

Bidrag fra intermitterende fejl til hyppigheden af farlig fejl i et system opbygget med composite fail-safety.

1.1 Formål

Dette dokument skal være et oplæg til diskussion af, om man kan tage vare på sikkerheden (styre hyppigheden af farlig fejl) i et composite fail safe system med de "normalt" anvendte metoder for at sikre sig mod permanente fejl. Det skitseres hvorledes, man ved at gøre nogle forudsætninger om intermitterende fejls natur, kan vise, at "man bare kan regne, som man plejer".

Dette dokument forudsætter nogen baggrundsviden om failsafe systemer og de bekymringer, som har ført til nedenstående overvejelser.

1.2 Indledning

Løst formuleret er problemstillingen følgende:

Et composite fail safe system er to kanals og designes til at kunne detektere fejl i hver kanal ved at udføre en periodisk test i kanalerne enkeltvis eller ved at sammenligne information (interne tilstande eller output) mellem de to kanaler. Kun når kanalerne er fejlfrie, og output fra de to kanaler er ens, vil objekter i den ydre verden blive styret til en anden end deres sikre tilstand.

Når fejl i en kanal detekteres, bringes systemet hurtigt og irreversibelt til en sikker tilstand. I den tid der går fra 1. fejl opstår i den ene kanal, og til den detekteres, og systemet derefter bringes i sikker tilstand, er der mulighed for, at en "tilsvarende" fejl opstår i den anden kanal, således at det resulterer i fejlagtig og farlig output fra systemet.

I forbindelse med intermitterende fejl kunne man tænke sig at detektionstiderne for fejl kunne blive meget lange og at hyppigheden af farlig fejl derfor kunne blive uacceptabel stor. Hvis det er tilfældet kan systemet ikke opfylde sikkerhedskravet formuleret som en maksimal værdi af hyppighed af farlig fejl, som følge af random fejl.

To problemstillinger kunne være interessante at undersøge lidt nærmere.

Den første drejer sig om farlige fejl opstået som en kombination af en intermitterende fejl og en permanent fejl eller to intermitterende fejl.

Hvis en fejl i en kanal er intermitterende, således at fejlen er aktiv i korte tidsrum i forhold til tiden mellem to periodiske tests, kan man forestille sig, at fejlen ikke vil blive detekteret, og at man blot skulle vente på at en fejl (intermitterende eller permanent) i den anden kanal opstod, og at fejlene blev aktive samtidig, hvorefter det ville føre til farlig fejl. Denne problemstilling behandles i afsnit 1.4.

Den anden problemstilling der er en variant af problemet kan opstå, hvis en fejl (F1) kan skjule andre fejl. F1 bringer output til sikker side (fail safe). F.eks. kunne "Passiv" eller "Nul" være sikkert output. Hvis F1 er permanent og fail safe behøver den ikke at være detekterbar på anden måde end som funktionsfejl, næste gang output skulle have været "Aktiv" eller "Een". Fejlen har jo uden videre foranstaltninger bragt systemet irreversibelt til en sikker tilstand¹.

¹ Bemærk at systemet stadig kan betragtes som et composite fail safe system. Fejlen bliver detekteret og negeret umiddelbart (uden tidsforsinkelse).

Men hvis F1 kan "forsvinde igen" (fejlen er intermitterende) er output fra systemet altså ikke "låst" i en sikker tilstand. Hvis testmekanismen til detektion af fejl i systemet er sådan, at en yderligere fejl (F2) i samme kanal ikke kan detekteres, når F1 er tilstede, kan et usikkert output fra kanalen opstå, når F1 "forsvinder". Først når F1 forsvinder kan F2 detekteres. Detektionstiden for F2 kan derfor blive "lang", og man kunne frygte, at en modsvarende fejl (F3) i den anden kanal i mellemtiden kunne opstå, der sammen med F2 styrede output til en farlig fejl. Denne problemstilling behandles i afsnit 1.5.

1.3 Om intermitterende fejls natur.

En elektronisk konstruktions korrekte funktionen er afhængig af størrelsen af og samspillet mellem en mængde parametre for alle de indgående komponenter. Hvis en funktion baserer sig på en værdi for en parameter for en komponent, således at en lille (og sandsynlig) ændring i parameterens værdi medfører fejlfunktion er der tale om at systemet er bygget indeholdende en systematisk fejl. Hvis man "uforvarende er kommet til" at fejldimensionere, så konstruktionen er ustabil, f.eks. fordi en forventelig variation (f.eks. som funktion af temperaturen eller forsyningsspændingens størrelse) af en vigtig parameter, bringer værdien udenfor det område, hvor konstruktionen fungerer korrekt, er at betragte som en systematisk fejl (en fejldimensionering). Hvis man "uforvarende er kommet til" at benytte en komponent, som ikke har parameterværdier, som forudsat i dimensioneringsberegningerne, er der ligeledes tale om en systematisk fejl (idet man enten har indkøbt en gal komponent, eller producenten ikke har fremstillet komponenten, så den overholder sine specifikationer). Systematiske fejl skal man sikre sig imod ved at have godt styr på designprocessen.

Her vil vi ikke behandle problemer omkring sikring mod systematiske fejl, men betragte problemer med randomfejl i et "perfekt" designet og fremstillet system.

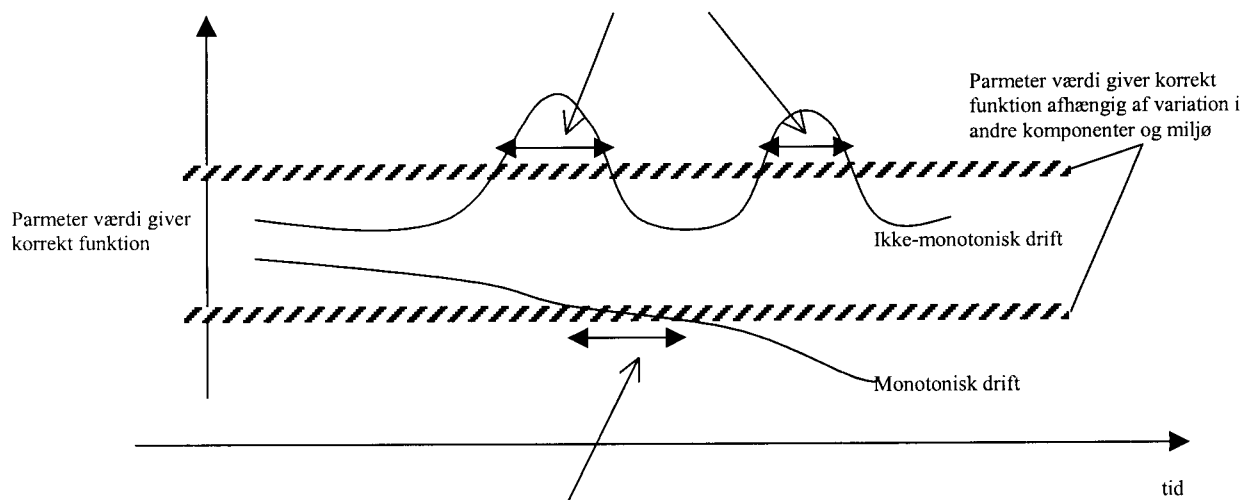
Man kan dele komponentfejl i bratfejl (catastrophic failures), der er pludselig uoprettelig ophør af komponents funktion og driftfejl (degradation failures), der igen kan deles i monotonisk drift og ikke-monotonisk drift.

Hvis ikke en komponent er redundant (eller der er tale om en beskyttelseskomponent), vil en bratfejl normalt føre direkte til en funktionsfejl for konstruktionen. Disse bratfejl, der normalt medfører permanent fejl, vil heller ikke blive behandlet nærmere her.

En driftfejl vil, hvis den er monotonisk, også føre til en funktionsfejl (permanent fejl), når parameteren er drevet "langt nok". En ikke-monotonisk driftfejl eller en monotonisk driftfejl, der "ligger lige på vippen", vil give sig udtryk i intermitterende funktionsfejl.

En intermitterende fejl i en konstruktion er altså en følge af enten:

- en monotonisk driftfejl, der har gjort, at konstruktionen bliver "overfølsom" for påvirkninger fra omgivelserne eller "forventelige" variationer i parametre for andre komponenter i konstruktionen eller
- en ikke monotonisk driftfejl, som måske med en vis ret også kan siges at komme af en "overfølsomhed" for påvirkninger fra omgivelserne, idet fejlen jo "trigges" af en eller anden ændring, som vi ofte blot ikke er i stand til at identificere.



Figur 1. Driftsfejl fører til intermitterende fejl

De påvirkninger, som komponenten bliver overfølsom overfor, kan f.eks. være af elektrisk, magnetisk, mekanisk, termisk eller kemisk art. Udtrykket "overfølsom" dækker over, at konstruktionen fejler som følge af en påvirkning, som er indenfor grænserne for det specificerede miljø, som den skal kunne fungere i, eller en variation af en anden komponents parametre, og som den fungerer korrekt sammen med, hvis driftfejlen ikke er tilstede.

Når en konstruktion fungerer korrekt i nogle perioder og er fejlbehæftet i de mellemliggende perioder, taler man om en intermitterende fejl. Komponenten, der er årsag til den intermitterende fejl, er enten ramt af monotonisk drift (og "parameterværdien ligger lige på vippen") eller ikke-monotonisk drift med perioder, hvor parameterværdien skiftevis ligger i det område der giver korrekt funktion, og det område der giver fejlfunktion.

Om konstruktionen er i en "fejlperiode" (fejlen er aktiv) eller i en "ej fejlperiode" (fejlen er passiv) er afhængig af, om den eller de påvirkninger/variationer, der trigger fejlen til at give sig udtryk, er tilstede eller ej. Ofte er det ikke muligt at bestemme, hvilke påvirkninger/variationer, der "trigger" fejlen, og den synes derfor at optræde spontant og tilfældigt.

En monotonisk driftfejl har kun en kortere periode (hvad kortere så end er!), hvor de befinder sig i "af og til acceptabel-området", og resulterer i intermitterende fejl, hvorefter parameterværdien driver ud i det uacceptable område og medfører permanent fejl i konstruktionen.

En ikke monotoniske driftfejl kan i princippet fortsætte med at give sig udtryk i intermitterende fejl indtil komponenten udskiftes enten fordi fejlen lokaliseres eller fordi komponenten udskiftes i forbindelse med udbedring af en anden fejl.

Generelt vil en komponent anses for fejlet, når en parameter ikke længere ligger inden for visse specifikationsgrænser². De erfaringstal, der opgives for elektroniske komponenter, som middeltiden til fejl (MTTF), skal være baseret på tests og målinger, der er i stand til at registrere bratfejl, monotoniske driftfejl og ikke-monotoniske driftsfejl. MTTF må altså indeholde summen af hyppigheden af alle tre typer af fejl. Det betyder også at de tre typer af fejl (hvis de kunne skilles ad) hver for sig ville udvise en middeltid til fejl større end MTTF.

1.4 Farlig fejl som følge af intermitterende fejl kombineret med permanent fejl eller kombinationen af to intermitterende fejl

Afhængig af hvor følsom konstruktionen er med hensyn til komponentens parameter, vil konstruktionens funktion fejle før eller efter parameteren driver uden for disse specifikationsgrænser. En konstruktion kan altså fungere korrekt selv om en komponent er uden for sine specifikationsgrænser. En konstruktion indeholder en konstruktionsfejl, hvis den fejler på grund af værdien for en parameter for en komponent, der er indenfor sine specifikationsgrænser.

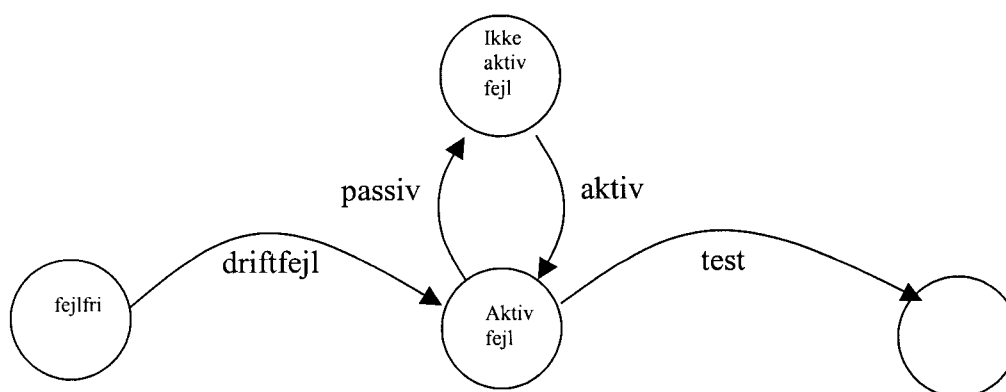
Hvis vi for nemheds skyld regner med, at konstruktionens funktion fejler, når ”komponenten fejler”, vil tiden til fejlfunktion være knyttet nært sammen med MTTF for komponenten.

Hvis der er lavet ”burn in” af konstruktionen, således at eventuelle eksemplarer indeholdende ”svage” komponenter er sorteret fra, er det tilladeligt at regne med at funktionsfejl vil optræde med en hyppighed, der er summen af hyppigheden for fejl i de indgående komponenter.

Konstruktionen starter altså sit liv som ”fejlfri” og rammes i forbindelse med den første komponentfejl af enten en permanent fejl (hvis komponenten får bratfejl) eller af intermitterende fejl (hvis komponenten får driftsfejl).

De permanente fejl behandles ikke yderligere her, hvorimod de intermitterende fejls udtryk vil blive undersøgt lidt nærmere.

² Det kan givetvis medføre en del overvejelser at fastsætte, hvad man skal forstå ved specifikationsgrænserne for en aktuel parameter for en aktuel komponent.



Figur 2. Model af intermitterende fejl i en kanal.

For hver af de to uafhængige kanaler i systemet illustrerer ovenstående figur, at først skal en komponent i konstruktionen rammes af driftfejl, derefter vil konstruktionen være ramt af en intermitterende fejl, hvor den skifte mellem aktiv fejlfunktion og passiv fejlfunktion (latent fejl), indtil fejlen fanges af systemets indbyggede selvtest.

Driftsfejl er en del af de fejl der er årsag til en komponents MTTF-værdi. Fejlene optræder med konstant hyppighed.

Da man tit ikke kan konstatere, hvad der "trigger" komponenten til at udvise funktion i modstrid med sine specifikationer, kunne det være nærliggende at erklære, at fejlen blev aktiv med konstant hyppighed og, når den var opstået, blev passiv med en anden konstant hyppighed.

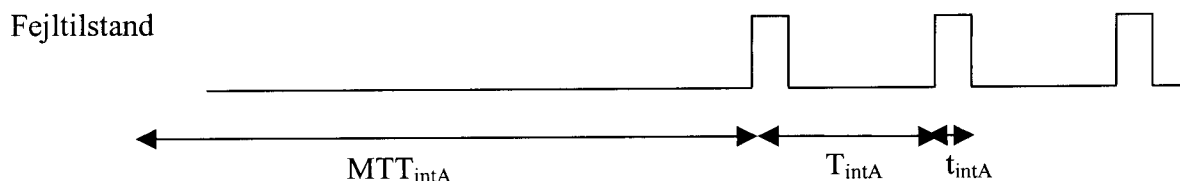
Selvtesten foretages typisk med faste intervaller. Hyppigheden af test er altså også konstant.

Ovenstående kan der givetvis regnes på som en Markov proces. De udregninger overlades til eksperterne.

I første omgang foretages for illustrationens skyld lidt "høkerregning". Modellen i figur 2 vil som "gennemsnitsbetragtning" give et billede som vist neden for i figur 3.

I gennemsnit går der "middeltid til intermitterende fejl" (MTT_{intA}) før komponenten fejler med driftfejl. Derefter udviser konstruktionen fejlfunktion og ikke-fejlfunktion med en længde af tidsperiode med aktiv fejl (t_{intA}) og med periodetiden (T_{intA}). T_{intA} og t_{intA} er ikke konstante, men set over en tidsperiode med et antal aktive perioder kunne man formode, at det vil være ladeligt at regne forholdet mellem T_{intA} og t_{intA} for konstant.

Figur 3 Skitse af en intermitterende fejls tidsmæssige forløb



1.4.1 Antagelser om intermitterende fejl

A0. Tidligere (s. 4 nederst) er gjort den antagelse, at når "komponenten fejler" (medtages her for fuldstændighedens skyld)

A1. Intermitterende fejl optræder med hyppighed $\lambda_{intA} = \lambda_A = 1/MTTF$

Tidligere er argumenteret for, at de intermitterende fejl er et resultat af driftfejl, og at driftfejlene er en delmængde af de fejl, der er indeholdt i en komponents MTTF erfaringstal. Antagelsen A1 svarer til, at alle fejl giver intermitterende fejl og er derfor meget pesimistisk worst case.

A2. Når komponenten er fejlet, er det tilladeligt at regne med at den intermitterende fejl er aktiv med et fast forhold mellem aktiv og passiv.

A3. Det betragtede system består af to kanaler (A og B), der er uafhængige. I begge kanaler findes en periodisk test af, der kan afsløre enhver komponentfejl i kanalen. Det er ideen i et composite fail safe system (se evt CLC 129 appendix B3). Da enhver intermitterende fejl er resultat af en driftfejl, der også kunne have resulteret i en permanent fejl, vil der ikke være andre (nye) fejlmodes for komponenten, som skal tages i betragtning end de fejlmodes som optræder som permanente fejl. Testen der kan finde alle permanente fejl kan altså også finde alle intermitterende fejl (se dog også A5).

A4. Testtidspunktet for den periodiske test af en komponent i kanalen kan betragtes som tilfældigt i forhold til, hvornår bristen giver sig udtryk i, at den intermitterende fejl er aktiv. Det indebærer bl.a. at der er fuldstændig uafhængighed mellem testens udførelse og om den intermitterende fejl er aktiv eller passiv. F.eks. "trigger" testens start ikke fejltilstanden til at forsvinde og testens afslutning "trigger" ikke fejltilstanden til at opstå.

A5. Testvarigheden er kort i forhold til varigheden af den periode, komponenten befinder sig i fejltilstand.

Hvis der testes på et tidspunkt, hvor komponenten er i fejltilstand, vil fejltilstanden altså blive detekteret, fordi testtiden med tilnærmelse kan regnes for forsvindende i forhold til varigheden af fejltilstanden.

1.4.2 Beregning af hyppighed for to tilfælde hvor intermitterende fejl kan medføre farlig fejl.

Der bliver to tilfælde, hvor intermitterende fejl kan føre til farlig fejl, og som derfor skal overvejes. Enten opstår første en intermitterende fejl i den ene kanal og derefter en permanent fejl i den anden eller også opstår først en intermitterende fejl i den ene kanal og efterfølgende en intermitterende fejl i den anden.

I. Intermitterende fejl i en kanal kombineret med permanent fejl i den anden.

a1. Der opstår en driftfejl i en komponent i kanal A. Hvis der efterfølgende i perioden indtil den intermitterende fejl i kanal A bliver detekteret, og systemet bliver bragt i sikker tilstand (detection time plus negation time) opstår en permanent fejl i en modsvarende komponent i kanal B, og den intermitterende fejl i kanal A er aktiv, er systemet fejlet farligt.

Denne hændelsessekvens giver et negativt estimat for hyppigheden af farlig fejl, idet den permanente fejl i kanal B i nogle tilfælde bliver detekteret af testen i kanal B og systemet blive bragt til sikker tilstand, før fejlen i kanal A bliver aktiv. Desuden vil visse af de farlige fejl udregnet ovenfor ikke medføre hazarder i "den virkelige verden", idet de er så kortvarige, at output fra systemet ikke er en hazard (signallamper kan måske ikke nå at tænde, sporskiftmotorer kan ikke nå at bevæge sig).

a2. Der opstår en permanent fejl i komponenten i kanal B. Før denne fejl er detekteret og negeret opstår en brist i en modsvarende komponent i kanal A og den intermitterende fejl i kanal A bliver aktiv.

b. Tilfældet hvor bristen opstår i kanal B og den permanente fejl i kanal A, skal også medtages. Tilfældet er helt ækvivalent med ovenstående.

II. Intermitterende fejl i en kanal kombineret med intermitterende fejl i den anden.

a. Der opstår en driftfejl i den betragtede komponent i kanal A. Inden fejlen, der giver sig udtryk i en intermitterende fejl i kanal A, er detekteret, opstår efterfølgende en driftfejl i modsvarende komponent i kanal B, der giver sig udtryk i en intermitterende fejl i kanal B. I perioden indtil en af de intermitterende fejl bliver detekteret og systemet bliver bragt i sikker tilstand (detection time plus negation time), vil systemet fejle farligt, hvis de to fejl bliver aktive samtidig.

I: Hyppighedsbidrag til farlig fejl fra intermitterende fejl i den ene kanal kombineret med permanent fejl i den anden.

a1: Detektion af den intermitterende fejl sker, når den periodiske test bliver udført i en periode, hvor den intermitterende fejl er aktiv. Den intermitterende fejl er aktiv i brøkdelen $t_{\text{intA}} / T_{\text{intA}}$ af tiden, når først komponenten er ramt af driftfejl. Derfor er det kun et spørgsmål om tid, før testen bliver udført i en periode, hvor fejlen er aktiv. Jo større brøkdelen af tiden fejlen er aktiv, jo før bliver den detekteret. Der regnes på en worst case betragtning. Det kan jo teoretisk lade sig gøre at teste i fejlens ikke-aktive perioder til evig tid. At det skulle blive tilfældet er dog meget lidt sandsynligt og som et konservativt³ estimat for detektionstiden for intermitterende fejl ($t_{\text{det intA}}$) kunne derfor bruges:

$$t_{\text{det intA}} = (T_{\text{intA}} / t_{\text{intA}}) * t_{\text{dA}}$$

Populært sagt er den intermitterende fejl af en bestemt type detekterbar ligesom den permanente fejl af samme type. Detektionstiden bliver blot længere.

Hyppigheden af farlig fejl (λ_{ff}) i tilfælde a1+a2 kan herefter tilnærmet udregnes til:

$$\lambda_{\text{ff}} = \lambda_{\text{intA}} * \lambda_{\text{B}} * ((T_{\text{intA}} / t_{\text{intA}}) * t_{\text{dA}}) + t_{\text{nA}} * t_{\text{intA}} / T_{\text{intA}} + \lambda_{\text{B}} * \lambda_{\text{intA}} * (t_{\text{dB}} + t_{\text{nB}}) * t_{\text{intA}} / T_{\text{intA}}$$

λ_{intA} er hyppigheden af driftsfejl, der medfører intermitterende fejl i A. Med brug af A1 gælder at $\lambda_{\text{intA}} = \lambda_{\text{A}}$.

λ_{B} er hyppigheden af alle fejl i B.

³ Det bør undersøges at der vitterligt er tale om et konservativt estimat.

t_{dA} (t_{dB}) er hhv. detektionstiden for permanent fejl i A (B) (=varigheden af perioden mellem to test)

t_{nA} (t_{nB}) er negation time (tiden der medgår for at bringe systemet i sikker tilstand når fejl er detekteret i kanal A (B)).

Hvis man antager,

at t_{nA} er lille i forhold til $(T_{intA} / t_{intA}) * t_{dA}$

t_{nB} er lille i forhold til t_{dB}

kan udtrykket reduceres til:

$$\lambda_{ff} = \lambda_A * \lambda_B * t_{dA} * t_{intA} / T_{intA} + \lambda_B * \lambda_A * t_{dB} * t_{intA} / T_{intA}$$

og hvis man antager at $t_{dA} = t_{dB}$ og da t_{intA} / T_{intA} er ≤ 1 medfører det at

$$\lambda_{ff} \leq 2 * \lambda_A * \lambda_B * t_{dA}$$

Da man også skal medtage tilfældet hvor den intermitterende fejl opstår i kanal B og den permanente fejl i kanal A, bliver det konservative estimat for hyppigheden af farlig fejl som følge af intermitterende fejl i kombination med permanente fejl mindre end 4 gange hyppigheden for farlig fejl som følge af sammenfaldende permanente fejl i kanal A og kanal B. Det betyder, at hvis man sikrer sig mod for høj hyppighed af farlig fejl som følge af permanente fejl, har man (hvis forudsætningerne for beregningen ovenfor holder) også sikret sig mod for høj hyppighed af farlig fejl som følge af en intermitterende fejl i en kanal kombineret med hyppigheden af en permanent fejl i den anden kanal.

II: Hyppighedsbidrag til farlig fejl fra intermitterende fejl i den ene kanal kombineret med intermitterende fejl i den anden.

På samme måde som ovenfor bruges et negativt estimat for detektionstiden for intermitterende fejl i hhv. kanal A og kanal B.

Hyppigheden af farlig fejl i tilfælde II kan herefter tilnærmet udregnes til:

$$\lambda_{ff} = \lambda_{intA} * \lambda_{intB} * ((T_{intA} / t_{intA}) * t_{dA}) + t_{nA}) * t_{intA} / T_{intA} * t_{intB} / T_{intB} +$$

$$\lambda_{intA} * \lambda_{intB} * ((T_{intB} / t_{intB}) * t_{dB}) + t_{nB}) * t_{intB} / T_{intB} * t_{intA} / T_{intA}$$

Hvis man som ovenfor antager at t_{nA} og t_{nB} er små kan udtrykket reduceres til:

$$\lambda_{ff} = \lambda_A * \lambda_B * t_{dA} * t_{intB} / T_{intB} +$$

$$\lambda_A * \lambda_B * t_{dB} * t_{intA} / T_{intA}$$

og hvis man antager at $t_{dA} = t_{dB}$ og da t_{intB} / T_{intB} og t_{intA} / T_{intA} er ≤ 1 medfører det at

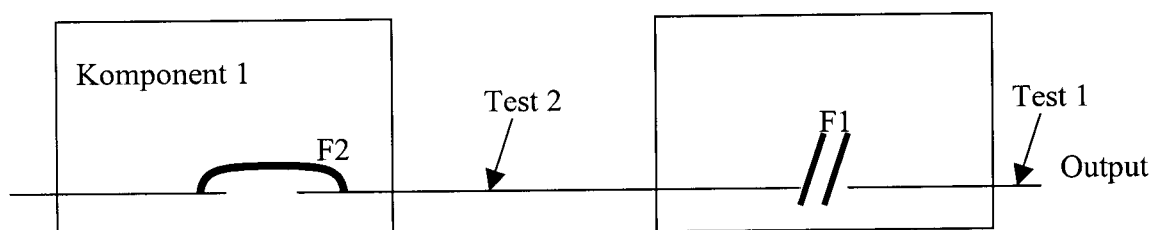
$$\lambda_{ff} \leq 2 * \lambda_A * \lambda_B * t_{dA}$$

hvor højresiden er identisk med det dobbelte af hyppigheden for farlig fejl som følge af sammenfaldende permanente fejl i kanal A og kanal B. Det betyder, at hvis man sikrer sig mod for høj hyppighed af farlig fejl som følge af permanente fejl, har man under forudsætningerne for udregningen ovenfor også sikret sig mod for høj hyppighed af farlig fejl som følge af en intermitterende fejl i en kanal kombineret med hyppigheden af en intermitterende fejl i den anden kanal.

1.5 En intermitterende fejl, der skjuler en anden fejl

Hvis en fejl (F1) automatisk bringer output til sikker side (fail safe) behøver kanalen ikke at være designet til at kunne detektere F1 på anden måde end som funktionsfejl.

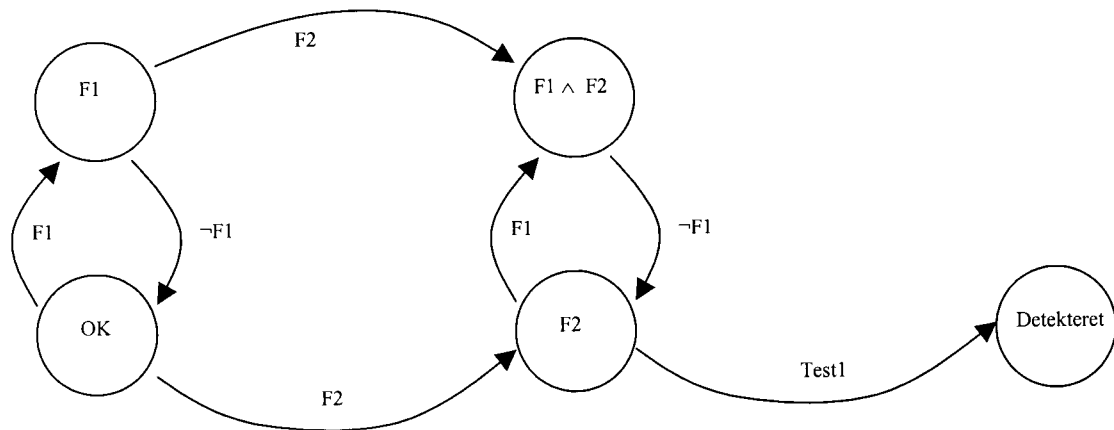
Detektionen foregår da typisk ved at et output forbliver passivt næste gang det burde have været aktivt. Dermed er systemet irreversibelt bragt til en sikker tilstand ikke "låst" i en sikker tilstand. Hvis testmekanismerne til detektion af fejl i systemet er sådan, at en yderligere fejl (F2) i samme kanal ikke kan detekteres, når F1 er tilstede, kan et usikkert output fra kanalen opstå, når F1 "forsvinder". Først når F1 forsvinder kan F2 detekteres. Detektionstiden for F2 kan derfor blive "lang", og man kunne frygte, at en modsvarende fejl (F3) i den anden kanal i mellemtiden kunne opstå, der sammen med F2 styrede output til en farlig fejl. Problemet er skitseret i figur



Figur 4 En sikker fejl F1 skjuler en usikker fejl F2.

I figur 4 er for en kanal skitseret et output som har en sikker værdi, når F1 er tilstede. På figuren er F1 illustreret med en afbrydelse og den sikre tilstand af output er, når der ikke går strøm i output. F2 er på figuren illustreret med en kortslutning. Test1 sker ved at sammenligne output for denne kanal med output fra den anden kanal. I de perioder hvor output i overensstemmelse med den ønskede overføringsfunktion skal være "ej strøm" vil der være overensstemmelse mellem de to kanalers output uafhængig af om F1 er tilstede eller ej. Test1 kan derfor ikke detektere F1. Test1 kan detektere F2, hvis F2 opstår, når F1 ikke allerede er opstået. Men hvis F1 er opstået, når F2 opstår vil F1 skjule F2. Hvis der eksisterede en Test2, der kunne sammenligne "mellemløbsresultater mellem de to kanaler indbyrdes, ville det være muligt at detektere F2. Men det er ikke altid hensigtsmæssigt (eller muligt) at have en sådan test2.

Her vil vi antage at kun Test1 eksisterer, og at F1 er en intermitterende fejl mens F2 er en permanent fejl. En model af fejl og detektering af fejl i en kanal vil derfor kunne se ud som på figur 5 nedenfor.



Figur 5. En intermitterende fejl F1 skjuler en permanent fejl F2

Figur 5 er ikke et fuldstændigt billede hvad angår tilstande og overgange. F. eks. vil F1 være detekterbar som en funktionsfejl, idet output ikke vil kunne blive aktivt i overensstemmelse med overføringsfunktionen, når F1 er tilstede.

1.6 Konklusion

Ovenstående ”høkerberegninger” antyder, at hvis man sikrer sig mod for høj hyppighed af farlig fejl som følge af sammenfaldende permanente fejl i de to kanaler i et composite fail safe system, har man også sikret sig mod for høj hyppighed af farlig fejl som følge af intermitterende fejl.

1.7 Forbehold

Forudsætningerne skal udsættes for kritisk analyse af personer der er kyndige i fejlmekanismer, som kan resultere i intermitterende fejl. Hvis det er muligt skal erfaringsdata fremskaffes for at underbygge eventuelle forudsætninger. I den forbindelse skal man være opmærksom på at der måske kunne være stor forskel på at betragte en simpel komponent som en modstand og en kompliceret IC-kreds som en CPU eller hukommelses kreds.

Matematikken (hyppighedsberegningerne) skal eventuel revurderes, hvis modellen af intermitterende fejl viser sig at være forskellig fra modellen for permanente fejl. Og i alle tilfælde bør beregningerne (inklusive tilnærmelserne) udsættes for kritisk analyse og strammes op, så det sikres, at de holder i alle tilfælde.

Desuden burde der måske gøres nogle overvejelser om hvad sker, når man genstarter et system med en intermitterende fejl i kanal A eller kanal B eller begge, fordi de intermitterende fejl ikke fanges umiddelbart, når systemet foretager opstartstest, enten fordi testen ikke er total, eller fordi fejlene ikke er aktive.

