Inledning

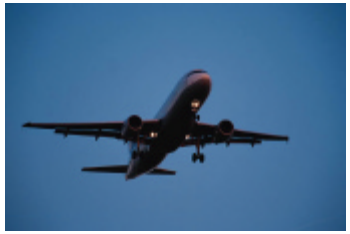
Joakim Ohlsson
CR&T

Tillämpningar

kärnkraft

rymd

försvar

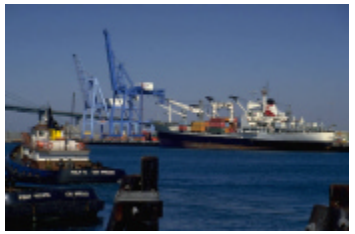


luftfart

medicin

bilar

järnvägar



sjöfart

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

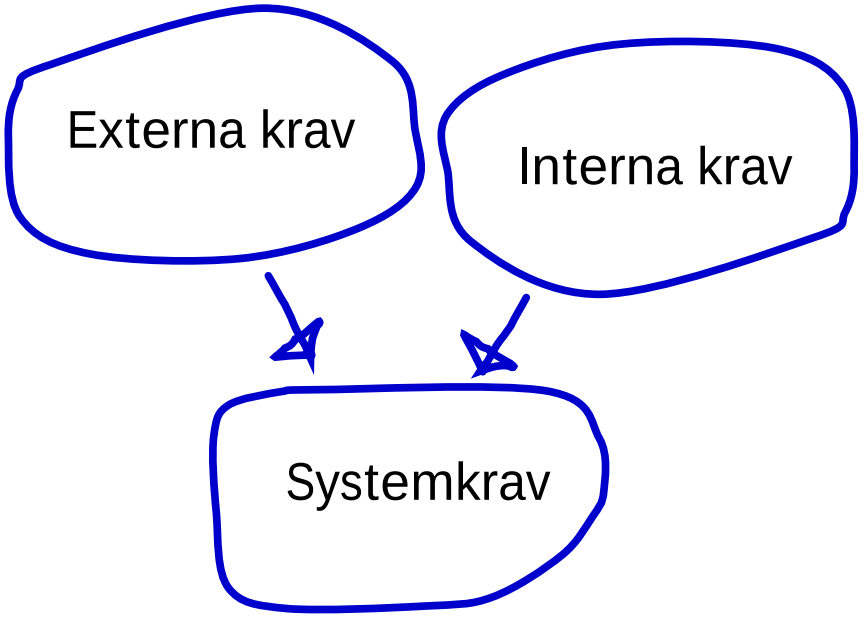
Likheter och skillnader

- Stora skillnader:

Jämförelsepunkt	Nyckelord
kravbild	explicit - implicit
riktlinjer och standarder	styrande - vägledande
verifiering	test - analys
felstatistik baserat på fältdata	få system – många system

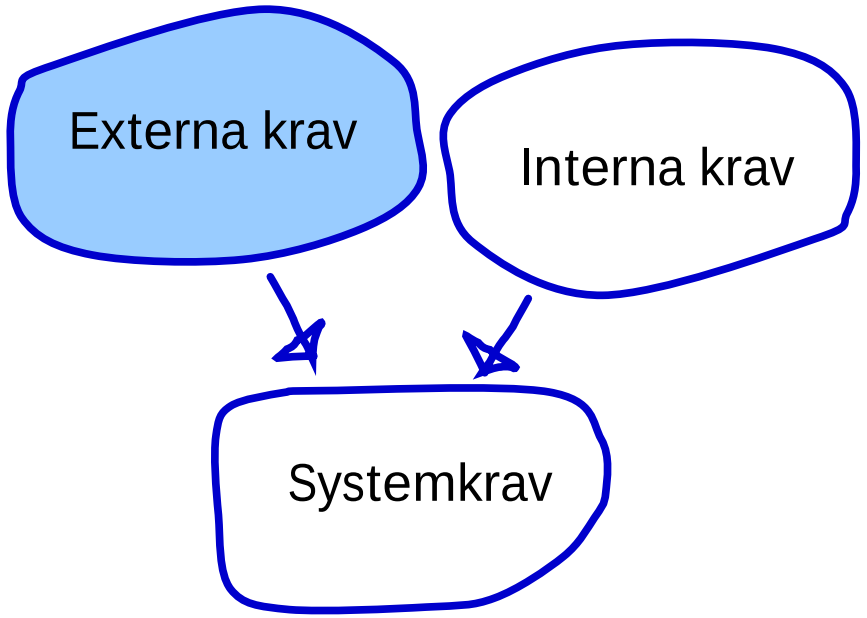
- men ändå många likheter:
  - komplex programvara och elektronik
  - liknande krav
  - likheter i tillämpningarna

Kravidentifiering



Kravidentifiering

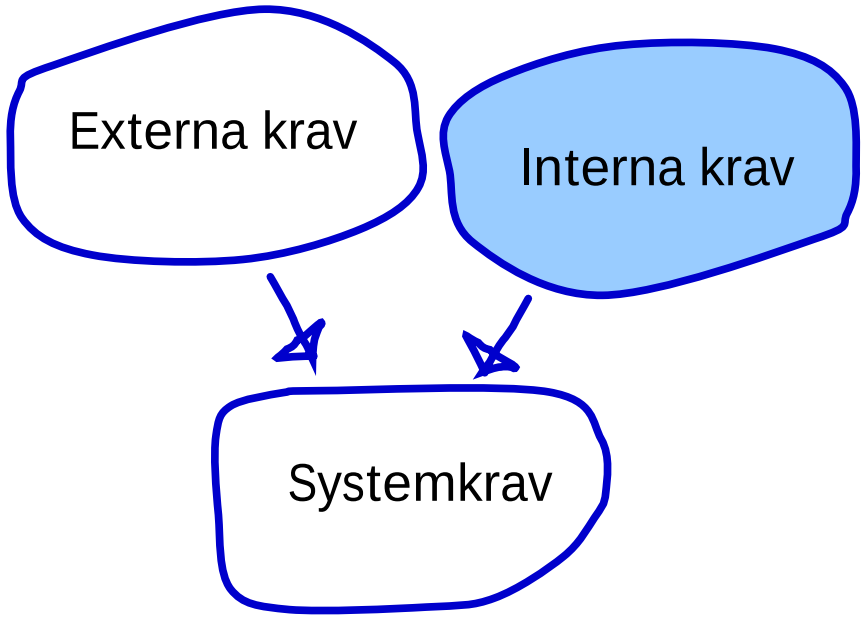
- myndighetskrav
  - produktsäkerhet
- praxis
  - riktlinjer
- ALARP
  - produktansvar



CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Kravidentifiering

- Image
  - ”säker”
- Olycksstatistik
  - ”lika bra”
- utvecklings- och enhetskostnader
  - begränsade resurser
- Efterkostnader
  - domstol
- Exponering
  - antal system ute



Standarder och riktlinjer

- Ramverk
  - kravställning
    - risk matrix, safety integrity etc
  - design
    - kodningsregler etc
  - verifiering
    - hazard & risk analysis

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Standarder och riktlinjer

ECS-Q-40A
Safety

DO-178B
AMJ 25.1309

MISRA
Guidelines

IEC 60880

IEC 61508

CENELEC EN
50126/7/9

IEC 60601

MIL-STD-882D
UK MoD 00-54/55/56
H SystSäk
H ProgSäk

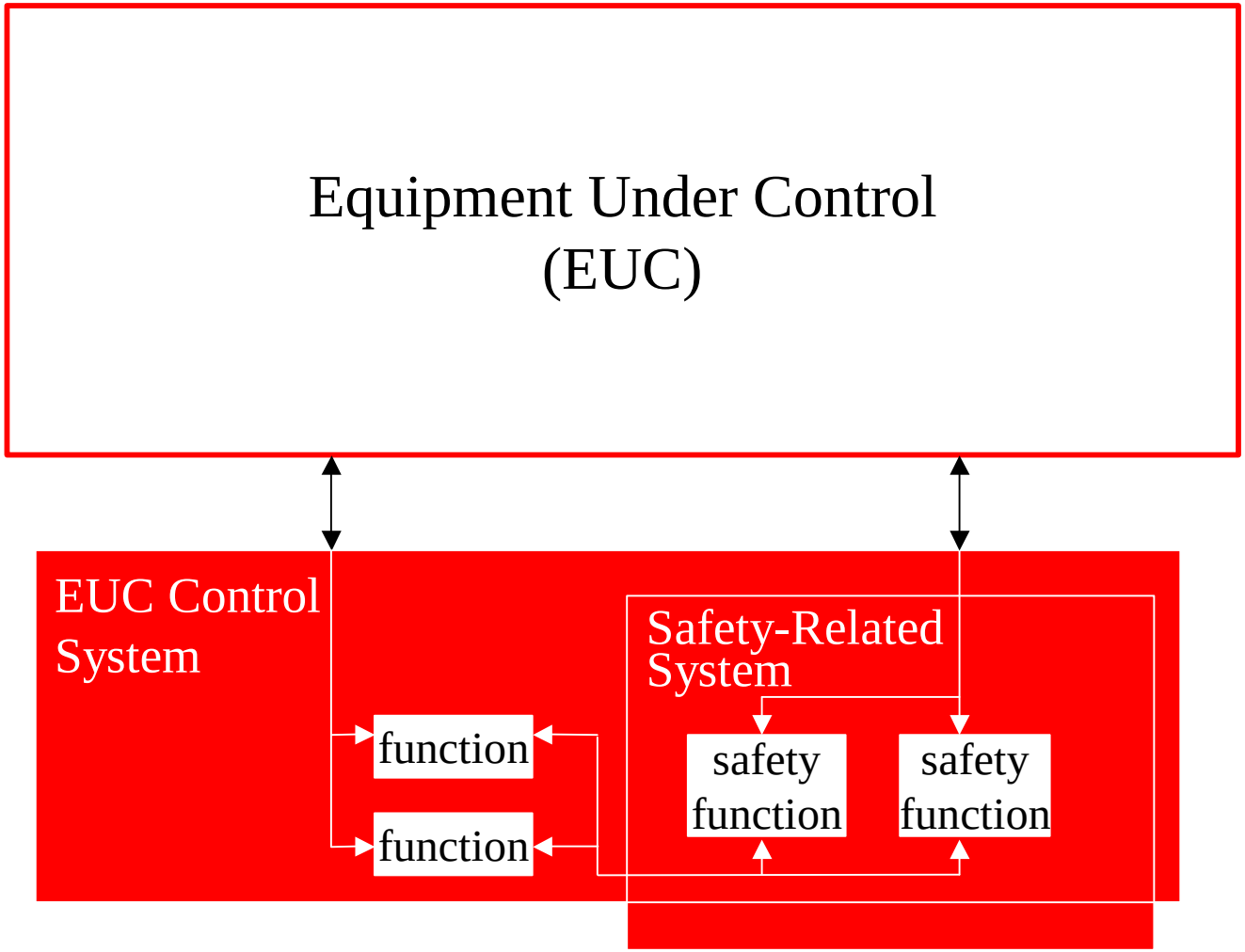
SJÖFS

IEC 61508

- Introducerar/definierar begrepp
  - safety function
  - safety integrity
  - risk reduction

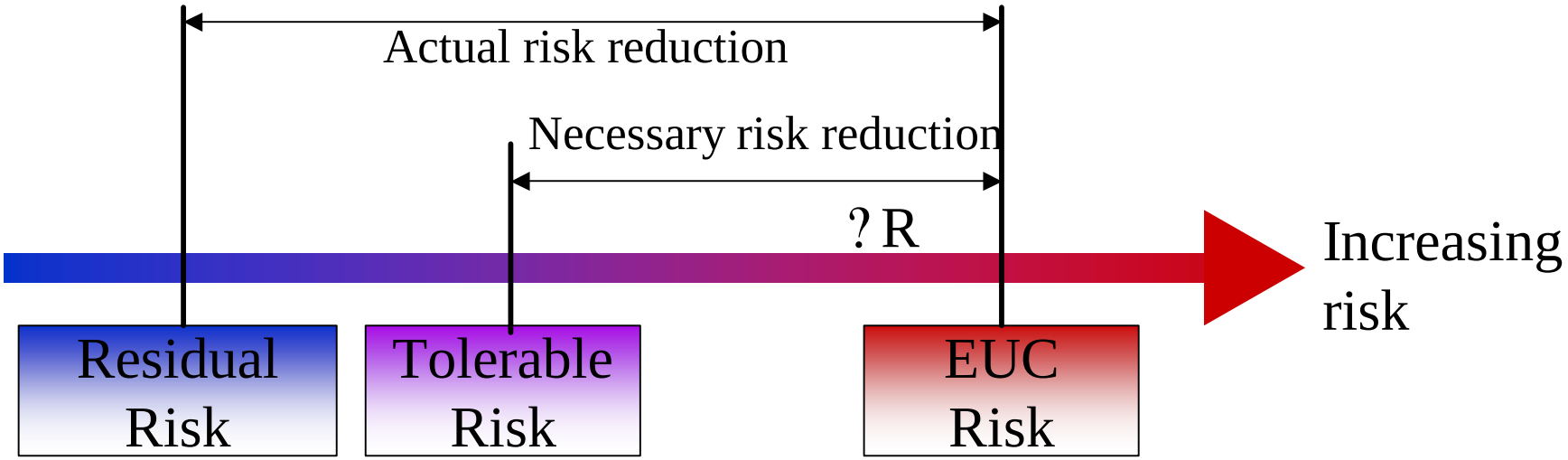
CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

IEC 61508


Equipment Under Control
(EUC)
EUC Control System
function
function
Safety-Related System
safety function
safety function

IEC 61508

- Risk Reduction



IEC 61508

- Kvantitativa krav

Safety Integrity Level	Low demand mode of operation	High demand or continous mode of operation
4	$<10^{-4}$	$<10^{-8}\ h^{-1}$
3	$<10^{-3}$	$<10^{-7}\ h^{-1}$
2	$<10^{-2}$	$<10^{-6}\ h^{-1}$
1	$<10^{-1}$	$<10^{-5}\ h^{-1}$

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

IEC 61508

– Software safety requirements specification

Technique/Measure	SIL1	SIL2	SIL3	SIL4
Computer-aided specification tools	R	R	HR	HR
Semi-formal methods	R	R	HR	HR
Formal methods for example CCS, CSP, HOL, LOTOS, OBJ, temproal logic, VDM and Z	-	R	R	HR

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Verifiering

- Dynamisk test
  - structural/functional coverage
  - certification tests
- Statisk analys
  - designgranskning
  - felprediktering baserat på t ex MIL-HDBK-217F

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Certification Tests

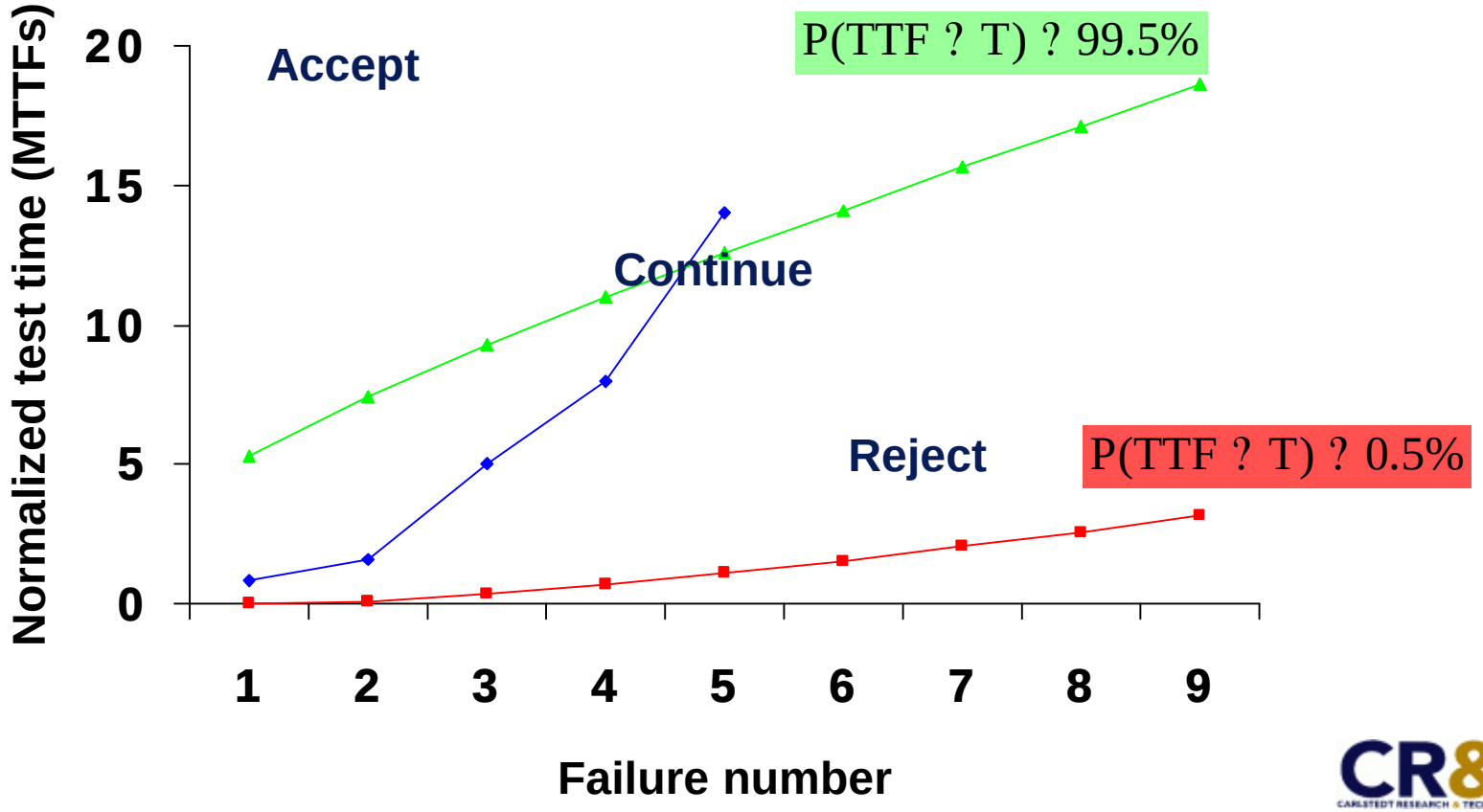
- Oberoende av felmodell
  - relevant testprofil
  - oförändrat system
- Krävd felfri testtid (ex)

Felintensitet	testtid i timmar	
	c=99%	c=99.99%
10^{-6} h^{-1} (IEC 61508 SIL1)	4.6?10^{6}	9.2 ?10^{6}
10^{-7} h^{-1} (IEC 61508 SIL2)	4.6?10^{7}	9.2 ?10^{7}
10^{-8} h^{-1} (IEC 61508 SIL3)	4.6?10^{8}	9.2 ?10^{8}
10^{-9} h^{-1} (IEC 61508 SIL4)	4.6?10^{9}	9.2 ?10^{9}

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Certification Tests

- Krävd testtid givet att R fel inträffar



Incidentuppföljning

- Felprediktering baseras normalt på
  - data från komponentleverantörer
  - felprediktionsmodeller (t ex MIL-HDBK 217F)
  - egna data (oftast på systemnivå)

- Vilken är mest tillförlitlig?

CR&T
CARLSTEDT RESEARCH & TECHNOLOGY AB

Incidentuppföljning

- Egen data är bäst
  - om datainsamlingen är väldefinierad