

Hur hanterar man krav på säkerhet?

Agenda

- **Introduktion**
- Krav i förhållande till en kvalitetsmodell
- Mål
- Policy
- Krav
- Säkerhet som kvalitetsfaktor
- kvalitetsfaktorn
- Den gemensamma underliggande kvalitetsfaktorn, försvar
- Gemensamma kvalitetsfaktorer på säkerhet
- Underliggande kvalitetsfaktorer



Introduktion

Eftersom vi förlitar oss mer och mer på programvaruintensiva system så har vi också kommit att förlita oss mer på att dessa system fungerar på ett säkert sätt.



Introduktion

Större olyckor beror ofta på sällsynta risker, faran är en kombination av förhållanden som ökar sannolikheten för olyckor!



Flygolyckan på Teneriffa, 27 mars 1977
Två Boeing 747-plan kolliderade och
583 människor omkom.

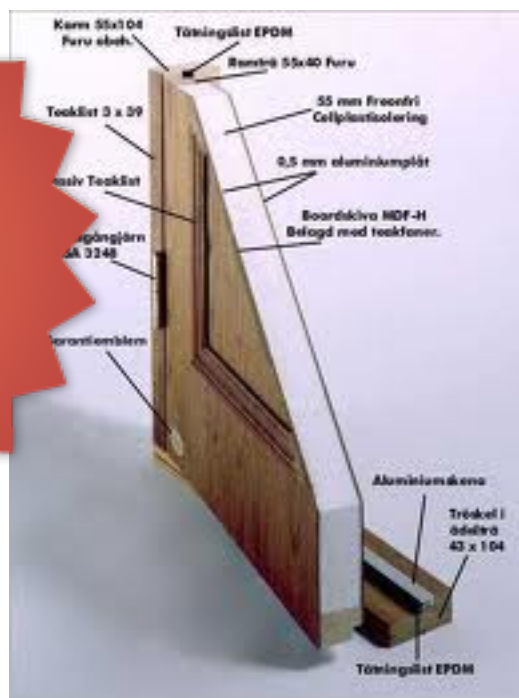


Kvalitet

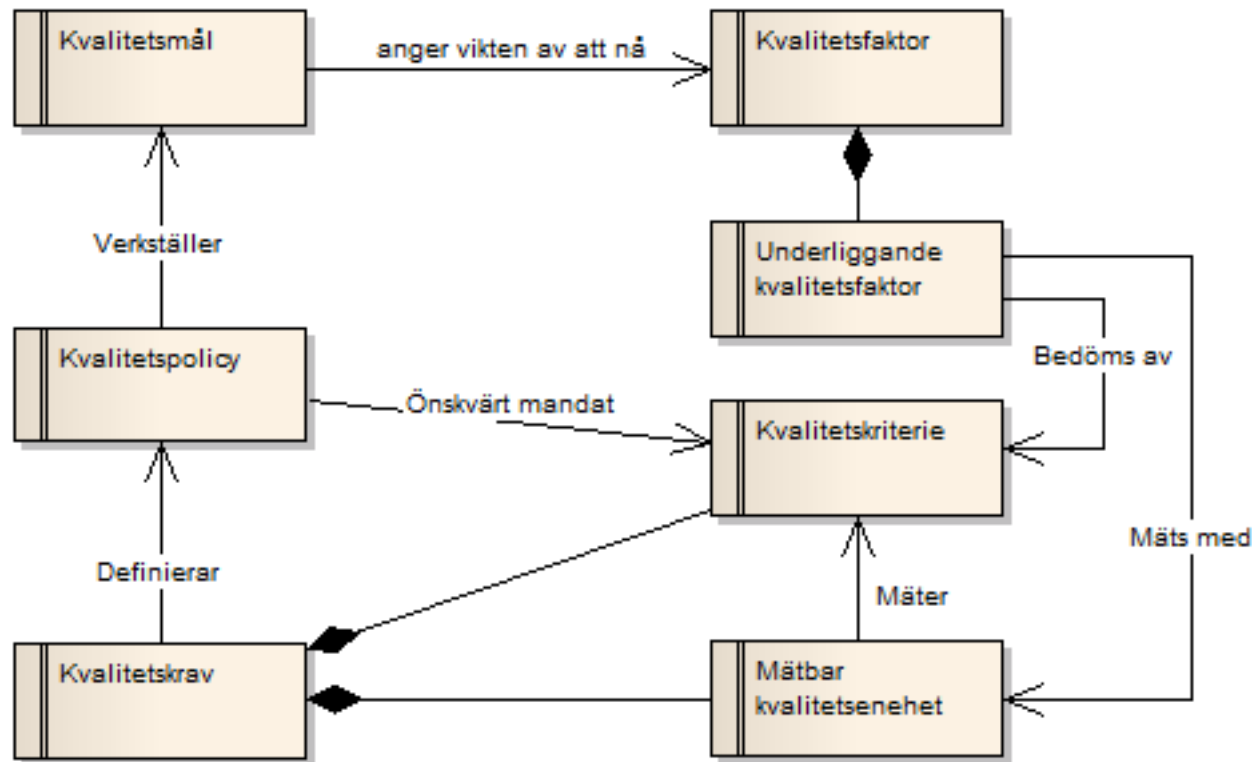
“Kvalitet är gratis. Den är inte en gåva, men den är gratis. Det som kostar pengar är sådant som inte är kvalitet – allt det som innebär att man inte gör sitt jobb rätt första gången”

Philip B. Crosby

**DYRARE
MAT
NU!**



Krav i förhållande till en kvalitetsmodell



Kvalitetskrav består av kvalitetsspecifika kriterier som bygger på underliggande faktorer tillsammans med mätbara enheter.

T.ex. olyckor per tidsenhet, skadekostnad, etc.



Mål

- **Mål**
 - **Kvalitetsmål**
 - **Säkerhetsmål**



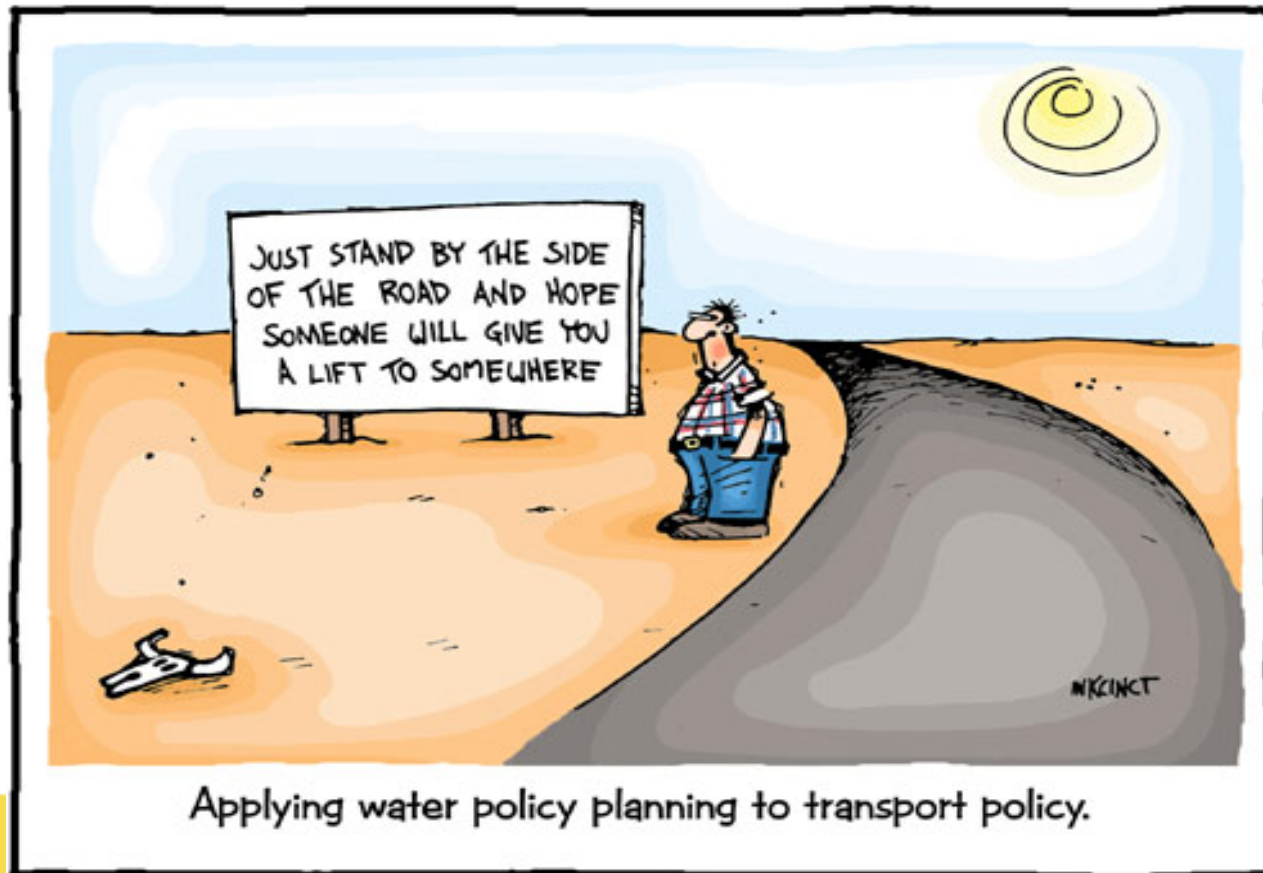
Mål

- **Ett Mål** är ett uttalande om vikten av att uppnå en önskad nivå med avsikt på vissa beteenden, datum, egenskaper, gränssnitt eller begränsningar. Det är på politisk nivå och för oformaliserat för att kunna verifieras
 - **Kvalitetsmålet** är ett mål som anger vikten av att uppnå ett önskat mål för kvalitetsfaktorer
 - **Säkerhetsmålet** är ett kvalitetsmål som anger vikten av att uppnå önskat mål för säkerhetsfaktorer



Policy

- **Policy**
 - **Kvalitetspolicy**
 - **Säkerhetspolicy**



18/01 2007-043 © John Ditchburn



Policy

- **En Policy** är ett strategiskt beslut som upprättar ett önskat mål.
 - **En kvalitetspolicy** bidrar med kriterier för kvalitetsfaktorer
 - **En säkerhetspolicy** är en kvalitetspolicy som bidrar med säkerhetskriterium, T.ex. "Raffinaderiets styrsystem måste hålla trycket i oljetankarna betydligt lägre än deras maximala tryck".



Krav

- **Krav**
 - **Kvalitetskrav**
 - **Säkerhetskrav**

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



search ID: man1354

"HERE'S YOUR 'CHEF'S SURPRISE,'
SIR--I'M LEGALLY REQUIRED TO TELL
YOU THAT YOU HAVE ONE LAST
CHANCE TO CHANGE YOUR MIND."



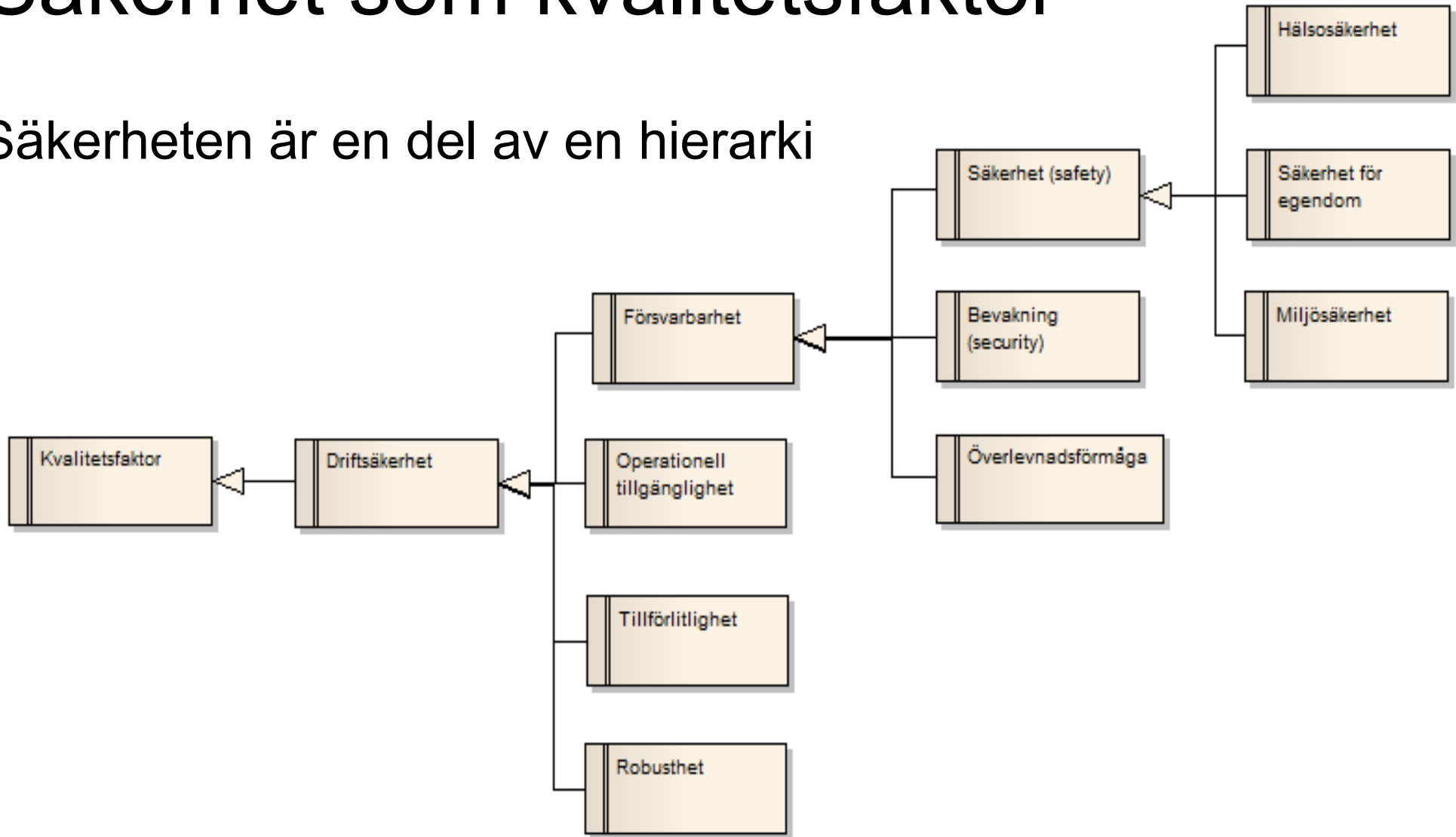
Krav

- **Ett Krav** är något obligatoriskt, externt observerbart, kontrollerbart (t.ex. testbart) och validerbart beteende, datum, egenskap eller gränssnitt.
 - **Ett kvalitetskrav** är ett krav med ett antal kvalitetsfaktorer, underliggande faktorer med kriterier och mätbart data.
 - **Ett säkerhetskrav** är ett kvalitetskrav med ett antal säkerhetsfaktorer, underliggande faktorer med kriterier och mätbart data.
T.ex. "Raffinaderiets styrsystem måste alltid hålla trycket i oljetankarna 30% under deras maximala tryck".



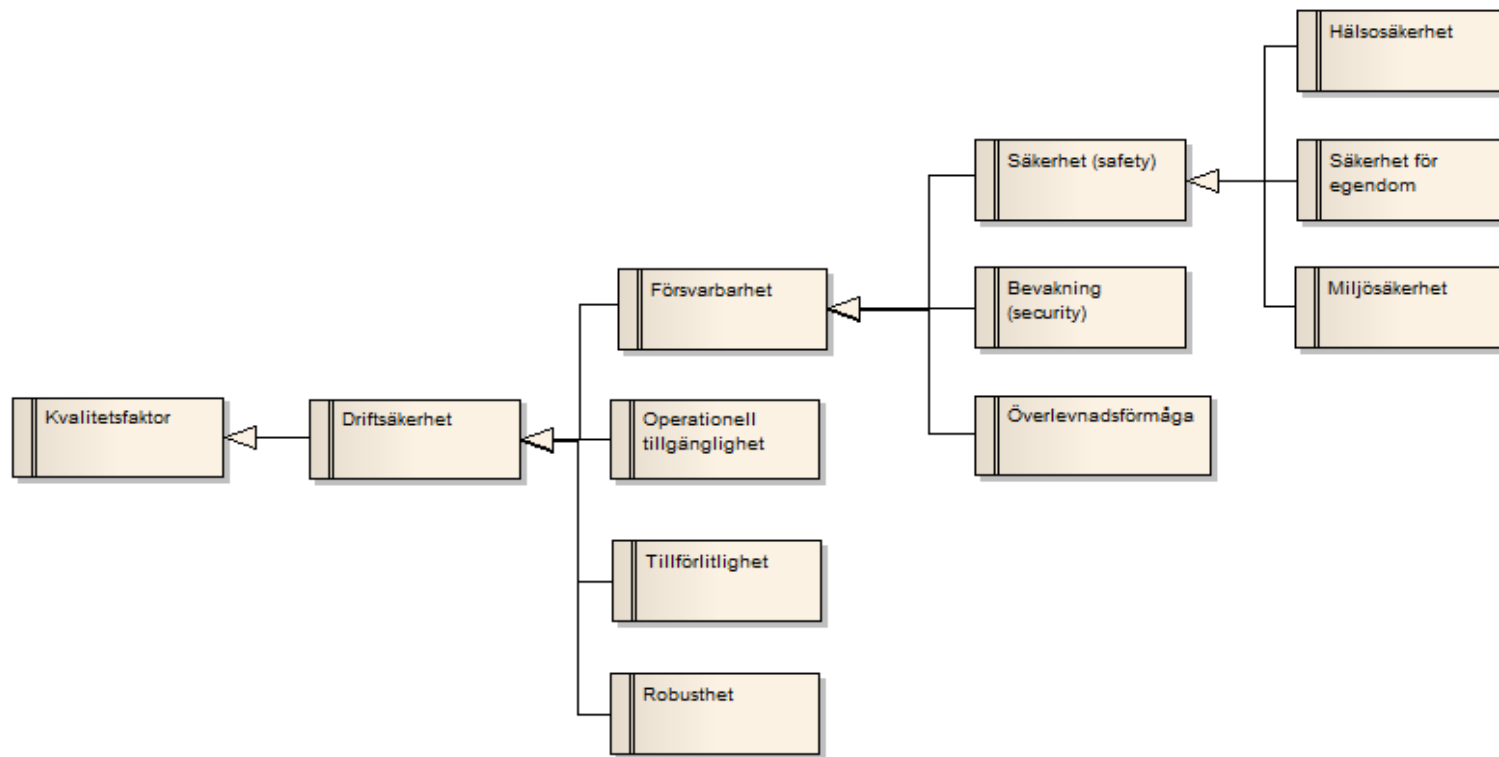
Säkerhet som kvalitetsfaktor

Säkerheten är en del av en hierarki



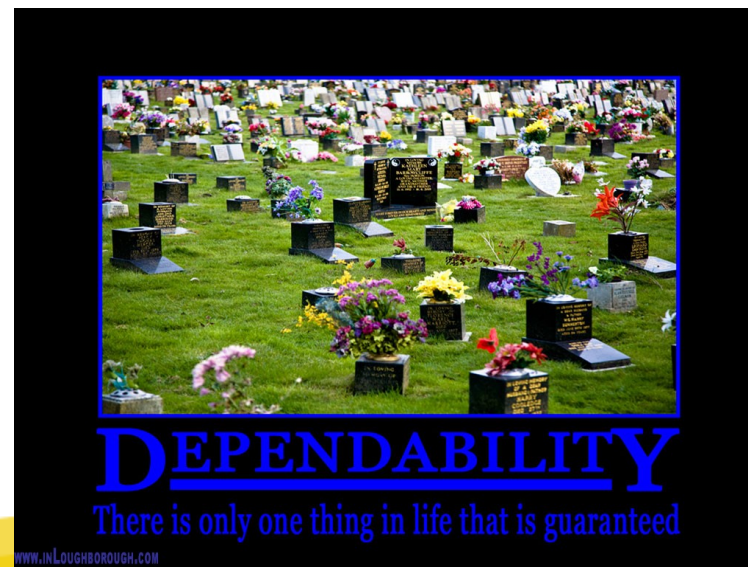
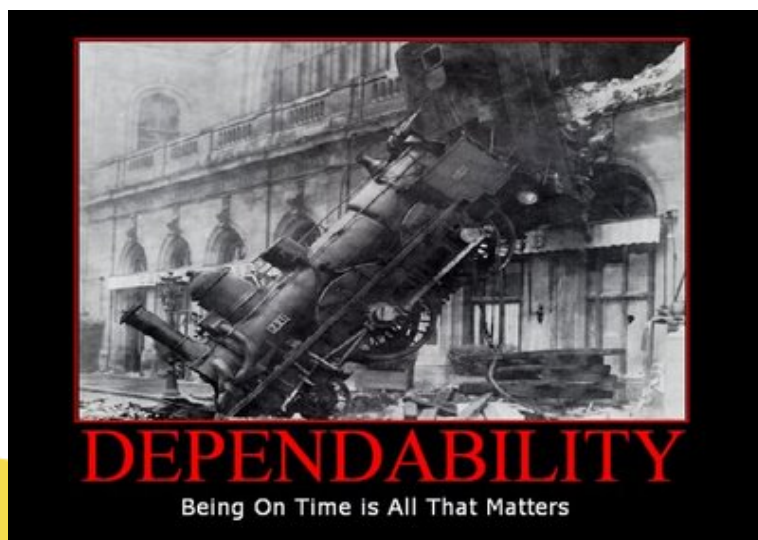
Säkerhet som kvalitetsfaktor

Kvaliteten på säkerhet utgörs av kraven på driftsäkerhet och försvar etc, säkerhetsfaktorers krav!



Kvalitetsfaktorn - Tillförlitlighet

- **Tillförlitlighet** (Dependability) är i vilken grad olika typer av användare kan lita på att kunna utföra sin arbetsuppgift.
 - Försvar (Defensibility) är i vilken grad systemet kan försvara sig självt mot faror, hot och olyckor(fel)
 - Säkerhet (Safety) är i vilken grad oavsiktlig skada hanteras t.ex. förhindras, identifieras, reaktion, anpassning



Kvalitetsfaktorn - Hälsosäkerhet

- **Hälsosäkerhet** (Health safety) är i vilken grad sjukdom, skada och död förhindras, upptäckas och hanteras. Hälsosäkerhet involverar alla människor som rimligen kan förväntas att skadas av systemet under en olycka
 - Till exempel, hälsosäkerhet för ett fordons styrsystem kan omfatta förare, passagerare, fotgängare och mekanik.



Exempel på säkerhetskrav

Underliggande säkerhetsfaktor	Exempel på Säkerhetskrav
Skadeskydd	Flygplatsens automatiserade tunnelbana får inte skada passagerarna så att sjukhusvård krävs med i genomsnitt mer än 0,000 000 1 passagerare per resa. (OBS: detta beräknas bli högst cirka 5 skadade passagerare per år.)



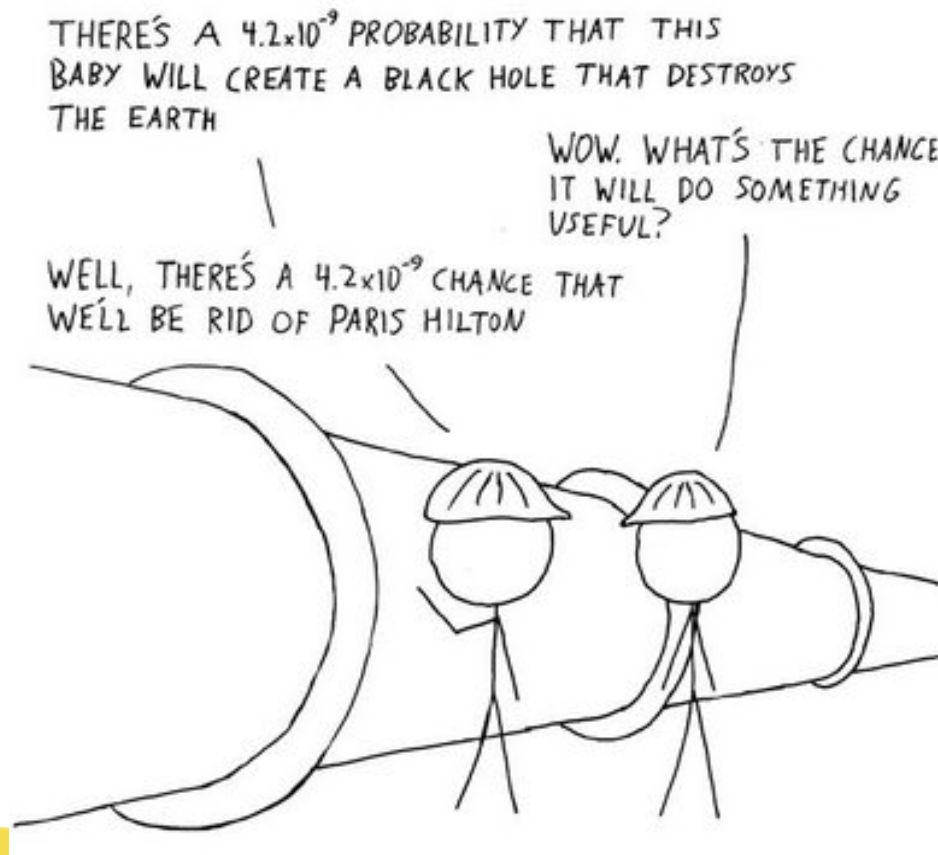
Kvalitetsfaktorn - Säkerhet för egendom

- **Säkerhet för egendom** (Property safety) är i vilken grad skador och förstörelse av egendom förhindras, upptäcks och hanteras. Detta kan inkludera egendom som ingår i systemet och egendom utanför systemet.



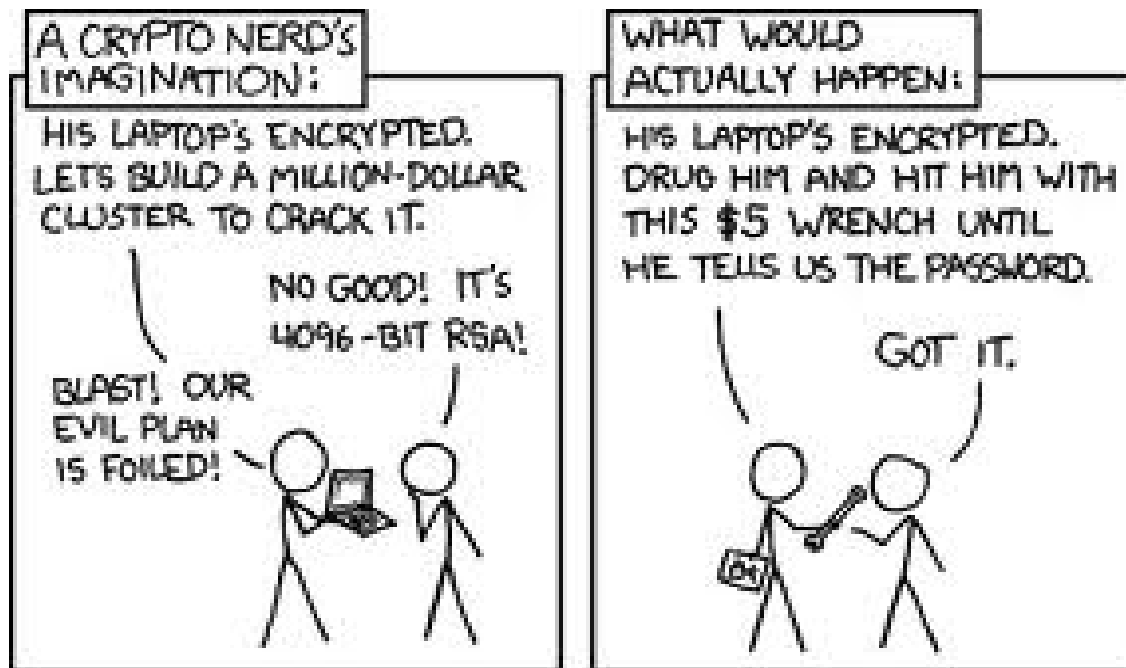
Kvalitetsfaktorn - Miljösäkerhet

- **Miljösäkerhet** (Environmental safety) är i vilken grad oavsiktliga skador och förstörelse av miljön förhindras, upptäcks, och hanteras. Kan vara den omgivning användaren befinner sig och naturen.



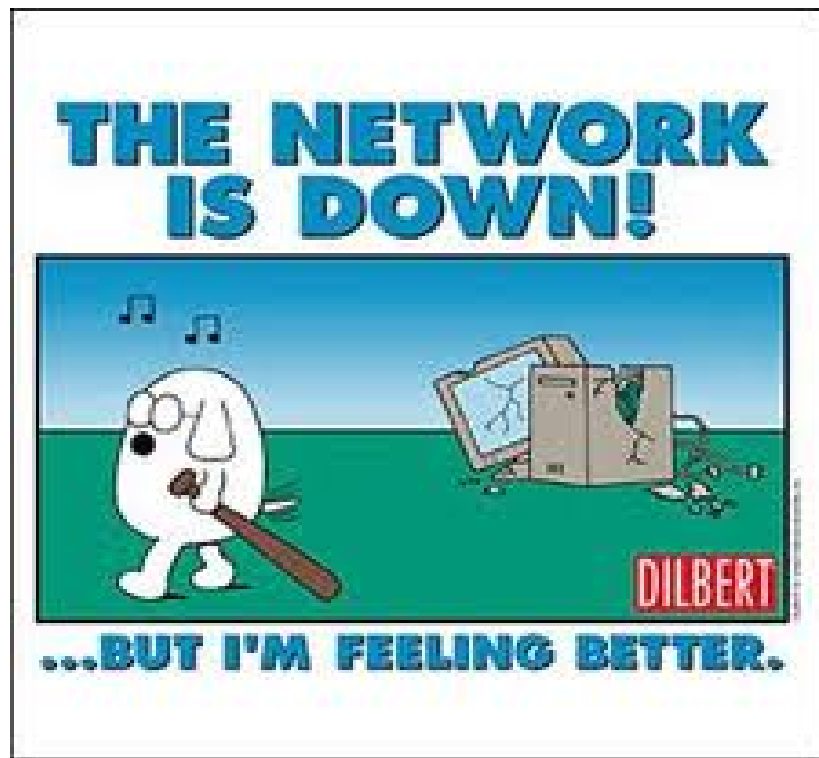
Kvalitetsfaktorn - Bevakning (security)

- **Bevakning (security)** är i vilken grad uppsåtlig skada hanteras T.ex. förhindras, identifierats, reagerar på, och anpassade till



Kvalitetsfaktorn - Överlevnadsförmåga

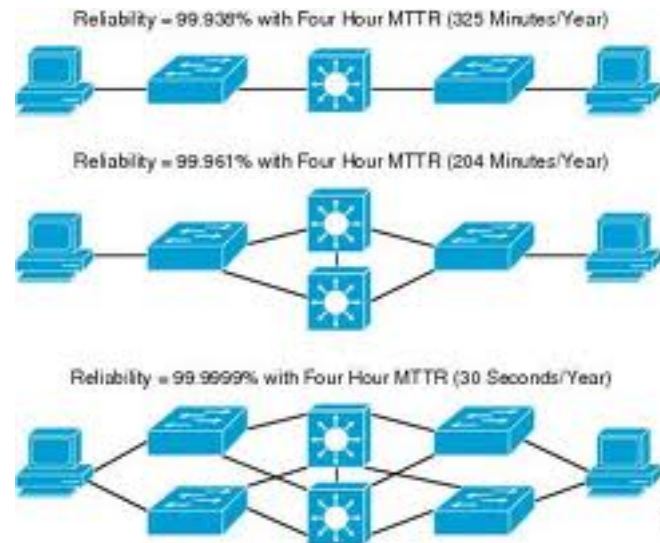
- **Överlevnadsförmåga** (Survivability) är i vilken grad nödvändiga verksamhetskritiska tjänster kan fortsätta att tillhandahållas trots antingen oavsiktlig eller avsiktlig skada



Kvalitetsfaktorn - Operativ tillgänglighet

- **Operativ tillgänglighet** (Operational availability) är i vilken grad systemet är i drift och tillgängligt för användaren

**24 Hours
A Day**
**7 Days A
Week**



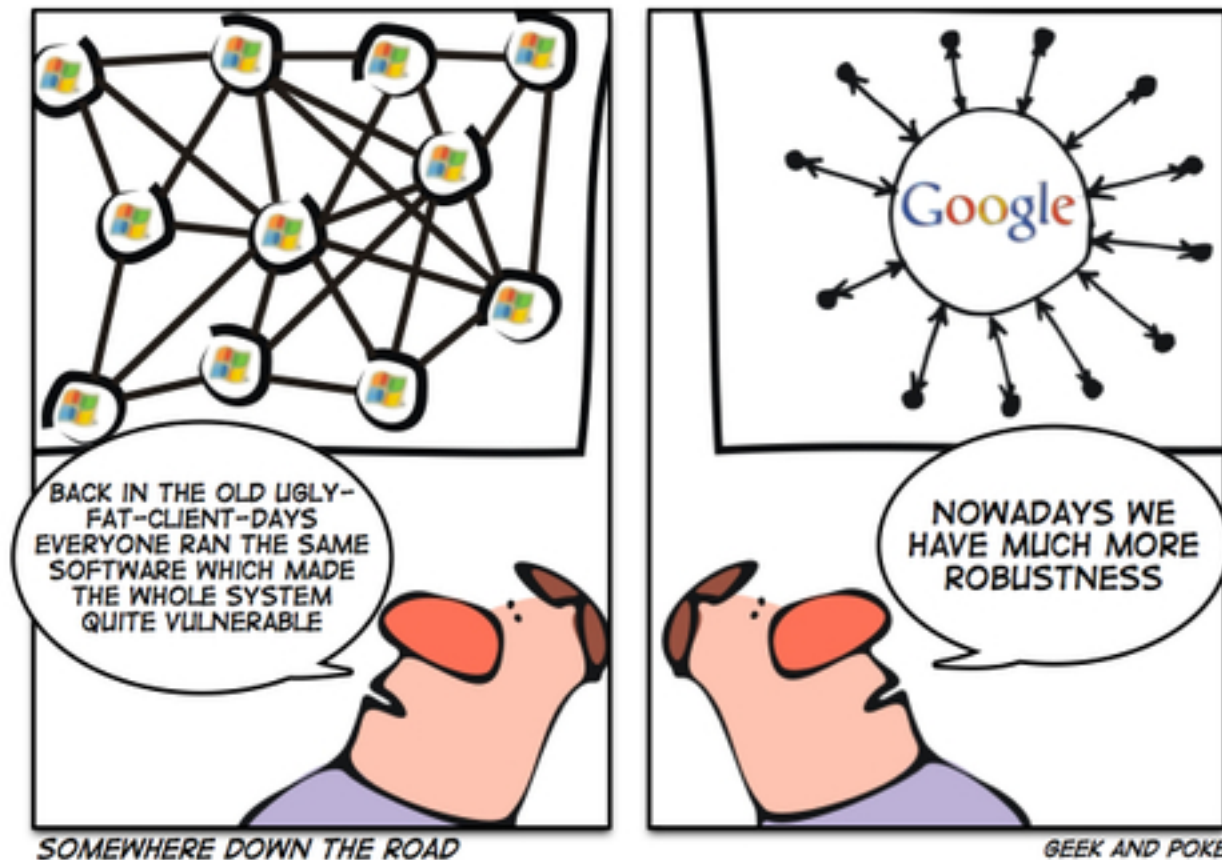
Kvalitetsfaktorn - Pålitlighet

- **Pålitlighet** (Reliability) är i vilken grad systemet fungerar utan fel under givna normala förhållanden under en given tidsperiod.



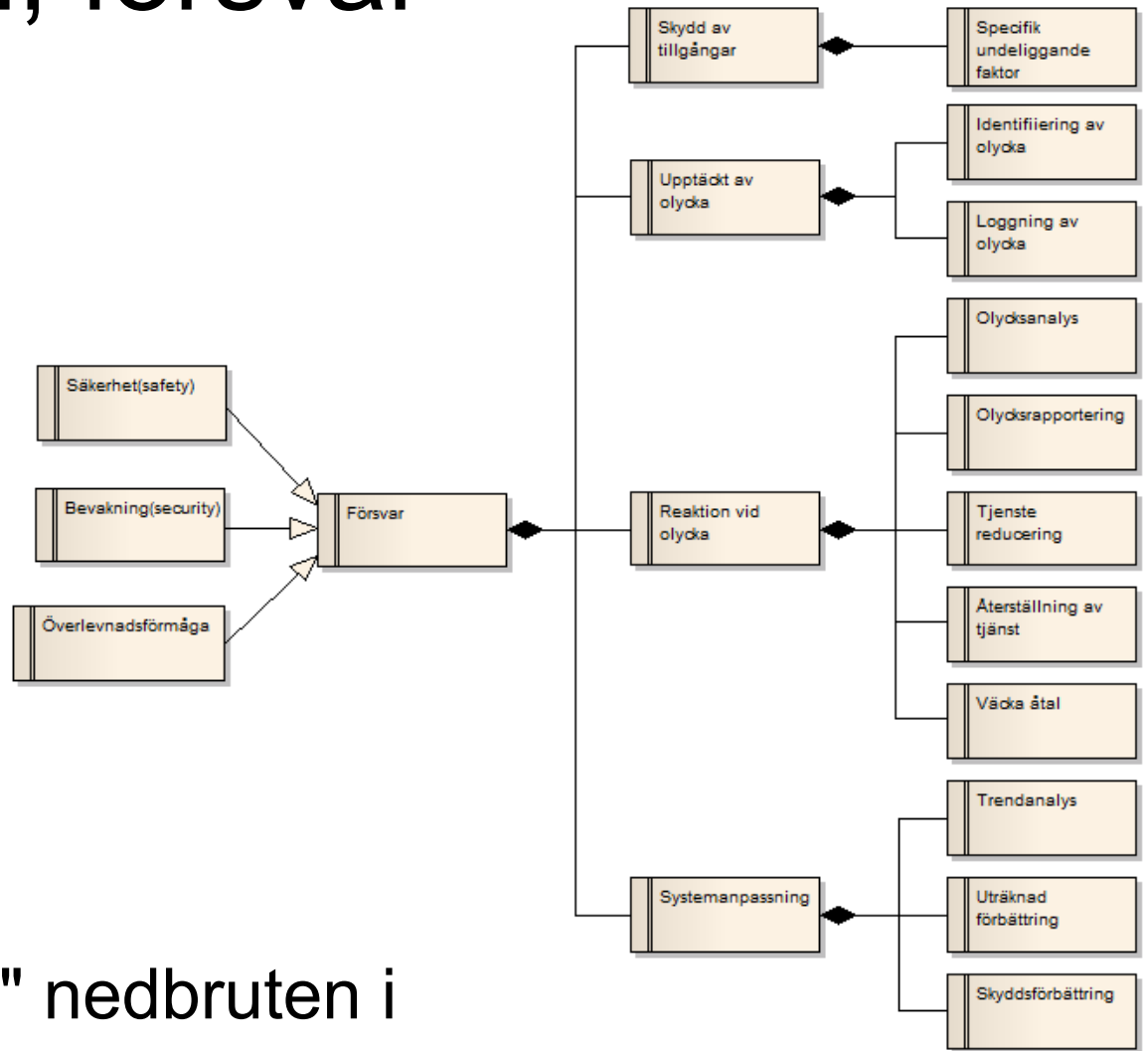
Kvalitetsfaktorn - Robusthet

- **Robusthet** (Robustness) är i vilken grad systemet fortsätter att fungera under onormala förhållanden, t ex felaktigt data eller error



Den gemensamma underliggande kvalitetsfaktorn, försvar

Genom att skapa en hierarki av underliggande faktorer kan en checklista skapas för att se om det saknas några säkerhetskrav

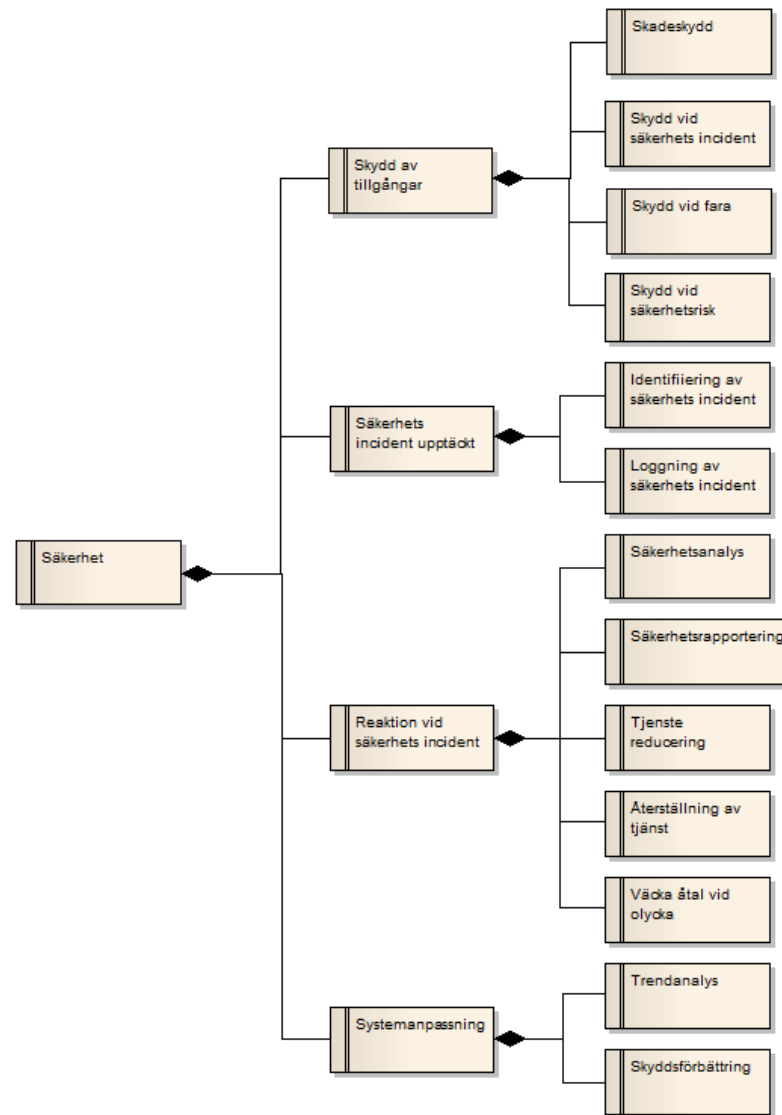


Kvalitetsfaktorn "försvar" nedbruten i underliggande gemensamma kvalitetsfaktorer



Gemensamma kvalitetsfaktorer på säkerhet

Säkerhet ärver de gemensamma kvalitetsfaktorerna men har också specifika faktorer för säkerhet



Underliggande kvalitetsfaktorer

- **Skydd av tillgångar** är i vilken grad värdefulla tillgångar skyddas.
 - **Skadeskydd** är i vilken grad risken för skada på tillgångar elimineras eller minskas.
 - **Skydd vid säkerhetsincident** är i vilken grad risken för säkerhetsincidenter elimineras eller minskas
 - **Olycksskydd** är i vilken grad risken för olyckor elimineras eller minskas.
 - **Skydd mot olycksrisk** är i vilken grad risken för olyckstillbud elimineras eller minskas.



Underliggande kvalitetsfaktorer

- **Skydd vid fara** är i vilken grad risken för faror elimineras eller minskas
- **Skydd vid säkerhetsrisk** är i vilken grad risken för säkerhetsrisker elimineras eller minskas.

Underliggande säkerhetsfaktor	Exempel på Säkerhetskrav
Skydd vid fara	Flygplatsens automatiserade tunnelbanetåg får inte börja röra på sig när dörrarna fortfarande är öppna mer än en gång per år.



Underliggande kvalitetsfaktorer

- **Säkerhetsincident upptäckt** är i vilken grad säkerhetsincidenter eller olyckshändelser känns igen så systemet kan reagera på rätt sätt. t ex meddela operatörer, säkerhetspersonal, upprätthålla kritiska tjänster ...
 - **Säkerhetsincident identifiering** är i vilken grad olyckor och tillbud identifieras när de uppstår.
 - **Säkerhetsincident loggning** är i vilken grad relevant information om tillbudet loggas när säkerhets incidenter inträffar



Exempel på säkerhetskrav

Underliggande säkerhetsfaktor	Exempel på Säkerhetskrav
Säkerhets incident upptäckt	Flygplatsens automatiserade tunnelbanesystem måste i 99,99% av fallen upptäcka när ett tåg är i rörelse med sina dörrar öppna.



Underliggande kvalitetsfaktorer

- **Reaktion vid säkerhetsincident** är i vilken grad systemet återhämtar sig efter en säkerhetsincident.
 - **Analys av säkerhetsincident** är i vilken grad händelsen loggas och analyseras.
 - **Incidentrapportering** är i vilken grad loggade och eventuellt analyserade händelser rapporteras.



Exempel på säkerhetskrav

Underliggande säkerhetsfaktor	Exempel på Säkerhetskrav
Incident-rapportering	Flygplatsens automatiserade tunnelbanesystem skall rapportera förekomster av identifierade säkerhetsincidenter till säkerhetsansvarig minst 99,999% av tiden.



Underliggande kvalitetsfaktorer

- **Tjänstereducering** är i vilken ordning systemtjänster stängs av till följd av en olycka. T.ex. att stödjande tjänster försvinner innan viktiga tjänster.
- **Återställning av tjänst** är i vilken grad systemets tjänster omedelbart återställs efter att ha stängts på grund av en olycka.
- **Väcka åtal vid olycka** är i vilken grad lagöverträdelse är orsak till olyckan. Detta är mer en trygghets faktor än en säkerhetsfaktor men kan ändå vara aktuellt då grov vårdslöshet orsakar allvarlig skada



Underliggande kvalitetsfaktorer

- **Systemanpassning** är i vilken grad systemet anpassar sig (baserat på tidigare tillbud) så att det i framtiden kan skydda sig bättre.
 - **Trendanalys** är i vilken grad systemet spårar trender när det gäller förekomst och verkan av säkerhetsincidenter.
 - **Skyddsförbättring** är i vilken grad systemet förbättrar säkerhetsåtgärder som en följd av tidigare tillbud och resultatet av trendanalys.



Olyckor inträffar när systemet gör fel saker eller gör rätt sak vid fel tidpunkt eller i fel ordning.

Programvara kan inte orsaka dessa olyckor av sig självt.

Programvara orsakar bara olyckor i gränssnittet med hårdvara (t.ex. kontrollerar ställdon, kommunicerar med andra system) eller när det tillhandahåller felaktig information (t.ex. felaktiga eller inaktuella uppgifter) till människan.



Frågor?

torbjorn.andersson@inceptive.se



References

- Donald G. Firesmith: “Engineering Safety Requirements, Safety Constraints, and Safety-Critical Requirements”, in Journal of Object Technology, vol. 3, no. 3, March-April 2004, pp. 27-42. http://www.jot.fm/issues/issue_2004_03/column3
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.6736&rep=rep1&type=pdf>
- Verkt yg f or b ttre kvalitet p  krav: www.hood-group.com en plug-in till word som heter DESIRe



Thank You!



torbjorn.andersson@inceptive.se