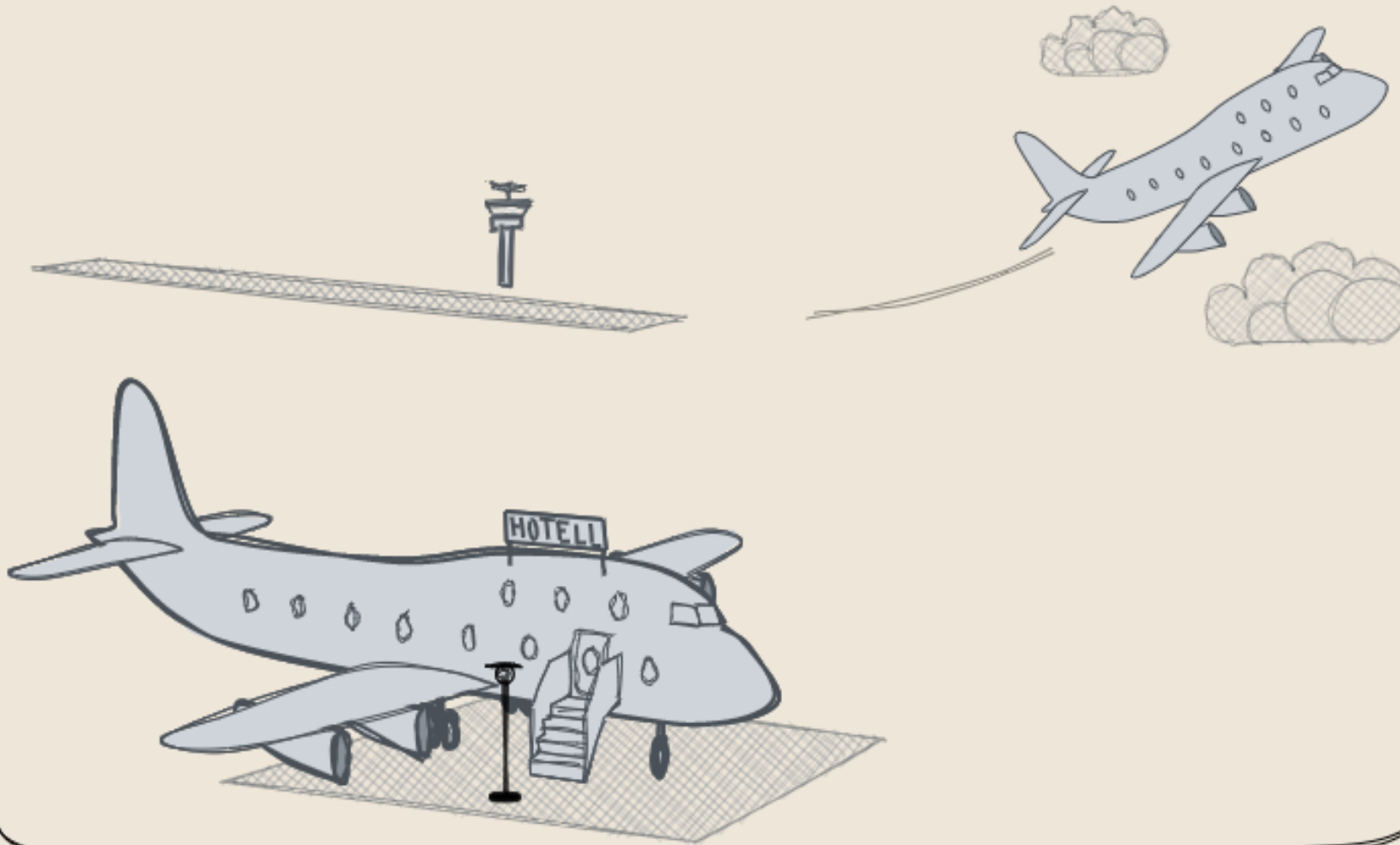
Syfte

- Förstå säkerhet
- Inte rädd för spöket...

Innehåll

- Safety Integrity Level
- Säkerhetssystem
- ISO27001
- Kap 4 Sammanhang
- Kap 5 Ledning
- Kap 6 Planering
- Kap 7 Support
- Kap 8 Operativt arbete
- Kap 9 Sammanhang
- Kap 10 Förbättring

Safety Integrity Level



Vad är det?

- ~~ISO 27000~~ IEC 61508
- Systemets behov av säkerhet
- Riskerna utan skydd

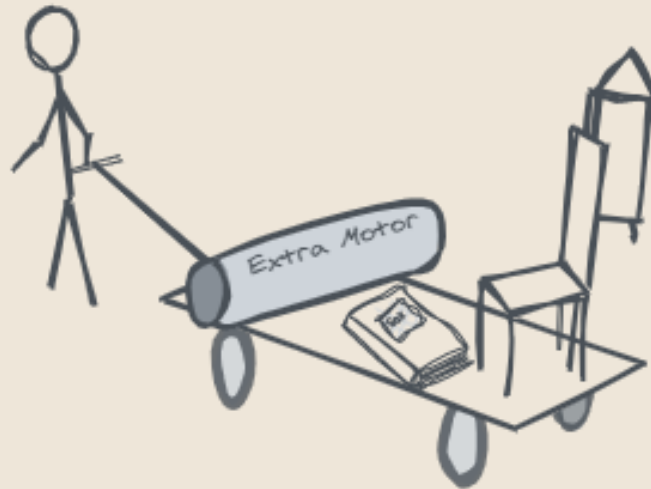
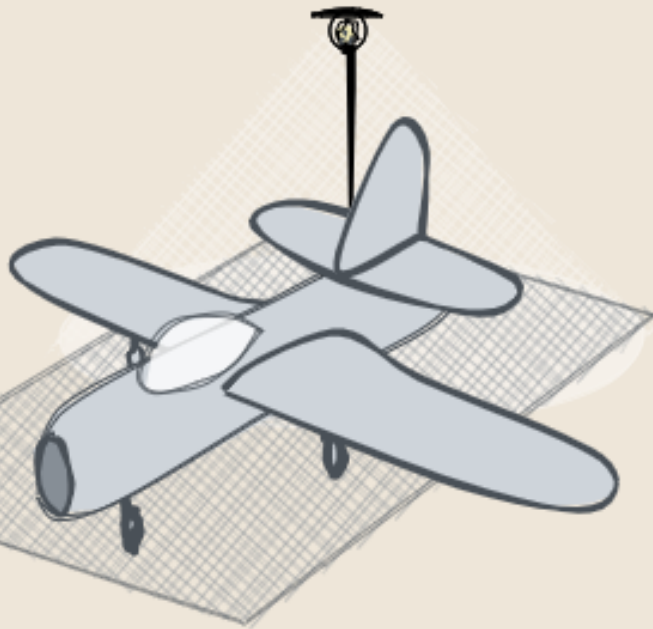
Varför tänka så?

- Rätt skydd
- Rätt arkitektur

Vad är nyttan?

- Effektivitet
- Säkerhet

Säkerhetssystem



(Ledningssystem....)

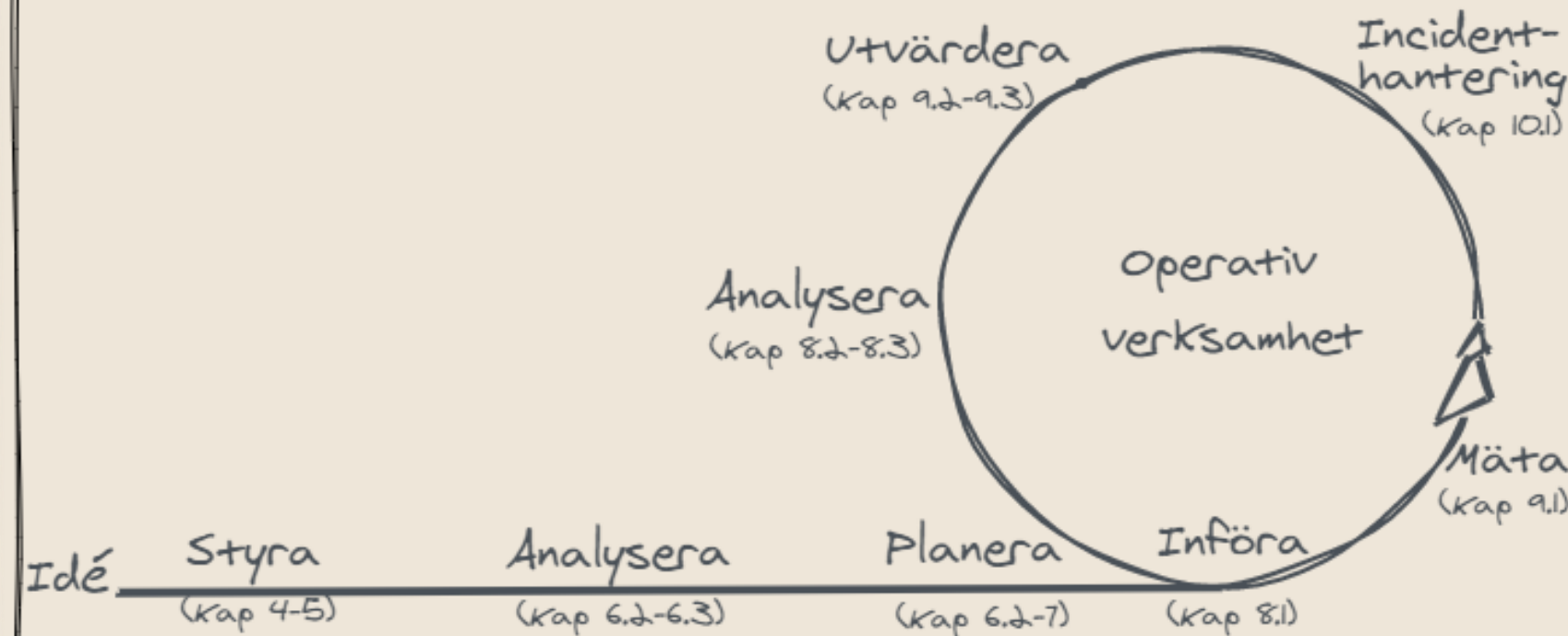
Systematiskt angreppssätt:

- Designa
- Implementera
- Använda
- Utvärdera
- Förbättra

"Företeelser" i verksamheten:

- Policies
- Instruktioner
- Guidelines
- Personal
- System
- Aktiviteter

ISO 27000 !



Serien ISO 27000

- 45 standarder
- 27000, definitioner
- 27001, krav säkerhetssystemet
- 27002, 114 kontroller
- 27005, hantering av risker

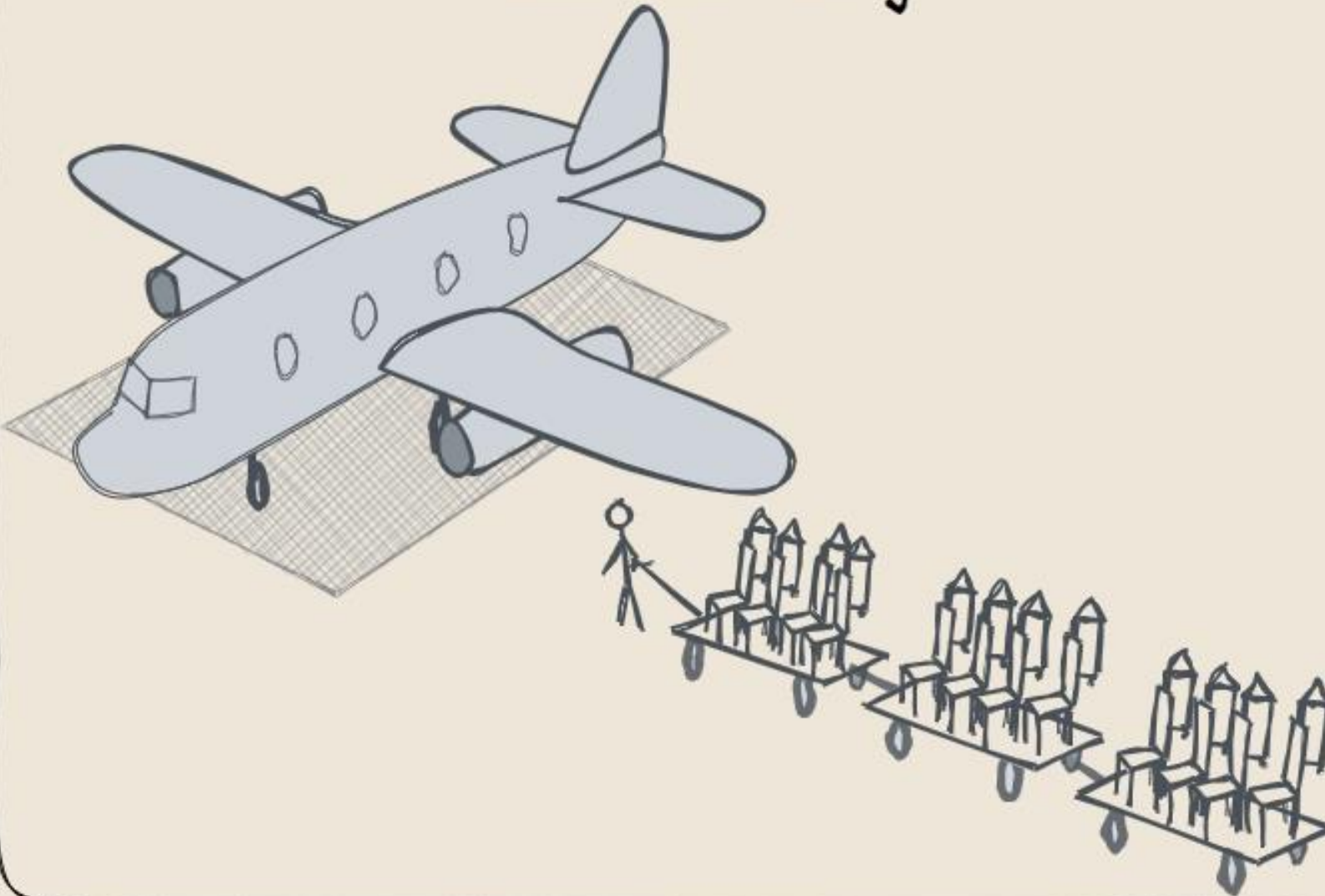
ISO 27001

- Krav mot säkerhetssystemet
- 7 kapitel bondförnuft
- Process: Plan, Do, Check, Act

Nyttan:

- Slipper uppfinna hjulet
- Effektiv väg till säkerhet
- Uppvisad kvalitet (certifiering)

Sammanhang



Kap 4, ISO 27001

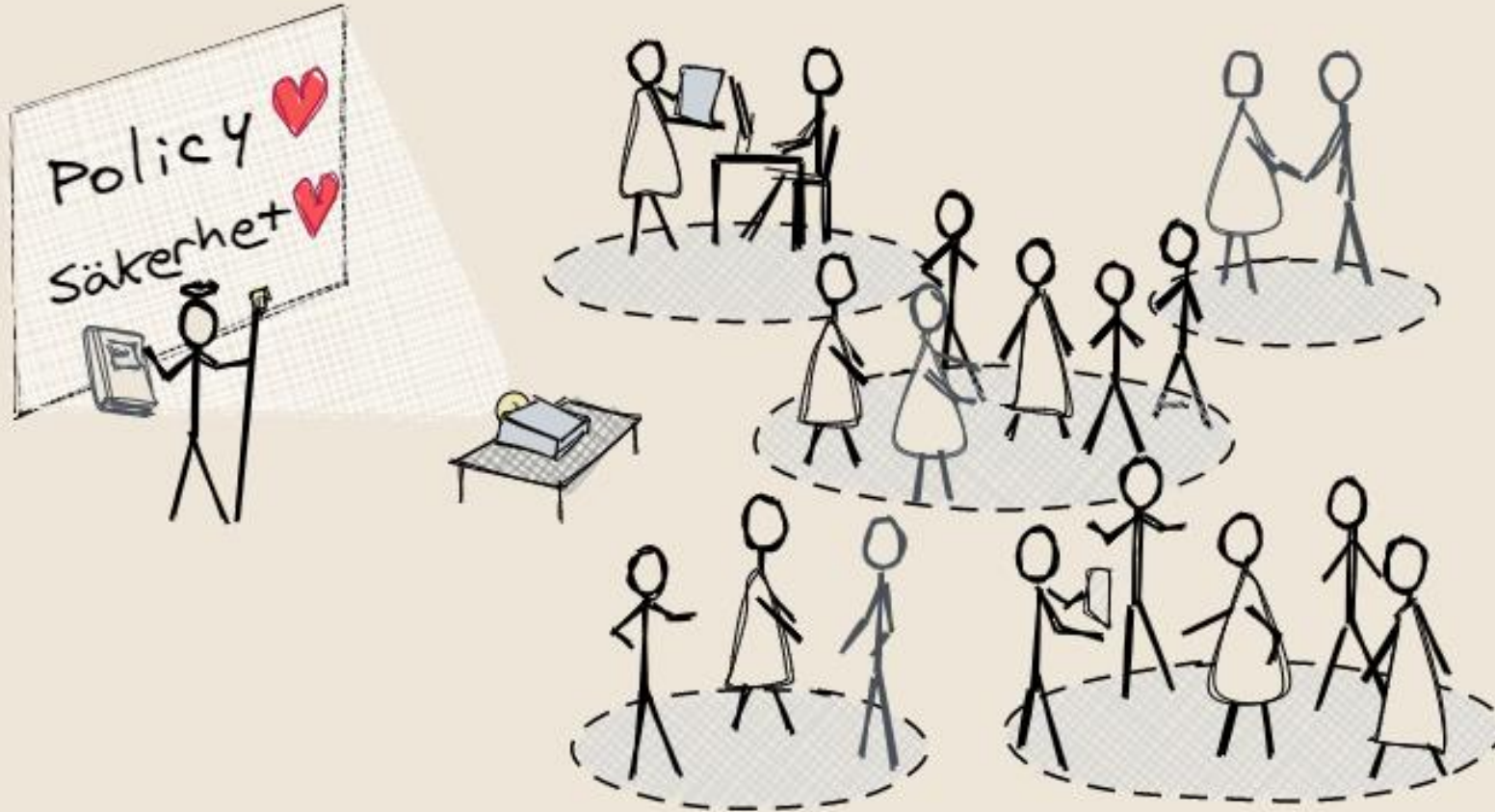
Organisationen ska identifiera:

- Frågor som påverkar förmågan att uppnå säkerhetsmålet
- Behov och krav hos alla säkerhetssystemets intressenter
- Beroenden mellan såväl externa och interna aktiviteter

Organisationen ska definiera:

- Säkerhetssystemets omfattning med hänsyn tagen till punkt 1-3

Ledarskap

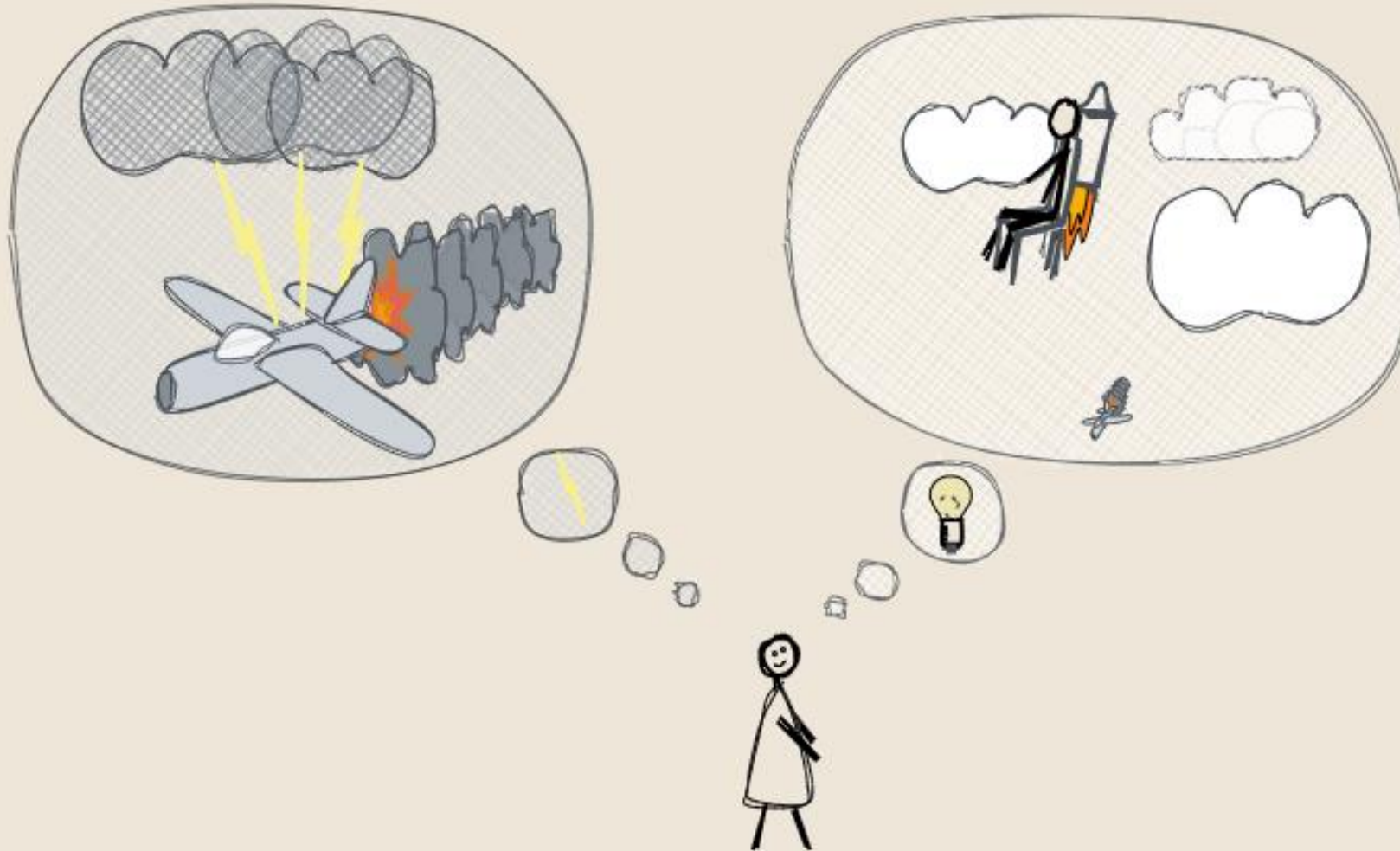


Kap 5, ISO 27001

Högsta ledningen ska:

- **Visa ledarskap och engagemang:**
 - Policy förenlig med strategin
 - Tillsätta och styra resurser
 - Kommunicera vikt av säkerhet
- **Etablera en säkerhetspolicy**
 - Lämplig för organisationen
 - Definierar säkerhetsmålen (på hög nivå)
 - Dokumenterad, kommunicerad och tillgänglig
- **Sätta ansvar & befogenheter**
 - Definierade
 - Kommunicerade

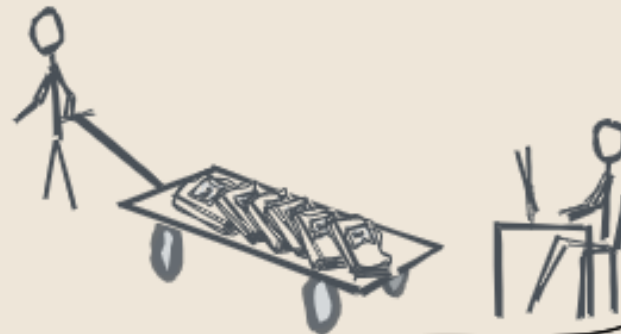
Risker och hantering av risker



Kap 6, ISO 27001, Planering

- **Process för riskanalys:**
 - Riskkriterier (t ex riskacceptans)
 - Identifiera risker
 - Analysera risker
 - Utvärdera risker
- **Process för hantering av risker**
 - Väljer hanteringssätt, kontroller
 - Statement of Applicability
 - Plan för åtgärder
- **Säkerhetsmål**
 - Förenliga med säkerhetspolicy
 - Kommunicerade
- **Plan för hur målen uppnås**
 - Vad, vem, hur, när

Resurser

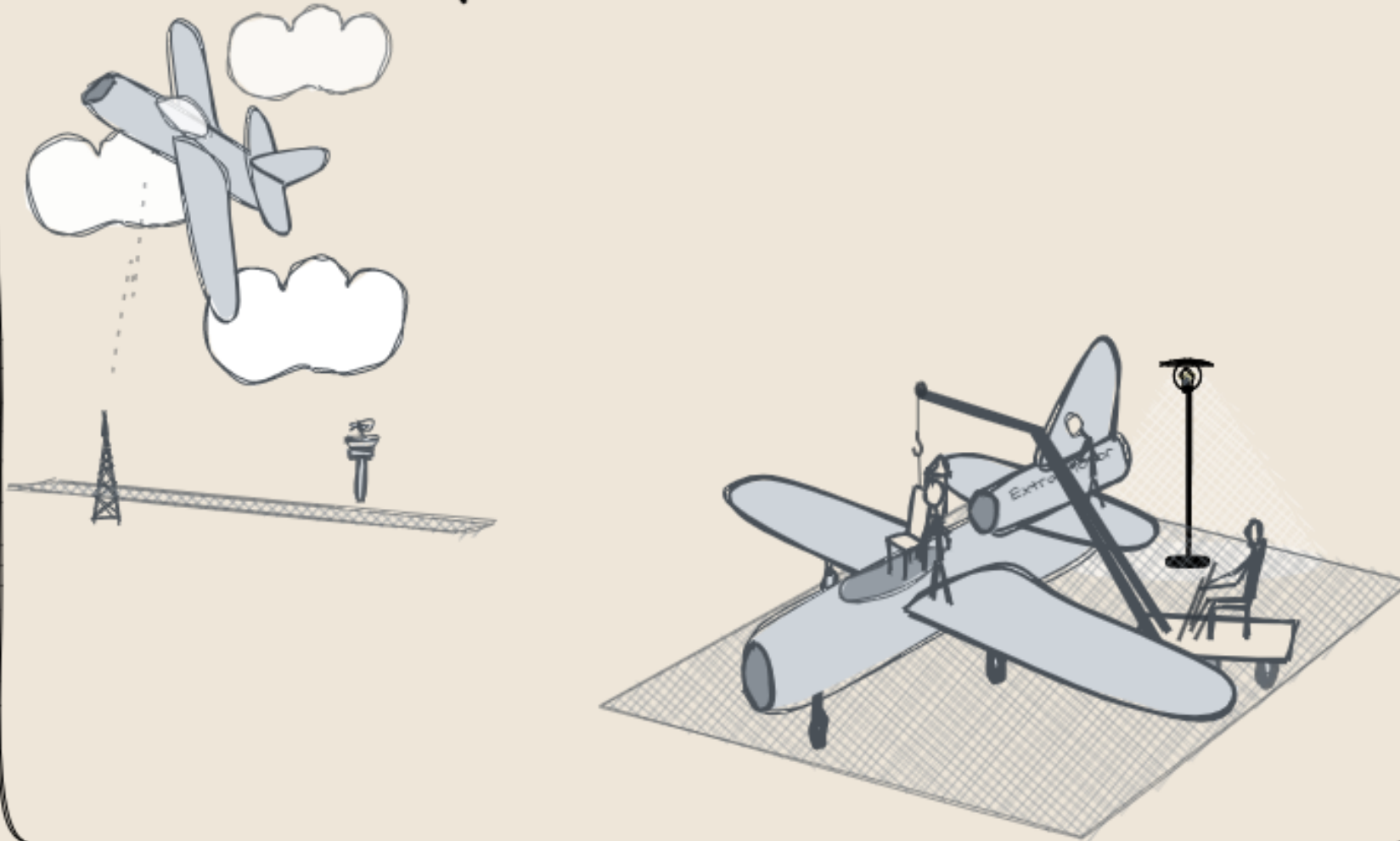


Kap 7, ISO 27001, Support

- **Nödvändiga resurser**
 - Definierade & tillhandahållna
- **Kompetens**
 - **Säkerhetspåverkande personal**
 - Fastställda kompetenskrav
 - Rätt utb, träning och erfarenhet
 - **Övrig personal**
 - Säkerhetspolicyn
 - Sin påverkan
- **Kommunikation**
 - Fastställa behov: när, vem, hur
- **Dokumentation**
 - Den ISO 27001 & du kräver
 - granskad och godkänd
 - versionshanterad, upprättad
 - Lagrad, distribuerad, skyddad



Operativt arbete

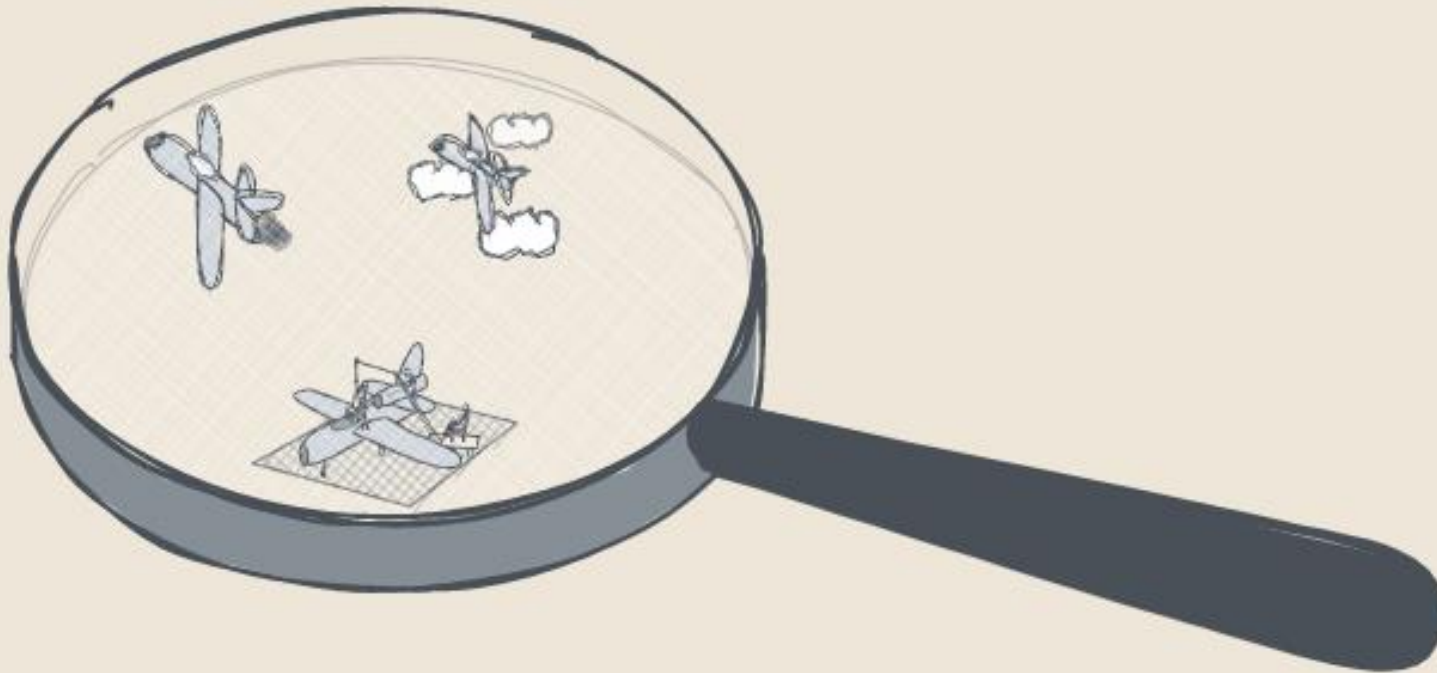


Kap 8, ISO 27001

Organisationen ska:

- **Realisera krav/mål enl kap 6:**
 - Planera processer
 - Implementera processer
 - Följa upp resultat
- **Ändringar**
 - Styra kontrollerade
 - Hantera oönskade
- **Hantera risker enligt kap 6:**
 - Återkommande
 - Vid ändringar

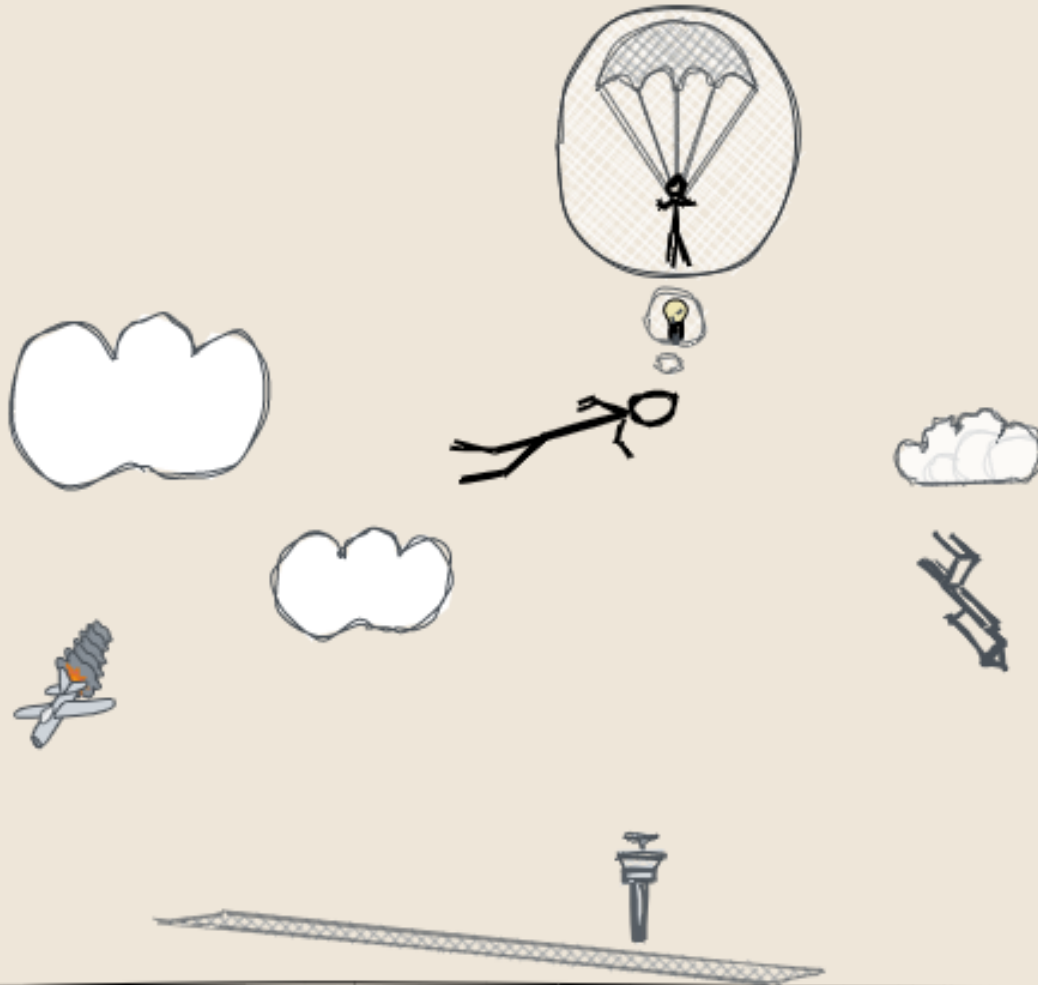
Utvärdering



Kap 9, ISO 27001

- **Utvärdera Effektivitet & resultat**
- **Övervakning & utvärdering**
 - Fastställa vad, hur, när av vem
 - Dokumentera och lagra resultat
- **Regelbundna internrevisioner**
 - Program: planera, förvalta
 - Revisioner: enligt program
- **Ledningens granskning:**
 - Status för tidigare frågor
 - Förändringar relevanta för säkerhet
 - Resultat av riskanalyser
 - Status planer
 - Förbättringsmöjligheter

Förbättringar



Kap 10, ISO 27001

10.1 Incidenter

- Ta kontroll över avvikelser
- Hantera konsekvenserna
- Vid behov eliminera orsaken
- Ändra säkerhetssystemet
- Dokumentera avvikelserna

10.2 Kontinuerlig förbättring

Lösningen kan bli komplex!

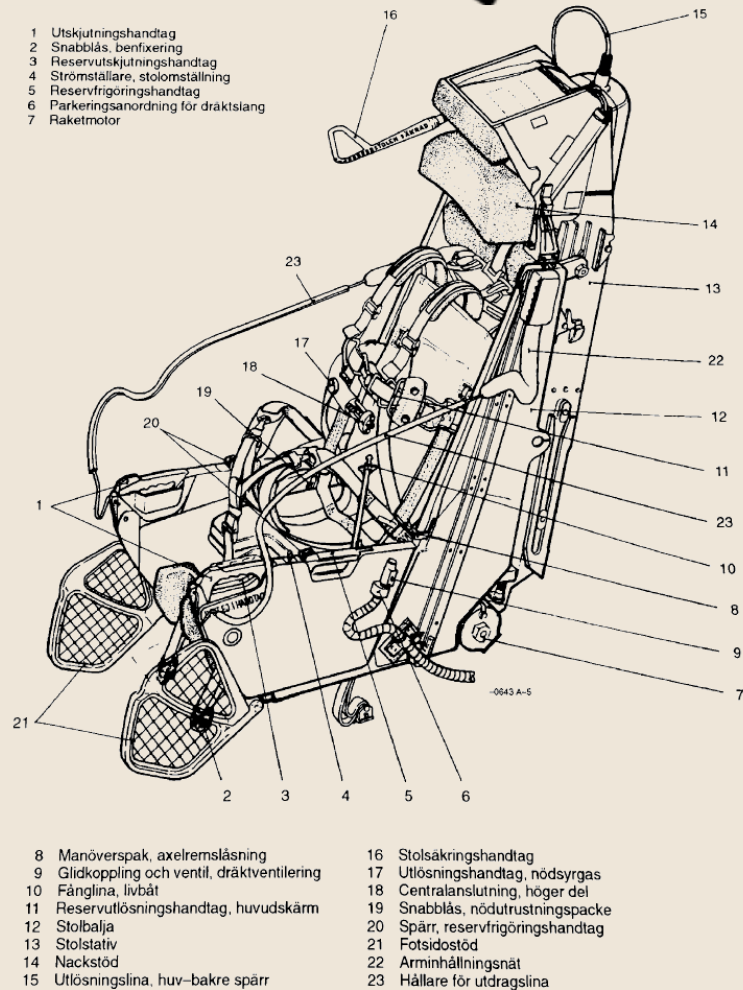


Bild 1. Stol, översikt

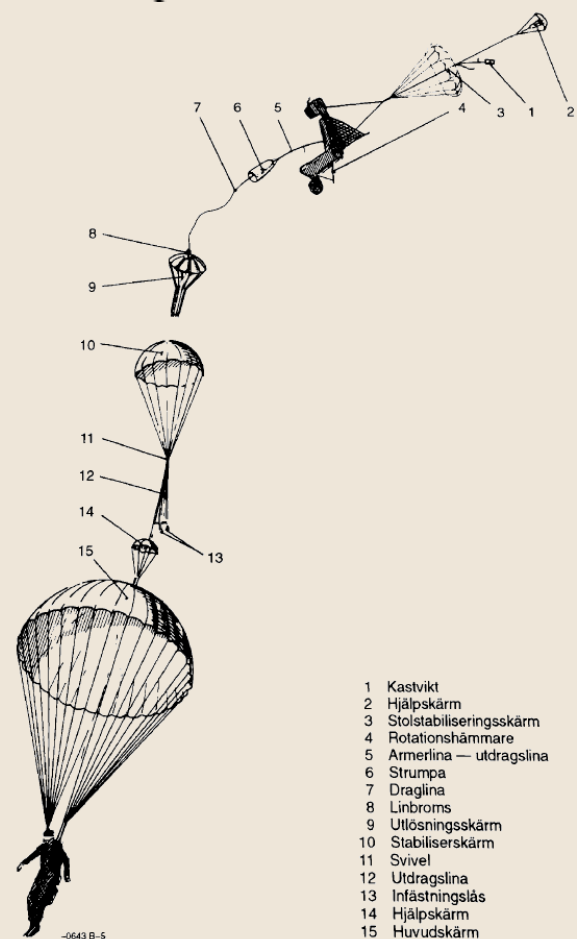
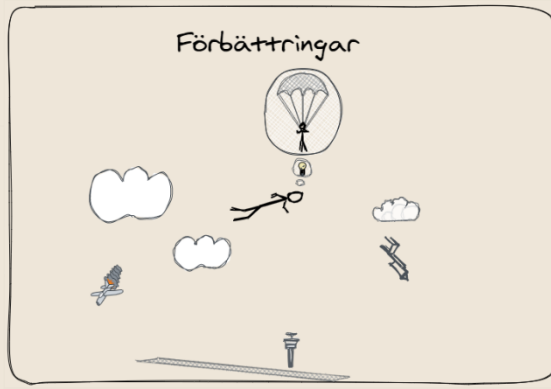
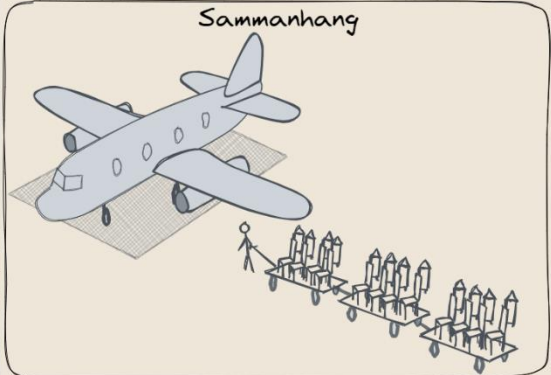


Bild 2. Stolstabilisering och fallskärmsutlösning, principschema

Säkerhetssystemet

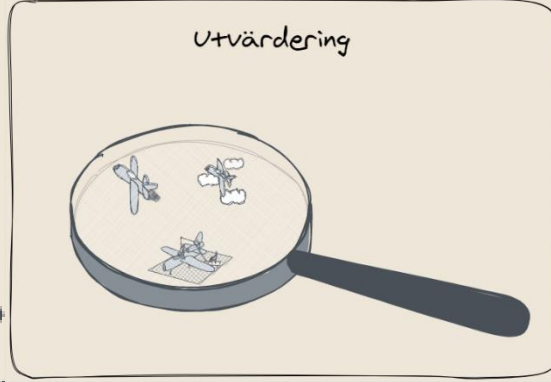
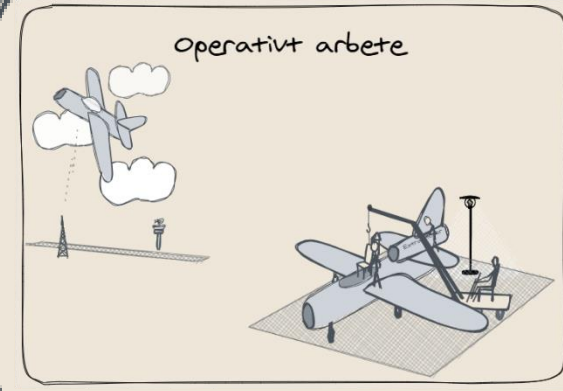
- Säkert konstruerat fpl
- Rätt underhållet fpl
- Speciell Förarinstruktion
 - Handhavande
 - Nödinstruktion
 - Prestanda
 - Tekniska beskrivningar
- Simulator
- "Trafikregler"
- Utbildning
- Medicinska kontroller
- Brand och räddning
- Räddningshelikoptrar
-



Utvärdera
(kap 9.2-9.3)

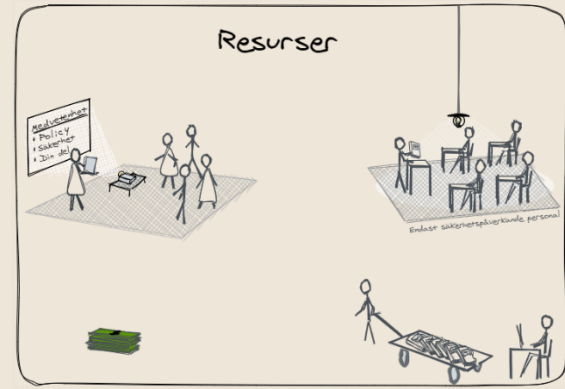
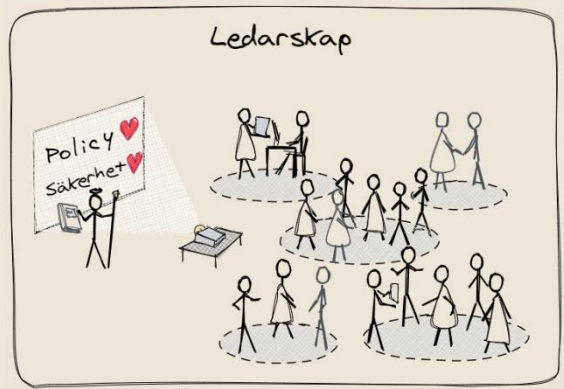
Incident-
hantering
(kap 10.1)

Analysera
(kap 8.2-8.3)



Mäta
(kap 9.1)

Idé Styra Analysera Planera Införa
(kap 4-5) (kap 6.2-6.3) (kap 6.2-7) (kap 8.1)



Tack!

