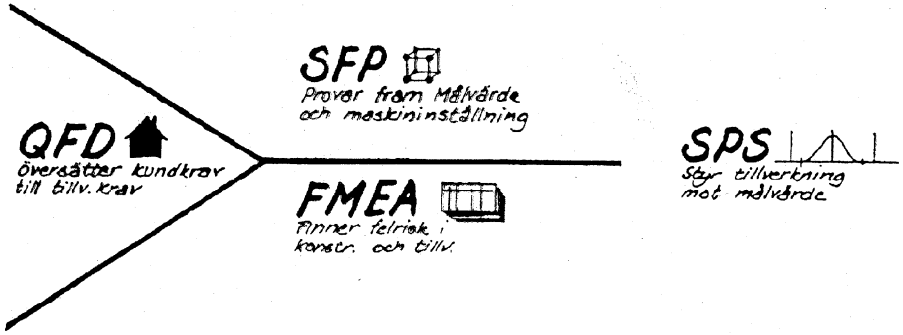
STÄNDIG KVALITETSFÖR-
BÄTTRING ÄR INTE NÖD-
VÄNDIG

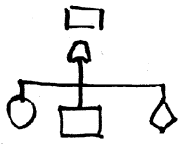
ALLA FÖRETAG BEHÖVER
INTE ÖVERLEVA

VÄGEN TILL NÖJD KUND

* RÄTT FRÅN BÖRJAN
* STÄNDIGA FÖRBÄTTRINGAR



FTA (PSA)



redundans
Säkerhets-
kritiskt
sannolikhets-
uppskattningar

- Lär känna din process/system
- Gör det väl eller inte alls

FTA = Fault Tree Analysis =
PSA = Probabilistic Safety Assessment

TÄNK EFTER FÖRE

kreativitet ⟷ systematik
(brainstorm) (kom ihåg)

rutin ⟷ slentrian
(lär av erfar-
enheter)

benchmarking, "mentor"

kräver resurser, tid, uthållighet

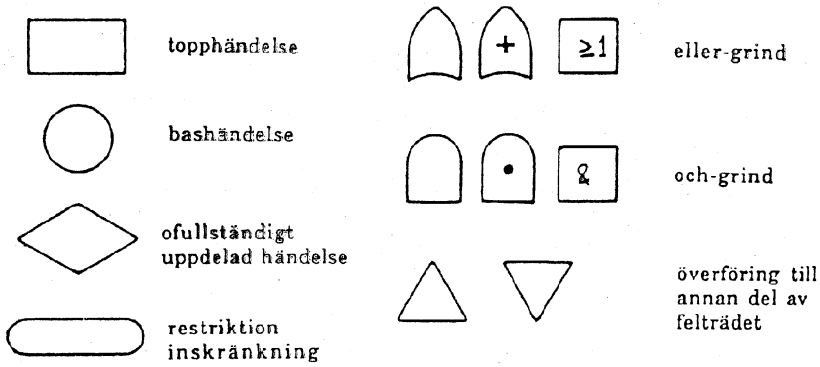
gör det bra, eller inte alls

ÖKAD FÖRSTÅELSE AV
SYSTEM + PROCESSER

Felträdsanalys (B&K kap 18)
(HQR avsn. {3.6 / 4.4})

redundanta system
multipla fel
sannolikhetsberäkning
säkerhetskritiska funktioner

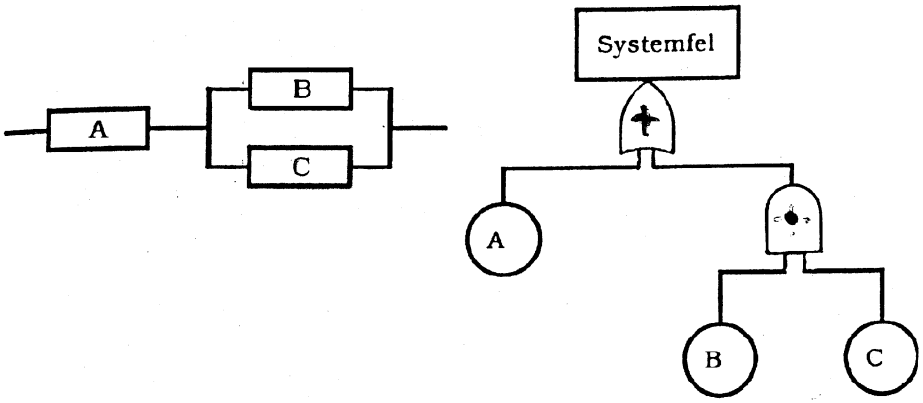
- ökad förståelse av systemet
- finna svaga punkter
- jämföra alternativa konstruktioner
- beräkna sannolikheter ?



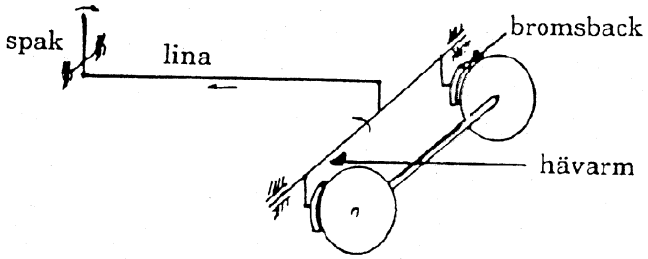
Figur 18.1 De vanligaste symbolerna i felträdsanalysen.

Top down: Börja med icke önskvärd topphändelse, tänk successivt ut orsaker

många av de praktiska synpunkterna [redacted] från FMEA är också tänkvärda i FTA

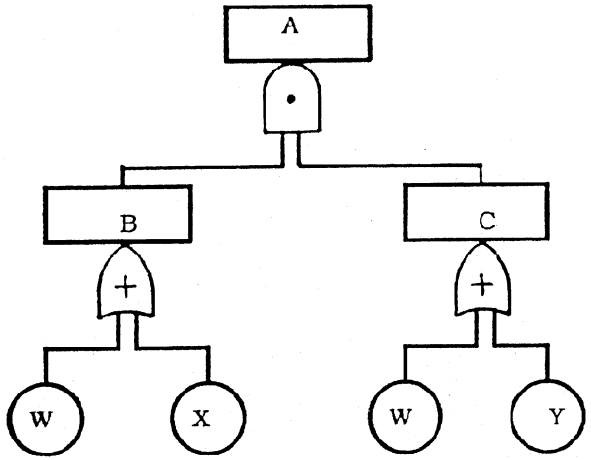


Figur 18.3 Jämförelse mellan tillförlitlighetsblockschema och felträd.

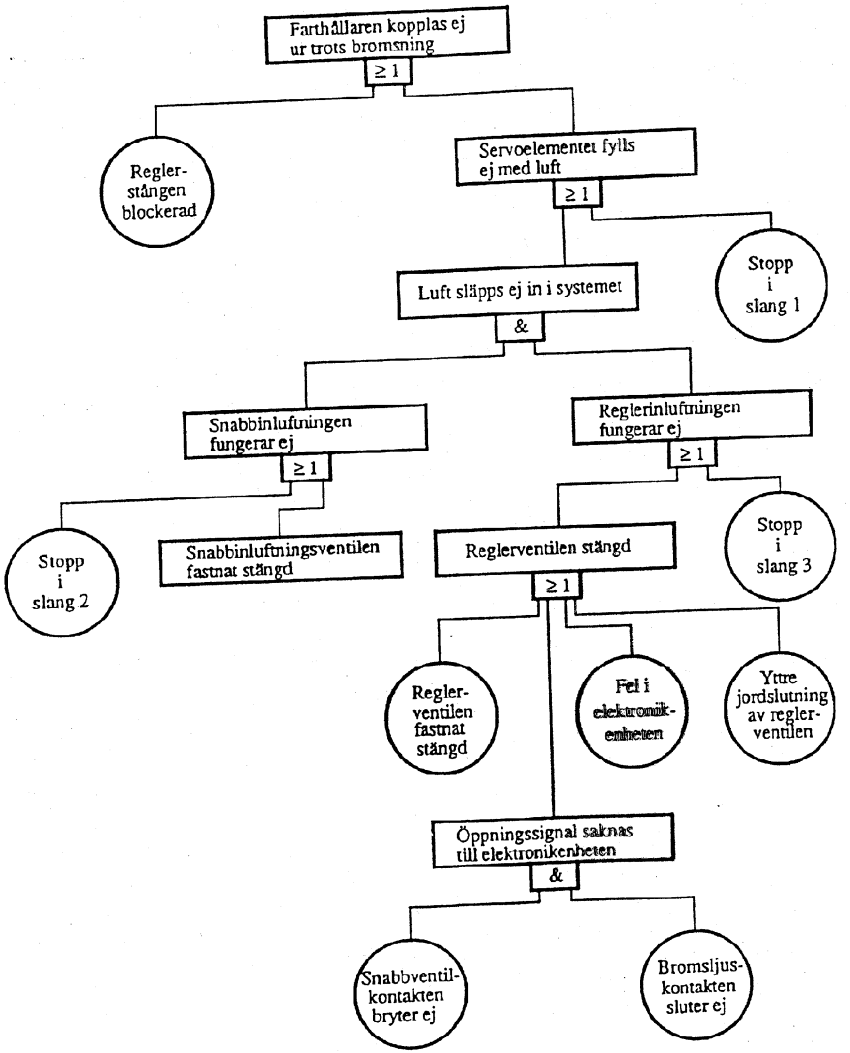


Figur 18.4 Illustration av ett handbromssystem. (Från Schnittger, 1972.)

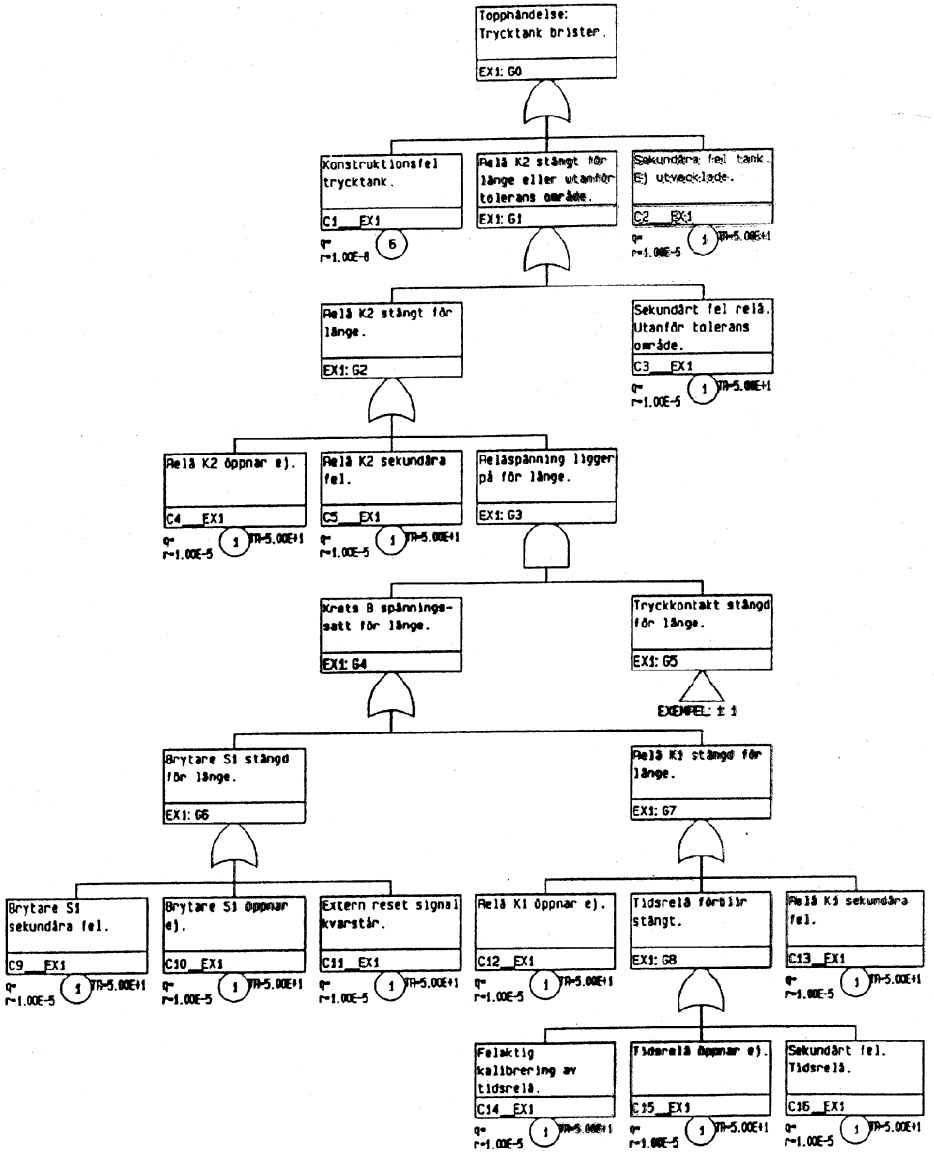
A: Ingen bromsverkan
B: Ingen bromsverkan på vänster hjul
C: Ingen bromsverkan på höger hjul
X: Vänster bromsback sliten
Y: Höger bromsback sliten
W: Bromslinan är av



Figur 18.5 Felträd över bromssystemet i figur 18.4.



Figur 18.6 Felträd över topphändelsen "Farthållaren blir inte urkopplad vid inbromsning". Felträdet ingår i en säkerhetsanalys av en viss typ av farthållare, som förutom elektronik innehåller mekanik och pneumatik. Analysen är utförd av FOA på uppdrag av Trafik-säkerhetsverket. (Från Gunnerhed, 1988)



Figur 18.8 *Felträd ritatt med programmet **RISK SPECTRUM** utvecklad av RELCON Teknik AB. Topphändelsen är "spricka i trycktanken" hos en kärnkraftsreaktor.*

avbrott = mängd av händelser som gör att topphändelsen inträffar

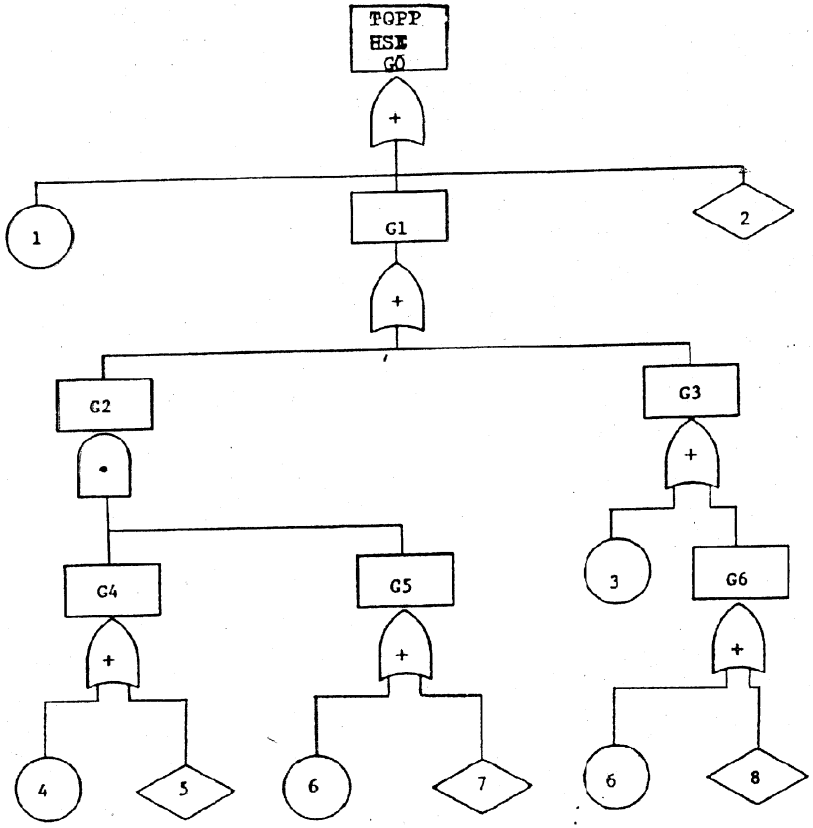
minimalt avbrott = avbrott där alla händelserna "behövs"

avbrott = cut set

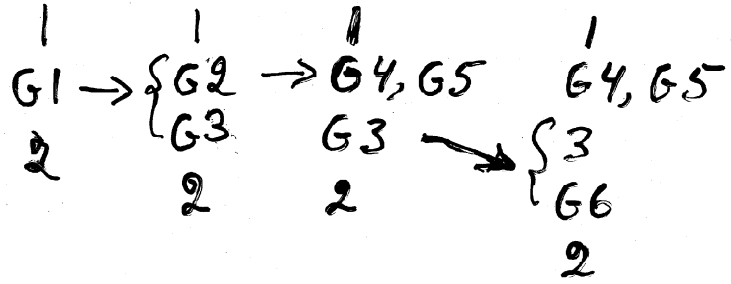
väg = mängd av händelser som gör att topphändelsen inte inträffar

minimal väg = väg där alla händelserna behövs

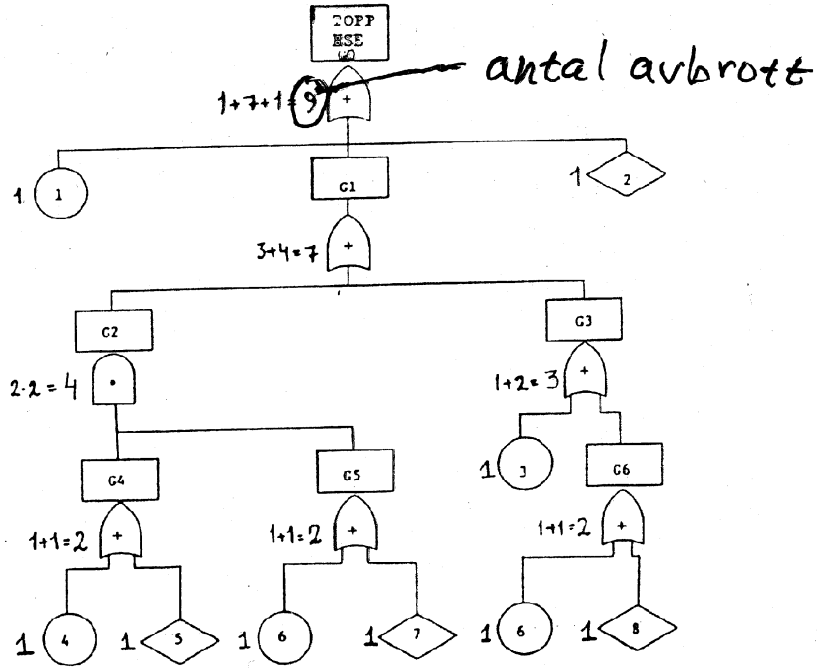
väg = path set



MOCUS-algoritmen



Beräkning av totalt antal avbrott (kontroll att man inte glömt bort något)



kvalitativ bedömning

- händelser som finns med i många minimala avbrott är "farliga"
- minimala avbrott med få händelser är "farligare" än minimala avbrott med många händelser

"farligare"

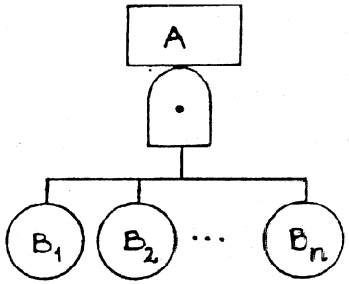
- mänskligt felhandlande
- fel i aktiva system
- fel i passiva system

"gå igenom" alla avbrott (om möjl.)

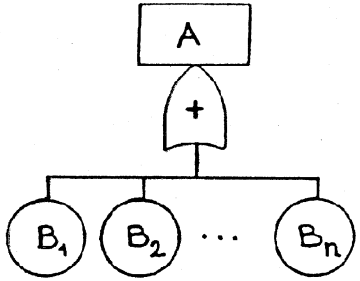
g'

ev. FMEA på viktiga dubbelfel och trippelfel

kvantitativ bedömning



$P(A) = P(B_1)P(B_2)...P(B_n)$
om $B_1, B_2, ..., B_n$ är oberoende



$P(A) = P(B_1) + P(B_2) + ... + P(B_n)$

t. ex. $m = 2$

$= 1 - P(B_1^* \cap B_2^* \cap ... B_m^*)$

$= 1 - P(B_1^*) \cdot ... \cdot P(B_m^*)$ om oberoende

$= 1 - (1-P(B_1)) \cdot ... \cdot (1-P(B_n))$

$A = B_1 \cup B_2$

$P(A) = P(B_1 \cup B_2) = P(B_1) + P(B_2) - P(B_1 B_2)$

≈ 0 (?)

$[= P(B_1 + B_2)]$

Bokens beteckning

Boken skriver $B_1(t)$, $B_2(t)$, osv.

Boolesk algebra

$A + A = A$ $\qquad$ $A + AB = A$

$AA = A$ $\qquad$ $A + BA = A$

Handbromssystemet

$$A = BC = (W+X)(W+Y)$$
$$= WW + WY + XW + XY$$
$$= W + WY + XW + XY$$
$$= W + XY$$

$$P(A) = P(W) + P(XY) - P(WXY)$$
$$= P(W) + P(X)P(Y) - P(W)P(X)P(Y)$$

t.ex $= 0.01 \quad 0.01 \cdot 0.01 \quad 0.01 \cdot 0.01 \cdot 0.01$ ($\cong 0$)

$\cong 0.0101$

(exakt 0.01001717)

$$P(\text{topphändelse}) \overset{(\leq)}{\cong} \sum_j P(\text{minimalt av } j \text{ brott inträffar})$$

$$\overset{(\leq)}{\cong} 1 - \prod_j (1 - P(\text{minimalt } j \text{ avbrott inträffar}))$$

Simulering

generellt

pekar ut svaga punkter

tidskrävande (Importance Sampling)

CCF = Common Cause Failures
= beroende fel
= "en händelse orsakar flera fel"

tidsberoende (↔ Markov, Petri)

otillräcklig felstatistik

bortglömda händelsekedjor

⇒

beräknade sannolikheter ofta osäkra eller för låga

CAFTAN	Part of the CARA program with modules for FMECA, cause consequence analysis, and life data analysis. CARA is developed by SINTEF Safety and Reliability, N-7034 Trondheim, Norway
SALP-PC	Developed by the Joint Research Centre of the Commission of the European Communities, 21020 Ispra (Varese), Italy
IRRAS	Developed by Idaho National Engineering Laboratory, EG&G Idaho, Inc. Idaho Falls, Idaho 83415
CAFTA	Developed by Science Applications International Corporation, 5150 El Camino Real, Suite C-31, Los Altos, CA 94022
FRANTIC ABC	Developed by Applied Biomathematics, 100 North Country Road, Setauket, NY 11733
Reliability Toolbox	Includes a fault tree analysis program module. Available from Innovative Timely Solutions, 6401 Lakerest Court, Raleigh, NC 27612
Risk Spectrum Fault Tree	Developed by Relcon Teknik AB, Box 1288, S-17206 Sundbyberg, Sweden, also available from Innovative Software Designs, Inc. Two English Elm Court, Baltimore, MD 21228
FaultTree	Developed by OMI Logistics Limited, Item Software, Wellow House, 14 Little Park Farm Road, Fareham, Hampshire, PO15 5TD, England
FaultrEASE	Developed by Arthur D. Little, Inc. Acorn Park, Cambridge, Massachusetts 02140-2390 (available for PC/Windows and Macintosh)