

Forskning

---

## Erfarenheter från International Common Cause Failure Data Exchange-projektet (ICDE)

### Rev 0

Tillämpning av kunskaperna om common cause failures från ICDE-projektet i SKI:s tillsynsinsatser

Sandra Lindberg  
Gunnar Johansson  
Ralp Nyman

April 2008

## **SKI-perspektiv**

Rapporten ger grundläggande information om common cause failure (CCF) konceptet och insikter från drifterfarenheter om inträffade CCF-händelser i säkerhetsrelaterade komponenter i såväl utländska som inhemska kärnkraftanläggningar.

De drifterfarenheter som förmedlas i rapporten är avsedda att utgöra ett planeringshjälpmedel för SKI:s personal som inspekterar, granskar en tillståndshavares ärenden och gör anläggningsbesök.

CCF-insikter som vunnits i ICDE-projektet bl.a. från såväl utländska som inhemska kärnkraftverk om nödkraftdieslar (DG), motormanövrerade ventiler (MOV), backventiler (CV), centrifugalpumpar (CP), batterier (BA), nivåmätinstrumentering (LM), säkerhets- och avblåsningsventiler (SRV), brytare (BR), styrstavar och drivdonsmekanismer (CRDA) presenteras i denna rapport. Datainsamlingen av CCF på värmeväxlare har nyligen påbörjats. Denna informationskälla utgör ett väsentligt tillskott eller komplement av beroendefelsinformationen till den samlade svenska beroendefelsstatistiken.

## **Bakgrund**

Beroendefel, av typen CCF, är fortfarande dominerande faktorer i många svenska och utländska probabilistiska säkerhetsanalyser – PSA. Inom det internationella ICDE-projektet har man under en längre tid samlat in och kvalitetssäkrat en ansevärd mängd beroendefelsinformation från driften av kärnkraftverk i projektets medlemsländer. Det bedöms som väsentligt att all den offentliga ICDE-rapporteringen bearbetas ytterligare på nationell och lokal nivå, i detta fall inom SKI. För SKI:s del är det angeläget att den samlade informationen anpassas så att SKI:s tillsynsverksamhet kan ta stöd och tillämpa de samlade erfarenheterna i denna rapport, då en inspektion eller granskning planeras och genomförs.

I ett samarbete mellan nordiska anläggningar och myndigheter, NAFCS-projektet, har mycket material avseende CCF tagits fram och data bearbetats. En stor del av det arbetet ligger även till grund för denna rapport. Se referens [6].

Efter F1-händelsen 2006, finns det ett ytterligare skäl till att sammanställa denna typ av information så att resultaten från forskningsprojektet kommer SKI:s tillsyn till gagn så fort som möjligt och så brett som möjligt.

## **Syfte**

Rapportens syften är flerdådiga. Bl.a. att redovisa de senaste 10 årens samlade resultat från ICDE-projektet, att ge värdefull återkoppling från forskningen till SKI:s tillsynsverksamhet, att ge en bättre förståelse och kunskap om inträffade beroendefel av typen CCF samt att visa och förklara dessa händelser på ett tydligt sätt.

För att kunna ta del av rapportens budskap bedöms det som väsentligt att beskriva hur det s.k. CCF-konceptet inom ICDE är definierat och tillämpat, då information om CCF-händelser samlas in i projektets medlemsländer. Flera olika kriterier måste vara uppfyllda innan en händelse kan kallas för en CCF-händelse, dessa och flera andra parametrar relaterade till CCF kommer därför att beskrivas i rapporten.

Ett viktigt syfte är att visa exempel samt att sprida information och kunskaper inom SKI avseende CCF och inträffade CCF-händelser i ICDE projektets medlemsländer. (Dock ges anonym information för utländska anläggningar på grund av konfidentialitetsregler inom OECD/ICDE.) Rapporten skall kunna utgöra ett stöd vid planering och genomförande av en tillsynsinsats (t.ex. en inspektion, granskning, anläggningsbevakning) inom SKI:s och nya Strålsäkerhetsmyndighetens tillsynsområden.

## **Resultat**

Rapporten summerar upp och beskriver de i ICDE projektet identifierade svenska och utländska CCF-händelserna. Väsentlig kvalitativ information om CCF presenteras och beskrivs i rapportens bilagor. Rapportens resultat kan också användas då försvarsåtgärder mot CCF diskuteras, även att visa det motsatta, att ett s.k. enkelfel föreligger. Rapporten demonstrerar också vikten av att ha ett RO-rapporteringssystem som tydligt anger behovet av den kvalitativa informationen som ICDE-projektets kodguider efterfrågar och vill få svar på.

Sveriges mängd av insamlade CCF-händelser i ICDE projektet utgör ca 8% av alla den registrerade händelsemängden. För Sveriges del är därför utväxlingen mycket hög. Arbetsformen i OECD/ICDE projektet är sådan att de medlemsländer som delger CCF information om en viss komponentgrupp också kan ta del av andra länders CCF-erfarenheter. Det är till stora delar dessa kunskaper som nu redovisas i denna forskningsrapport, då erfarenheter nu kan börja dras ur den befintliga ”CCF-massan”.

Rapporten ger även en vägledning för beaktande av CCF vid tillsynsverksamhet, vilket kan nyttjas vid både planering och genomförande av tillsynsinsats.

## **Effekt på SKI:s verksamhet**

Erfarenheterna om kända CCF:s i ICDE projektets medlemsländer, som nu redovisas för första gången på ett mycket brett och samlat sätt, bör komma myndighetens medarbetare till gagn i tillsynsarbetet. Resultaten och värderingarna om beroendefel som redovisas, skall kunna användas direkt i tillsynsarbetet – vid planering och genomförande av en inspektion, anläggningsbevakning eller i granskningen av ärenden eller inkommen händelserapportering som beaktar inslag av CCF.

## **Fortsatt verksamhet inom området**

Detta är ett område där det kontinuerligt sker nya framsteg och därför bör vikten av att ständigt hålla rapporter av den här typen uppdaterade poängteras. Ett alternativt sätt för vidare bearbetning är att vidareutveckla informationen i denna rapport för framtagande av Tillsynshandbok i ämnet. Mycket av informationen presenterad i denna rapport kan nyttjas för en sådan handbok, genom vidare bearbetning och anpassning av innehåll till förekommande tillsynsverksamhet.

## **Projektinformation**

SKI:s handläggare har varit:

Ralph Nyman - RA.

Projektnummer

2007 02 020

SKI diarienummer:

SKI 2007/1647

Övrigt:

Rapporten refererar till många publicerade och offentliga OECD/NEA rapporter. Dessa kan läsas och laddas ner från projektets hemsida på Internetadressen [www.eskonsult.se/ICDE](http://www.eskonsult.se/ICDE)

## **SKI-perspective**

This report provides fundamental information about the concept of common cause failure (CCF) and insights from occurred CCF events in safety related components in both international and Swedish plants.

The operational experiences presented in the report are intended to assist the SKI personnel who are performing inspections, reviewing a licensee's matters and making plant visits.

CCF insights gained within the ICDE (international common cause failure data exchange) project from both international and Swedish plants concerning emergency diesel generators (DG), motor operated valves (MOV), check valves (CV), centrifugal pumps (CP), batteries (BA), level measurement instrumentation (LM), safety- and relief valves (SRV), breakers (BR) and control rods and drive assemblies (CRDA) are presented in this report. The collection of CCF data on heat exchangers has recently begun. This source of information offers an important contribution, or complement, to the dependent failure information for the Swedish statistics on dependent failure.

## **Background**

Dependent failures, of CCF character, are still dominating factors in many Swedish and international probabilistic safety analyses (PSA). Within the ICDE project a great amount of information on dependent failure at the nuclear power plants of the member countries has, during a long time, been collected and quality assured. It is considered to be important that the public reporting by ICDE is further treated at national and local level, in this case within SKI. Considering SKI it is essential that the collected information is modified so that the inspection activities can make use of and be supported by the obtained experiences when an inspection or review is planned and performed.

Within a joint project between Nordic plants and authorities, the NAFCS project, a lot of material concerning CCF was gathered and a lot of data processed. A great part of that work is also used as basis for this report, see reference [6].

After the event at Forsmark 1 in 2006 it is even more motivated to gather this kind of information so that the results from the research project serves the interest as soon as possible and as widespread as possible.

## **The aim of SKI and the Report**

There are several purposes of this report. Among them are to present the results of the last 10 years of work within the ICDE project, to give valuable feedback from the research to the inspection activities by SKI, to provide a more profound understanding and knowledge about occurred dependent failures of CCF character and also to show and explain these events in a understandable way.

To be able to appreciate the idea of the report it is considered as important to describe how the concept of CCF is defined and applied within ICDE, since information on CCF events are collected from the member countries of the project. Several criteria are to be fulfilled for an event to be defined as a CCF event. These criteria and a number of other parameters connected to CCF information are therefore presented in the report.

A significant aim of the report is to show examples and spread information and knowledge, within SKI, about CCF and CCF events that occurred in the member countries of ICDE. (Only anonymous information is provided concerning foreign events though, due to ICDE confidentiality rules.) The report is to provide assistance when planning and performing inspection activities (e.g. inspection, review, plant surveillance) within SKI and the areas of inspection for the new authority Swedish Radiation Safety Authority.

## **Results**

The report summarizes and describes the identified Swedish and foreign CCF events collected within ICDE. Essential qualitative information about CCF is presented and described in the appendices of the report. The results of the report can also be used in discussions concerning defences against CCF, and also to be used to prove the opposited, i.e. that a current case is a single failure. The report also demonstrates the importance of having an efficient system for reporting (LER reporting) that incorporates qualitative information as required in the ICDE coding guideline.

The amount of Swedish events represents about 8 % of all registered events within the ICDE project. For Sweden the received amount of information is therefore much larger than the one provided. The procedure within ICDE is such that the member country providing CCF information for a certain component group is also allowed to acquire the experiences of other countries for this particular component group. It is to a large extent these experiences that are now presented in this report, since information is now beginning to be able to be pulled out of the mass of collected CCF data.

The report also provides guidance on how to consider CCF in inspection activity, which can be used both when planning and performing an inspection.

## **Impact on the operation of SKI**

The experiences of known CCF events in the member countries of the ICDE project, which are now presented in a wide and arranged way, should become of use for the personnel of the authority and inspections activities. The results and valuation of dependent failures being presented shall be useful directly in the inspection activities – when planning and performing an inspection, plant surveillance or when reviewing matters or event reporting considering CCF aspects.

## **Continuing work within the research area**

This is an area where continuously progress are made and it is therefore significant to state the importance of keeping this kind of report up to date. An alternative for supplementary work is to further develop the information of this report to produce a manual for the subject. A lot of the information in this report can be made use of for such a manual by having the material worked up and modified to better suit the existing activities concerning inspections.

## **Project information**

Project responsible at SKI:

Ralph Nyman - RA

Project number:

2007 02 020

Dossier number:

SKI 2007/1647

Other:

This report refers to a lot of published and public OECD/NEA reports, that can be viewed and downloaded from the homepage of the project at [www.eskonsult.se/icde](http://www.eskonsult.se/icde).

## Forskning

---

# Erfarenheter från International Common Cause Failure Data Exchange-projektet (ICDE)

## Rev 0

Tillämpning av kunskaperna om common cause failures från ICDE-projektet i SKI:s tillsynsinsatser

Sandra Lindberg ES-Konsult AB  
Gunnar Johanson ES-Konsult AB

Svetsarvägen 7, SE-17141 Solna

Ralph Nyman SKI

Klarabergsviadukten 90, SE-10658 Stockholm

April 2008

Denna rapport har gjorts på uppdrag av Statens kärnkraftinspektion, SKI. Slutsatser och åsikter som framförs i rapporten är författarens/författarnas egna och behöver inte nödvändigtvis sammanfalla med SKI:s.





## Sammanfattning

Rapporten ger grundläggande information om common-cause failures (CCF) och insikter från drifterfarenheter om inträffade CCF händelser i säkerhetsrelaterade komponenter som modelleras i utländska som inhemska kärnkraftanläggningars PSA:er.

De drifterfarenheter som förmedlas är avsedda att utgöra ett planeringshjälpmedel för SKI:s personal som inspekterar, granskar en tillståndshavares ärenden och gör anläggningsbesök.

CCF-insikter som vunnits i ICDE projektet bl.a. från utländska som inhemska kärnkraftverk om nödkraft dieslar (DG), motormanövrerade ventiler (MOV), backventiler (CV), centrifugalpumpar (CP), batterier (BA), nivåmätinstrumentering (LM), säkerhets- och reglerventiler (SRV), brytare (BR), styrtavar och drivdonsmekanismer (CRDM) och värmeväxlare presenteras i denna rapport. Denna informationskälla utgör ett väsentligt tillskott eller komplement av beroendefelsinformation, till den samlade svenska beroendefelsstatistiken.

P.g.a. konfidentialitetsregler inom OECD/ICDE projektet, kommer inga namn och annan fakta att avslöjas i denna rapport om utländska kärnkraftanläggningar.

Modellen för rapporten baserar sig delvis på en USNRC-aktivitet från år 2006, se [4, 5].



## Summary

The report present basic information on common-cause failures (CCF) and insights gained from operating experience and CCF events in safety related components that are modelled in PSA at both national and international plants.

The experiences being presented are intended to provide a tool for SKI personnel supervising nuclear power plants.

Gained insights, on a international level, within the ICDE project concerning emergency diesel generators, motor operated valves, check valves, centrifugal pumps, batteries, level measure instrumentation, safety- and relief valves, breakers, control rod and drive assemblies and heat exchangers are presented in this report. The ICDE database and the collected amount of information provide a contribution and offer a complement to the collected Swedish data and statistics for dependent failures.

Due to confidentiality regulations within ICDE, some information concerning international plants is left out in the presented material.

The model for this report is partially based on a USNRC activity in 2006 [4, 5].



# Innehållsförteckning

<b>1</b>	<b>Introduktion .....</b>	<b>1</b>
1.1	Bakgrund.....	1
1.2	Syfte med rapporten.....	1
1.3	Rapportens disposition.....	2
<b>2</b>	<b>Krav.....</b>	<b>3</b>
<b>3</b>	<b>Kort beskrivning av OECD/ICDE forskningsprojektet.....</b>	<b>3</b>
<b>4</b>	<b>Bevis om oberoende .....</b>	<b>5</b>
4.1	Common Cause Failure - CCF.....	6
4.2	Illustration av en CCF händelse.....	10
<b>5</b>	<b>Försvar mot beroenden och beroendefel .....</b>	<b>11</b>
<b>6</b>	<b>Vägledning vid tillsyn .....</b>	<b>15</b>
<b>7</b>	<b>Slutsatser.....</b>	<b>17</b>
<b>8</b>	<b>Referenser .....</b>	<b>18</b>
	<b>Bilaga 1: Viktiga CCF-parametrar, händelserapportering och CCF-analys .....</b>	<b>20</b>
	<b>Bilaga 2: Exempel på signifikanta svenska och utländska ICDE händelser.....</b>	<b>30</b>
	<b>Bilaga 3: Vägledning – erfarenheter från insamling av CCF-händelser på styrstavar och drivdon (CRDA) .....</b>	<b>56</b>
	<b>Bilaga 4: Vägledning – erfarenheter från insamling av CCF-händelser på nivåmätinstrumentering (LM) .....</b>	<b>64</b>
	<b>Bilaga 5: Vägledning – erfarenheter från insamling av CCF-händelser på batterier (BA).....</b>	<b>73</b>
	<b>Bilaga 6: Vägledning – erfarenheter från insamling av CCF-händelser på brytare (BR).....</b>	<b>79</b>
	<b>Bilaga 7: Vägledning – erfarenheter från insamling av CCF-händelser på säkerhets- och avblåsningssystem (SRV).....</b>	<b>87</b>
	<b>Bilaga 8: Vägledning – erfarenheter från insamling av CCF-händelser på motordrivna centrifugal pumpar (CP).....</b>	<b>93</b>
	<b>Bilaga 9: Vägledning – erfarenheter från insamling av CCF-händelser på backventiler (CV) .....</b>	<b>101</b>
	<b>Bilaga 10: Vägledning – erfarenheter från insamling av CCF-händelser på motormanövrerade ventiler (MOV) .....</b>	<b>107</b>
	<b>Bilaga 11: Vägledning – erfarenheter från insamling av CCF-händelser på nödkraftdieslar (DG).....</b>	<b>114</b>
	<b>Bilaga 12: Vägledning – erfarenheter från insamling av CCF-händelser på värmeväxlare (VXX) .....</b>	<b>123</b>
	<b>Bilaga 13: Identifierade svenska CCF-händelser i ICDE-projektet.....</b>	<b>129</b>



# 1 Introduktion

## 1.1 Bakgrund

Inom det internationella OECD/ICDE-projektet (International Common Cause Failure Data Exchange) har man nu till dags datum samlat på sig en ansenlig mängd beroendefelsinformation av typen ”Common Cause Failure”, CCF.

Flera slutrapporter från ICDE projektet finns nu sammanställda av OECD/CSNI för olika säkerhetsrelaterade komponentgrupper, och är vida spridda inom OECD:s medlemsländer. De tills nu publicerade projektrapporterna är angivna i [8-15]. Dessa rapporter är offentliga rapporter.

Det bedöms som väsentligt att all den offentliga ICDE rapporteringen bearbetas ytterligare på nationell och lokal nivå, i detta fall inom SKI, och att den samlade informationen anpassas så att SKI:s tillsynsverksamhet kan ta stöd och tillämpa de samlade erfarenheterna i denna rapport, då en inspektion eller granskning planeras och genomförs.

I ett samarbete mellan nordiska anläggningar och myndigheter, NAFCS-projektet, har mycket material avseende CCF tagits fram och data bearbetats. En stor del av det arbetet ligger även till grund för denna rapport, genom SKI-rapporten *Dependency Defence and Dependency Analysis Guidance*. Se referens [6]. Ytterligare en viktig rapport i sammanhanget är USNRC-rapporten *Common-Cause Failure Database and Analysis System*, se referens [7].

Efter F1-händelsen 2006, finns det ett ytterligare skäl till att sammanställa denna typ av information så att resultaten från forskningsprojektet kommer SKI:s tillsyn till gagn så fort som möjligt och så brett som möjligt.

## 1.2 Syfte med rapporten

Rapporten skall kunna utgöra ett stöd vid planering och genomförande av en tillsynsinsats (t.ex. en inspektion, granskning, anläggningsbevakning) t.ex. inom följande tillsynsinsatser;

Händelsestyrd tillsyn

- utföra en RASK utredning (Risk Analys av Störningar i Kärntekniska anläggningar)

Anläggningsbevakning

- utföra en riktad händelseuppföljning, som en anläggningsbevakning AB)
- utföra en uppföljning- och datainsamlingsinsats efter en inträffad händelse
- kontinuerligt följa tillståndet i en struktur, system eller komponent (SSK)



Planerad tillsynsaktivitet

- utföra en inspektion
- granska ett tillståndsärende

Ett annat syfte är att visa exempel, sprida information och kunskaper inom SKI, om inträffade CCF händelser i de länder som är aktiva medlemmar i ICDE projektet. Dock ges anonym information för utländska anläggningar på grund av konfidentialitetsregler inom OECD/ICDE.

Rapportens syfte är också att leverera något påtagligt och nyttigt till SKI, så att kostnad och nytta med ICDE-projektet kan motiveras som kostnadseffektivt för SKI. Nu finns det tillräckligt med dokumenterade ICDE kunskaper om inträffade CCF-händelser som tas tillvara och tydligt informeras om i denna rapport för SKI.

Målgruppen för rapporten är personalen vid SKI, men vänder sig givetvis även till alla som söker introduktion till, och bred information om, CCF.

Data som presenteras i denna rapport utgörs av sammanställningar av den information som finns i databasen för insamlade uppgifter inom ICDE. För tillgång till ICDE-databasen kontaktas Ralph Nyman vid SKI.

### **1.3 Rapportens disposition**

För att kunna ta del av rapportens budskap bedöms det som väsentligt att beskriva hur det s.k. CCF-konceptet inom ICDE är definierat och tillämpat, då CCF-händelser i projektets medlemsländer samlas in. Flera olika kriterier måste vara uppfyllda innan en händelse kan kallas för en CCF-händelse, dessa kommer därför att beskrivas i rapporten. Huvudrapporten, är avsedd ge en introduktion till och grundläggande förståelse för CCF. Här ges även sammanfattad information om vilka krav som ställs på svenska kärnkraftanläggningar och hur man kan arbeta för att minska risken för beroendefel. En central del finns i kapitel 6, där vägledning ges för hur kunskaper om CCF kan nyttjas vid planering och genomförande av tillsynsinsatser.

I bilaga 1 presenteras de viktigaste begreppen om CCF:er enligt de accepterade definitionerna inom ICDE projektet. I bilaga 2 ges exempel på inträffade svenska och utländska händelser av CCF-karaktär. Bilaga 3-12 ger information om olika komponentgrupper, för vilka CCF-data har samlats inom ICDE, och hur erfarenheterna ser ut genom statistik för olika parametrar. I en sammanfattande rapport från ICDE finns även en kortare redogörelse för den samlade erfarenheten från projektet [17]. I den sista bilagan, 13, listas de svenska CCF-händelser som registrerats i ICDE-databasen.

## **2 Krav**

I SKIFS 2004:1 och 2004:2 ges ett antal krav relaterade till CCF [19, 20].

I SKIFS 2004:2, § 10 ställs kravet att ”Vid konstruktion, tillverkning, installation, idrifttagning, drift och underhåll av säkerhetssystem skall rimliga tekniska och administrativa åtgärder vidtas för att motverka uppkomst av fel med gemensam orsak.”

Vidare anges i SKIFS 2004:2, allmänna råd till § 10, att: Med tekniska åtgärder avses åtgärder för diversifiering. En lämplig och rimlig diversifiering bör tillämpas vid konstruktionen av säkerhetsfunktionerna enligt 3 §, med anpassade analysförutsättningar och acceptanskriterier, för händelser till och med händelseklassen ej förväntade händelser, där rörbrotten dock kan undantas. Vid utformningen av en sådan diversifiering kan den befintliga elförsörjningen av anläggningens samtliga system tillgodoräknas. Reaktorskyddssystemet bör så långt det är rimligt och möjligt vara konstruerat så att skyddsbehov identifieras och skyddsåtgärder initieras genom minst två olika parametrar, exempelvis tryck och neutronflöde, vid alla händelser till och med händelseklassen ej förväntade händelser. De olika sätten att detektera en händelse bör vara funktionellt separerade.

I SKIFS 2004:1, 4 kap § 1, anges att: Anläggningen skall analyseras med probabilistiska metoder för att ge en så allsidig bild som möjligt av säkerheten.

Vidare finns även krav angående rapportering av händelser, vilka ges i SKIFS 2004:1, kap 7, § 1-3.

## **3 Kort beskrivning av OECD/ICDE forskningsprojektet**

ICDE projektet drivs och organiseras som ett paraplyprojekt inom OECD/NEA/CSNI/PWG1. Se mera information på [www.nea.fr/html/nsd](http://www.nea.fr/html/nsd).

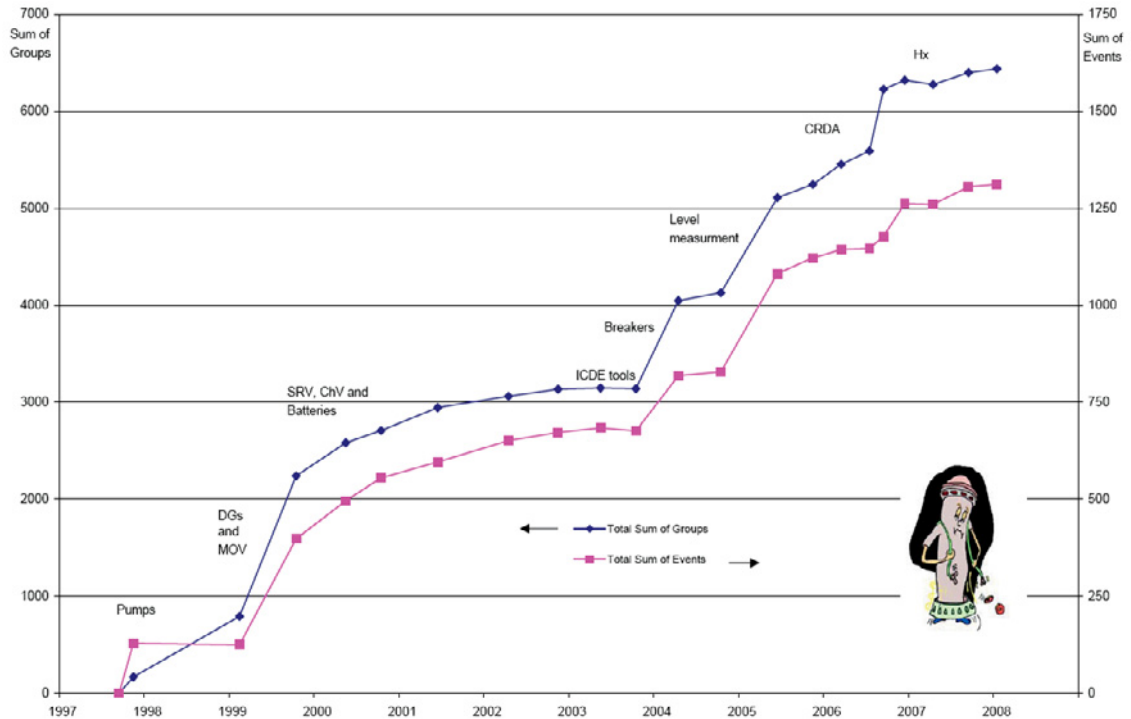
På följande Internetadress finns mera information om ICDE projektet - <http://www.eskonsult.se/ICDE/>.

I ICDE projektet deltar följande OECD medlemsländer och organisationer.

Land	Organisation
Canada	CNSC
Finland	STUK
Frankrike	IPSN
Tyskland	GRS
Japan	JNES
Korea	KAERI
Spanien	CSN
Sverige	SKI
Schweiz	HSK
England	NII
USA	USNRC

Tabell 1. Medverkande länder och organisationer i OECD/ICDE projektet.

I figuren nedan syns tydligt hur mängden insamlad data stigit med åren, där datainsamling för olika komponentgrupper har påbörjats vid olika tillfällen under projektets gång.



Figur 1. Mängd insamlad data inom ICDE-projektet över tid.

## 4 Bevis om oberoende

Säkerhetssystemen i nordiska kärnkraftverk kännetecknas av en hög grad av redundans<sup>1</sup>, separation<sup>2</sup> och diversifiering<sup>3</sup>. Det gäller både systemen i sig och deras hjälpsystem. Detta ger hög tillgänglighet och tillförlitlighet i systemen, men innebär också att anläggningarnas riskprofil normalt är dominerad av beroendefel, d.v.s. av fel med gemensam orsak som samtidigt drabbar fler än ett stråk i säkerhetssystem. I sammanhang där redundans används som ett sätt att öka säkerhetssystemets tillförlitlighet finns det alltid ett antal fysiska och funktionella beroenden som kan leda till att redundanta komponenter, system eller strukturer samtidigt blir otillgängliga på grund av någon gemensam orsak. Redundans har införts där man inte når tillräckligt långt med andra metoder att förbättra enskilda komponenter (hög kvalitet, felsäkerhet, m.m.), och ses som ett sätt att uppnå de tillförlitlighetskrav som ställs på system och anläggning. Detta syns också i de krav som ställs på kärnkraftverk, och som innehåller krav på redundans. De grundläggande krav på konstruktion som ställs på redundanta utrustningar för att de inte skall försvagas av fel med gemensam orsak är krav på separation och diversifiering.

Den stora komplexitet som finns hos en stor och avancerad anläggning som ett kärnkraftverk innebär att det kan vara svårt att försäkra sig om att det inte finns delade komponenter och fysiska beroenden. Redundanser uppfyller ibland inte det grundläggande kravet att inte dela komponenter. Detta är ofta medvetna beslut i konstruktionsprocessen, men kan också vara misstag. Syftet med fysisk separation är att skydda mot ett antal olika typer av händelser som samtidigt kan påverka mer än ett redundant stråk (exempelvis brand). Diversifiering används för att minska risken för fel med gemensam orsak beroende av lika faktorer hos konstruktion, miljö och organisation. Diversifiering innebär t ex användning av olika funktionsprinciper som en eldriven pump i det ena stråket och en ångdriven pump i det andra stråket.

Erfarenheten visar att gemensamma felorsaker och de mekanismer som kopplar samman komponenter kan vara både kända eller okända. Kända faktorer kan analyseras och behandlas specifikt i säkerhetsanalysen. Okända faktorer däremot brukar behandlas som ett restberoende som benämns CCF, vilket är en förkortning för ”Common Cause Failure”, d.v.s. fel med gemensam orsak. Detta restberoende representerar kopplingsmekanismer som är svåra att analysera explicit, men dess säkerhetspåverkan kan ofta uppskattas ur erfarenhetsdata, och representeras med CCF-modeller i säkerhetsanalysen. Kopplingsmekanismen bakom beroenden kan vara av två huvudtyper, funktionell och fysisk. En funktionell koppling innebär att redundanta funktioner eller ett system kan fela p.g.a. gemensam felorsak, genom att det inträffar fel i delade komponenter eller hjälpfunktioner. En fysisk koppling innebär att driftmiljön är gemensam för en grupp komponenter, och att avvikelser i miljön kan medföra att denna grupp av komponenter påverkas.

---

<sup>1</sup> Två eller flera alternativa, identiska eller olika, system eller komponenter som oberoende av varandra utför samma säkerhetsuppgift.

<sup>2</sup> System eller komponent som är fysiskt åtskilda, genom avstånd eller barriärer eller en kombination av dessa.

<sup>3</sup> Två eller flera alternativa system eller komponenter som oberoende av varandra utför samma säkerhetsuppgift men på principiellt olika sätt eller genom att ha olika egenskaper.

Beroende	Känt	Okänt
Funktionellt beroende En delad felorsak gör två eller flera komponenter otillgängliga	Beroendet sker genom kopplade system, strukturer eller komponenter: Kylning, ventilation, signaler, gemensamma delar (även delade passiva komponenter och systemdelar), procedurer, verktyg, personal, etc.	Felorsaker och kopplingsmekanismer är ej explicit kända: CCF (Common Cause Failure)
Fysiskt beroende En delad miljöbetingelse gör två eller flera komponenter otillgängliga	Beroendet uppkommer genom delad känslighet mot yttre faktorer: Rumshändelser (brand, översvämning, etc.), yttre händelser (transportolyckor, extrem väderlek, etc.), dynamiska effekter vid rörbrott.	

Tabell 2. Grundläggande typer av beroenden.

#### 4.1 Common Cause Failure - CCF

I svenska som utländska probabilistiska säkerhetsanalyser (PSA) av kommersiella kärnkraftverk är *fel med gemensam felorsak* (eng. common-cause failures, CCF) betydande orsakskällor till frekvensen för härdskada, F(HS).

Det är viktigt att CCF händelser är korrekt identifierade och modellerade i PSA:er och utförligt beskrivna i händelseanalyser och –rapporter typ RO (rapportvärda omständigheter), AO (arbetsorder) och speciella utredningsrapporter. Det är viktigt att denna typ av händelser bevakas i SKI:s tillsynsinsatser vid våra egna svenska kärnkraftverk.

Generellt definieras CCF som beroendefel vid vilket två eller flera komponenter felar samtidigt eller inom ett kort tidsintervall, och felan har en gemensam orsak. I ICDE-projektet gäller följande definition av en CCF-händelse (följer NUREG/CR-6268):

En försvagning, med inverkan på två eller flera redundanta komponenter (för en given funktion), som existerar över en relevant tidsrymd, och är ett direkt resultat av en delad orsak.

Som relevant tidsperiod ansätts (inom ICDE) två testintervall för komponenten. Med delad orsak avses att orsaken, eller orsakerna, till felandet är gemensam för inträffade fel. Med kopplingsmekanism avses något gemensamt mellan två eller flera (företrädesvis redundanta) som medför att komponenter felar på grund av samma orsak.

Kriterier för en CCF-händelse är följande:

- 1) 2 eller fler individuella komponenter måste fela eller vara degraderade, där felet härrör från
  - fel vid behov,
  - föreskriven periodisk provning (eng. inservice testing), eller
  - svaghet som skulle ha resulterat i ett fel om en signal om ett behov skulle ha erhållits.
- 2) 2 eller fler individuella komponenter måste fela eller vara degraderade under en vald tidsperiod, på så sätt att en lyckad drift enligt PSA-modellen inte kan garanteras.
- 3) Komponentfel eller degraderingar måste vara ett resultat från
  - en enskild men delad orsak, och
  - en kopplingsmekanism.
- 4) Komponentfel är inte orsakade av fel som härrör från utrustning utanför den definierade komponentavgränsningen. Komponentavgränsningar anges i del 2 i T-Boken, [22].

Det är vid analys av CCF underförstått att analysen avser kända och okända beroenden som inte analyseras explicit någon annanstans. Det är viktigt att få ta del av ett brett spektrum av händelser orsakade av beroenden mot vilka man kan känna igen uppkomna situationer i sitt eget arbete, vilket kan leda till ökad vaksamhet och medvetenhet om möjliga problem i framtiden. Tabell 3 sammanfattar viktiga bidragande orsaker till beroendefel hos diesellaggregat i svenska kärnkraftverk.

Beroendekategori	Bidragande orsaker
Hårdvarurelaterat	Åldring (elektriska och mekaniska komponenter)
MTO-relaterat	Bristande egenkontroll (och även kollektiv) (STARK) Bristande arbetsorganisation (Arbetspreparering, planering och driftklarhetsverifiering) Bristar i befintliga procedurer Dålig ergonomi och design med avseende på åtkomst vid underhåll, testning och kalibrering.

Tabell 3. Sammanfattning av de viktigaste bidragande orsakerna till restberoenden hos diesellaggregat i svenska kärnkraftverk.

Nedan, i avsnitt 4.1.1 – 4.1.2, beskrivs ICDE-projektets samlade erfarenheter beträffande de viktigaste orsakerna till fullständiga CCF<sup>4</sup> och de viktigaste kopplingsmekanismerna som orsakar fullständiga CCF. Ovanstående, samt avsnitt 4.1.1-4.1.2 härrör från [6], vilket är en givande referens för vidare läsning av denna typ av information.

<sup>4</sup> Fullständiga CCF är händelser där alla, t ex 2 av 2 eller 4 av 4 , redundanta komponenter felar till följd av en gemensam orsak

#### 4.1.1 Orsakskategorier

Händelserna i ICDE databasen har delats in i två orsakskategorier, nämligen mänskligt orsakade händelser och hårdvarurelaterade orsaker. Mänskligt orsakade händelser benämns ofta MTO-relaterade (Människa – Teknik – Organisation).

Viktiga MTO-aspekter är:

- Felaktiga ingrepp, d.v.s. fel i underhåll eller procedurer
- Fel i drift- eller underhållsprocedurer som skapar förutsättningar för att flera komponenter påverkas

MTO-aspekterna kan delas in i tre underkategorier:

- Utebliven eller otillräcklig testning efter underhåll/repairation/ombyggnad (eventuellt kombinerat med fel i driftklarhetsverifiering, DKV)
- Felaktig testning eller underhållsåtgärd p.g.a. felaktig eller ofullständig procedur, otillräcklig arbetskontroll.
- Felaktigt operatörsingrepp (t.ex. felaktig ventilmanöver eller felställd brytare eller omkopplare)

Viktiga hårdvaruaspekter är fel orsakade vid design eller tillverkning. Bland händelser med koppling till design, tillverkning och konstruktion dominerar designfrågor.

#### 4.1.2 Kopplingsmekanismer

Erfarenheter från ICDE-projektet, gällande internationella data, visar att:

- två av tre fullständiga CCF-händelser har MTO-koppling, d.v.s. beror helt eller delvis på felaktiga åtgärder av anläggningspersonal eller entreprenörer, samt att
- det enskilt största bidraget, till fullständiga CCF-händelser, kommer från felaktig testning och underhåll till följd av felaktiga och/eller ofullständiga procedurer, och från otillräcklig arbetskontroll.

Relativt sett varierar fördelningen mellan MTO-aspekter och hårdvaruaspekter obetydligt mellan olika grad av redundans.

Andelen fullständiga CCF bland de rapporterade ICDE-händelserna minskar väsentligt med ökande redundansgrad och påvisar att högre redundans är ett effektivt försvar. Men hög redundansgrad eliminerar inte fullständiga CCF.

Det finns i samband med CCF många parametrar definierade, och som är av stor vikt vid exempelvis tolkning och kvantifiering. Ytterligare redovisning av viktiga parametrar och analys av CCF-händelser ges i Bilaga 1. Vidare diskussion avseende kvantifiering av CCF ges även i rapport från nordisk-tyska arbetsgruppen för CCF-analys [3].

#### 4.1.3 Driftstatistik

Den samlade drifterfarenheten i Sverige år 2007 är i storleksordningen 325 reaktorår. De andra länderna i ICDE projektet står för totalt ca 92% av alla registrerade CCF-

händelser i världen. Detta betyder att den samlade svenska CCF statistiken är och förblir liten jämfört med vad som finns totalt i övriga världen. Detta betyder också att Sveriges har mycket god utväxling av medlemskapet i ICDE genom att få tillgång till mycket stor andel data trots att vi endast bidrar med en mindre mängd. Att basera parameteruppskattningar (ex. sannolikheten att 2 *Komp X* felar givet ett enkelfel, att 3 *Komp X* felar givet att 2 redan tidigare felat o.s.v.) enbart på svensk data låter sig inte göras med lätthet och osäkerheterna i sådana uppskattningar blir mycket stora.

CCF-händelser är lågfrekventa händelser, men trots detta är de riskdominerande i många PSA:er. Det är därför fortfarande väsentligt att denna typ av riskdominerande fel samlas och klassas på ett kvalitetssäkrat sätt inom den internationella forskningen.

#### 4.1.4 Viktigt att känna till

Den som använder och värderar utländsk CCF data bör känna till följande:

- I vissa amerikanska datasammanställningar, studier, redovisas CCF faktorer för t.ex. 4-faldiga redundanser. Analytikern bör känna till att amerikansk driftstatistik från t.ex. 4-stråks anläggningar är betydligt lägre än den samlade Europeiska. Detta innebär att man måste kunna ifrågasätta ett CCF värde för 4-subbade stråk från USA. I USA använd vanligtvis s.k. mapping-up metoder för bestämning av CCF-parametrar eftersom man har många 2 och 3 stråks anläggningar. Det är därför viktigt att känna till vad summeringen *Statistisk datablad (statistical record)* säger om ackumulerade drifttider för olika komponentgrupper. För beskrivning av statistiskt datablad, se bilaga 1.

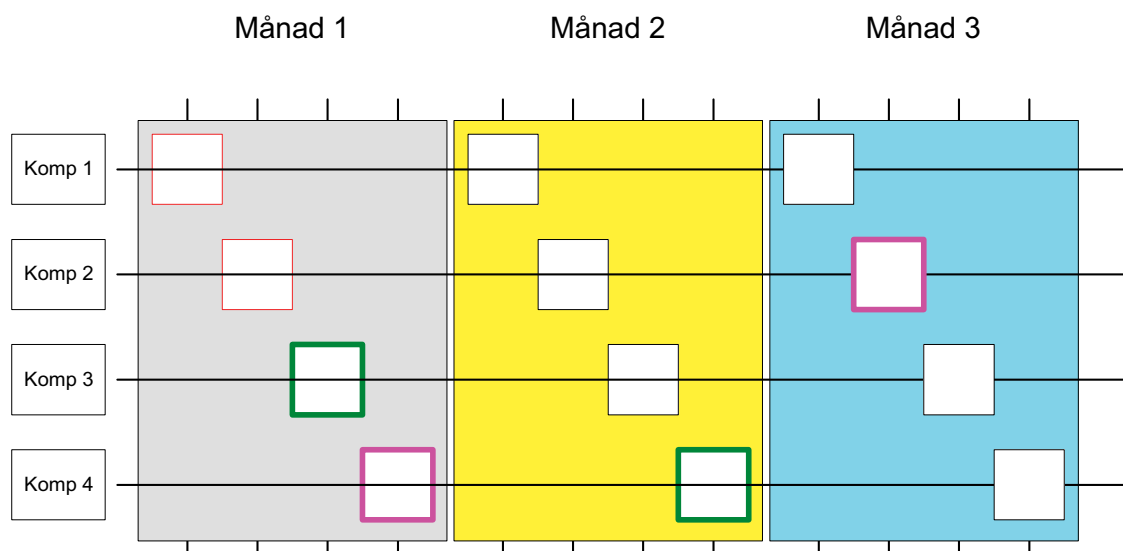
Följande är viktigt att känna till om CCF datainsamling:

- För att kunna förstå de faktorer, mekanismer som ligger bakom ett inträffat beroendefel, är det viktigt att all tillgänglig kvalitativ informationen efterfrågas och insamlas så fort som möjligt om CCF-händelsen. Själva bakgrundsanalysen måste dock få ta sin tid. Dokumentationen av CCF-händelsen måste också vara tillräckligt utförlig så att efterföljande ansträngningar om att förstå och värdera händelsen underlättas. Inspektör, granskare, analytiker måste anstränga sig en del och efterfråga väsentlig kvalitativ information om ett beroendefel skall förstås. En erfarenhet är att RO-materialet många gånger är för magert.
- För att säkerställa så bra kvalitativ information som möjligt om ett beroendefel av typen en CCF-händelse (ett CCF, degraderad tillgänglighet, begynnande fel) är det viktigt att det i händelserapporteringen anges analysfakta enligt exemplen som ges i bilaga 1 – exempel på *Group Record*, *Statistical Record* och *Event Record* enligt krav och definitioner i ICDE projektet. I bilaga 1 ges också exempel på hur kvalitativ information om en komponentfunktion kan ställas upp, beskrivas och förklaras i avsnittet om CCF-analys. Där ges också en beskrivning av hur en s.k. *Impact Vector* analys bör utföras.



## 4.2 Illustration av en CCF händelse

Många beroendefel upptäcks vid periodiska prov enligt STF, vid test och prov efter en underhållsåtgärd. Figuren nedan visar en vanlig provsituation (staggered testing) enligt ett STF-krav i ett fyrsubbat system. Elektriskt tillhör Komponent 1 och Komponent 3 A/C-sub och Komponent 2 och Komponent 4 B/D-sub.



Figur 2. Exempel på en tidbaserade CCF-händelser.

Nedan ges exempel på 2-faldiga CCF händelser. Testintervallet är var 4:e vecka för komponenterna i figuren ovan.

- komponent 1 och 2 drabbas av en likadan felorsak i test #1 månad 1 eller fel vid ett påkallat behov
- komponent 4 (test #1/månad 2) uppvisar samma felorsak som komponent 3 (vid test #1/månad 1) - fel inom ett testintervall
- komponent 2 (test #1/månad 3) och komponent 4 (test #1/månad 1) uppvisar samma felorsaker – fel inom två testintervall

Observera här att ett tidbaserat beroendefel enligt figuren kan variera mellan *Månad 1/komp 1* till *Månad 3/komp 4* för observationsgruppen. En extremvariant kan alltså uppstå då beroendefel upptäcks vid s.k. årsprov, då tiden mellan två testintervall blir mycket lång.

Se bilaga 2 för exempel på signifikanta svenska och utländska ICDE-händelser.

## 5 Försvar mot beroenden och beroendefel

Redundans införs när hög kvalitet och felsäkerhet inte är tillräckligt för att uppnå den önskade tillförlitligheten hos ett system eller anläggning. I anläggningar med redundans finns dock en mängd möjliga fysiska och funktionella beroenden som kan leda till att redundanta komponenter, system och strukturer blir otillgängliga samtidigt på grund av någon gemensam orsak.

Det finns alltså en risk för att system med redundanta utrustningar försvagas av fel med gemensam orsak (beroenden). System med *redundans*, måste därför ha skydd mot beroenden. En grundläggande strategi för att undvika beroenden är att redundanta utrustningar inte skall dela på gemensamma komponenter, t ex att två pumpar inte ska vara beroende av samma kraftmatning. En annan strategi är *fysisk (rumslig) separation* i syfte att skydda mot olika typer av händelser som samtidigt kan påverka mer än ett redundant stråk (exempelvis brand).

Det förekommer dock att redundant utrustning av olika skäl delar på komponenter, och även att den fysiska separationen är ofullständig. Detta är ofta medvetna beslut i konstruktionsprocessen, t.ex. att två redundanser delar på en passiv komponent, såsom ett rörsegment. På grund av rörsegmentets förväntade låga felsannolikhet, så uppnås ändå en tillräcklig barriär (låg sannolikhet) för att undvika utebliven funktion i systemen. Ett annat exempel kan vara ett kontrollsystem, där man har många viktiga komponenter inom ett begränsat utrymme. I detta fall kan skyddet mot t ex brand förstärkas med hjälp av brandskydd i kontrollrum (detektering och automatisk släckning). Det finns alltså möjlighet att vidta kompensande åtgärder i fall med ofullständig funktionell och fysisk separation.

En tredje strategi för att undvika beroenden är *diversifiering*, som införs på så sätt att olika systemdelar har olika konstruktion och olika driftförhållanden. Exempel är användning av dieslar och gasturbiner för att producera reservkraft, styrstavar och bor för att kontrollera reaktivitet och ett högtryckssystem och ett kombinerat trycknedtagnings- och lågtryckssystem för spädmatning. Diversifiering är dock sällan (om någonsin) fullständig. De flesta redundanser innehåller likheter i såväl passiva som aktiva komponenter. Via kopplingsfaktorerna hårdvara, organisation och miljö utgör de därmed risk för fel med gemensam orsak. Detta gäller också fall med till synes diversifierad utrustning, där det kan finnas delar av de diversifierade komponenterna eller systemen som är lika. Exempel kan vara interna delar som packningar och säkringar.

Fall med delad utrustning, delade utrymmen och likheter hos konstruktion och driftförhållanden innebär en risk för fel med gemensam orsak (CCF).

Samtidiga fel hos två komponenter i olika redundanta stråk kan bero på svagheter i grundläggande funktionell och fysisk separation, exempelvis genom att två redundanta komponenter visade sig ha ett ”dolt” signalberoende, eller att de delade på samma miljö vilken efter ett antal år oväntat leder till nedsatt funktion. Det kan också bero på beroenden via verktyg, instruktioner, personal, åldring, design, m.m. Som ett exempel, kan en felaktig specifikation leda till felaktig installation av en komponent; när samma specifikation används vid installation av flera komponenter finns risken att redundanta stråk påverkas.

Det är en omfattande och svår uppgift att etablera och påvisa fullständigt oberoende i alla dess aspekter mellan redundanta utrustningar, och det finns alltid en risk att något förbises. Man måste dock sträva efter att ha kontroll över de beroenden som finns och att införa åtgärder som är lämpliga och rimliga, och som används för att hålla nere risken för att beroenden försvagar den barriär som förväntas av anläggningens redundansgrad.

Det faktum att beroenden minskar styrkan hos anläggningens barriärer mot härdsador, kan hållas under kontroll (styras) genom att man har en robust installation med avseende på komponenters gränssnitt mot anläggningen.

Grundläggande kunskap om möjliga källor till beroenden gör det lättare att förstå hur enskilda felorsaker kan fortplantas till att påverka och försvaga anläggningens redundanser. Detta innebär att kunskap om beroenden är en del av försvaret mot fel med gemensam orsak. Kunskap kombinerat med professionell drift, underhåll och testning/kalibrering är en av de viktigaste mjuka barriärerna för att förebygga och upptäcka fall som kan leda till fel med gemensam orsak. Kraftbolagens egenkontroll STARK - Stanna upp, Tänk efter, Agera, Reflektera, Kommunicera – utgör också en viktig försvarslinje i strävan efter att minimera effekterna av fel med gemensam orsak.

Exempel på en inträffad händelse där delad utrustning påverkade säkerheten ges nedan.

<p><b>B2 - RO 4/99 – Bortfall av hjälpkylvatten</b></p> <p><b>Händelse</b></p> <p>Vid periodisk provning i system 711 stängdes av misstag 8 stycken ventiler för intag av havsvatten till hjälpkylsystemens pumpgröpar. Detta medförde att kylkapaciteten i hjälpkylsystemen 712, 713 och 714 uteblev helt. Automatiskt stopp av huvudcirkulationspumparna 313 P1-P4 erhöles på grund av hög oljetemperatur i frekvensomformarnas hydraulkoppling. Effektdrift kunde ej upprätthållas.</p> <p><b>Konsekvens</b></p> <p>Kortvarig utebliven kylkapacitet i samtliga hjälpkylsystem för kylning av dieselaggregat, resteffektkylsystem och inneslutningssprinkling. Bedömning enligt INES = 2. Manuellt reaktorsnabbstopp.</p> <p><b>Orsak</b></p> <p>Felaktig ventilmånöver vid periodisk provning i system 711 på grund av bristande egenkontroll vid provningens utförande.</p>
--

Figur 3. Exempel på inträffad händelse.

Exempel på händelse som visar på rumsberoende ges nedan.

ICDE id 40 – Byggnadsställning i batterirum orsakar kortslutning och beroendefel i batterier

### Händelse

En byggnadsställning orsakade en plötslig kortslutning i ett batterirum. Byggnadsställningen som var tillverkad av aluminium placerades olämpligt och kortslöt de oisolerade skenorna för 50 V DC systemet.

### Konsekvens

Kortslutningen slog ut samtliga batterier och utlöste snabbstopp på två reaktorer.

### Orsak

Orsaken till händelsen var bl.a. en (ur kortslutningssynpunkt) ogynnsam konstruktion av elsystemet, samt att arbetet utfördes med felaktig metod och av personal med bristande kompetens om de oisolerade skenarna och faran med detta.

Figur 4. Exempel på inträffad händelse.

Ett sätt att kompensera för otillräcklig funktionell och fysisk separation och diversifiering är *tidsseparation*. Tid är en viktig faktor som kan nyttjas för att undvika att de beroenden som trots allt alltid finns, påverkar redundanta komponenter. Tidsseparation kan möjliggöra upptäckt och därmed ge möjlighet till åtgärd av felorsaker som kan leda till att samma fel samtidigt uppstår hos flera komponenter, oavsett om dessa är redundanta eller ej. Detta är en åtgärd som huvudsakligen skyddar mot konstruktionsfel, installationsfel, underhålls- och testfel och åldring/miljöpåverkan. De typer av separation i tid som kan utnyttjas är:

- stegvis introduktion av ny utrustning för att samla erfarenheter innan fullständigt införande,
- stegvis introduktion av ny utrustning för att ha utrustning med olika ålder (vilket gör det möjligt att tidigt upptäcka fel till följd av åldring),
- tidsförskjutet testning, d.v.s. testning sker fördelad i tiden (t.ex. en sub per vecka). Alternativet är sekventiell testning, där samtliga komponenter testats sekventiellt (i turordning) vid samma tillfälle, och
- tidsförskjutet underhåll, d.v.s. underhåll sker fördelad i tiden (t.ex. en sub per vecka).

Tidsseparation blir ett ännu kraftfullare verktyg om det kombineras med ett effektivt system för *felrapportering och erfarenhetsåterföring*. Effektiv felrapportering kräver ledningens stöd och uppskattning, rutiner och verktyg, samt skicklig och motiverad personal med låg rapporteringströskel, d.v.s. god säkerhetskultur. Erfarenhetsåterföring och utbyte av erfarenheter med andra anläggningar och organisationer är ett annat område som behöver ha en god kvalitet för att bidra till upptäckt och spridning av information om möjliga beroenden. Effektiva ledningssystem för erfarenhetsåterföring, förebyggande underhåll och avhjälpande underhåll spelar här en viktig roll för

uppföljning och begränsning av åldersrelaterade fel både i elektronik och i mekanisk utrustning.

En bra *anläggningsdokumentation och –databas* för rapportering och erfarenhetsåterföring är ett väsentligt stöd för att på ett effektivt sätt kunna hantera beroenden. Detta gäller inte minst för att tidigt kunna upptäcka och förebygga fel med gemensam orsak i system där man av olika skäl inte har separation och diversifiering. Dokumentationen och databasen måste ha tillräcklig detaljnivå för att möjliggöra spårning av de gemensamma faktorer som finns, och speciellt för de komponenter, system och strukturer som är kritiska för säkerheten.

Man kan använda ett riskinformerat synsätt när man väljer detaljnivå för denna information för olika delar av anläggningen. Anläggningsdatabasen bör ha information om alla ändringsarbeten, ålder hos installerad utrustning, testscheman, rapporterade RO, och arbetsordrar. Säkerhetsbetydelsen hos enskilda komponenter/system och strukturer kan vara underlag för prioritering av såväl test och underhåll som övervakning och utformning av anläggningsdatabasen.

### **Sammanfattning**

Tre viktiga försvarsprinciper är:

- Grundkravet på redundans (genom undvikande av gemensamma system, komponenter och strukturer)
- Fysisk separation (genom avstånd och väggar)
- Diversifiering (grundläggande olikhet i konstruktion)

Till ovan kommer utnyttjande av tid och andra kompenserande åtgärder.

## 6 Vägledning vid tillsyn

I det följande avhandlas vilken information angående CCF som kan vara användbar vid tillsynsinsatser. Intressanta frågor ges, som kan vara till hjälp vid såväl förberedelse av tillsynsinsats som själva utförandet.

Nedan ges ett antal exempel på frågor som allmänt kan var lämpliga att ställa avseende beroendefel av CCF-karaktär vid en tillsynsinsats:

- Vilka är de risksignifikanta komponenterna?
- Vilka är de dominerande felmoderna?
- Vilka är de oftast återkommande felorsakerna?
- Vilka hjälpsystem och/eller –komponenter är felbenägna eller oftast drabbade av fel?
- Vilka är de riskviktiga kopplingsfaktorerna?
- Vilka är de viktiga försvarsåtgärderna mot ett återuppreppande?
- Vilka exempel från ICDE-projektet kan visa på unika CCF händelser som inträffat?
- Vilka ”CCF strategier” tillämpar tillståndshavarna vid t.ex. test och underhåll eller vid anläggningsändringar i flera subbar?

Efter F1-händelsen är följande en relevant fråga att försöka besvara:

- Vilka beroenden kan eventuellt finnas mellan säkerhetssystem och driftsystem (djupförsvarssystem)?

Information från PSA-analyser kan samlas in och summeras på system- och komponentnivå. Denna information kan användas för att identifiera vilka system, komponenter och felmoder som är mest risksignifikanta. Kunskap om CCF kan vara till hjälp för att veta vad man bör leta efter vid en tillsynsinsats. Nedan listas ett antal frågor som kan vara till hjälp vid förberedelse och genomförande av en tillsynsinsats, vid såväl tillsyn av PSA-verksamhet som annan verksamhet.

Exempel på frågor att ställa, på systemnivå:

- Vilka system eller delsystem är de mest risksignifikanta avseende CCF?
- Vilka komponenter är de mest risksignifikanta avseende CCF?
- Vad är det dominerande bidraget till frekvensen för härdskada?

Exempel på frågor att ställa, på komponentnivå:

- Är detta en risksignifikant komponenttyp?
- Hur viktigt är CCF för denna komponenttyp?
- Vilka är de dominerande felorsakerna för inträffade CCF-händelser hos denna komponenttyp?
- Vilken är den vanligaste felmoden?
- Hur upptäcks CCF-händelserna?
- Vilka är de vanligaste kopplingsmekanismerna?

- Hur kan man undvika att denna händelse återupprepas?

Följande frågor kan vara till hjälp för att samla in information i samband med en inträffad händelse:

- Är risksignifikanta komponenter inblandade i händelsen?
- Kan det bevisas att det inte är frågan om CCF?
- Vad kan man lära sig av drifterfarenheten från denna händelse?
- Vad säger CCF-historiken om detta fel?
  - Hur har CCF-händelserna upptäckts?
  - Hur är felen sammankopplade?
- Hur kan man undvika att denna händelse återupprepas?

Med utgångspunkt i de olika typer av försvar som redovisats i tidigare avsnitt framkommer ett antal områden som kan vara intressanta att belysa vid en tillsynsinsats. Nedan listas ett antal frågor som kan vara värt att fundera kring i samband med förberedelse och utförande av tillsynsinsats. Beroende på typen av tillsyn kan frågorna specificeras och formas efter behov.

- Undviks delade komponenter/system/strukturer?
- Undviks delade utrymmen?
- Har man strävat efter diversifiering?
- Finns medvetenhet om beroenden?
- Har man valt enkla lösningar?
- Hur behandlas kunskap och erfarenhet?
- Är säkerhetskulturen god?
- Finns effektiv erfarenhetsåterföring?
- Tillämpar man granskning i flera steg?
- Tillämpas tidsförskjuten testning?
- Hur används informationssystem (anläggningsdatabas)?

Ytterligare förkovran om beroende, beroendefel och försvar mot desamma, se SKI Rapport 2004:01 volym 1 och 2.

En annan rapport som ger mycket fakta om CCF är NUREG/CR-6268.

## 7 Slutsatser

Nyckeln till att undvika att beroenden försvagar anläggningen är att ha en fortlöpande kontroll av beroenden under anläggningens konstruktion, byggnation och drift. Det händer att diversifiering beskrivs som lösningen på problemet, men i denna diskussion bör det påpekas att även detta är en åtgärd som måste vägas mot redundanser och inte minst att komplicerade konfigurationer är riskfyllda i CCF-sammanhang. Det enda som egentligen kan ge svaret om huruvida lösningen ligger i diversifiering eller inte är kommande erfarenheter av denna typ av skyddsåtgärd.

För analys och insamling av erfarenheter av CCF är det av stor vikt att ha bra RO-rapportering och uppföljning av de för anläggningen analyserade felmoderna. Att detta görs på ett kvalitativt sätt är viktigt för att informationen ska vara användbar och ge bättre analysarbete, vilket i sin tur leder till ett mer kostnadseffektivt arbete.

Tillgången till information genom ICDE-projektet har här visat sig vara synnerligen kostnadseffektiv, då datautbytet i stor omfattning är till fördel för Sverige som endast svarar för en mycket liten andel av den totala tillgängliga datamängden vilket betyder att vi i utbyte mot en mindre mängd data får tillbaka en mycket större mängd.

En av uppgifterna med denna rapport har varit att ta fram exempel på frågor tillämpliga i granskningssammanhang. Slutresultatet har visat att detta har varit framgångsrikt, samtidigt som det också kan poängteras att stora möjligheter för utveckling finns avseende detta genom vidareutveckling av informationen till att anpassas för specifika tillämpningar.

Vid beaktande av behandling av CCF bör man vara medveten om att detta är ett område där det kontinuerligt sker nya framsteg. Nya data samlas ständigt in samtidigt som mer och mer erfarenheter fås med tiden. Det bör därför även poängteras att det är angeläget att ständigt hålla rapporter av den här typen uppdaterade och att utrymme finns för vidare utveckling. Ett alternativt sätt för vidare bearbetning är att vidareutveckla informationen i denna rapport för framtagande av Tillsynshandbok i ämnet. Mycket av informationen presenterad i denna rapport kan väl utgöra underlag för en sådan handbok, men det återstår en del arbete i form av bearbetning av innehåll och anpassning av innehåll till förekommande tillsynsverksamhet.

Detta är också ett område som på olika sätt utvecklas i något parallella spår. Olika länder och anläggningar använder sig av olika databaser och för varierade syften. Det är dock önskvärt att i den mån det är möjligt att följa redan antagna konventioner för att möjliggöra/underlätta nyttjande av informationskällor. Exempel på detta är utformning av händelsedatabaser, som om möjligt kan rekommenderas följa etablerad ICDE-klassning. I denna typ av databaser bör även grundinställningen vara att en inträffad händelse är en CCF-händelse, något som ska gälla tills motsatsen är bevisad (inte tvärtom vilket ofta tillämpas). Förekommande klassning inom ICDE är även något som kan användas för att faktiskt utesluta att det handlar om en CCF-händelse (finns ingen gemensam orsak eller kopplingsmekanism är det inte heller frågan om en CCF-händelse, även om det bör poängteras att detta är faktorer som inte sällan är svåra att identifiera).



## 8 Referenser

- [1] A. Mosleh, D. M. Rasmuson and F. M. Marshall (USNRC). *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. November 1998. NUREG/CR-5485.
- [2] Atkins. *International Common Cause Failure Data Exchange, A Report Analysing the Occurrence of Common Cause Failure Events on UK Safety Relief Valves*. April 2005. Rapport id 5028120/D005 Rev 000.
- [3] Becker G, Jänkälä K, Johanson G, Knochenhauer M, Lindberg S, Schubert B, Vaurio J, Wohlstein R. *Dependency analysis guidance, Nordic/German Working Group on Common Cause Failure Analysis, Phase 1 project report: Comparison and application to test cases*. Oktober 2007. SKI rapport 2007:041.
- [4] Dale Rasmuson (USNRC). *Use of ICDE Event Information in Inspections of Nuclear Power Plants*. Presentation held at the ICDE workshop in Liverpool, October 2006.
- [5] Dale Rasmuson, Peter Appignani (USNRC). *Use of Common-Cause Failure Information in Inspections of Nuclear Power Plants*. Augusti 2006.
- [6] G Johanson, P.Hellström, T.Mankamo, J-P. Bento, M.Knochenhauer, K.Pörn. *Dependency Defence and Dependency Analysis Guidance*. October 2003. SKI Rapport 2004:04 volym 1 och 2.
- [7] M. Marshall, A. Mosleh and D. M. Rasmuson (USNRC). *Common-Cause Failure Database and Analysis System (Volym 1-4)*. Juni 1998. Rapport id NUREG/CR-6268.
- [8] OECD NEA. *ICDE Project Report: Collection and Analysis of Common-Cause Failures of Batteries*. September 2003. Rapport id NEA/CSNI/R(2003)19.
- [9] OECD NEA. *ICDE Project Report: Collection and Analysis of Common-cause Failures of Centrifugal Pumps*. October 2007. Rapport id NEA/CSNI/R(1999)2.
- [10] OECD NEA. *ICDE Project Report: Collection and Analysis of Common-Cause Failures of Check Valves*. May 2003. Rapport id NEA/CSNI/R(2003)15.
- [11] OECD NEA. *ICDE Project Report: Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators*. February 2001. Rapport id NEA/CSNI/R(2000)20.

- [12] OECD NEA. *ICDE Project Report: Collection and Analysis of Common-Cause Failures of Motor Operated Valve*. Februari 2001. Rapport id NEA/CSNI/R(2001)10.
- [13] OECD NEA. *ICDE Project Report: Collection and Analysis of Common-Cause Failures of Safety and Relief Valves*. October 2002. Rapport id NEA/CSNI/R(2002)19.
- [14] OECD NEA. *ICDE Project report: Collection and Analysis of Common-Cause Failures of Switching Devices and Circuit Breakers*. Oktober 2007. Rapport id NEA/CSNI/R(2008)1.
- [15] OECD NEA. *ICDE Project report: Collection and Analysis of Common-Cause Failures of Heat Exchangers*. Draft Ralph Nyman, to be finished shortly. (Rapport id NEA/CSNI/R...).
- [16] OECD NEA. *International Common-cause Failure Data Exchange: ICDE General Coding Guidelines (Technical note)*. Rev.5. Rapport id NEA/CSNI/R(2004)4.
- [17] OECD NEA. *Summary of the ICDE project*. 2004. Rapport id ICDEPR00.
- [18] Sandra Lindberg. *Common cause failure analysis: Methodology evaluation using Nordic experience data*. Maj 2007. UPTEC STS07 024 (Uppsala Universitet).
- [19] SKI. *Statens kärnkraftinspektions föreskrifter om konstruktion och utförande av kärnkraftsreaktorer*. 2004. SKIFS 2004:2.
- [20] SKI. *Statens kärnkraftinspektions föreskrifter om säkerhet i kärntekniska anläggningar*. 2004. SKIFS 2004:1.
- [21] Tuomas Mankamo, Avaplan Oy. *Common Cause Failure Analysis of Control Rods and Drives in the Swedish and Finnish BWR plants, Operating Experiences in 1983-2003*. November 2006. SKI rapport id 2006:05. (Denna rapport uppdaterar tidigare SKI Rapport 1996:77).
- [22] TUD-kansliet. *T-Boken version 6, Tillförlitlighetsdata på komponenter i nordiska kärnkraftreaktorer*.
- [23] Tuomas Mankamo Avaplan Oy. *Common Cause Failure Analysis of Control Rods and Drives in the Swedish and Finnish BWR Plants Operating Experiences in 1983-2003*. Presentation at the RADDA seminar 2007-02-15.
- [24] Tuomas Mankamo, Avaplan Oy. *Presentation of the Nordic CRDA Study - Assessment and Merging of Impact Vectors, Estimation of CLM Parameters*. Held at the ICDE Quantification workshop in Stockholm 24th of April 2007.

# Bilaga 1: Viktiga CCF-parametrar, händelserapportering och CCF-analys

## CCF-parametrar

Vid granskning och analys av CCF-händelser finns ett antal parametrar som är av stor betydelse. Viktiga CCF-parametrar, knutna till de fyra kriterierna för en CCF-händelse angivna i huvudrapportens fjärde kapitel, är följande:

Kriterium 1 – Komponentpåverkan (eng. impairment):

- Storlek på exponerad population
- Omfattning av komponentdegradering

Kriterium 2 – Tidsramar för inträffade fel:

- Tidsfaktorer

Kriterium 3 – Orsak till felen:

- Grundläggande felorsak (eng. root cause)
- Kopplingsfaktor
- Gemensam och delad felorsaks faktor

Andra viktiga parametrar är:

- Upptäcktssätt
- Korrigering åtgärder

I följande avsnitt ges mer detaljerad beskrivning av dessa parametrar. Mer detaljerade beskrivningar av parametrar, kategoriseringar, etc. ges i [16].

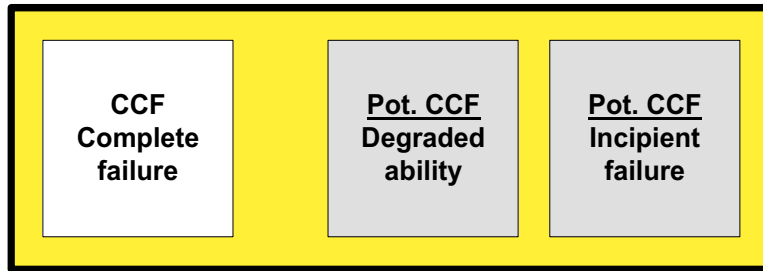
### **Storlek på exponerad population (number of exposed components)**

En exponerad population är den mängd av liknande eller identiska komponenter som faktiskt har exponerats för aktuell gemensam felorsak men kan ändå påverkas i olika omfattning, vid en observerad CCF-händelse. Se vidare kapitel 2 för beskrivning av indelning i populationer och grupper.

### **Komponentdegraderingen (component impairment)**

Konsekvensen av en CCF händelse är också viktig att känna till i ett risk- och PSA sammanhang, eftersom den kan variera mellan fullständigt utebliven funktion, degraderad och obetydlig påverkan på en funktion.

Vid en inträffad händelse kan ingående komponenters funktion ha påverkats i olika omfattning. Om CCF misstänks vara inblandat i händelsen utgör omfattningen av aktuell påverkan en viktig del i bedömningen av händelsen. Detta illustreras i figur 1 nedan.



Figur 1. Illustration av en CCF händelse.

Ett komponentdegraderingsvärde är ett mått på en komponents funktionella status i en komponentgrupp. Följande koder tillämpas:

- Complete CCF* (kod C) Fullständigt fel på komponent som förhindrar dess funktion  
*Degraded ability* (kod D) Degraderad tillgänglighet på komponent som påverkar dess funktion och en felfria drift  
*Incipient failure* (kod I) ett fel i begynnelse stadiet, begynnande. Felet förhindrar ännu inte komponentfunktionen men kan göra det vid ett påkallat behov  
*Working* (kod W) komponent inom komponentgruppen fungerar på avsett sätt, (en sådan komponent är viktig att känna till för att kunna bestämma vilken utbredning en CCF händelse har).

I syfte att utföra kvantifiering tilldelas även koderna numeriska värden enligt:

Kod C	1
Kod D	0.5
Kod I	0.1
Kod W	0

Den utförda klassningen kan sedan representeras som en komponentdegraderingsvektor. I tabellen nedan ges ett exempel på hur utfallet av klassningen kan se ut vid en CCF-händelse.

Påverkade komponenter	Kod/ degraderingsvektor	Numeriskt värde/numerisk degraderingsvektor
Komponent 1	C	1
Komponent 2	C	1
Komponent 3	W	0
Komponent 4	I	0,1
	(C, C, W, I)	(1, 1, 0, 0.1)

Tabell 1. Exempel på klassning av en CCF-händelse.

### Tidsfaktor (time factor)

Tidsfaktorn är ett mått på simultaniteten hos de multipla degraderingarna vid inträffad händelse, vilken bestäms av tiden som passerar mellan upptäckterna av felhändelserna.

Liksom vid klassning av komponentdegradering tilldelas även numeriska värden. Tillämpade koder anges nedan.

Kod:	Numerisk värde:
High (H)	1.0
Medium(M)	0.5
Low (L)	0.1

### **Felorsak (root cause)**

En root cause är den mest grundläggande, gemensamma, orsaken till komponenternas felande vid en CCF-händelse. Följande kategorisering av felorsaker görs inom ICDE:

- State of other component(s) (ICDE kod C)
- Design, manufacture or construction inadequacy (ICDE kod D)
- Abnormal environmental stress (ICDE kod A)
- Human actions (ICDE kod H)
- Maintenance (ICDE kod M)
- Internal to component, piece part (ICDE kod I)
- Procedure inadequacy (ICDE kod P)
- Other (ICDE kod O)
- Unknown (ICDE kod U)

### **Kopplingsfaktor (coupling factor)**

Kopplingsfaktor, eller kopplingsmekanism, är något gemensamt mellan två eller flera komponenter (företrädesvis redundanta) som medför att komponenter felar på grund av samma orsak. Inom ICDE görs kategorisering av dessa mekanismer enligt nedan:

- Hardware (component, system configuration, manufacturing quality, installation configuration quality) (ICDE kod H)
  - Hardware design (ICDE kod HC)
  - System design (ICDE kod HS)
  - Hardware quality deficiency (ICDE kod HQ)
- Operational (maintenance/test (M/T) schedule, M/T procedures, M/T staff, operation procedure, operation staff) (ICDE kod O)
  - Maintenance/test (M/T) schedule (ICDE kod OMS)
  - M/T procedure (ICDE kod OMP)
  - M/T staff (ICDE kod OMF)
  - Operation procedure (ICDE kod OP)
  - Operation staff (ICDE kod OF)
- Environmental (internal, external) (ICDE kod E)
  - Environmental internal (ICDE kod EI)
  - Environmental external (ICDE kod EE)
- Unknown (ICDE kod U)

### **Faktor för gemensam felorsak (shared cause factor)**

Enligt definitionen är en CCF-händelse ett resultat av en ensam gemensam orsak till degradering. En händelsrapport innehåller dock inte nödvändigtvis alltid tillräckligt med information för att bestämma om den bakomliggande orsaken är gemensam, eller om felen orsakats av olika orsaker. Denna parameter utgör ett verktyg för att bedöma *tillförlitligheten* för att det faktiskt handlar om en gemensam bakomliggande orsak till aktuella degraderingar, där en hög faktor indikerar att förtroendet är högt för att påverkan på komponenterna är ett resultat av gemensam orsak. Liksom vid klassning av komponentdegradering och tidsfaktor tilldelas även numeriska värden. Tillämpade koder anges nedan.

Kod:	Numerisk värde:
High (H)	1.0
Medium(M)	0.5
Low (L)	0.1
No	0

### **Upptäcktsätt (detection mode)**

Denna parameter indikerar hur respektive komponentfel har upptäckts. ICDE tillämpar följande kategorisering:

- Monitoring on walkdown (ICDE kod MW)
- Monitoring in control room (ICDE kod MC)
- Maintenance/test (ICDE kod MA)
- Demand event (ICDE kod DE)
- Test during operation/annual overhaul/laboratory (ICDE kod TI/TA/TL)
- Unscheduled test (ICDE kod TU)
- Unknown (ICDE kod U)

### **Korrigerande/avhjälpande åtgärder (corrective actions)**

Parametern beskriver de korrigerande/avhjälpande åtgärder som vidtagits av tillståndshavaren för att motverka att CCF-händelsen återupprepas. Kodning görs inom ICDE enligt:

- General administrative/procedure controls (ICDE kod A)
- Specific maintenance/operation practices (ICDE kod B)
- Design modifications (ICDE kod C)
- Diversity (ICDE kod D)
- Functional/spatial separation (ICDE kod E)
- Test and maintenance policies (ICDE kod F)
- Fixing of component (ICDE kod G)
- Other (ICDE kod O)
- Unknown (ICDE kod U)

## CCF-rapportering

I ett PSA-sammanhang identifieras och analyseras CCF traditionellt mellan två eller flera liknande komponenter i redundanta stråk och i ett gemensamt system. En grupp av komponenter som anses ha hög potential för fel med gemensam orsak benämns som en ”*Common Cause Component Group*” (CCCG). Ett exempel på en CCCG är en anläggningsuppsättning av dieselgeneratorer (DG). DGer finns i Sverige och i Europa finns vanligtvis i 2- och 4-stråksanläggningar, dvs CCCGer av storlekarna 2 och 4. Inom ICDE används även konceptet ”population”. En *observerad population* (observed population), OP, är en grupp av liknande eller identiska komponenter. I allmänhet är en OP en samling av alla liknande komponenter inom ett system, t ex alla motormanövrerade ventiler i hjälpmavassystemet, men en OP kan även bestå av komponenter från mer än ett system. Om möjligt och passande kan OP definieras av bestämd CCCGer. En *exponerad population* (exposed population), EP, är en samling av liknande eller identiska komponenter som faktiskt har blivit utsatt för den specifika gemensamma orsaken i en observerad CCF-händelse. I vissa fall är OP, EP och CCCG identiska. Storleken på EP är ofta densamma som storleken på CCCGen, men eftersom ett specifikt fel inte nödvändigtvis påverkar alla komponenter i OP, kan storleken på EP vara mindre än storleken på OP.

För varje unik OP/CCCG skall en *komponentgruppsdefinition* (group record) och ett *statistisk datablad* (statistical record) upprättas. Exempel på sådana i ICDE-projektet ges i tabell 2 och 3. En komponentgruppsdefinition ska innehålla information om bl.a. anläggning, komponenttyp, testintervall, populationsstorlek. Ett statistisk datablad utgörs av parameterinformation om en aktuell OP/CCCG så att diverse beräkningar kan utföras. Exempel på ingående parametrar är felmoder, observationsstart, observationslut, antal oberoende fel, antal behov.

För varje rapporterad CCF-händelse ska ett *händelseregister* (event record) skapas. Detta register ska innehålla information om bl.a. felmod, händelsebeskrivning, tolkning av händelsen, felorsak, kopplingsfaktor. Vidare ska även specifikation göras som omfattar upptäcktsätt, datum om tid för upptäckt, latent tid och komponentdegradering. Se exempel i tabell 4 och 5.

**Observed Population Record:**

<b>G0 OP Name:</b>	USA\US-XXA\3.AF\12\RV-PO\A.2c		
<b>Country:</b>	USA	<b>Reactor Type:</b>	PWR
<b>G2 Plant Code:</b>	US-XXA	<b>Plant Name:</b>	Plant A
<b>G3.1 System Type:</b>	3.AF		
<b>System:</b>	Pressure control (includes primary safety relief valves)		
<b>G3.2 System Sub:</b>	12		
<b>System Sub Type:</b>	No data		
<b>G4 Component Type:</b>	RV-PO		
<b>Component:</b>	PWR pressurizer power operated relief valve		
<b>G4.1 Comp. Sub Type:</b>	A.2c		
<b>Comp. Sub Type:</b>	Pneumatic pilot valve		
<b>G5.1 Test Interval:</b>	1350 days		
<b>G5.2 Test Procedure:</b>	Staggered		
<b>G6 Group Size:</b>	2		
<b>G7 Manufacturer:</b>	Unknown		
<b>G8 OP Number:</b>	na		
<b>G1 Definition:</b>	Pressure control (includes primary safety relief valve PWR pressurizer power-operated relief valve)		

Tabell 2. Exempel på en komponentgruppsdefinition.

**Statistical Records:**

<b>S1 Failure Modes</b>	<b>S3 Obs. Start</b>	<b>S4 Obs. End</b>	<b>S5 Ind. Count</b>	<b>S5 Flag</b>	<b>S6 Comp Exp.</b>	<b>S7 Number of Demands</b>	<b>Obs. Time</b>
IL	1990-01-01	1995-12-31	0.00	Real Count	na	na	6.0 yrs
FOL	1990-01-01	1995-12-31	0.00	Real Count	na	na	6.0 yrs
FC	1990-01-01	1995-12-31	0.00	Real Count	na	na	6.0 yrs

Tabell 3. Exempel på ett statistiskt datablad.



**C01 Event identifier:**D-XXX-92-0758-CC

**C03 Failure mode:** FO (Failure to open)

**C04 Number of Exposed Components:** 4

**G06 Population Size:** 4

**C05 Event Description:**

04/29/92 Power Level- 99%. On 10/5/92, it was determined that prior to 5/1/92 Unit 2 could have potentially been in a condition that was outside of the plant's design basis. It was determined that prior to 5/1/92, both loops of the Torus cooling mode of the Residual Heat Removal System may not have been able to provide containment cooling under certain design basis events. On 4/29/92, the Torus cooling injection motor-operated valve MO-2-10-34B was found to have cracks in the valve yoke. On 8/7/92, the Torus cooling injection MO valve MO-2-10-34A in the redundant loop was also discovered with cracks in the yoke. The cause of the potential loss of Torus cooling capability is due to cracks in the yokes of the Torus cooling injection valves. The exact cause of the cracking is uncertain; however potential causal factors have been identified. There were no actual safety consequences as a result of this condition. The Torus injection valves were repaired and inspected for cracks and none were found. An evaluation will be performed to review other valves.

**C07 Event Interpretation:**

Torus cooling MOVs had cracks in valve yolk 34A & 34B.

**C08 Component Impairment:** I I W W

**C09 Root Cause:** Internal to component, piece part

**C10 Coupling Factor(s):** Hardware (component part, system configuration, manufacturing quality, installation/configuration quality)

**C11 Shared Cause Factor:** High

**C12 Corrective Action:** General administrative/procedure controls

**C14 Timing Factor:** Low

**Event Specification:**

C2-1 Event Date	C2-2 Latent Time	C8 Component Impairment	C6 Detection
4/29/1992	274	Incipient failure	Maintenance/test
8/7/1992	–	Working	–
8/7/1992	–	Working	–
8/7/1992	274	Incipient failure	Maintenance/test

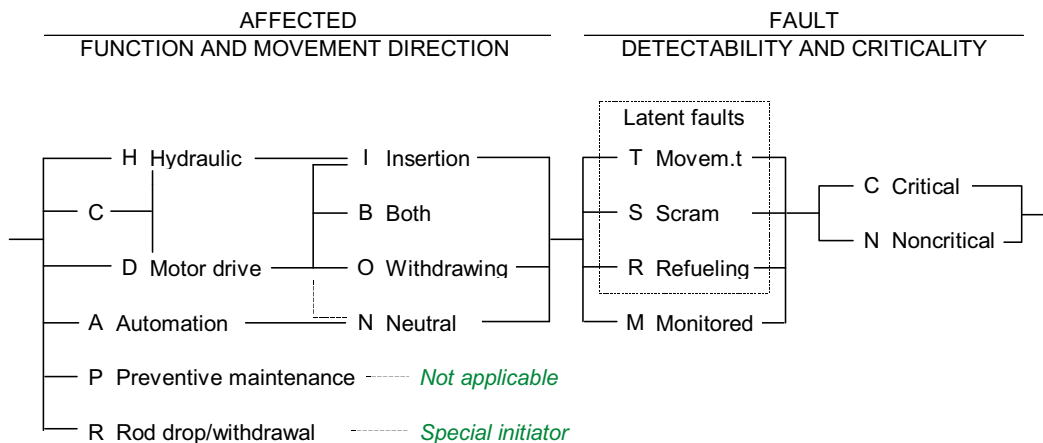
Tabell 4. Exempel på ett händelseregister.

## CCF-analys

Det finns i olika sammanhang ett behov att värdera den inverkan som beroenden har på säkerheten. Syftet kan vara både att få en uppskattning av storleken hos säkerhetspåverkan från beroenden, att identifiera betydande men okända beroenden, eller att få en möjlighet att prioritera bland möjliga åtgärder syftande till att minska beroenden. En mycket viktig aspekt är att identifiering och modellering av specifika beroenden i sig är en viktig del av försvaret mot flertalet typer av beroenden. Detta innebär att det finns ett behov av metoder för att analysera olika typer av beroenden. Metoderna skiljer sig något åt för olika typer av beroenden. Normalt bedrivs analyserna inom en PSA, men kan även ske separat.

I det följande ges ett exempel på hur en beroendefelsanalys skall utföras.

I sammanställningen nertill visas funktionen för styrostavar och analysstegen för att bestämma kritiska fel och felmoder för analys i ett PSA sammanhang och när dessa kan upptäckas.



#### AFFECTED FUNCTION

H Hydraulic function  
D Motor drive function  
C Common to hydraulic and motor drive function  
A Automation and instrumentation, including position measurement

#### AFFECTED MOVEMENT DIRECTION

I Insertion only  
B Both directions  
O Withdrawing only  
N Neutral or negligible

#### SPECIAL CLASSES

P Preventive, scheduled maintenance, undertaken in plant shutdown state  
R Rod drop or inadvertent withdrawal, special type of initiator

#### FAULT DETECTABILITY

L Latent faults  
T Detectable in periodic movement tests  
S Detectable only in scram test or demand  
R Refueling outage: overhaul inspections and maintenance  
M Monitored faults (detected shortly by instrumentation or process symptoms)

#### FAULT CRITICALITY

C Critical  
N Noncritical

#### GENERIC CLASSES OF FAILURE MECHANISMS

FrObj Foreign object, jamming  
Fulns Fully inserted position, jammed into pos. = 0%  
NutSp Drive nut separation at pos. > 0%  
MetPd Metal powder problem at TVO I in 1989-90  
MTrip Moment trip  
CrRod Cracking of control rod  
PosMs Position measurement failure  
DChkV Drive check valve blocked  
SLeak Seal leaks, external leaks  
ErrRM Faults introduced in repair or maintenance

#### Special classes

PrevM Preventive maintenance  
RDrop Rod drop or inadvertent withdrawal

I dataanalyser av CCF-händelser tillämpas ofta *impact vector*-tekniken. En impact vector är en generaliserad representation av utfallet av ett behov, i form av antalet felande komponenter i en CCCG. I en CCCG av storlek "n" har dess impact vector "n+1" element;  $v = [v_0, v_1, \dots, v_n]$ . I det mest grundläggande fallet, där funktionen hos

varje komponent vid behovet är fullständigt känt som helt fungerande eller fullständigt felande, kan antalet fel bestämmas exakt; impact vector-elementen är då 0, förutom för de komponenter som felat enligt nedan.

$v = [1, 0, \dots, 0]$ , då all komponenter fungerade

$v = [0, 1, 0, \dots, 0]$ , då en komponent felade och "n-1" fungerade

$v = [0, 0, 1, \dots, 0]$ , då två komponenter felade och "n-2" fungerade

$v = [0, 0, \dots, 1]$ , då alla komponenter felade

Den svåraste delen av CCF-analys är tolkningen och utvärderingen av de multipla komponenthändelserna, vilka ofta representeras av otydliga fall där dessutom tillgänglig information oftast är bristfällig. Den vanligaste tekniken för att hantera detta är scenariometoden, vilken går ut på att olika scenarier ansätts för olika alternativa tolkningar av en händelse. Tekniken är mycket användbar i situationer där ett specifikt utfall inte är helt känt, utan möjligheten finns för olika alternativa utfall, dvs där impact vector-elementen inte är 0 eller 1 utan antar värden däremellan. I analysen visas expertbedömningar på hur CCF-händelser bedöms kunna påverka olika redundansgrader, dvs en analys för uppskattning av sannolikheter för CCF för olika redundansgrader och analysbetingelser om de skulle uppstå vid ett verkligt behov.

Exempel på konstruktion av Impact Vector, med tillämpning av scenariometoden, ges nedan.

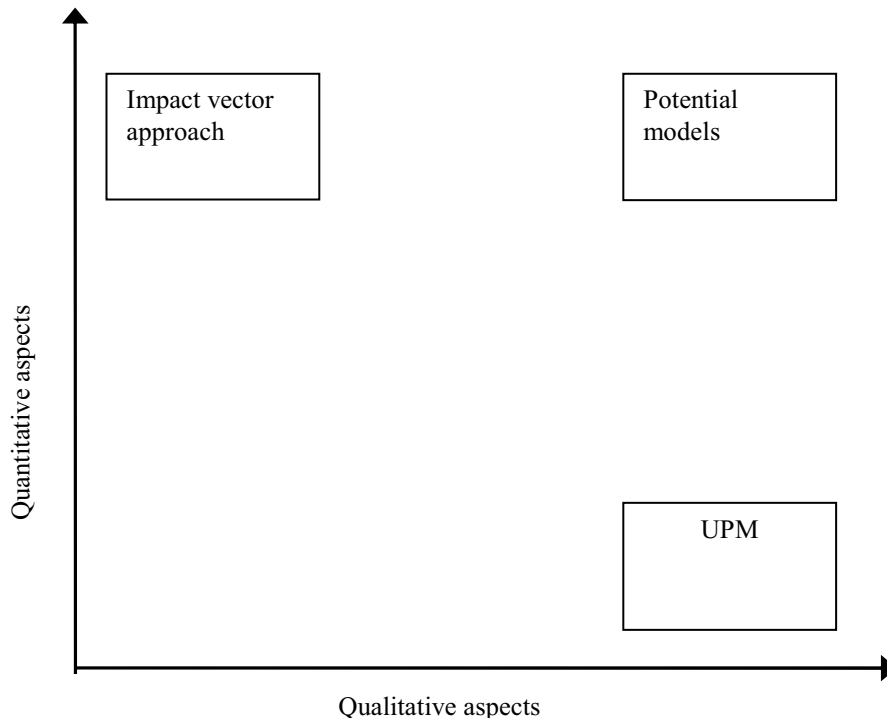
För en CCF-händelse i en grupp av tre centrifugalpumpar ansågs pump A vara "completely failed" på grund av en lagerskada, lagren i pump B fanns också vara degraderade medan en ytterligare inspektion visade att pump C var opåverkad. Detta resulterar i två tänkbara scenarier. Scenario (1) innebär att endast pump A felar vid ett faktiskt behov, motsvarande impact vector (0, 1, 0, 0). Scenario (2) innebär att både pump A och pump B felar vid ett faktiskt behov, motsvarande impact vector (0, 0, 1, 0). Sannolikhetsfördelningen mellan de olika scenarierna anges som vikt för respektive scenario. Resultatet, i form av en impact vector, ges sedan av multiplikation mellan ansatt vikt för respektive scenario och motsvarande impact vector. Se exempel i tabell 6 nedan.

Scenario	Weight	Impact vector elements				Element sum
		0	1	2	3	
1. Only pump A would fail given actual demand mission	0.9	0	1	0	0	1
2. Pumps A and B would fail ..., while C would survive the mission	0.1	0	0	1	0	1
Net Impact Vector		0	0.9	0.1	0	1

Tabell 5. Exempel på en Impact Vector-analys.

Metoden beskrivs utförligt i [1, 6].

För modellering av CCF kan två separata vägar urskiljas, där den ena fokuserar på kvantitativa och den andra på kvalitativa aspekter. Ett vanligt sätt att hantera CCF-analys är tillämpning av impact vectors så som beskrivits ovan. Detta är dock en metodik som inte behandlar kvalitativa aspekter. Ett exempel på metod inriktad på det andra spåret är UPM (Unified Partial Method), vilken hanterar delar av de aspekter som impact vector-tekniken saknar men å andra sidan inte tillhandahåller tillfredställande kvantifiering. Detta är en situation som i stor utsträckning representerar förhållandena inom området, där kvalitativ och kvantitativ utvärdering i regel sker separerade från varandra.



Figur 2. Positionering av olika CCF-metoder.

Ovan illustreras situationen med olika metoder för CCF-modellering och hur de förhåller sig till varandra avseende kvalitativa och kvantitativa aspekter. I figuren indikeras också "potentiella modeller", vilket avser metoder som hanterar båda dessa aspekter. En studie av möjligheterna att närma sig en sådan modell ges i [18].

Det som i detta avseende är viktigt att notera är betydelsen av att ha bra data, såväl kvalitativt och kvantitativt, för att öka möjligheterna att skapa realistisk modellering och tolkning. Detta betyder i praktiken att bra händelseanalys och RO-rapportering är av mycket stort värde.

## Bilaga 2: Exempel på signifikanta svenska och utländska ICDE händelser

### **ICDE id 40 Byggnadsställning i batterirum orsakar kortslutning och beroendefel i batterier**

#### **Händelse**

En byggnadsställning orsakade en plötslig kortslutning i ett batterirum. Byggnadsställningen som var tillverkad av aluminium placerades olämpligt och kortslöt de oisolerade skenorna för 50 V DC systemet.

#### **Konsekvens**

Kortslutningen slog ut samtliga batterier och utlöste snabbstopp på två reaktorer.

#### **Orsak**

Orsaken till händelsen var bl.a. en (ur kortslutningssynpunkt) ogynnsam konstruktion av elsystemet, samt att arbetet utfördes med felaktig metod och av personal med bristande kompetens om de oisolerade skenorna och faran med detta.

### **ICDE id 6030 Kraftiga vibrationer orsakar beroendefel i backventiler**

#### **Händelse**

Under ett återkommande test av backventiler i reaktorns kylsystem uppstod plötsligt mycket kraftiga vibrationer.

#### **Konsekvens**

Vibrationerna var så kraftiga att två 15 mm dräneringsrör gick av.

#### **Orsak**

Orsaken till denna CCF var felaktigt underhåll och en misslyckad montering av ventilernas grafitpackningar. Packningarna dimensionerades fel och utgjorde helt enkelt ett fysiskt hinder för kolven i ventilerna när de skulle stängas.

### **ICDE 9057 Tömd tank orsakade beroendefel på dieselgeneratorer**

#### **Händelse**

Vid underhållsarbete förväxlades A och B diesel vilket ledde till att man tömde fel dieseltank. Detta resulterade i att båda dieslarna blev utan bränsle.

#### **Konsekvens**

Båda dieslarna var under viss tid icke driftklara.

#### **Orsak**

Mänsklig faktor.

### **ICDE id 6094 Felaktig montering av låsmuttrar orsakar beroendefel i backventiler**

#### **Händelse**

Vid en rutinkontroll upptäckte man vatten i högtryckskylsystemets evakueringsrör. Reaktorn var vid detta tillfälle i drift.

#### **Konsekvens**

Kylsystemet förklarades funktionsodugligt och reaktorn togs ur drift.

#### **Orsak**

Orsaken var att låsmuttrarna på 4 backventiler hade monterats med ett felaktigt vridmoment enligt en felaktig monteringsinstruktion.

### **ICDE id 3021 Trasig temperaturgivare orsakar frysning av returledning och beroendefel i centrifugalpumpar**

#### **Händelse**

Returledningen från bränslebassängens nödkylpumpar visade sig vid ett tillfälle vara frusen.

#### **Konsekvens**

Pumparna förklarades som otillgängliga och nödkylsystemet var därmed satt ur funktion.

#### **Orsak**

Orsaken till problemet var en trasig temperaturgivare i bränslebassängen. Detta medförde att cirkulationen i returledningen stoppades och därefter frös ledningen. Det visade sig att det rådde kunskapsbrist hos personalen angående betydelsen med ett flöde i returledningen.

### **ICDE id 3004 Handhavandefel vid FU stoppar flera centrifugalpumpar**

#### **Händelse**

Samtliga pumpar för högtrycksnödkylsystemet var vid samma tillfälle otillgängliga under en kortare tid.

#### **Konsekvens**

Pumparnas otillgänglighet orsakade dock inga konsekvenser för reaktorns tillstånd.

#### **Orsak**

Orsaken var att man skulle utföra FU på pumparna och råkade av misstag vrida om fel brytare så att alla pumpar stannade.

## **ICDE id 9004 Kapad kabel orsakade beroendefel på dieselgeneratorer**

### **Händelse**

Under ett moderniseringsarbete råkade en arbetare av misstag kapa en kabel som hade till uppgift att manövrera och verifiera dieselenheternas tillstånd.

### **Konsekvens**

Samtliga dieselgeneratorer (2 stycken) blev p.g.a. detta otillgängliga. Reaktorn befann sig då i tillståndet kall avställd reaktor. Enligt de tekniska specifikationerna måste minst en av dieselenheterna vara tillgänglig under dessa förhållanden.

### **Orsak**

Orsaken till detta var helt enkelt ett mänskligt misstag.

## **ICDE 9043 Sprayfärg orsakade beroendefel på dieselgeneratorer**

### **Händelse**

Vid ett återkommande prov misslyckades man med att uppfylla driftklarhetskraven för två dieselgeneratorer. Dieslarna startade men nådde inte erforderlig effekt inom det tidsintervall som framgår av konstruktionskraven.

### **Konsekvens**

Båda dieslarna fick tas ur drift i drygt 3 timmar.

### **Orsak**

Problemet identifierades och visade sig vara sprayfärg som hamnat på kommutatorn i generatorerna. Färgen var avsedd för andra ändamål men hade olyckligtvis hamnat på strömförande ytor vilket resulterade i detta problem.

## **B2 - RO 4/99 Bortfall av hjälpkylvatten**

### **Händelse**

Vid periodisk provning i system 711 stängdes av misstag 8 stycken ventiler för intag av havsvatten till hjälpkylsystemens pumpgröpar. Detta medförde att kylkapaciteten i hjälpkylsystemen 712, 713 och 714 uteblev helt. Automatiskt stopp av huvudcirkulationspumparna 313 P1-P4 erhöles på grund av hög oljetemperatur i frekvensomformarnas hydraulkoppling. Effektdrift kunde ej upprätthållas.

### **Konsekvens**

Kortvarig utebliven kylkapacitet i samtliga hjälpkylsystem för kylning av dieselaggregat, resteffektkylsystem och inneslutningsprinkling. Bedömning enligt INES = 2. Manuellt reaktorsnabbstopp.

### **Orsak**

Felaktig ventilmanöver vid periodisk provning i system 711 på grund av bristande egenkontroll vid provningens utförande.

## **B2 – RO 19/91 Oplanerat stopp av resteffektkylningen**

### **Händelse**

Under natten mot söndag 8/9 1991 pågick förberedelsearbete för demontage av reaktortankklocket. Detta lyftes klockan 08.15 och strax därefter försämrades atmosfären i reaktorhallen av ånga från reaktorn. Hallen utrymdes klockan 09.00. Kontrollrummet meddelades och kunde snabbt konstatera att resteffektkylpumparna i system 321 stod stilla. Pumparna startades omedelbart och maximal kylning etablerades. klockan 10.20 gavs tillträde till hallen och klockan 12.50 kunde tankflänsarbetena på nytt upptas. Luftprov gav aktivitetsvärden i paritet med de prov som tagits tidigare ca 0,2 Dac<sup>5</sup>.

### **Konsekvens**

Vid tidpunkten för det inträffade var säkerhetsmässiga betydelsen mer av arbetarskyddskaraktär. Då 321-pumparna stoppade var röranslutningar på tankklocket demonterade och medgav utrymme för ångutströmning och termisk exponering. Utebliven resteffektkylning tidigare under natten kunde ha gett en tryckökning och om vattennivån då, mot instruktionen, varit vid tankflänsen, så hade det även gett risk för kalltryckning av tanken.

### **Orsak**

321-pumparna har stoppat samtidigt klockan 05.17, sannolikt som följd av att försök då gjordes att manövrera 314 V50 och V51, som har pneumatiska styrventiler matade från tryckluftsystemet 754. Detta system matar även 321 V1, skalventil på 321-pumparnas sug sida. Vid försvinnande öppnaindikering på denna stoppar pumparna automatiskt (komponentskydd). Enligt CK-personal kom lågtryckslarm från system 754 men man har ej uppmärksammat att 321 stoppat.

## **B2-RO 26/93 Automatik för stopp av pumpar i kylsystem för reaktorinneslutningen delvis ur funktion**

### **Händelse**

Vid enstaka tillfälle under ett par veckors tid har utrustning för differenstryckmätning över sugsidar i system 322 och 323 givit signal för fel. Felet har endast varit aktivt korta stunder (minuter) varför omfattande felsökning ej givit resultat. 93-08-03 erhöles återigen felet, denna gång varaktigt. Felet lokaliserat till den gränsvärdesenhet som vid högt differenstryck över 322 C1 och C2 ger stopp av 322 P1 och P2.

### **Konsekvens**

Vid igensättning av 322 C1 eller C2 skulle 322 P1 och P2 ej ha stoppat automatiskt.

### **Orsak**

Utredning pågår. Kondensator i gränsvärdesdonets matningsenhet felaktig. Enligt leverantören av gränsvärdesenheten är kondensatorerna i enstaka leverans från underleverantör behäftade med fel.

<sup>5</sup> DAC = Derived air concentration (luftkoncentrationen av en radionuklid)



## **B2-RO 45/92 Igensatta sugsilrar i 322 C1 o C2**

### **Händelse**

28/7 klockan 05.39 inträffade I-isolering vid första värmning till 69 bar efter RA vid 30 bar. Det konstaterades att direktblåsningsventilen 314 V12 öppnade obefogat. Händelsen är beskriven i RO 29/92. Vid blåsningsen slets ca 200 kg isolering loss i området runt V12 varav 100 kg isolering spolades ner i kondensationsbassängen och satte igen silarna till inneslutningskylning, 322. Ca 70 min efter utlöst I-isolering erhöles differensstryckslarm, 200 mbar, från silövervakningen.

### **Konsekvens**

Analys av händelsen har visat på att risk finns att silarna till härdnöd- och inneslutningskylningen kan sätta igen inom ca 20 min vid rörbrott med manuella insatser som följd. Manuella insatser inom 30 min avviker från konstruktionsförutsättningar, 30-minutersregeln.

### **Orsak**

Delar av den mineralull som utgör termisk isolering på primärsystemen i reaktorinneslutningen slits loss av den utströmmande ångan/vattnet efter rörbrottet och kommer via nedblåsningsrören ned i kondensationsbassängen. Mängden isolering och effekten av att inneslutningssprinklingen spolrar ned denna har underskattats vid de utredningar som utfördes i samband med att backspolningsmöjlighet infördes. Vidare utreddes inte effekterna av att isoleringen åldras och påverkas av värme från rören. Sannolikt blir åldrad isolering fortare våt än ny sådan och sjunker därmed snabbare ned till silarnas nivå.

## **O1 RO 18/88 323 P1 och P2 ej driftklara. Frånskiljarna till pumparna var enligt driftordern för avställningen öppna för att förhindra trycksättning av kall reaktortank**

### **Händelse**

Stationen avställd, i första hand för att åtgärda vätagasläckage i generatorerna. När arbetena på reaktordelen var klara påbörjades 18.20 stavdragning/värmning. Detta gjordes utan att 323 P1 och P2 var driftklara. Frånskiljarna till pumparna var enligt driftordern för avställningen öppna för att förhindra trycksättning av kall reaktortank. Reaktortemperaturen 100° C passerades kl. 20:00. Vid en genomgång av driftordern upptäcktes att punkten där pumparnas frånskiljare skulle slutas, ej var utförd. Frånskiljarna slöts kl. 22.45. Reaktortemperaturen var då 160° C.

### **Konsekvens**

Båda pumparna blir otillgängliga p.g.a. ett enskilt fel. P.g.a. att frånskiljarna till pumparna är öppna, är konsekvensen den att pumpfunktionen skulle ha uteblivit vid ett vid ett påkallat behov.

### **Orsak**

Punkten i driftordern där 323 P1 och P2 skulle återställas uppmärksammades inte inför värmningen. När man gick igenom driftordern i samband med skiftavlämningen upptäcktes att punkten ej var avsignerad.

## **B2 RO 59/94 Lösa skruvar i 500A greppsäkringar**

### **Händelse**

Vid kontroll av brytare för 713 P2 upptäcktes en lös skruv, utgångad ca 1 cm, på en säkring i ett angränsande brytarfack. Brytaren i det angränsande facket tillhör 327 P3. Felet bedömdes som nödvändigt att åtgärda omedelbart. Reservpumpen 327 P4 provkördes och därefter elblockerades 327 P3 klockan 11.10 för att kunna byta säkring. 327 var åter driftklar klockan 11.20. Avbrottstid 10 min. Vid ytterligare kontroll upptäcktes en saknad skruv på en säkring för 322 P1. Säkringen misstänkts ligga i brytaren för 322P1 varför en kontroll krävdes omedelbart. 322 P2 kopplades in på 322 krets 1. 323 P1 och P2 provkördes. 322 P1 elblockerades klockan 14.40. Brytaren undersöktes men den försvunna skruven gick inte att hitta. klockan 15.54 provkördes 322 P1 och förklarades driftklar. Härefter upptäcktes även en lös skruv, utgångad ca 5 mm, på 322 P2. Även denna krävde en omedelbar åtgärd varför 322 P2 elblockerades klockan 16.02. Någon ny provkörning av 323 P1 och P2 gjordes inte eftersom så kort tid gått sedan förra provkörningen. klockan 16.35 var 322 P2 åter driftklar. Avbrottstid 37 min. Tillåten reparationstid Enligt STF 3.4C 7 dygn.

### **Konsekvens**

Om skruvarna i fallen med 327 P3 och 322 P2 hade ramlat ned i brytarna samt om den saknade skruven i fallet med 322 P1 hade legat i brytaren hade risk funnits att inte få brytarna till sina tillägen. Pumparna hade inte startat vid påkallat behov.

### **Orsak**

Orsaken varför skruvarna lossnat har inte kunnat fastställas till 100 %. Tillverkaren anger dock följande möjliga förklaringar:

För lågt åtdragningsmoment.

Fel på verktyget eller felinställt verktyg.

För stum packning mellan keramikropp och plåtgavlar.

Vibrering av säkringen vid sandpåfyllning.

Tillverkaren har justerat upp åtdragningsmomentet till min 1,5 och max 1,7 Nm.

## **O1 RO 4/1996 315 ej driftklart, blockerat av felaktig temperatursignal. 315 V5 och V6 obefogad stängning. 315 ej antagen tillgänglig**

### **Händelse**

Vid inkoppling av 315 för nedkylning av reaktorn stängde 315 V5 och 316 V6. Vid felsökning upptäcktes att ventilerna stängde felaktigt via villkor "hög temperatur". Logiken för stänga är 2/3 kopplat villkor "hög temperatur" plus flöde >20 kg/s. Temperaturmätningarna ingår endast i logikbildning och är ej larmade i system 517

### **Konsekvens**

System 315s uppgifter är:

Att under de första 100 sek efter reaktorns snabbstopp tillsammans med system 314-316 utgöra värmesänka för reaktorns resteffekt om 311 V1-V4 är stängda eller dumpförbud råder.

Att inkopplas som extra säkerhetsåtgärd vid för högt tryck i reaktorn.

System 315 var ej tillgängligt för att automatiskt lösa ovanstående uppgift. Manuell inkoppling gjordes.

### **Orsak**

Temperaturmätningen är ombyggd under FENIX avställningen. De gamla termostaterna är ersatta med Pt 100-givare och gränsvärdesdon. Vid denna ombyggnad gjordes en felkonstruktion. Inkopplingen på gränsvärdesdonen gjordes arbetsströmkopplad men skulle ha varit vilostromkopplad. Vid provning enligt provprogram testades funktionen till första mellanrelä. Vid logikprovning som utfördes Enligt underhållsinstruktion 1-U3.315.1 aktiverades mellanreläet till draget läge. Detta innebär att felet ej upptäcks vid logikprovning.

## **O2 RO 12/00 Ej driftklar inmatning från 649 T13 och T23 till 6 kV-skenor. Differentialskydden till båda felkopplade**

### **Händelse**

Vid startsekvensprovning 4/7-00 klockan 16.39 löste inmatningen från 649 G23 ut på gasturbintransformator 649 T23s differentialskydd när stora 6 kV-objekt startades. Vid felsökning upptäcktes att differentialskyddets strömkretsar var felaktigt kopplade vilket i sin tur innebar att skyddet registrerade 6 kV-objektens startström som en felström och löste ut brytarna runt gasturbintransformatorn. Både T23s och T13s differentialskydd var kopplade på samma sätt vilket gjorde att felet fanns på både A- och B-sub. Efter det att felet lokaliserades togs beslut att koppla bort (klockan 19:30) differentialskydden varvid startsekvensprovet kunde avslutas. I och med detta verifierades gasturbinaggregatens driftklarhet. Den felaktiga kopplingen av 649 T23s differentialskydd gjordes i projekt AFSIE vid gasturbinavställning vecka 015 (10/4-15/4) samt av 649 T13s differentialskydd vecka 019 (8/5-13/5). Differentialskyddet är ett komponentskydd och har till uppgift att skydda transformatorn. Skyddet känner av stora strömrusningar genom transformatorn som kortslutningsströmmar kan ge. Transformatorn är även försedd med bl.a. jordfels- och kortslutningsskydd samt gasvaktskydd. Gasvakten betraktas som redundant till differentialskyddet eftersom deras utlösningstider är ungefär lika snabba. Eftersom åtgärderna i projekt AFSIE utfördes i två etapper kom hindertider och senaste driftklarhetsverifiering att innehålla olika tider för 649 G13/T13 och G23/T23: Hindertid enligt sida 1: Hindertiden har preliminärt beräknats Enligt I-0964 "Klassificering och rapportering Enligt SKIFS 1998:1" avsnitt 3.14 pkt 5. Med detta innebär att hindertiden är beräknad från den tidpunkt felet uppstod fram till den tidpunkt då ej driftklarhetskrav förelåg på kraftmatningskällorna 649 G13/T13 och G23/T23. D.v.s. fram till övergång från STF kap 3 till STF kap 7, 27/5 klockan 09:00. 1. 649 G23/T23 avställd 10/4 klockan 04:06. G23/T23 driftklart 4/7 klockan 19:30. Hindertid 1132 h och 54 min.

### **Konsekvens**

System 649 - Gasturbinanläggningen har följande säkerhetsuppgifter enligt SAR: Förse stationens kategori A-objekt, som ingår i säkerhetsfunktioner med erforderlig elkraft vid bortfall av yttre nät. Systemet ingår i följande anläggningsvisa tvärfunktion: Elkraftförsörjning (SAR Allmän del, avsnitt 5.3.1). Enligt STF 3.10 A2 ska Elkraftutrustningen i alla driftlägen utom kall, avställd reaktor vara driftklar i den utsträckning som krävs för säker avställning av verket. Den del av elkraftutrustningen som System 649 - Gasturbinanläggningen är driftklar i detta avseende om villkor 3.10 A är uppfyllt. A2 Gasturbiner, system 649: System 649 ska vara driftklart. System 649 är driftklart då följande villkor är uppfyllt. Båda gasturbinaggregaten 649 G13 och G23 med transformatorer 649 T13 och T23 ska vara driftklara. En halva av ett av aggregaten tillåts dock ej vara driftklar under förutsättning att aggregatet kan leverera halva märkeffekten. Konstateras ovanstående vara ej uppfyllt, ska nedgång till kall avställd reaktor ske. Dock gäller följande undantag: Om antingen ett helt gasturbinaggregat eller en halva av vardera aggregatet är driftklara får reaktorn kvarhållas i sitt driftläge i högst 30 dygn. De driftklara halvorna ska provas omedelbart och därefter en gång per sju dygn. Ej driftklart gasturbinaggregat innebär att de objekt i verket som får sin reservkraftmatning från endast detta aggregat ska betraktas som ej driftklara. Detta gäller när reparationskriterium tillämpas på system 649. Hindertid: Hindertiden har

beräknats Enligt I-0964 "Klassificering och rapportering Enligt SKIFS 1998:1" avsnitt 3.14 pkt 5. Med detta innebär att hindertiden är beräknad från den tidpunkt felet uppstod fram till den tidpunkt då ej driftklarhetskrav förelåg på kraftmatningskällorna 649G13/T13 och G23/T23, D.v.s. fram till övergång från STF kap 3 till STF kap 7, 27/5-00, klockan 09:00. 1. 649 G23/T23 avställd 10/4 klockan 04:06. G23/T23 driftklart 4/7 klockan 19:30. Hindertid 1132 h 54 min. 2. 649 G13/T13 avställd 8/5 klockan 02:55. G13/T13 driftklart 4/7 klockan 19:30. Hindertid 463 h 55 min. Senast verifierad driftklar: 649 G23/T23: 6/4; 649 G13/T13: 8/5. Konsekvens på systemnivå: Red. systemfunktion: Tiden mellan 10/4 klockan 04:06 till 8/5 klockan 02:55. Totalt bortfall: Tiden mellan 8/5 klockan 02:55 till 4/7 klockan 19:30. Bedömningen är att 649 G23 icke varit driftklar från och med v015, vid tillfällena där behov av stora 6 kV-objekt funnits, D.v.s. då behov och driftklarhetskrav på 312-pumparna förelåg. 649 G13 har med samma resonemang icke varit driftklar från och med v019. Från denna tidpunkt har både G23 och G13 icke varit driftklara vid tillfällena där behov av stora 6 kV-objekt funnits. Slutsatsen av den säkerhetsmässiga bedömningen att båda gasturbinerna varit ej driftklara under en viss tid, Enligt riskanalyser, reg nr 2000-07278 blir ändå resultatet att reaktorsäkerheten varit acceptabel under tiden då båda reservkraftmatningarna från 649 T13 och T23 ej var driftklara. INES-bedömning: Den slutliga bedömning som gjorts gemensamt med OKG:s INES-koordinator grundar sig på följande: Djupförsvarskriteriet, tab. 1 (utan inledande händelse). Funktionstillgänglighet för bränslekylning, C tillräcklig. Frekvens för inledande händelse bortfall av yttre nät, 1 väntad. Detta leder till grundrating nivå 1 alt 2. För O2 uppstår det förväntade behovet i samband med utebliven dieselmotning till system 327 hjälpmatarvattensystem. Den bedömda åtgärdstiden för blockering av de felaktiga skyddena har bedömts till max 4 h, vilket bedömts kort jämfört med tiden fram till förväntat behov. Omständigheten motiverar val av grundnivå 1. I den slutliga bedömningen har tillkommande faktorer Enligt III-5 prövats. Det fanns inte tillräckliga motiv för uppgradering av INES, D.v.s. nivån är oförändrad, INES = 1.

### **Orsak**

Projekt AFSIE har nya ställverk för matning av system 327/733 installerats. Dessa ställverk spänningsmatas normalt från dieselsäkrad skena på O2, vid händelser där 323-behov finns eller vid brand i centrala eldelen ska det nya ställverket kopplas över för matning från gasturbiner. Ställverken i AFSIE har färdigställts under våren 2000. Spänningsmatningen från gasturbiner färdigställdes under gasturbinavställningar vecka 015 respektive 019. Under dessa avställningar byggdes även T13 och T23s differentialskydd om för anpassning till de nya ställverken. Ombyggnad och avprovning av differentialskyddna gjordes Enligt framtagna och gällande rutiner. Det fanns dock ej möjlighet med vad som då bedömdes rimliga åtgärder att genomföra provning med belastning på hjälpkraftnätet eftersom det vid normalt driftläge ej finns några objekt kopplade till aktuella skenor. Kontroll av förbindningar mot gällande dokumentation och sekundärprov gjordes dock i full omfattning. Vid tidigare tillfälle, eventuellt redan vid första driftsättningen av gasturbinanläggningen har omkopplingar av skyddet gjorts, vilka uppenbarligen inte blivit dokumenterade på rätt sätt. I det arbete som nu gjordes förlitade projektet sig på den gällande dokumentationen. Eftersom utrustningen fungerat utan anmärkning har det inte ifrågasatts att dokumentationen skulle kunna vara fel.

## **O2 RO 43/96 System 323 ej driftklart**

### **Händelse**

Periodiskt prov av system 323 krets 1 och 2 skulle utföras under eftermiddagen den 13/11, man upptäckte då att pumparna 323 P1 och P2 inte startade och vid kontroll visade det sig att frånskiljarna till pumparna ej var slutna. Återställning av system 323 efter RA2-96 var utfört 26/10 och systemet verifierades driftklart efter utfört periodiskt årligt prov, 26/10 klockan 20.00, och startsekvensproven avslutades 27/10 klockan 12.30, vilket också verifierade systemet. Då 323 P1 och P2 skulle frånskiljas inför täthetsprovningen av reaktorinneslutningen Enligt instruktion 2-D2.1.6, 27/10 var redan båda pumparna frånskilda och uppmärkta med arbetsbeskedsnummer. Inför täthetsprovning av reaktorinneslutningen ställs yttre system som har kontakt med RA av för att störningar ej skall uppstå vid provningen. Efter avslutat täthetsprov återställdes systemen Enligt instruktion 2-D2.1.6, men frånskiljarna till 323 P1 och P2 blev ej slutna Enligt punkt M.9.3 och M.9.4.

### **Konsekvens**

System 323 har som säkerhetsuppgift att tillföra reaktortanken erforderlig mängd vatten för kylning av härden, vid kylmedelsförlust p.g.a. brott på rörledningar tillhörande RCPB eller anslutna till RCPB innefattande ett momentant giljotinbrott på den grövsta ledningen ansluten till reaktortanken (H3 och H4 händelser). När rörbrottet leder till ett läckage av måttlig storlek är system 312 ett diversifierat system till system 323 vad avser att tillföra reaktortanken erforderlig mängd vatten för kylning av härden. Vid stora brott är det system 323 som ensamt svarar för nödkylning av härden. Det betyder att totalt bortfall av systemfunktionen har förelegat för system 323 vid händelser i klass H3 och H4 då systemfunktionen utmanas. För händelser i klass H3, små brott, har säkerhetsfunktionen "härdsnödkylning" haft en reducerad redundans under den tid som system 323 ej varit driftklart, eftersom system 312/442/733 varit driftklart under denna tid. Händelsen har värderats mot INES och befunnits vara en nivå 1- händelse.

Händelsen kan eventuellt uppgraderas en nivå om kommande utredning visar att fog för uppgradering föreligger. I MTO-rapport 96-12317 har i sak inget framkommit som föranleder en uppgradering av händelsen från nivå 1 till nivå 2. Emellertid har en liknande händelse inträffat på block 1 1988. Vid denna händelse gjordes en genomgång på block 1 vad avser rutiner för att verifiera att system 323 är driftklart i samband med uppstart. Händelsen på block 2 visar att möjliga lärdomar ej dragits p.g.a. Händelsen på block 1 och att det p.g.a. detta finns anledning att uppgradera händelsen till nivå 2.

### **Orsak**

De administrativa barriärerna har brutit. Påbörjad utredning syftar till att utröna varför och vilka förbättringar som ska vidtas. Se MTO-rapport reg nr 96-12317. Oskarshamn 2 - MTO-analys - sprinklersystem för reaktorhård 323 ej driftklart, bil 1.

## **O3 RO 14/98 Huvudångskalventil 311 VA3 och 311 VC3 stängde ej på order.**

### **Händelse**

Vid ordinarie ångskalventilprov den 28 augusti klockan 10.30 vid 60 % effekt erhöles utebliven skalventilfunktion för två av de yttre skalventilerna i ångledningarna. Vid manövreringen öppnade ej styrventil 311 VA3.V3 och 311 VC3.V3 på order vilket medförde utebliven stängning av yttre huvudångskalventil 311 VA3 i ångledning 1 och 311 VC3 i ångledning 3. Enligt villkoren i STF krävs nedgång till kall avställd reaktor vid felfungerande skalventil. I detta läge, med två skalventiler som inte kunde stängas, påbörjades effektnedgången genom att försöka stänga de två felfungerande skalventilerna genom att "knacka" på deras styrventiler. Skalventilerna kunde stängas efter att styrventilerna 311 VA3.V3 och 311 VC3.V3 påverkades (knackades loss) manuellt lokalt i ångschaktet. Ventilen manövrerades sedan från CKR ytterligare ett par gånger utan anmärkning. Övriga inre huvudångskalventilers stängningstid låg mellan 1.144-1.191 sekunder och de övriga yttre huvudångskalventilerna låg på 1.181-1.201 sekunder D.v.s. under acceptanskriteriet 1.45 sekunder. Samtliga huvudångskalventiler provades senast i samband med ett kortstopp den 29 juli-1 augusti utan anmärkning. Då skalventilerna kunde manövreras utan anmärkning och då alla tider var klart under acceptansgränserna (även vid första stängningen av 311 VA3.V3 och 311 VC3.V3) beslutades att betrakta skalventilerna som driftklara.

### **Konsekvens**

Enligt FSAR krävs att huvudångskalventilerna i system 311 ska vara täta samt snabba. De ska hinna stänga innan vatten, p.g.a. trycksänkning, "jäst" upp till underkant på ångstudsarna. Orsaken till denna förutsättning är att man inte kan verifiera att ventilen stänger i tvåfasblandning som orsakats av nivåhävning i reaktorn vid rörbrott. Dimensionerande fall är ett giljotinbrott på en ångledning i turbinhallen. Acceptanstiden för stängning av huvudångskalventilerna är satt till 1.45 sekunder för att ventilen inte ska stänga i ång-vattenblandning med utebliven skalventilfunktion som följd. Den uteblivna stängningen på 311 VA3 och 311 VC3 skulle ha inneburit att, i ett postulerat fall med "single failure" på den inre skalventilen i samma ångledning, stängningen av 311 VA3/VC3 och tätheten på densamma inte kunnat garanteras. Ordinarie ventilprov var planerat till kvällen fredagen den 28 augusti men manöver av ventilerna utfördes på förmiddagen i samband med kraftbalansreglering vid 60 % effekt. Ventilproven ska verifiera systemfunktionen och visar i detta fall att en förändring har skett för 311 VA3/VC3 mellan provet som utfördes den 1 augusti och manövern den 28 augusti. Utförda FSAR-beräkningar för Oskarshamn 3 visar att någon risk för härden och dess integritet vid ett ångledningsbrott vid 109,3% effekt inte föreligger. Slutlig RO: Utförda PSA-beräkningar för Oskarshamn 3 visar att bidraget för härdskada är litet vid ett ångledningsbrott vid 109,3% effekt även med två icke fungerande ångskalventiler. Denna händelse med att två ventiler inte stänger vid samma provtillfälle (fel med gemensam orsak) är helt ny och har aldrig inträffat tidigare på O3.

## Orsak

Under RA3-98 byttes samtliga styrventiler ut i position 311 VC3.V3 och 311 VC4.V3 monterades två modifierade styrventiler. Dessa två modifierade styrventiler funktionsprovades före installation i provriggen TRYM hos ABB Atom i Västerås för verifiering av funktionen vid fullt tryck och temperatur. Ändring nr 3-97.009. Den 29 juli under kortstoppet fick man problem med styrventilen 311 VC3.V3 som inte öppnade på order (RO-O3-98/013). Orsaken till den uteblivna funktionen har konstaterats till föroreningar i ventilen som troligen kommit från provriggen TRYM. Båda ventilerna byttes mot ersättningsventiler. De uteblivna manövrerna på styrventilerna 311 VA3.V3 och 311 VC3.V3 vid provningstillfället den 28 augusti kan sannolikt bero på oxidtillväxt i styrventilens ventilhus. Detta resonemang bygger på att om det varit föroreningar i ventilerna hade inte manövrering hjälpt utan felorsaken hade kvarstått med allt längre öppningstider på styrventilen. Ventilfunktionen hade till slut helt upphört om föroreningar varit felkällan. Tidigare erfarenhet har visat att på ventildelar med rengjorda metallytor ökar oxidtillväxten snabbt efter återmontage. Detta fenomen har man tidigare sett i bl.a. nivåvakterna i ångledningarna där man hade stora problem med utebliven funktion som berodde på rengjorda metallytor och snabb oxidtillväxt. På likartat sätt har man påvisat samma sak i oljesystemen i turbinanläggningen. Oxidtillväxten kan brytas vid motionering alternativt av existerande systemvibrationer eller genom påtvingade systemoscillationer (detta är fallet med turbinens oljesystem). Ångledningsvibrationerna har mer än halverats i och med baffelmontaget på fuktavskiljaren varför de existerande vibrationerna har minskat vilket har gynnat oxidtillväxtens förmåga att "klibba" ihop de rengjorda styrventilernas metallytor med resultatet att ventilfunktionen förhindrats. Sedan kortstoppet den 29 juli till 1 augusti har drift med reducerad effekt skett av kraftbalansskäl vilket bidragit till att oxidtillväxten har skett då vibrationerna i systemen varit tillräckligt låga för att de bildade oxidskikten skulle kunna "klibba" ihop metallytorna. Man har tidigare försökt demontera "klibbande" styrventiler i syfte att undersöka fenomenet i ventilerna. Dessa försök har misslyckats då oxid "klibbningen" bryts upp så fort man börjar demontera ventilen (jämför med att knacka på ventilen). Studier av demonterade "klibbande" styrventiler visar inga synliga fel mer än oxiderade metallytor. Med dessa erfarenheter och de erhållna resultaten från manövreringarna av de nu driftklara skalventilerna (minskande gångtider vid varje manöver) ansågs det ej längre finnas krav på att gå ner med anläggningen. Grundorsaken till missad ventilfunktion hade man med stor sannolikhet inte hittat då oxid "klibbningen" bröts isär när styrventilerna öppnades inför nedgång till kall avställd reaktor (genom "knackning") vilket utfördes lokalt i ångschaktet. De efterföljande manövrerna från CKR visade heller inga tecken på "klibbning" i styrventilerna utan tiderna minskade för varje manöver.

För att verifiera att ventilerna är driftklara har en utökad provning av skalventilerna i ångledningarna verkställts som bekräftar ovanstående resonemang. Komponenttyp: Fabrikat Sulzer typ MGV25/15 Slutlig RO: Problemet med felfungerande styrventiler har inte uppträtt efter RA-89 när ökat spel mellan ventilspindel och pilotkägla infördes i kombination med kickfunktionen. Vid samma tillfälle september 1989 höjdes effekten till 109 %. Införandet av baffelplåtar RA-97 har gjort att vibrationsnivån vid 60 % nu är mellan 0,6-1,3 mm/s mot 2,3-4,2 vid 109 %. Vid samtliga felfunktioner har enbart de yttre berörts, detta kan förklaras med den lägre vibrationsnivån.



Störningarna har uppträtt i början av driftsäsongen vilket skulle kunna förklaras med att oxidtillväxten avtar med tiden. Den troligaste orsaken till felfungerande styrventiler, är oxidsammanväxning. Vissa likheter med nivåvakten i ÅL4 som felfungerade RA-92 kan göras. På alla rena metallytor som utsätts för ångmiljö sker en oxidtillväxt som i ogynnsamma fall, små spalter, kan leda till funktionsstörningar. Befintliga spel har varit tillräckliga för att ventilerna ska fungera. Vid nuvarande driftförhållande (låg effekt och låga ångledningsvibrationer) krävs troligen större spel för att undvika felfunktioner. För denna händelse finns ingen koppling till provningsriggen TRYM i Västerås. (RO-O3-98/13) Komponenttyp: Fabrikat Sulzer typ MGV25/15

## **F1-RO-006/2000 Felaktiga indata till hårdövervakningen för Forsmark 1, 2 och 3**

### **Händelse**

Under mars månad upptäcktes fel i indata för hårdövervakningsprogrammet POLCA. Första identifierade felet bestod i att fel spaltvidder använts vid tvärsnittsberäkning till F2, rörande ersättningsladdningarna e15-e17. Kontroll av samtliga tvärsnitt för F1, F2 och F3 visade inga fel men däremot uppdagades ett fel i k-faktorer för det Siemensbränsle som finns installerat på F1 och F3. K-faktorerna är ett mått på bränslestavarnas inbördes känslighet för dryout. Felen har legat i indata sedan driftsättning av POLCA i september 1999. Ingen driftmässig konsekvens på F1 och F3. Driftmässig konsekvens för F2 var att reaktoreffekten fick reduceras någon procentenhet för att innehålla den felaktigt beräknade dryout-marginalen då denna beräknades ca 3 enheter konservativt.

### **Konsekvens**

Felen i indata har haft ringa eller ingen säkerhetsmässig betydelse. Felet på F2 verkade i konservativ riktning. På F1 och F3 verkade felet upp till ca 6 enheter icke konservativt. Inget överskridande av gränsvärde för dryout har skett när marginalen till dryout-gränsvärdet hela tiden varit större än 6 enheter för de berörda bränslepatronerna. INES-bedömning: händelsen klassas till utanför skalan.

### **Orsak**

I fallet med F2 är felet orsakat av felaktig filhantering varvid två filer bytt namn med varandra i samband med inläggning i Forsmark efter leverans från Vattenfall Bränsle. I fallet med F1 och F3 hade indata till k-faktor-programmet "rättats" i tron att det stod fel i indatafilerna. "Rättningen" ledde till att den gamla algoritmen för beräkning av k-faktorer felaktigt användes.

## **R1-RO-20/2000 För lång responstid på grund av felaktigt inkopplade pulsationsdämpare i transmittar för jäsningsvakter**

### **Händelse**

Vid brusmätningar på instrument signaler upptäcktes avvikelser i dynamiskt beteende mellan 211K419 och 211K416-418. Mät punkterna har till uppgift att bilda gränsvärde och snabbstoppa rektorn vid hög reaktornivå. Vid felsökning som instrumentavdelningen gjorde under revisionsavställningen upptäcktes att det fanns pulsationsdämpare monterade i mätledningarna för K416-418, K419 som är reserv och normalt inte inkopplad hade ingen dämpare. Pulsationsdämpare användes när mätsignalen är mycket brusig. De felaktigt inkopplade pulsationsdämparna har inte inneburit någon driftmässig konsekvens, däremot har jäsningsvakternas funktion med avseende på snabbhet ej varit uppfyllt.

### **Konsekvens**

Gjord analys har inte kunna visa att acceptanskraven i FSAR uppfyllts med monterade rensnålar i pulsationsdämparna. D.v.s. att 411's skalventiler stänger i ångfas för händelser i PC1-PC5. Det fall som det gäller är obefogad öppning av 2 eller 4 dumpreglerventiler vid varm avställning. Analysen visar att fallet med obefogad öppning av 4 dumpreglerventiler är så osannolik att den ligger bortom PC5. Detta fall har sålunda haft försumbar säkerhetsmässig betydelse. Fallet med obefogad öppning av två dumpreglerventiler vid varm avställning har en sannolikhet på mindre än 10<sup>-4</sup>/år. D.v.s. är en PC5 händelse vilket gör att den säkerhetsmässiga betydelsen av denna har varit låg. Det fall som ger den högsta jäsningshastigheten och därmed täcker alla andra fall är obefogad snabböppning av två dumpventiler vid varm avställning. Sådan händelse har inträffat vid två tillfällen med den gamla turbinregulatorn, med nuvarande regulator är det låg sannolikhet för att det åter inträffar. Första tillfället var 1975-02-09 (snabbstopp nr 33) och andra tillfället var 1976-05-19 (snabbstopp 81).

De aktuella transmittarna installerades i november 1974. Signalbilden vid båda tillfällena visade inte att något vatten kommit ut i ångledningarna. Därmed är det verifierat genom erfarenhet att kraven i FSAR, med avseende på att skalventilerna stänger i ångfas, har varit uppfyllda även med pulsationsdämpare monterade. Avvikelsen har bedömts enligt INES User's Manual tabell 1, kriterier för allvarlighetsklassning av försämrat djupförsvar utan inledande händelse.

Tillgänglighet för säkerhetsfunktion: Otillräcklig (D) Frekvens/sannolikhet för inledande händelse: Låg/osannolik (3) Detta innebär, avvikelse från driftvillkor INES = 1.

### **Orsak**

Pulsationsdämparna finns inte dokumenterade för denna mätkrets och skall inte finnas eftersom de ger en otillåten fördröjning. Orsaken till att de finns och tidpunkten för när de har monterats har inte gått att utreda trots efterforskning bakåt i tiden. Transmittarna installerades under effektprovdriften hösten 1974 och ersatte direktvisande bartonceller med kvicksilverkontakter. De byttes ut därför att de var vibrationskänsliga och gav obefogade snabbstopp vid STF-prov. Möjligen kan dämparna ha monterats på de gamla vakterna för att underlätta provningen och inte demonterats då transmittarna infördes.

## **F1-RO-015/2000 Manöversäkring utlöst vid start av kylvattenpump (potentiell CCF)**

### **Händelse**

Manuell start av kylvattenpump 322P1 utfördes inför kemiprovtagning, men pumpen startade inte trots upprepade försök. 322P1 är en av fyra kylvattenpumpar för kylning av kondensationsbassängen. Eloperatören kontrollerade status i ställverk och konstaterade att en av två manöversäkringar löst ut. Efter utbyte av båda manöversäkringarna utfördes driftklarhetsverifiering utan anmärkning.

### **Konsekvens**

En av de fyra 322-kylkretsarna i kylkedjan var ej driftklar under tiden från utlöst manöversäkring till dess att nya manöversäkringar var anbringade. INES-bedömning: händelsen betraktas som en mindre avvikelser i djupförsvaret. INES = 0.

### **Orsak**

Vid utredning av händelsen konstaterades att aktuella 2A-manöversäkringar är "på gränsen" till utlösning vid det tillfälle då kontaktorn får tillslagssignal. Under föregående driftsäsong byttes ställverkskomponenter till 322P1-P4 och 711P1-P4. De nya kontaktorer har en tillslagseffekt på 1430VA medan tidigare utförande hade 1300VA i tillslagseffekt. Höjd tillslagseffekt och det faktum att säkringarna idag inte finns i snabba respektive tröga utföranden kan resultera i att en manöversäkring löser ut vid tillslag. De nya kontaktorer är Klöckner-Moeller typ DIL 8M.

## **F2-RO-021/1996 Felaktiga säkringar i utmatningsfack för AC21:5:1 och AC 21:5:2, batterisäkrat nät**

### **Händelse**

Vid besiktning av ställverket för ett helt annat arbete upptäcktes att fel dimensionerade säkringar placerats i utmatningsfack för 20656 A102, 125 ampere, och A103, 200 amper. Det sattes en 125A säkring i A103 och en 200A säkr i A102.

### **Konsekvens**

Utmatningen från A102 betraktas som degraderad med avseende på selektiviteten, medan A103 är degraderad med avseende på funktionaliteten. Betraktar man funktionaliteten så kan det här nämnas att båda utmatningarna, efter utredning om belastningar, säkras ner till 100A i samband med RA-96. Dock kvarstår degraderingen på selektiviteten på 103. INES-klassning: En mindre avvikelser i djupförsvaret D.v.s. INES=0.

### **Orsak**

Vid RA-92 har båda utmatningarna varit ursäkrade, de är placerade i ställverksfacken ovanför varandra, varvid säkringarna förväxlats. Kontrollen av återställningen har bevisligen också varit bristfällig.

## **F3-RO-013/2005 Ålar satte igen värmeväxlare**

### **Händelse**

Under revisionsavställningen genomfördes rengöring av plansil i det redundanta hjälpkylvattentiloppet (L2). Före demontage av ordinarie plansil (CB352) monterades en plansil i serie (CA352) (utanför, mot havet). I området mellan CB352 och CA352 befann sig ett antal ålar som, när CB352 lyftes, hamnade i sugledningarna till de kylvattenpumpar som var i drift. Plattvärmeväxlarna för resteffektkylning och kylning av dieselgeneratorer i 3 subar sattes igen så att systemflödet reducerades till ca 50 %. Den 4:e suben påverkades ej. Värmeväxlare i övriga system påverkades endast marginellt.

### **Konsekvens**

Resteffektkylningen ombesörjdes vid detta läge under revisionen dels av system 321, dels av system 324. Krav enligt STF tillåter att endast system 324 krediteras för resteffektkylning och vid aktuell händelse var denna funktion hela tiden driftklar. Den kylkapacitet som fanns kvar bedömdes tillräcklig för att säkerställa driftklarheten hos dieselgeneratorerna. Hindertiden är angiven som "ej tillämpbar" då erforderliga säkerhetsfunktioner bedömdes vara driftklara.

Det aktuella driftläget ställde inga krav på kylningen av kondensationsbassängen och 322-pumparna var sedan tidigare startblockerade.

### **Orsak**

Plansilarnas position medför att ett par meter av vattnet i kylvattentiloppet "slussas" förbi plansilarna. Vid detta tillfälle stod ett ogynnsamt stort antal ålar i denna "sluss".

## **F3-RO-010/1995 Styrventilerna 314 VA12, VA22, VA32, VA42 spänningslösa i samband med provning**

### **Händelse**

Vid funktionsprov av 314 ventiler med sänkt spänning måste omkopplingar ske inne i matningsskåpen via transformatorer för att erhålla den lägre spänningsnivån. Vid en omkoppling i skåp QAB 104 gjordes en felinställning på transformatorn och på så vis kortslöts matningssidan från system 677.

### **Konsekvens**

Vid spänningsavbrottet blev styrventilerna 314VA12, VA22, VA32 och VA42 utan matning. Detta medförde att säkerhets- och avblåsningsventilerna 314VA1, VA2, VA3 och VA4 inte gick att manövrera. När en säkerhets- eller avblåsningsventil ej är driftklar skall den termiska effekten sänkas med 210 MW. Detta medförde att den högsta tillåtna termiska effekten för F3 var 2460 MW vid spänningsavbrottet. F3s termiska nivå var vid tillfället 2088 MW. Händelsen bedöms ligga under INES-skalan eftersom inga minimikrav i driftvillkor har överskridits. Felet upptäcktes omedelbart och var lätt att korrigera. Händelsen utgjordes av ett enstaka mänskligt fel under en mycket begränsad tid.

### **Orsak**

Orsaken till spänningsavbrottet var att två säkringar löst ut i system 677 p.g.a. kortslutning då arbete skedde med att koppla om matningen till reducerad spänning, 85 %.

## **F1-RO-006/2002 Kortvarigt bortfall av yttre nät**

### **Händelse**

I samband med jordfelssökning i 400kV-ställverket FT 46, initierad av Svenska Kraftnät, erhöles obefogad signal för utlöst brytarfelsskydd på blockets båda aggregatbrytare varvid generatorbrytarna slog ifrån. Snabbomkoppling för matning av blockets 6kV-skenor från 70kV-nätet erhöles för tre av fyra 6kV-skenor. För den fjärde 6kV-skenan erhöles rensning och därefter spänningssättning med efterföljande startsekvens. Några sekunder in i startsekvensen erhöles utlösning av 70kV-transformatorn T19 varvid 6 kV-skenorna blev spänningslösa. Underliggande 500 V dieselsäkrade skenor spänningssattes via dieselgeneratorerna. Efter att ha konstaterat att spänning fanns på 400kV-nätet spänningssattes 6kV-skenorna via ordinarie väg från 400kV-nätet. Därefter spänningssattes även 70kV-transformatorn.

### **Konsekvens**

Händelsen innebar bortfall av yttre nät. Då samtliga fyra 500 V dieselsäkrade skenor spänningssattes via respektive dieselgenerator var spänningsmatningen till reaktorns säkerhetssystem säkrad för de funktioner som krävdes. INES-bedömning: Händelsen betraktas som en avvikelse i djupförsvaret. INES=0. Hindertid har beräknats som tiden från bortfallet till dess att samtliga 6kV ordinarie nät åter var spänningssatta.

### **Orsak**

Orsaken till den obefogade signalen för utlöst brytarfelsskydd beror på en konstruktionsbrist i 400kV-ställverkets likspänningsdel. Signaleringen för brytarfel har gemensam minusmatning för flera objekt. Konsekvensen förstärktes av att brytarfelsskydden för TA 11 och TA 12 fanns på samma minusmatning. Utredningen av händelsen har inte påvisat att några avsteg från rutin eller arbetspraxis skulle ha gjorts vid jordfelssökningen.

## **F1-RO-010/2005 Påfylld dieselolja utanför specifikation**

### **Händelse**

Den 21 mars 2005 fylldes 25 m<sup>3</sup> dieselolja i 763T1. 763T1 är en gemensam dieseloljetank för Forsmark 1:s och Forsmark 2:s dieselaggregat för hjälpkraftförsörjning. Den påfyllda dieseloljan visade sig senare vara av en kvalitet som avviker från kravet att paraffineringstemperaturen skall understiga -32°C. Då 763T1 innehöll 160m<sup>3</sup> dieselolja före påfyllningen blev utspädningen ca 15 % vilket innebar att paraffineringstemperaturen i 763T1 steg till -27°C.

### **Konsekvens**

Händelsen har ringa säkerhetsmässig betydelse, hjälpkraftdieslarna bedöms vara driftklara även efter fyllning av fel dieseloljekvalitet. Den bränsleblandning som nu finns i 763T1 är ett fullgott bränsle och har ingen negativ inverkan på funktionen hos dieselaggregaten. Att paraffineringstemperaturen höjts till -27°C har ingen säkerhetsmässig betydelse vid rådande utomhustemperatur. Om händelsen inträffat vid en tidpunkt med långvarig stark kyla hade respektive dieselaggregat haft dieselolja för två dygns kontinuerlig drift genom innehåll i tillhörande dagtank. Dagtankarna är placerade inomhus i rumstemperatur. Den mer intressanta frågeställningen är hur det var möjligt att felaktig dieseloljekvalitet kunde fyllas på. Hindertid är inte tillämplig då dieselaggregaten bedömts driftklara. Händelsen klassas till under INES-skalan. INES=0.

### **Orsak**

Bakomliggande orsak till att felaktig dieseloljekvalitet fylldes på var att gällande rutiner och instruktioner för beställning, mottagningskontroll och upphandling var bristfälliga och inte följdes fullt ut.

## **R1 RO 27/03 Kontaktorfel orsakade misslyckad snabbomkoppling av A-sub från 400kV till 130kV inmatningsväg**

### **Händelse**

I samband med avställning av 400kV inmatningsväg misslyckades snabbomkoppling av A-sub till 130kV inmatningsväg och dieselsekvensautomatik gick därför i funktion med start av nödkraftaggregat DG110. Dock erhöles ej brytartilslag på DG110-S varför dieselsäkrat nät A-sub förblev spänningslöst. Åtgärder genomfördes enligt störningsinstruktion utan att lyckas spänningssätta D11-A6. Återinkoppling av H11-A6 till LT110 genomfördes och vid prov av förnyad snabbomkoppling lyckades detta varvid H11 matades via H91-6. DHC11 reservmatades via DHC12 och samtliga övriga dieselaggregat provkördes u.a. I överensstämmelse med STF-krav. Underhållspersonal kallades ut. Felsökning visade att den misslyckade dieselsekvensen berodde på två felfungerande kontaktorer som speglar brytarlägen för DHC11-DHC12-S och DHC12-DHC11-S i logiken för "isolerad" dieselskena och är ett villkor för att spänningssättning skall kunna ske. Kontaktorerna byttes och provades (komponent DKV). Därefter återställdes DG110, D11-A6 och DHC11 till normal driftläggning och skarpt prov av dieselsekvensautomatiken genomfördes u.a. A-sub förklarades åter driftklar 2003-09-01 klockan 02:45. När felorsaken klarställdes insågs att även redundant skena D12-B6 varit påverkad av samma felande kontaktorer och hade vid eventuellt spänningsbortfall uppvisat motsvarande blockering av dieselsekvens varför även D12-B6 varit ej driftklar. Ingen driftmässig konsekvens utöver störningsförloppet erhöles då blocket var kallt avställt för revisionsöversyn.

### **Konsekvens**

Dieselsäkrat nät är uppdelat på 4 subar och har till uppgift att försörja blockets säkerhetssystem med elkraft även vid eventuellt bortfall av yttre eller ordinarie nät. Aktuellt fel innebar att de båda redundanta skenorna D11-A6 och D12-B6 i händelse av yttre fel eller fel på ordinarie nät, inte hade gått att spänningssätta då samtliga inmatningsbrytare blockerats för tillslag. Detta hade i sin tur bl. a. medfört att samtliga drivdonsmotorer (10-221) och borinsprutningspumparna (10-351) blivit spänningslösa. Dock hade snabbstoppsfunktion via system 10-354 fungerat. Om felet identifierats under normal effektdrift hade detta inneburit omedelbar nedgång till kall avställd reaktor. I aktuellt fall var blocket kallt avställt för årlig revisionsöversyn varvid endast en av blockets båda redundanta sidor A/C och B/D av kraftförsörjningssystemet krävs för driftklarhet. Då även D12-B6 förklarades ej driftklar p.g.a. ej driftklar DG120 uppfylldes inte kravet på driftklar B/D-sida enligt STF. Endast A sub drabbades dock av spänningsbortfall och reservmatning kunde ske DHC12 till DHC11. Konsekvens på systemnivå är satt till extra reducerad redundans.

Snabbomkopplingen har ingen säkerhetsmässig funktion och används endast manuellt vid behov av avbrottsfri driftomläggning mellan de båda inmatningsvägarna. Dock skall utrustningen provas och befinnas funktionsduglig 1ggr/år vid revisionsavställning för att få användas.

### **INES-BEDÖMNING:**

Händelsen bedöms utgöra en avvikelse i djupförsvaret D.v.s. INES=1.



### **Orsak**

Se även rapport 1752569. Felaktiga kontaktorer har till uppgift att spegla brytarläge från för DHC11-DHC12-S och DHC12-DHC11-S och ingår som villkor för tillslag av D11-H11-6-S och DG110-S i dieselsekvensautomatik sub A samt villkor för tillslag av D12-H12-6-S och DG120-S i dieselsekvensautomatik sub B. Följande bakomliggande orsaker till händelsen kan identifieras: Kontaktorerna kärvade och gav felaktigt signal till logiken att brytarna låg i tilläge. Kärvningen är troligtvis orsakad av temperatur och åldring i plastmaterialet som medfört kärvning. Felbilden är sedan tidigare känd hos aktuell kontaktortyp, ASEA EG10L. Då problematiken upptäcktes genomfördes en inventering för att identifiera och byta kontaktorer av aktuell typ i applikationer med funktionsklass 1E. Aktuella kontaktorer har uppenbarligen inte kommit med i detta utbytesprogram. Utbyte av kontaktorer av aktuell typ har därefter skett löpande vid felupptäckt. Signal för indikering av brytarläge och signal till logiken för dieselsekvens är helt olika kretsar vilket gör att felet kan uppstå dolt. I samband med underhåll har brytarindikering i kontrollrum kontrollerats men lägesindikeringen till dieselsekvenslogiken har inte identifierats och provats. Under RA02 provades dieselsekvensen på samtliga subar utan anmärkning vilket innebär att felet uppträtt någon gång efter detta. Möjligen har "sista" kontaktorn felfungerat i samband med FU på sammankopplingsbrytarna som normalt sker under driftperioden. FU på aktuella brytare har skett 2003-02-27. Hinder tid beräknas därför från detta datum. Grundorsaken till den misslyckade snabbomkopplingen har inte gått att fastställa då felet inte upprepats vid provning. Troliga orsaker kan vara intermittent fel i omkopplingsautomatik eller tillfällig tröghet i brytarmekanismen.

**KOMPONENTTYP: Kontaktor ASEA(ABB) typ EG10L.**

## **R2-RO-014/2001 Felaktig beräkningsalgoritm i överlastskydd**

### **Händelse**

På morgonen den 20 juni löste ett överlastskydd ut i den ofavoriserade delen av elsystemet efter 32 minuter vid 60 % av sin märkström. En undersökning och provning av det aktuella skyddet inleddes. Även ett reservskydd kontrollerades. Proven visade att båda skydden löste ut för tidigt. Eftersom skydden finns i både favoriserat och ofavoriserat nät sammankallades en grupp med bred kompetens för att bedöma blockets driftklarhet. Följande framkom:

Felet hade introducerats under RA-01 vid åtgärd av en restpunkt i EK-projektet (modernisering av R2 elsystem). Som åtgärd byttes då ett så kallat EPROM i skydden. Restpunkten identifierades vid ett FAT – prov (Factory acceptance test). EK-projektet ansåg att skyddens mätfrekvens skulle kunna ge feltolkning av det skyddade objektets verkliga last och begärde en ändring till tätare mätfrekvens.

Skyddens antal är totalt 58 stycken varav 14 stycken ännu ej hade åtgärdats utan hade kvar ursprungligt EPROM, dvs. var felfria. Slutsatsen var att redan vid 40-50 % av sin märkström fanns risk för att skyddet skulle kunna lösa ut. Dieselmattningen av favoriserat 6kV-nät (D-skena) har inget överlastskydd av denna typ och berördes ej.

Gruppens bedömning var att elsystemet i den del som påverkas av dessa 44 skydd ej kunde garanteras vara driftklart. Rekommendationen var att överlastfunktionen skulle väljas bort i skydden och därmed återställa driftklarheten. Föreslagen åtgärd styrktes av utförda analyser vilka dokumenterats i rapporter inom Ekprojektet

Beslut fattades att så skulle ske och en handlingsplan gjordes upp för genomförandet. Denna innehöll både regler för genomförandet och prioritering av ordningen baserad på skyddens betydelse för reaktorsäkerheten, samt verifiering av att funktionen verkligen var borttagen. Efter bortkoppling av överlastskydden bedömdes anläggningen driftklar.

### **Konsekvens**

Överlastfunktionen finns i reläskydd för kablar och transformatorer. Dessa reläskydd har till uppgift att skydda mot skadlig uppvärmning. Belastningar (motorer) samt dieselgeneratorer är försedda med andra reläskydd och påverkas ej av denna händelse. Inställningsvärde för överlastfunktionen är baserad på den last som kablar och transformatorer termiskt kan överföra. Ringhals 2 elanläggning är kraftigt överdimensionerad ur termisk synpunkt för att hålla nere spänningsfall. Normalt utnyttjas endast runt 50 % av elanläggningens kapacitet.

Marginaler finns för samtliga reläskydds överlastfunktion. Minst marginal finns för skydden för transformatorerna mellan 6 kV och 500 V dieselsäkrat nät det vill säga i matningen till DHC 21, 22, 23 och 24. För denna förbindelse har en fördjupad analys gjorts i tre fall av intresse:

Bortfall av yttre nät med dieselsekvens och start av hjälpavapump (matas från DHC).

LOCA med yttre nät tillgängligt.

LOCA utan yttre nät tillgängligt.

Analysen (Rapp 1715892) visar att det belastningsmässigt värsta driftfallet är ”Bortfall av yttre nät med dieselsekvens och start av hjälpavapump”. Hjälpavapumparna har 500 volts motorer. Tidigare rapport 1601349 pekar ut DG210 som den mest belastade dieseln men då beaktas även belastningen från 6 kV-skenan.

Det värde som de felaktiga skydden skulle kunna lösa vid är lägst 56 % av inställt funktionsvärde. Detta värde är beroende av "noise" på de tre fasströmmarna, om toppvärdet varierar i tiden mellan perioderna. I anläggningen har uppmätts 0,4 % noise, värdet 56 % för utlösning är beräknat utgående från 2 % noise.

Utan noise skulle överlastfunktionen efter en viss tid ge utlösning vid en belastningsström på 123A. Med 2 % noise är utlösningvärdet 94A. Utförda tester har visat på att ökningen av det termiska innehållet som funktion av inställd tidskonstant i skyddet är starkt beroende på vilket noise som testen utförs vid.

Med uppmätt noise på 0,4 % erhålles ett högre lägsta värde än de 94A som gäller för 2 % noise. Detta gör att marginalerna nedan skall värderas mot den konservatism som finns inbyggt i antagandet att utlösningen erhålles vid 94A. Utlösningvärdena har en onoggrannhet på  $\pm 5\%$  (90 – 129 A).

Belastningsströmmarna i det värsta driftfallet ovan är för DHC21 86 A, DHC22 94,6A, DHC23 89A och för DHC24 82A. Marginalen mot utlösning till det felaktiga funktionsvärdet för DHC21, -23 och 24 är därmed större än den ursprungligt bedömda (2001-06-20). För DHC22 finns en möjlig påverkan om ett antal faktorer samverkar.

Det aktuella driftfallet "Bortfall av yttre nät med dieselsekvens och start av hjälpmavapump", har provats under uppstartssekvensen RA-01. Dessutom har det provats "skarpt" vid det snabbstopp som inträffade 2001-06-17 då gasvakten på transformator T22 löste ut brytare T22-400-S (400 KV på 22-sidan). DG 220 spänningsmatade då DHC 22 via D22-B6 och DG 240 DHC 24 via D24-D6 under 1 timme och 50 minuter respektive 2 timmar.

Vid dieselsekvens på Ringhals 2 startar enbart de objekt som tidigare varit i drift. Vid en mer trolig driftläggning finns marginal till funktionsvärdet eftersom objekt med redundans då matas från annan skena. För DHC21 och DHC22 är det sammanlagt 25,6A belastning som matas från en av skenorna, dvs. lasten på DHC22 ligger vid det analyserade fallet mellan 69A och 94,6A. Överlastskyddet löser ut efter mer än 30 minuter vid en last mellan 90 och 129 A. Den utförda fördjupade analysen visar att blockets konstruktion är robust och har så stora marginaler att påverkan på säkerhetssystemen är liten, begränsad till en DHC-skena och påverkar ej redundanta objekt.

Den tidigare preliminära säkerhetsbedömningen framstår efter den fördjupade analysen som alltför konservativ. Den säkerhetsmässiga betydelsen är endast reducerad redundans enligt instruktion DA 0652 (Ifyllnadsanvisning för Rapportvärda omständigheter kategori 1 och 2 samt snabbstopp).

Hindertiden är beräknad från att det första EPROM:et byttes. Fördelningen är 24 dygn under revision och 6 dygn under effektdrift.

### **Orsak**

Det EPROM som levererades och som inte skulle påverka annat än mätfrekvensen hade erhållit även andra egenskaper. Insikten om vad åtgärdandet av restpunkten innebar har inte uppfattats som en anläggningsändring (byte av EPROM) utan enbart som en parameterändring i befintliga EPROM. Ärendet har därför hanterats enligt normala underhållsrutiner med normal reläskyddsprovning.

## **R2-RO-34-2005 Hjälpmatarvattenpump ej driftklar**

### **Händelse**

Tisdagen 2005-08-30 skulle den eldrivna hjälpmatarvattenpumpen AFAPMD-01 testas enligt arbetsschemat för skiftet (AFS) och översynskravet SR 3.7.6.2. I startögonblicket löste pumpen på överström.

Eftersom indikeringen kunde vara kortslutning i motorn förklarades AFAPMD-01 ej driftklar klockan 03.19. Efter felsökning startades pumpen klockan 10.20 och provades med underhållspersonal närvarande utan anmärkning. Undersökning av det utlösta överströmsskyddet fortsatte. Efter beräkning av expertis på skydden togs beslut av driftledningen att ställa upp överströmsskyddet.

klockan 14.45 startades pumpen och provades utan anmärkning. Pumpen förklarades vara driftklar. Hindertiden för AFAPMD-01 sattes till 347 timmar 15 minuter, halva tiden från att pumpen senast verifierades driftklar plus åtgärdstiden. Händelsen hade ingen driftmässig konsekvens.

### **Konsekvens**

Hjälpmatarvattensystemet säkerställer att ånggeneratorerna (ÅG) förses med tillräckligt flöde för att kyla ned anläggningen till 177°C från normala driftförhållanden, i händelse av total förlust av kraftmatning från yttre nät.

Hjälpmatarvattensystemet består av två motordrivna hjälpmatarvattenpumpar och en ångturbindriven hjälpmatarvattenpump konfigurerade i tre separata kretsar. Varje motordriven pump ger 100 % och den turbindrivna pumpen ger 200 % av krävt flöde till ånggeneratorerna, enligt antaganden i haverianalysen.

Under reparationstiden hade ÅG1 inte kunnat fyllas med vatten enligt normal driftläggning. Genom en driftomläggning från kontrollrummet hade ÅG1 kunnat förses med vatten från de andra två hjälpmatarvattenpumparna. Eftersom två driftklara pumpar fanns tillgängliga, driftlagda till sina respektive ÅG och med en pumpkapacitet att mata alla tre ÅG efter driftomläggning, bedöms säkerhetspåverkan som låg.

### **Orsak**

Under RA-05 byttes samtliga MICOM-skydd typ P220 på A-sidan ut till en ny version typ P132. Utbytet skedde efter att ett antal falska larm och slutligen en blockering av en säkerhetskomponent inträffat. Av CCF-skäl byttes enbart skydden på A-sidan. Avsikten är att byta skydden på B-sidan RA-06. Bytet sköts i projekt "R2 Utbyte av reläskydd MICOM P220", projekt A.01036. Upptagna kurvor från skyddets störningsskrivare visade på att höga värden på strömmen erhålls under den första periodens första halva. Dessa strömtoppar ligger betydligt över den startström som därpå följer.

Jämfört med de skydd som sitter på B-sidan (P220) har A-skydden ingen tidsfördröjning på utlösning. På B-sidan finns en fördröjning på 20 ms. Denna fördröjning löser problemet då tiden motsvarar en period. Varför fördröjningen togs bort på de nya skydden förklaras med att i de nya skydden finns ett filter som eliminerar likströmskomponenten. Dock insågs inte att startspiken fortfarande kunde lösa ut skyddet under de första millisekunderna. Ny mätutrustning, sen ett par år, möjliggör att studera kurvans utseende i millisekundsskalan. Detta gjorde det möjligt att identifiera felorsak vid felsökningen. Gjorda prov visar att tidsfördröjningen krävs för att garantera robustheten på skydden.

Under onsdagen provkördes ett antal komponenter på A-sidan för att verifiera driftklarheten. Samtliga fungerade utan anmärkning men proven visade också på att tidsfördröjningen borde införas för att få större marginal mot utlösning av skyddet vid start. Motorn till AFAPMD-01 byttes år 2002. Eftersom varje motor har sin egen karakteristik och inga nya skrivarkurvor togs upp efter bytet kan detta ha bidragit till minskad marginal mot utlösning av skyddet.

## **R2-RO-013/1990 Bränslebassängkylning avbruten på grund av felfungerande CC-pumpar**

### **Händelse**

I samband med driftomläggning av komponentkylvattensystemet för arbeten skulle den av systemets 3 cirkulationspumpar som var driftlagd som driftpump stoppas för att undvika att pumpen skulle kavitera vid driftomläggningarna. Pumparna har en nyckelförregling som i automatkläge ger startimpuls till alla pumpar när differenstrycket mellan systemets säkerhets- och icke säkerhetsanknutna del blir för lågt eller vid bortfall av driftpumpen. I blockeringsläge blockera startsignalen från differenstrycket och endast funktionen med bortfall av driftpumpen är i ingrepp. Innan stoppet lades nyckelförreglingen i blockeringsläge för att pumparna inte skulle starta p.g.a. det låga differenstrycket som skulle uppstå när inga pumpar var i drift. Detta medförde att de två stillastående pumparna startade. Detta borde inte ha inträffat. När pumparna kort därefter åter stoppades resulterade detta i att alla pumpar återstartade. Förnyat stopp av alla pumpar gav samma resultat som vid det föregående tillfället. Vid det tredje försöket startade inga pumpar och driftomläggningen utfördes varefter driftpumpen skulle tas i drift. Detta visade sig vara omöjligt. Den driftmässiga konsekvensen blev att komponentkylsystemets cirkulationsflöde upphörde och därmed kylningen av bränslebassängerna under 2 timmar och 15 min. Temperaturen i bassängerna steg ca 5 grader under händelsen.

### **Konsekvens**

Bränslebassängernas kylsystem var ej driftdugligt under den tid komponentkylpumparna inte gick att starta. Samtidigt befann sig hela den nyligen urladdade härden i bränslebassängerna.

### **Orsak**

Vid upprättning av logikkretsarna för hjälpmatarvattenpumparna har även system 711's (komponentkylsystemet) logikkretsar som finns i samma skåp och även finns med på samma 'wiring diagram' som hjälpmavapumparna blivit upprättade i enlighet med befintligt kretsschema. Schemat var felaktigt, således innebar "upprättningen" att ett fel byggdes in i 711 logiken som gjorde att när en aut/blockomkopplare i KR2 i autoläge och alla pumpar i system 711 stoppades, blockerades återstart av pumparna.

Ursprungorsaken är avsteg mot STF 6.3 F.

## **R4-RO-19/98 Nedsatt funktion av labyrinttätningar i inneslutningens sprinklingspumpar**

### **Händelse**

Efter periodiskt test 981015 konstaterades vid rondning 981016, låg oljenivå i sprinklingspump 4:as (SPAPCS-04) lagerhus. 4MM fyllde under dagen på olja och provkörning utfördes för kontroll. Olja läckte externt ut via labyrinttätning till mellandränage och vidare till dränagesystemet (VD-352). I dränagesystemet är ett svagt undertryck upprättat för att kunna ta hand om eventuella gaser. Anslutningen från pumpen till dränagesystemet och olja återfylldes till lagerhuset. Pumpen kördes därefter under 1,5 timmar utan problem.

Under tiden felsökning/provkörning av SPAPCS-04 pågick, togs kontakt med beredare på 4MM för klarställande om exakt vad som utförts på pumpen under revision 1998. I samband med att pumpen provkördes efter bortkoppling av VD-anslutningen framkom det att SPAPCS-03 hade fått en ny typ av labyrinttätning monterad under årets revision. Det framkom då också att SPAPCS-03 fått motsvarande tätning monterad under revisionen (däremot inte SPAPCS-01/02).

Provkörning av SPAPCS-03 inleddes snarast och efter 40 minuters drift erhöles samma problem för denna pump. Ledningen mot dränagesystemet demonterades även på denna och förnyad provkörning inleddes. Efter en timmes drift utan problem gjordes bedömningen att pumparna fungerade utan anmärkning med VD-anslutningen bortkopplad.

De två återstående pumparna, SPAPCS-01 och -02 som ej har modifierats med avseende på labyrinttätningar provkördes under två timmar vardera utan problem. Normal drifttid vid periodisk test är 15 minuter.

### **Konsekvens**

Sprinklingssystemets två delsystem med vardera två led har tillsammans 200 % kapacitet och skall vara driftklara när reaktorkylmedlets (RCS) temperatur överstiger 93°C. Systemets funktion är att vid högt tryck i inneslutningen kondensera vattenånga och därigenom minska risken för att aktiva gaser sprids till omgivningen på grund av att inneslutningens tryck överstiger designtrycket. I recirkulationsfasen reduceras även eventuell frigjord jod genom att trinatriumfosfat tillsätts sprinklingsvattnet. Sprinklingspumparna var hela tiden driftklara trots utläckaget av smörjolja men händelsen visar på brister i rutinerna vid ändring i komponenter.

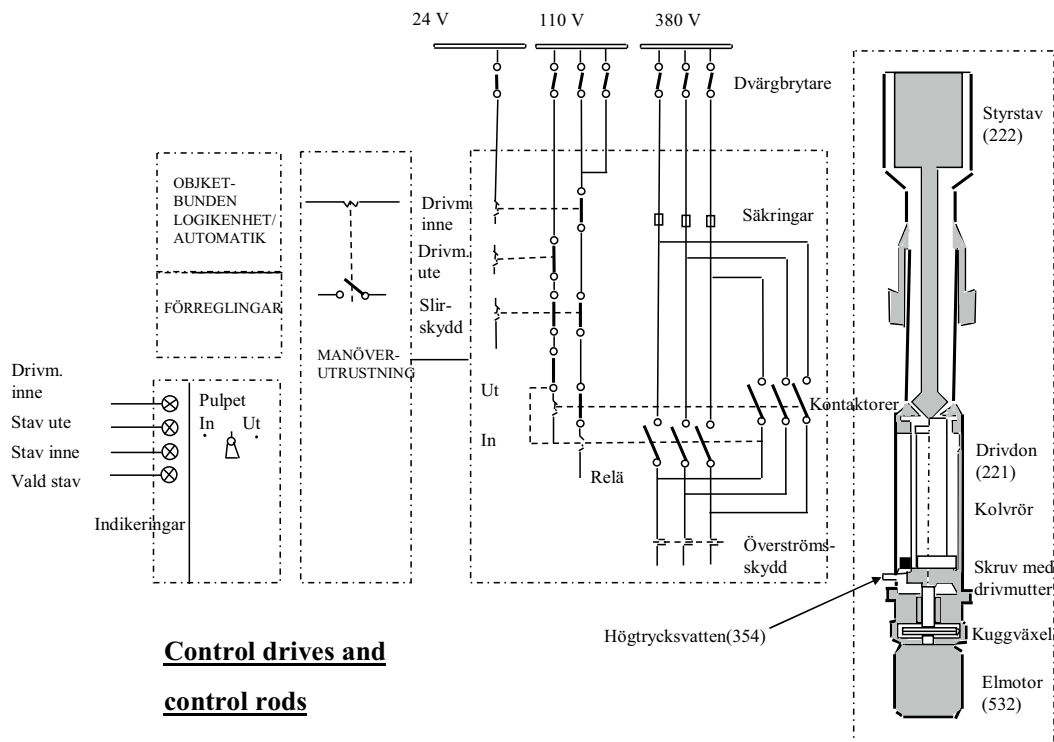
### **Orsak**

Den nya typen av labyrinttätning har en nedsatt funktion då ett svagt undertryck råder i tätningshuset. Med anledning av händelsen har 4MM utfört tester som verifierar att smörjoljeläckaget upphör efter en tids drift trots undertryck från anslutande system och att återstående mängd är tillräcklig för att smörja lagren även vid kontinuerlig drift.

## Bilaga 3: Vägledning – erfarenheter från insamling av CCF-händelser på styrstavar och drivdon (CRDA)

### Komponentgruppen styrstavar och drivdon

CRDA-system har två separata uppgifter; säkerhets- och driftuppgifter. Säkerhetsuppgiften är att införa en väsentlig mängd absorberande material till reaktorhärden. Driftuppgiften handlar om att säkerställa en acceptabel effektfördelning i härden under drift. Design för utformning av inskjutning/inskrivning av styrstavar varierar mycket mellan olika typer av anläggningar, där vissa typer utför inskjutning med hjälp av gravitation medan andra har hydraulisk inskjutning och/eller motordriven inskrivning. Ett exempel på utformning ges i figuren nedan.



**Control drives and control rods**

Figur 1. Exempel på CRDA komponentgrupp och gräns [22].

Inom ICDE samlas data in som berör komponentens säkerhetsuppgifter, men även fel avseende komponentens driftfunktion samlas in då det rör sig om fel som även kan relateras till komponentens säkerhetsuppgift.

Komponenten anses fela då den inte kan utföra sin säkerhetsuppgift, vilket innebär utebliven inskjutning/inskrivning eller fördröjd inskjutning/inskrivning av en (eller flera) stav(ar).

Storleken på CRDA grupperna varierar från 109 st. till 169 st. styrstavar i de Nordiska BWR anläggningarna.

Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

<b>Observerat antal kalenderår</b>	<b>CCCG storlek</b>	<b>Nordiska data</b>	<b>Internationella data (inkl. nordiska)</b>	
Observationsperioden för nordiska data är 1983-01-01 – 2003-12-31	3		28,00	
	4		77,00	
	6		147,05	
	8		14,00	
	12		42,01	
	16		21,00	
	Observationsperioden för internationella data är 1983-01-01 – 2004-12-31	24		28,01
		45		7,00
		48		123,04
		50		1200,55
		53		100,03
		57		179,05
		61		77,01
		65		180,05
		69		175,08
		73		28,12
76			360,16	
81			72,02	
89			36,01	
92			18,01	
101			18,01	
107			18,01	
109		58,95	75,44	
112		21,01	21,01	
121		42,02	42,02	
127			10,50	
130		14,00		
145		28,00		
157	21,01	21,01		
161	42,02	42,02		
169	36,02	36,02		
179		12,01		
185		1242,56		
193		56,02		
205		7,00		
370		816,37		
<b>Totalt</b>		221,03	5373,21	
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		29	167	

Tabell 1. Observationsperiod.



## Samlad statistik om komponentgruppen

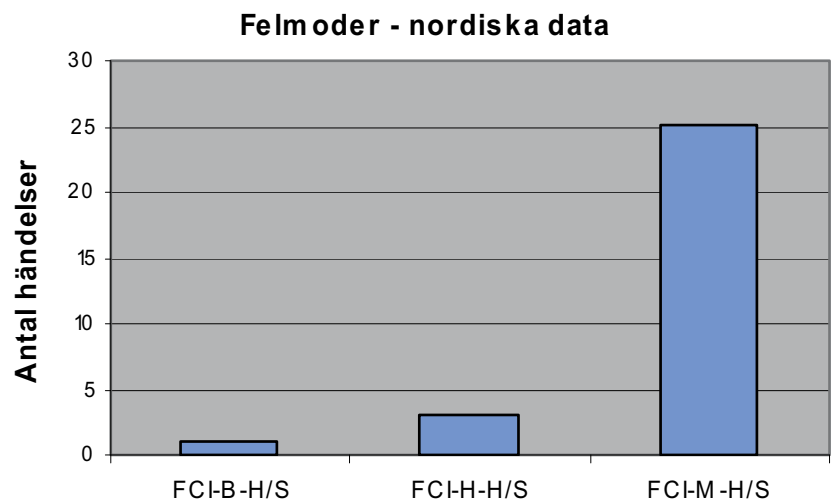
I en SKI-rapport [21] redovisas en dataanalys som nyligen utförts på CRDA komponentgruppen. I denna framgår det att endast en bråkdel av CRDA felen som påverkar den elektriska-mekaniska inskruvningen av styrtavar är detekterbara vid de återkommande manövertesterna, som utförs varannan vecka. Problem med friktion i nya och fräscha axeltätningar, vid uppvärmning upptäckts vanligtvis inte vid manövertester, däremot upptäckts eventuella problem i dessa först efter andra - tredje inskruvningsbehovet efter en reaktoravställning eller en underhållsåtgärd.

### Felmoder

För komponentgruppen är följande felmoder relevanta i ett PSA perspektiv och därmed tillämpade vid datainsamling inom ICDE.

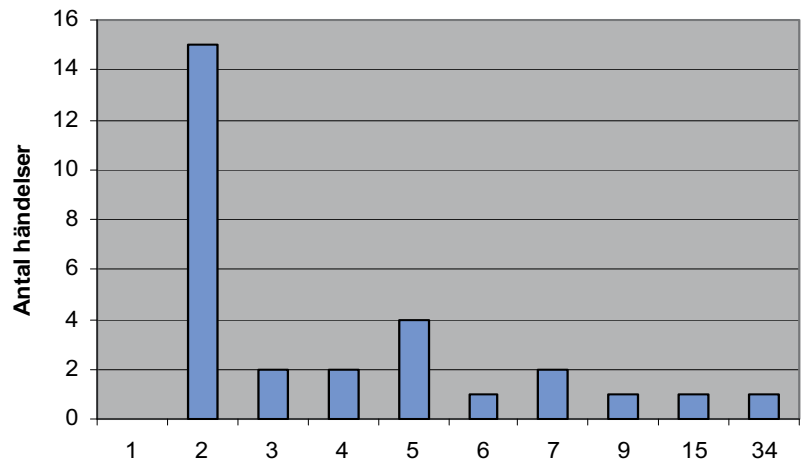
- FCI-B-H/S - Failure to completely Insert - Failure of both insertion function - Hydraulic/Screw Insertion System
- FCI-H-H/S - Failure to completely Insert - Failure of the hydraulic insertion function - Hydraulic/Screw Insertion System
- FCI-M-H/S - Failure to completely Insert - Failure of the electromechanical insertion function - Hydraulic/Screw Insertion System
- FCI-G – Failure to completely Insert - Gravity Insertion System
- FC - Failure to close (Valve)
- FO - Failure to open (Valve)
- – Other
- IC - Inadvertent Closure (Valve)
- HIT-H - High (large) Insertion Time, Hydraulic Function, control-rod cluster/rod insertion time exceeding Technical specifications

För nordiska data står felmoden FCI-M-H/S, dvs fel i den elektriska-mekaniska inskruvningen, för ca 86%, och är därmed överlägset den vanligaste felmoden (framför fel i hydraulisk inskruvningsfunktion).



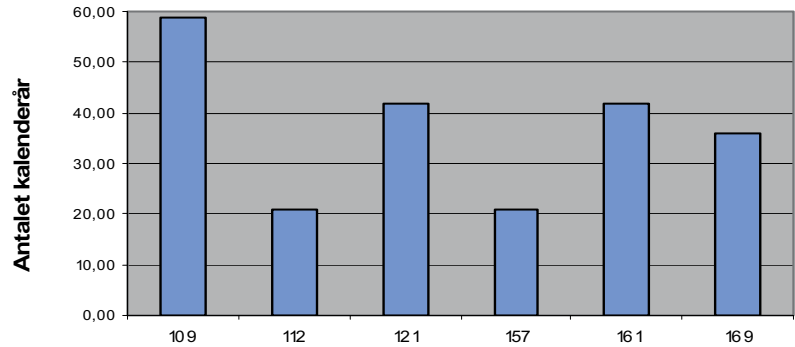
**Påverkade komponentgruppstorlekar**

**Storlek på exponerad populationr - nordiska data**



**Ackumulerade kalenderår per komponentgruppsstorlek**

**Kalenderår per KG-storlek - nordiska data**



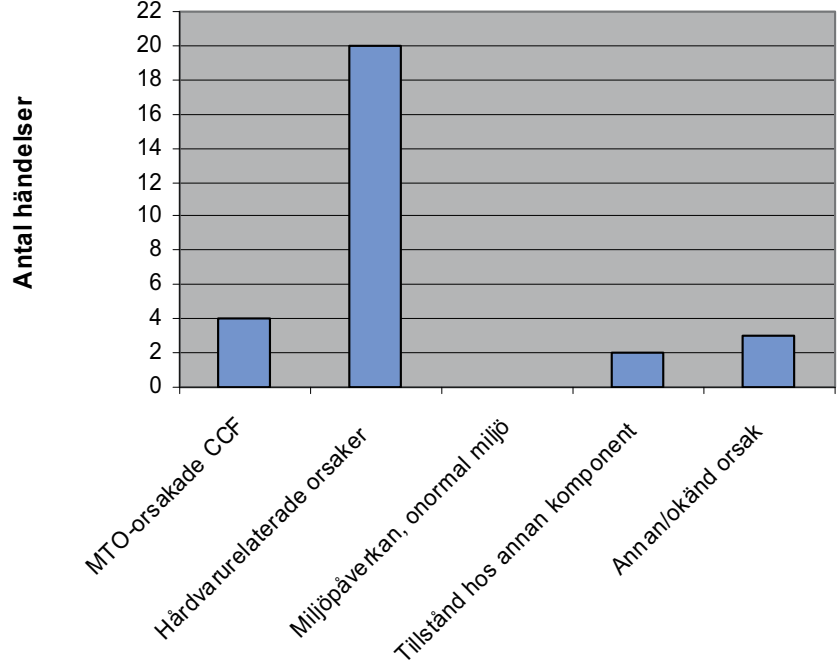
**Troliga felorsaker**

För nordiska data har den största andelen av händelserna hårdvarurelaterade orsaker, enligt nedanstående kategorier:

- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt

Inom gruppen av hårdvarurelaterade orsaker är brist i design konstruktion eller tillverkning den tydligt vanligaste kategorin.

**Root causer - nordiska data**



### Kopplingsfaktorer

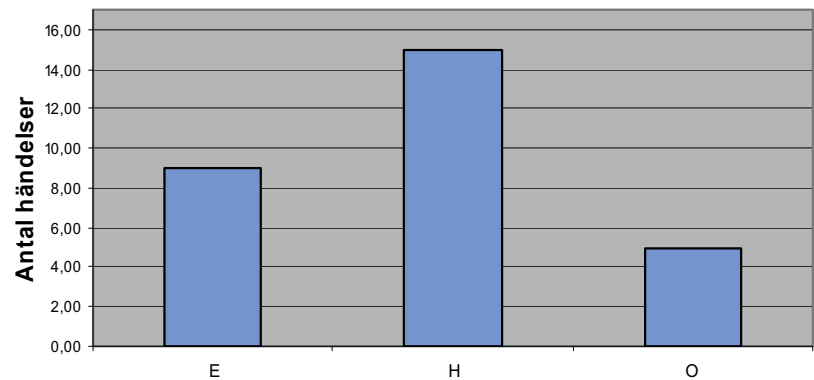
Kategorisering är gjord enligt nedan:

- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedure
  - Underhållsschema
  - Driftinstruktion

Den vanligaste gruppen är hårdvarurelaterade kopplingsfaktorer, vilken svarar för ungefär 50 %. Gruppen följs av miljörelaterade kopplingsfaktorer som står för ungefär 30 % av fallen.

Inom dessa grupperingar är de kommer de största enskilda bidragen från kategorierna hårdvarudesign (ca 45 % av händelserna) och intern miljö (ca 30 % av händelserna).

Kopplingsmekanismer, i gruppr - nordiska data

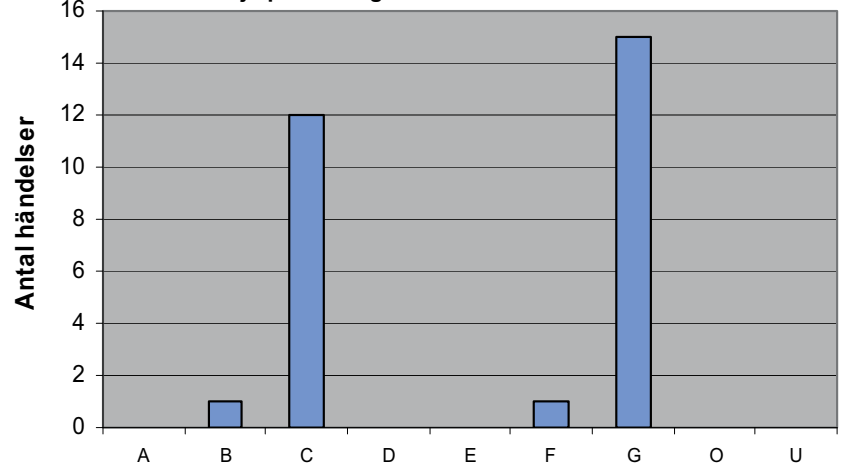


### Avhjälpande åtgärder

För nordisk data är den vanligaste insatta åtgärden kategori G (ca 52 % av händelserna), enligt kategorierna nedan:

- Administrative control or a procedure control (A)
- Specific maintenance or operational practice (B)
- Design modification (C)
- Diversity (D)
- Functional/spatial separation (E)
- Test and maintenance policies (F)
- Fixing of component (G)
- Other (O)
- Unknown (U)

Avhjälpande åtgärderr - nordiska data

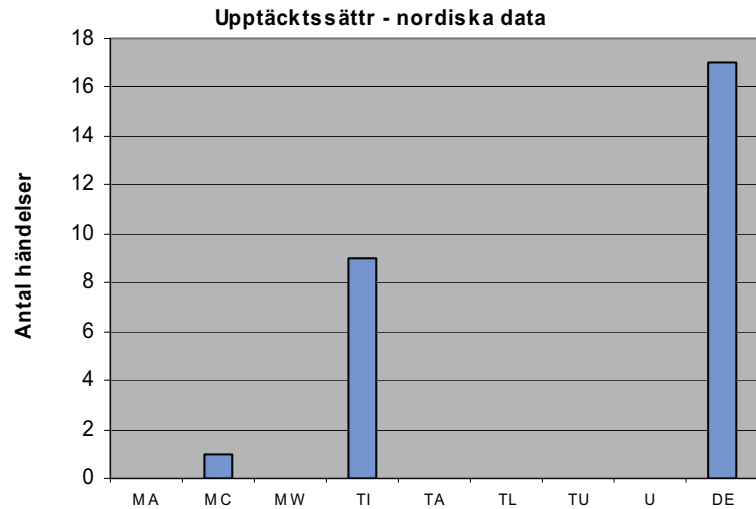


### Upptäcktssätt

Upptäcktssätt delas in i följande kategorier:

- Monitoring on walkdown (MW)
- Monitoring in control room (MC)
- Maintenance/test (MA)
- Demand event (DE)
- Test during operation/annual overhaul/laboratory (TI/TA/TL)
- Unscheduled test (TU)
- Unknown (U)

För nordiska data upptäcks de flesta händelser (nästan 60 %) vid behovssituationer (kategori DE). Det näst vanligaste upptäcktssättet är ”test under drift, kategori TI, som svarar för ca 30 % av fallen.



Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplings- faktor	Upptäckts- sätt	Komponent- degradering, vektor	Tidsfaktor/ faktor för gemensam orsak
CRDA	7	FCI-H-H/S (Failure to completely Insert - Failure of the hydraulic insertion function - Hydraulic/Scr ew Insertion System)	P (Procedure inadequacy)	OMP (Maintenance/ test Procedure)	DE/TU (Demand event / Un- scheduled test)	CCCDDDD	High

**Händelsebeskrivning:**

In annual overhaul 1992 of Ringhals 1 in total 24 control rod drives in two quadrants had been maintained. In cold state tests prior to start-up in January 1993 all control rods operated normally. In scram tests, in hot standby, the hydraulic insertion of 3 control rods slowed down and they stopped at about 50% - 40% withdrawn position, when low level was reached in hydraulic scram tanks. The screw function completed the insertion. The same symptoms recurred in subsequent investigation of the problem and repeated tests. Altogether 7 rods were affected by the failure mechanism, high friction in the graphite tightenings, resulting in low insertion speed of hydraulic function and stopping of the rod at intermediate position. All affected drives had new graphite tightenings. Normally many drive maneuvers are executed after installing new tightenings in order to get them well adapted. Afterwards it was observed that a smaller number of such post-maintenance maneuvers were carried out this time due to unknown reason. The likely explanation is increased friction at the fresh graphite tightenings due to dry friction phenomenon, arising at hydraulic insertion in operational conditions.

**Tolkning:**

The transition into dry friction state showed certain randomness. Therefore, the impairment of 4 CRDAs failing in additional tests but working in the initial start-up tests is set degraded (D). The randomness means also possibility that the failure mechanism could have remained undetected in the initial start-up tests, implying certain conditional CCF risk during the following power cycle. Time Factor = H according to Coding Guide. Quantitative analysis should take into account component-to component variation in the phase causing critical failure. Latent time is set zero, because failures were detected in start-up tests, i.e. not latent in power operation state.

*Tabell 3. Exempel på inträffad händelse.*

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplings- faktor	Upptäckts- sätt	Komponent- degradering, vektor	Tidsfaktor/ faktor för gemensam orsak
CRDA	2	FCI-M-H/S (Failure to completely Insert - Failure of the electro- mechanical insertion function - Hydraulic/ Screw Insertion System)	C (State of other component)	HC (Hardware Design)	DE (Demand event)	CC	High
<p><b>Händelsebeskrivning:</b> Moment trip of drives G55 and L75 occurred when V-chain (SS12) actuated, no causes identified. Moment trip of G55 recurred at insertion in 2% movement test on 1986-04-12, cause again unknown.</p> <p><b>Tolkning:</b> The failure type is likely to not be detected in periodic movement tests. Latent time is derived as maximum from the preceding demand, a reactor scram (SS1) on 85-06-03.</p>							

Tabell 4. Exempel på inträffad händelse.

### Vidare läsning

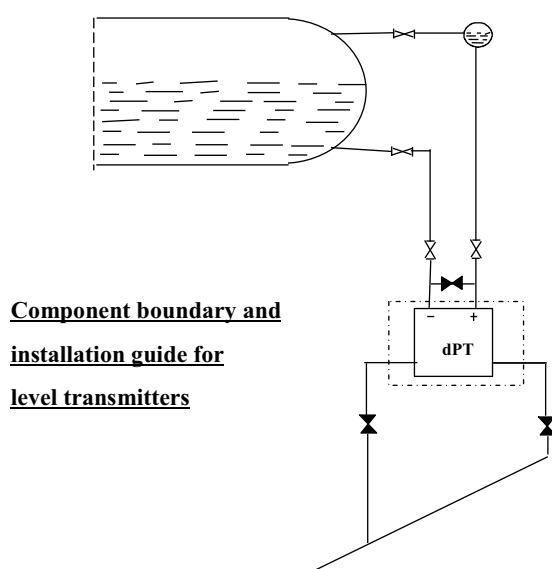
- ICDE General Coding Guidelines [16].
- Arbete genomfört av nordiska arbetsgruppen för CCF-studier (NAFCS) [6].
- Drifterfarenheter av komponenten [21].
- Presentationsmaterial om komponenten [23, 24].

## Bilaga 4: Vägledning – erfarenheter från insamling av CCF-händelser på nivåmätinstrumentering (LM)

### Komponentgruppen nivåmätinstrumentering

Komponentens funktion är att övervaka vätskenivån i tankar och ledningar av säkerhetsmässig betydelse. Utsignal från nivåmätutrustning används för utlösning av reaktorskyddssystem vid för hög eller för låg nivå. Komponenten finns i flertalet olika system (i såväl BWR- som PWR-anläggningar), och transmittar/sensorer finns i olika utföranden.

I komponenten ingår tryckmätare, ventil, transmitter/sensor, indikeringsinstrument, gränsbrytare.



Figur 1. Komponentgrupp och gräns.

Komponenten anses fela då den inte övervakar den verkliga nivån och utlöser gränsbrytare vid en förutbestämd nivå (kan vara låg eller hög).

Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

<b>Observerat antal kalenderår</b>	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för såväl nordiska som internationella data är 1983-01-01 – 2003-12-31	2	144,00	320,96
	3	304,15	1327,58
	4	492,25	742,73
	6	86,04	258,86
	8	72,04	206,5
	9	84,03	94,03
	10		17,76
	12	50,02	809,32
	15		326,14
	16	38,02	55,78
	18	42,02	42,02
	20		30,02
	24		28,01
	36	24,01	24,01
	64		8,88
<b>Totalt</b>	<b>1336,58</b>	<b>4292,6</b>	
<b>Antal observerade CCF-händelser</b>		<b>9</b>	<b>146</b>

Tabell 1. Observationsperiod.



## Samlad statistik om komponentgruppen

### Felmoder

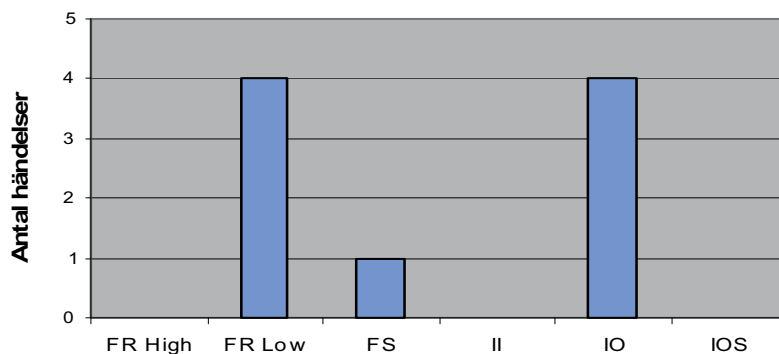
För komponentgruppen är följande felmoder relevanta i ett PSA perspektiv och därmed tillämpade vid datainsamling inom ICDE.

- FR High – Failure to indicate level during operation – failure to “High” signal
- FR Low – Failure to indicate level during operation – failure to “Low” signal
- FS – Failure to indicate changing level and failure to trigger limit switch on demand
- II – Instrument Inoperability
- IO – Unstable signal, spurious activation
- IOS – Instrument Out-of-Specification

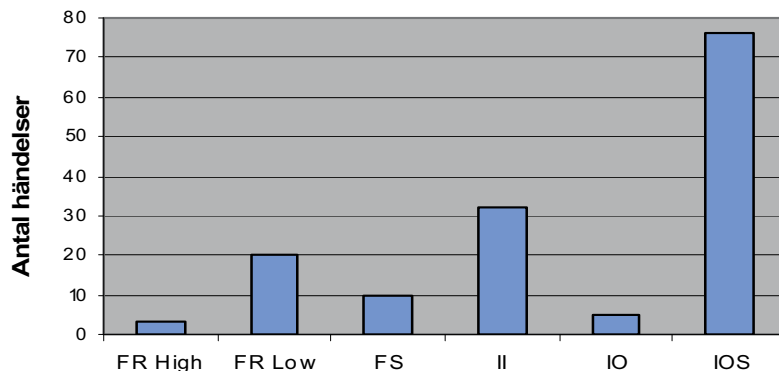
För nordiska data står felmoderna FR Low och IO för vardera ca 44%, medan FS står för ca 11%.

Ser man däremot till internationella data är den vanligaste felmoden IOS, som står för ca 52%.

Felmoder - nordiska data



Felmoder - internationella data

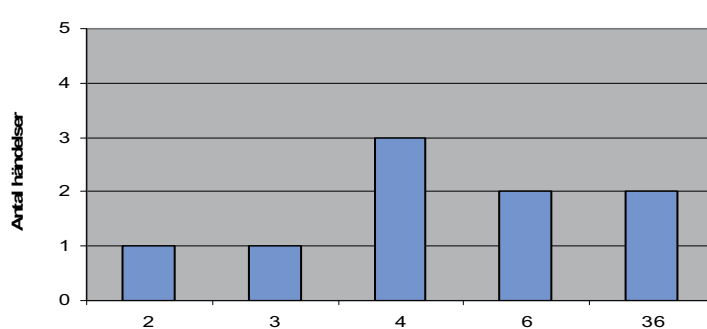


### Påverkade

#### komponentgruppstorlekar

Nordiska och internationella data är fördelade enligt kolumn till höger.

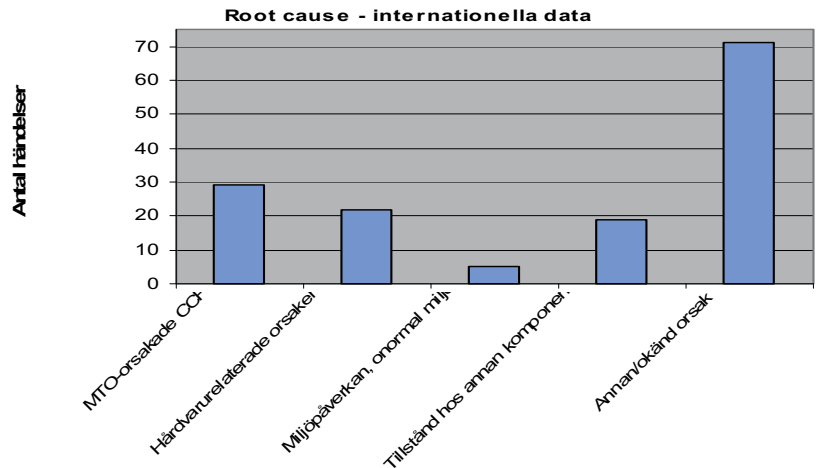
Storlek på exponerad population - nordiska data



	<p style="text-align: center;"><b>Storlek på exponerad population - internationella data</b></p> <table border="1"> <caption>Storlek på exponerad population - internationella data</caption> <thead> <tr> <th>Population Size</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>2</td><td>5</td></tr> <tr><td>3</td><td>13</td></tr> <tr><td>4</td><td>29</td></tr> <tr><td>6</td><td>7</td></tr> <tr><td>8</td><td>3</td></tr> <tr><td>12</td><td>21</td></tr> <tr><td>15</td><td>59</td></tr> <tr><td>20</td><td>1</td></tr> <tr><td>36</td><td>2</td></tr> </tbody> </table>	Population Size	Antal händelser	2	5	3	13	4	29	6	7	8	3	12	21	15	59	20	1	36	2																																		
Population Size	Antal händelser																																																						
2	5																																																						
3	13																																																						
4	29																																																						
6	7																																																						
8	3																																																						
12	21																																																						
15	59																																																						
20	1																																																						
36	2																																																						
<p><b>Ackumulerade kalenderår per komponentgruppsstorlek (KG)</b></p>	<p style="text-align: center;"><b>Kalenderår per KG-storlek, nordiska data</b></p> <table border="1"> <caption>Kalenderår per KG-storlek, nordiska data</caption> <thead> <tr> <th>KG Size</th> <th>Antalet kalenderår</th> </tr> </thead> <tbody> <tr><td>2</td><td>140,00</td></tr> <tr><td>3</td><td>300,00</td></tr> <tr><td>4</td><td>490,00</td></tr> <tr><td>6</td><td>80,00</td></tr> <tr><td>8</td><td>70,00</td></tr> <tr><td>9</td><td>80,00</td></tr> <tr><td>12</td><td>50,00</td></tr> <tr><td>16</td><td>40,00</td></tr> <tr><td>18</td><td>40,00</td></tr> <tr><td>36</td><td>20,00</td></tr> </tbody> </table> <p style="text-align: center;"><b>Kalenderår per KG-storlek, internationella data</b></p> <table border="1"> <caption>Kalenderår per KG-storlek, internationella data</caption> <thead> <tr> <th>KG Size</th> <th>Antalet kalenderår</th> </tr> </thead> <tbody> <tr><td>2</td><td>300,00</td></tr> <tr><td>3</td><td>1300,00</td></tr> <tr><td>4</td><td>750,00</td></tr> <tr><td>6</td><td>250,00</td></tr> <tr><td>8</td><td>200,00</td></tr> <tr><td>9</td><td>100,00</td></tr> <tr><td>10</td><td>20,00</td></tr> <tr><td>12</td><td>800,00</td></tr> <tr><td>15</td><td>300,00</td></tr> <tr><td>16</td><td>50,00</td></tr> <tr><td>18</td><td>50,00</td></tr> <tr><td>20</td><td>20,00</td></tr> <tr><td>24</td><td>20,00</td></tr> <tr><td>36</td><td>20,00</td></tr> <tr><td>64</td><td>10,00</td></tr> </tbody> </table>	KG Size	Antalet kalenderår	2	140,00	3	300,00	4	490,00	6	80,00	8	70,00	9	80,00	12	50,00	16	40,00	18	40,00	36	20,00	KG Size	Antalet kalenderår	2	300,00	3	1300,00	4	750,00	6	250,00	8	200,00	9	100,00	10	20,00	12	800,00	15	300,00	16	50,00	18	50,00	20	20,00	24	20,00	36	20,00	64	10,00
KG Size	Antalet kalenderår																																																						
2	140,00																																																						
3	300,00																																																						
4	490,00																																																						
6	80,00																																																						
8	70,00																																																						
9	80,00																																																						
12	50,00																																																						
16	40,00																																																						
18	40,00																																																						
36	20,00																																																						
KG Size	Antalet kalenderår																																																						
2	300,00																																																						
3	1300,00																																																						
4	750,00																																																						
6	250,00																																																						
8	200,00																																																						
9	100,00																																																						
10	20,00																																																						
12	800,00																																																						
15	300,00																																																						
16	50,00																																																						
18	50,00																																																						
20	20,00																																																						
24	20,00																																																						
36	20,00																																																						
64	10,00																																																						
<p><b>Troliga felorsaker</b> För nordiska data har den största andelen av händelserna hårdvarurelaterade orsaker.</p> <p>För internationella data är MTO-relaterade orsaker vanligare än hårdvarurelaterade, men de allra vanligaste orsakerna är kategoriserade som annan/andra, dvs ej inom ramarna för någon av de specificerade kategorierna. De definierade kategorierna är:</p> <ul style="list-style-type: none"> <li>• MTO-relaterade orsaker <ul style="list-style-type: none"> <li>- Operatörsåtgärder, anläggningspersonal</li> <li>- Underhåll</li> <li>- Brist i instruktioner</li> </ul> </li> </ul>	<p style="text-align: center;"><b>Root cause - nordiska data</b></p> <table border="1"> <caption>Root cause - nordiska data</caption> <thead> <tr> <th>Root Cause Category</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>MTO-orsakade COF</td><td>3</td></tr> <tr><td>Hårdvarurelaterade orsaker</td><td>5</td></tr> <tr><td>Miljöpåverkan, onormal milj.</td><td>5</td></tr> <tr><td>Tillstånd hos annan komponent</td><td>0</td></tr> <tr><td>Annan/okänd orsak</td><td>1</td></tr> </tbody> </table>	Root Cause Category	Antal händelser	MTO-orsakade COF	3	Hårdvarurelaterade orsaker	5	Miljöpåverkan, onormal milj.	5	Tillstånd hos annan komponent	0	Annan/okänd orsak	1																																										
Root Cause Category	Antal händelser																																																						
MTO-orsakade COF	3																																																						
Hårdvarurelaterade orsaker	5																																																						
Miljöpåverkan, onormal milj.	5																																																						
Tillstånd hos annan komponent	0																																																						
Annan/okänd orsak	1																																																						

(tvetydiga, ofullständiga, felaktiga)

- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt



### Kopplingsfaktorer

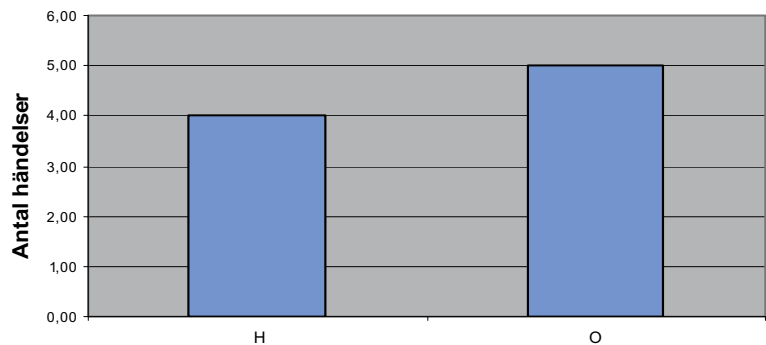
För nordisk data förekommer kopplingsfaktorer relaterade till hårdvara och drift, men inte sådana som är relaterade till miljö, enligt följande kategorisering:

- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedure
  - Underhållsschema
  - Driftinstruktion

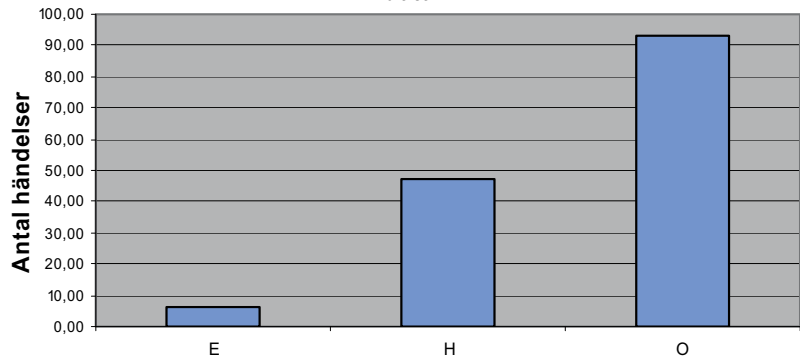
Även om det är ett mycket fåtal händelser det handlar om, visar det sig att internationella data pekar på samma trend enligt nedre figur i kolumnen till höger.

Vårt att notera är att av de händelser där bakomliggande orsak, root cause, är angiven som annan/okänd har ca 89% en kopplingsfaktor relaterad till underhållsschema (kategori O).

### Kopplingsmekanismer, grupperade - nordiska data



### Kopplingsmekanismer, grupperade - internationella data

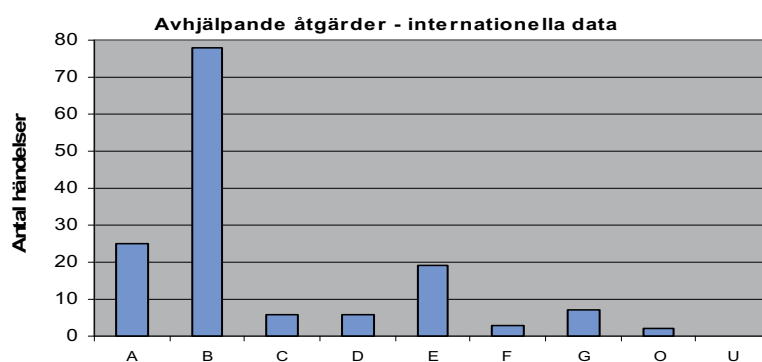
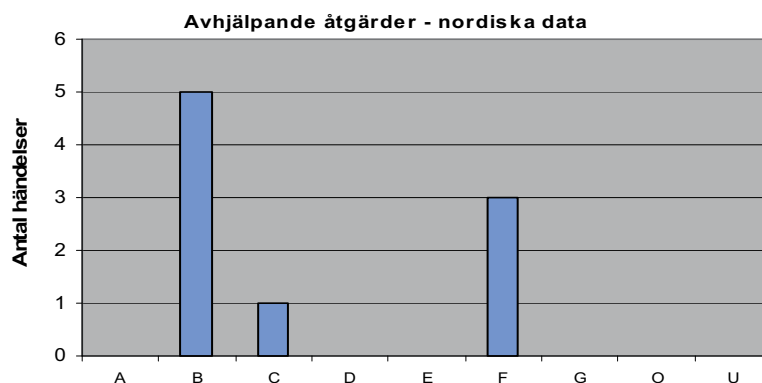


### Avhjälpan åtgärder

För nordiska data är den vanligaste insatta åtgärden kategori B, enligt avgränsningarna nedan.

- Administrative control or a procedure control (A)
- Specific maintenance or operational practice (B)
- Design modification (C)
- Diversity (D)
- Functional/spatial separation (E)
- Test and maintenance policies (F)
- Fixing of component (G)
- Other (O)
- Unknown (U)

Återigen handlar det om ett fåtal nordiska händelser, men liksom för identifierade kopplingsfaktorer ses samma trend, gällande vanligast tillämpade åtgärd, för nordiska och internationella data.



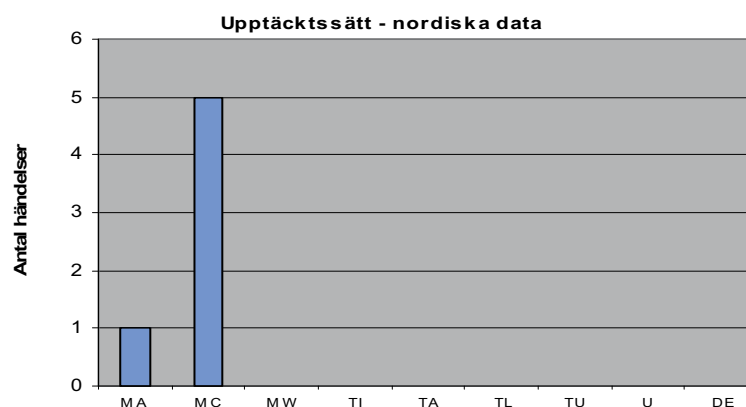
### Upptäcktsätt

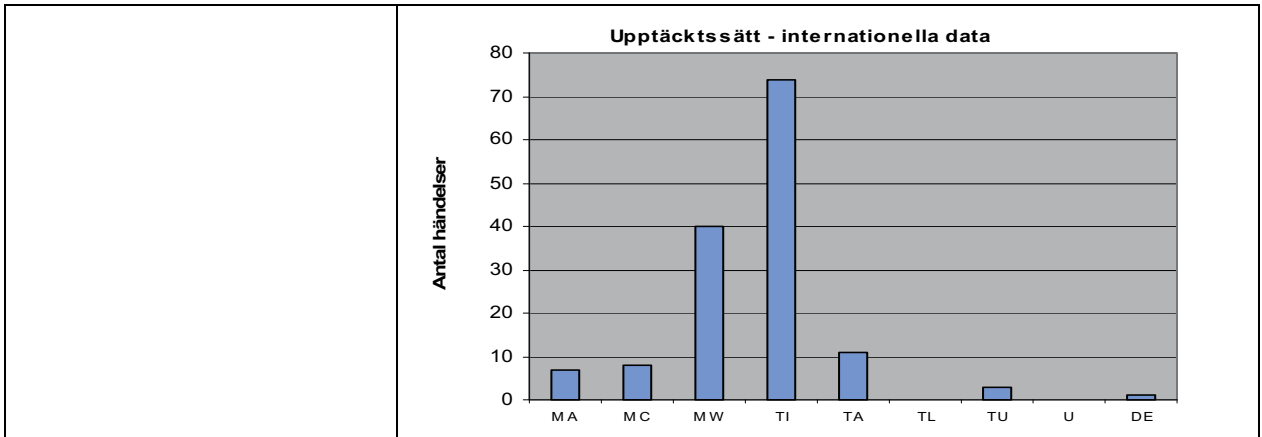
Upptäcktsätt delas in i följande kategorier:

- Monitoring on walkdown (MW)
- Monitoring in control room (MC)
- Maintenance/test (MA)
- Demand event (DE)
- Test during operation/annual overhaul/laboratory (TI/TA/TL)
- Unscheduled test (TU)
- Unknown (U)

Av de få nordiska händelser som finns i datainsamlingen har de flesta upptäckts genom "monitoring in control room". Det finns även ett par händelser där upptäcktsättet för de olika ingående felen varit olika.

För internationella data är den vanligaste upptäcktsformen "test during operation".





Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
System type: Reactor protection System sub type: Reactor pressure vessel (PWR, BWR) Component type: Pressure difference transmitter of membrane type with electric output signal	2	FS (Failure to indicate changing level and failure to trigger limit switch on demand)	H (Human actions, plant staff)	OMP (Maintenance/test Procedure)	MA (Maintenance / test)	CC	High
<p><b>Händelsebeskrivning:</b> The Oskarshamn 1 NPP was completely modernised in the years 2001-2002 (MOD-project). During the modernisation, the level switches were removed and replaced by a software system that handles the level indication. The following event took place during 1993, when limit switches still were used.</p> <p>LER (RO) 1993/006 Oskarshamn 1: 211K416 and K417 (level measurement instruments in the RPV) are supposed to trigger isolation of the auxiliary condenser (H8) in case of low level 4 (L4). This signal is given at level -1,75 meter (1,75 meters below the top of the core). 1993 the RPV was emptied because of a major renewal (FENIX project) and it was then discovered that the level L4 wasn't triggered for 211K416 and 211K417 until -2,3 meter. The reason was miscalibration due to a erroneous calculation of the theoretical calibration signal affecting both limit switches. This error has been present since 1989, when the calculation was made. Both 211K416 and K417 was affected in the same way.</p>							

Tabell 3. Exempel på inträffad ICDE-händelse.

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad , trolig felorsak	Kopplings- faktor	Upptäckts- sätt	Komponent- degradering, vektor	Tidsfaktor/ faktor för gemensam orsak
System type: Pressure control (includes primary safety relief valves) System sub type: Pressurizer (PWR, PHWR) Component type: Pressure difference transmitter of membrane type with electric output signal	3	FR Low (Failure to indicate level during operation – failure to “Low” signal)	P (Procedure inadequacy)	OMP (Maintenance/ test Procedure)	TA (Test during annual overhaul)	DDD	High
<b>Händelsebeskrivning:</b> On June 05, 1992, a unit was at refueling shutdown. During the preventive maintenance task (comparison between the pressurizer's level measurements), an erroneous calibration was detected in the three hot-calibrated level transmitters. The latent time is related to the time when these transmitters were modified in 1991. The cause of the failure was an erroneous data of the qualification procedure that had led to change the transmitter calibration. At nominal power, the actual level in the pressurizer was estimated to be 60cm above the measured level. The subsequent analysis of the potential consequences of this event revealed relevant safety consequences.							

Tabell 4. Exempel på inträffad ICDE-händelse.

## Vidare läsning

- ICDE General Coding Guidelines [16].

## Bilaga 5: Vägledning – erfarenheter från insamling av CCF-händelser på batterier (BA)

### Komponentgruppen batterier

Komponentgruppen utgörs av de batterier som tillhandahåller hjälpkraft (likspänning) till anläggningens säkerhetssystem vid händelse av bortfall av yttre nät. Spänningen som ska tillhandahållas är vanligen mellan 24 och 500 V likspänning.

Batterigruppen delas in i fyra undergrupper:

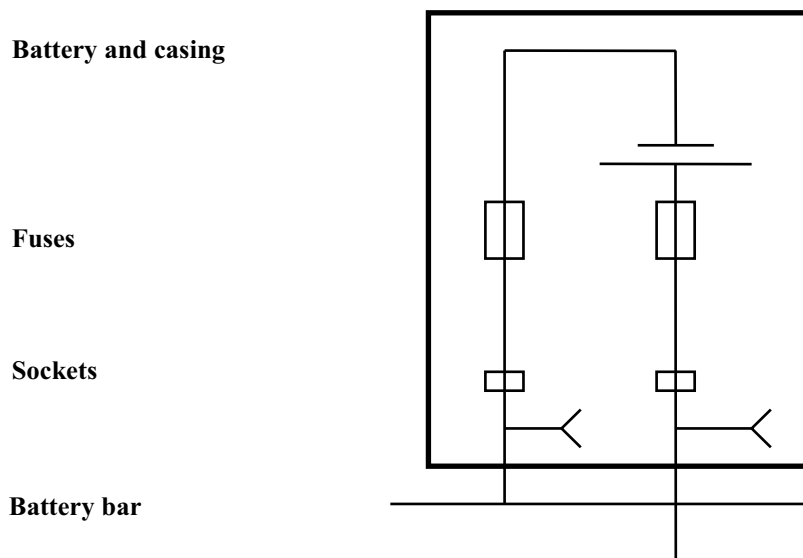
BVL – Mycket låg spänning ( $V=24$ )

BL – Låg spänning ( $24 < V < 50$ )

BM – Medium spänning ( $50 < V < 200$ )

BH – Hög spänning ( $V > 200$ )

Den fysiska omfattningen av komponenten utgörs av cell, hölje och deras respektive brytare och utmatningssäkringar. Komponentgränsen illustreras nedan.



Figur 2. Batterikomponenter och gräns.

Uppgiften för ett batteri är att vid behov tillhandahålla hjälpspänning till säkerhetssystemen. Batteriet anses fela då det misslyckas uppfylla sin uppgift vid ett påkallat behov. Fel hos en och samma cell, som tillhandahåller olika spänningsnivåer kan anses vara en giltig CCF.



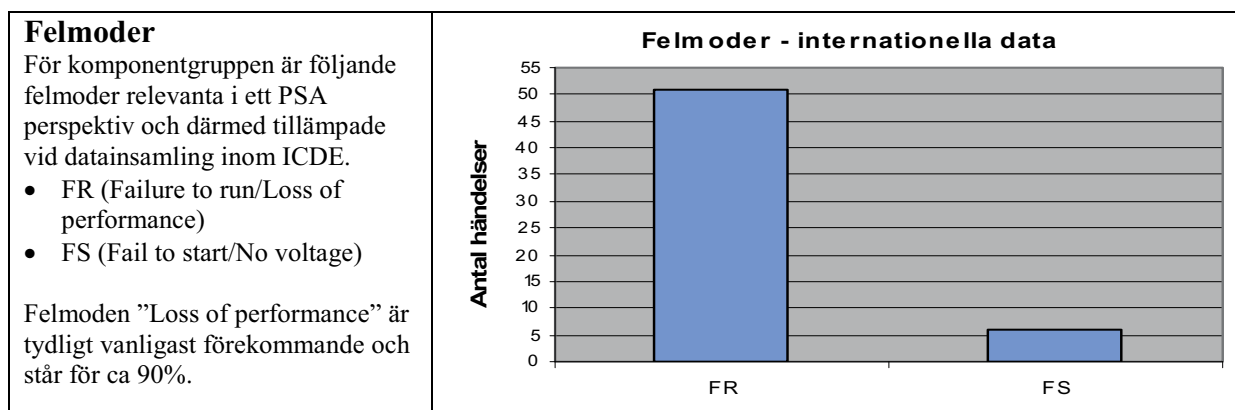
Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

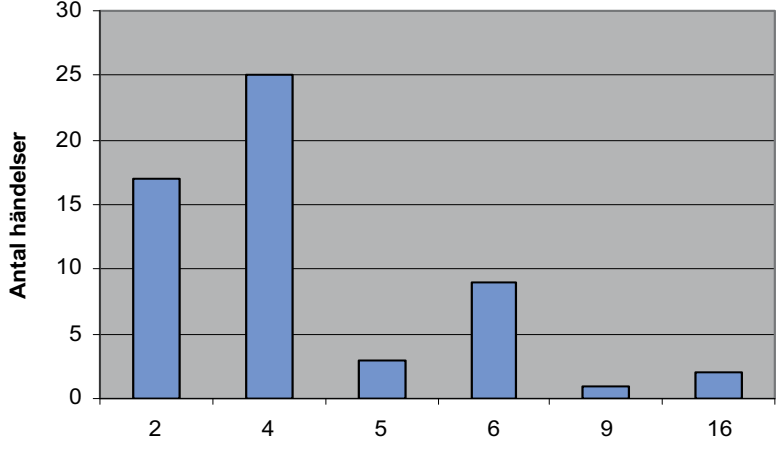
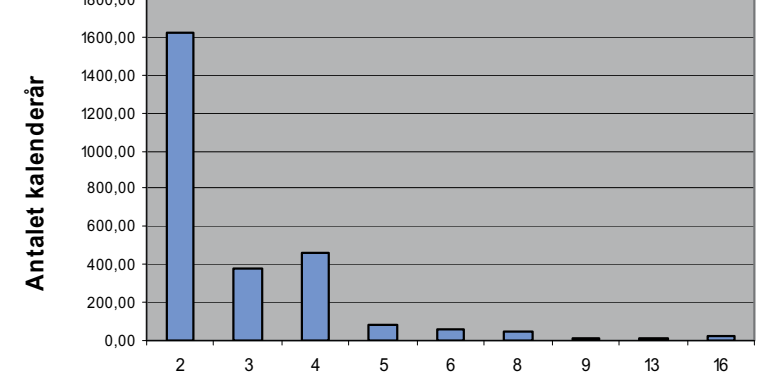
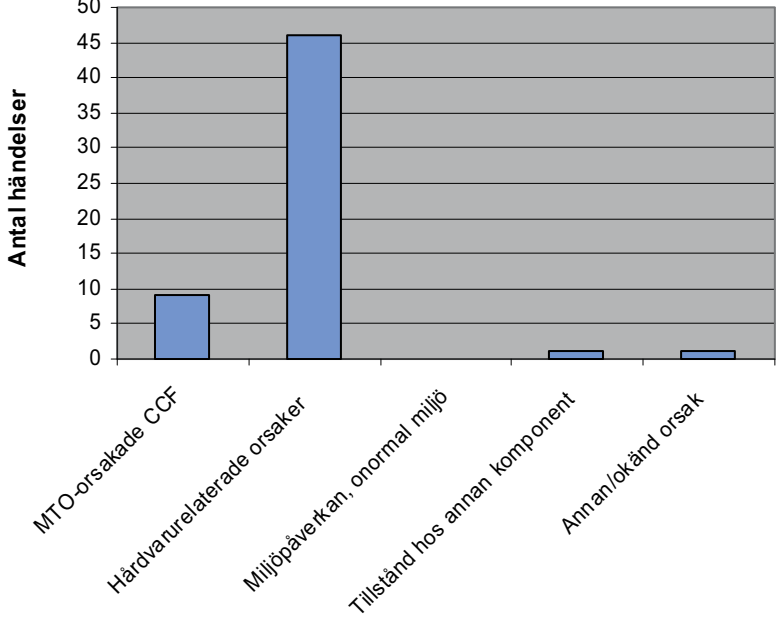
<b>Observerat antal kalenderår</b>	<b>CCCG storlek</b>	<b>Nordiska data</b>	<b>Internationella data (inkl. nordiska)</b>
Observationsperioden för nordiska data är 1982-01-01 – 2002-12-31	2	154,07	1625,04
	3	256,12	379,75
Observationsperioden för internationella data är 1980-08-01 – 2006-12-31	4		464,90
	5		80,10
	6		61,69
	8	51,02	51,02
	9		6,08
	13		8,00
	16		18,01
<b>Totalt</b>		461,21	2694,59
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		1	57

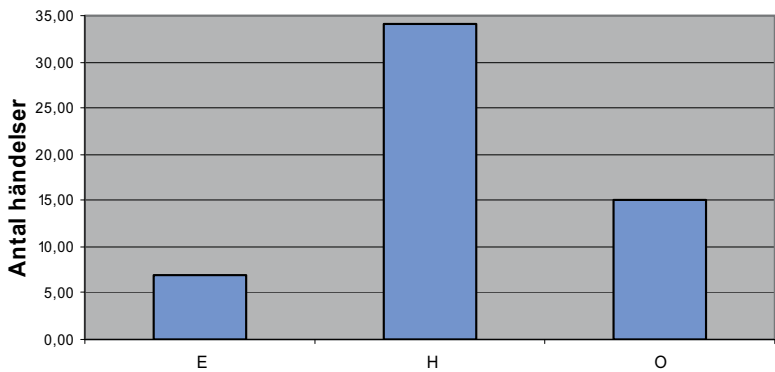
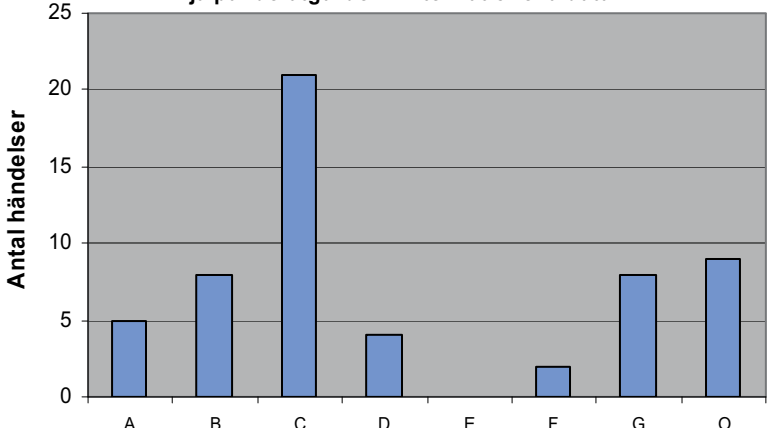
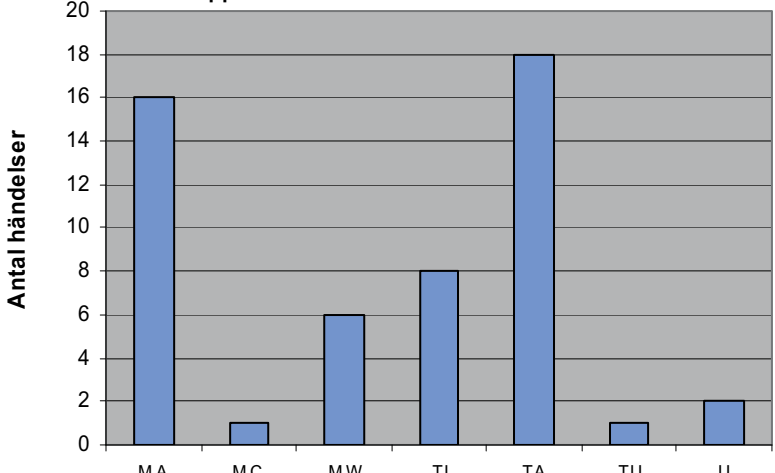
Tabell 1. Observationsperiod.

### Samlad statistik om komponentgruppen

För denna komponentgrupp är det inte särskilt givande att titta separat på de nordiska händelserna, då det endast finns en observerad CCF-händelse i datainsamlingen. För statistik över komponentgruppen redovisas istället internationella data, se nedan.



<p><b>Påverkade komponent gruppstorlekar</b></p>	<p><b>Storlek på exponerad population - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Storlek</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>2</td><td>17</td></tr> <tr><td>4</td><td>25</td></tr> <tr><td>5</td><td>3</td></tr> <tr><td>6</td><td>9</td></tr> <tr><td>9</td><td>1</td></tr> <tr><td>16</td><td>2</td></tr> </tbody> </table>	Storlek	Antal händelser	2	17	4	25	5	3	6	9	9	1	16	2						
Storlek	Antal händelser																				
2	17																				
4	25																				
5	3																				
6	9																				
9	1																				
16	2																				
<p><b>Ackumulerade kalenderår per komponentgruppsstorlek</b></p>	<p><b>Kalenderår per KG-storlek - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Storlek</th> <th>Antalet kalenderår</th> </tr> </thead> <tbody> <tr><td>2</td><td>1600,00</td></tr> <tr><td>3</td><td>380,00</td></tr> <tr><td>4</td><td>450,00</td></tr> <tr><td>5</td><td>100,00</td></tr> <tr><td>6</td><td>80,00</td></tr> <tr><td>8</td><td>70,00</td></tr> <tr><td>9</td><td>20,00</td></tr> <tr><td>13</td><td>10,00</td></tr> <tr><td>16</td><td>10,00</td></tr> </tbody> </table>	Storlek	Antalet kalenderår	2	1600,00	3	380,00	4	450,00	5	100,00	6	80,00	8	70,00	9	20,00	13	10,00	16	10,00
Storlek	Antalet kalenderår																				
2	1600,00																				
3	380,00																				
4	450,00																				
5	100,00																				
6	80,00																				
8	70,00																				
9	20,00																				
13	10,00																				
16	10,00																				
<p><b>Troliga felorsaker</b> De vanligaste identifierade bakomliggande orsakerna för inträffade CCF-händelser hos komponentgruppen batterier är relaterade till hårdvara. Se även kategoriseringen nedan.</p> <ul style="list-style-type: none"> <li>• MTO-relaterade orsaker <ul style="list-style-type: none"> <li>- Operatörsåtgärder, anläggningspersonal</li> <li>- Underhåll</li> <li>- Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)</li> </ul> </li> <li>• Hårdvarurelaterade orsaker <ul style="list-style-type: none"> <li>- Brist i design konstruktion eller tillverkning</li> <li>- Internt (inom komponent)</li> </ul> </li> <li>• Miljöpåverkan, onormal miljö</li> <li>• Tillstånd hos annan komponent</li> <li>• Annat/okänt</li> </ul>	<p><b>Root cause - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Orsak</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>MTO-orsakade CCF</td><td>9</td></tr> <tr><td>Hårdvarurelaterade orsaker</td><td>46</td></tr> <tr><td>Miljöpåverkan, onormal miljö</td><td>1</td></tr> <tr><td>Tillstånd hos annan komponent</td><td>1</td></tr> <tr><td>Annan/okänd orsak</td><td>1</td></tr> </tbody> </table>	Orsak	Antal händelser	MTO-orsakade CCF	9	Hårdvarurelaterade orsaker	46	Miljöpåverkan, onormal miljö	1	Tillstånd hos annan komponent	1	Annan/okänd orsak	1								
Orsak	Antal händelser																				
MTO-orsakade CCF	9																				
Hårdvarurelaterade orsaker	46																				
Miljöpåverkan, onormal miljö	1																				
Tillstånd hos annan komponent	1																				
Annan/okänd orsak	1																				

<p><b>Kopplingsfaktorer</b>  Liksom för identifierade bakomliggande orsaker är även de vanligast förekommande kopplingsmekanismerna relaterade till hårdvara. Se även kategorisering nedan.</p> <ul style="list-style-type: none"> <li>• Miljö (E) <ul style="list-style-type: none"> <li>- Extern miljö</li> <li>- Intern miljö</li> </ul> </li> <li>• Hårdvara (H) <ul style="list-style-type: none"> <li>- Hårdvarudesign</li> <li>- Hårdvarukvalitet</li> <li>- Systemdesign</li> </ul> </li> <li>• Drift (O) <ul style="list-style-type: none"> <li>- Driftpersonal</li> <li>- Underhållspersonal</li> <li>- Underhållsprocedure</li> <li>- Underhållsschema</li> <li>- Driftinstruktion</li> </ul> </li> </ul>	<p style="text-align: center;"><b>Kopplingsmekanismer, i grupp - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Kategori</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr> <td>E</td> <td>7</td> </tr> <tr> <td>H</td> <td>34</td> </tr> <tr> <td>O</td> <td>15</td> </tr> </tbody> </table>	Kategori	Antal händelser	E	7	H	34	O	15										
Kategori	Antal händelser																		
E	7																		
H	34																		
O	15																		
<p><b>Avhjälpande åtgärder</b>  De mest frekventa avhjälpande åtgärden är sådana som är relaterade modifiering av design, enligt kategorisering nedan:</p> <ul style="list-style-type: none"> <li>• Administrative control or a procedure control (A)</li> <li>• Specific maintenance or operational practice (B)</li> <li>• Design modification (C)</li> <li>• Diversity (D)</li> <li>• Functional/spatial separation (E)</li> <li>• Test and maintenance policies (F)</li> <li>• Fixing of component (G)</li> <li>• Other (O)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Avhjälpande åtgärder - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Kategori</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>5</td> </tr> <tr> <td>B</td> <td>8</td> </tr> <tr> <td>C</td> <td>21</td> </tr> <tr> <td>D</td> <td>4</td> </tr> <tr> <td>E</td> <td>0</td> </tr> <tr> <td>F</td> <td>2</td> </tr> <tr> <td>G</td> <td>8</td> </tr> <tr> <td>O</td> <td>9</td> </tr> </tbody> </table>	Kategori	Antal händelser	A	5	B	8	C	21	D	4	E	0	F	2	G	8	O	9
Kategori	Antal händelser																		
A	5																		
B	8																		
C	21																		
D	4																		
E	0																		
F	2																		
G	8																		
O	9																		
<p><b>Upptäcktsätt</b>  De vanligaste sätten för upptäckt av händelse är ”test during annual overhaul” och ”maintenance/test”. Se även kategorisering nedan. Dessa två kategorier står tillsammans för ca 60% av händelserna.</p> <ul style="list-style-type: none"> <li>• Monitoring on walkdown (MW)</li> <li>• Monitoring in control room (MC)</li> <li>• Maintenance/test (MA)</li> <li>• Demand event (DE)</li> <li>• Test during operation/annual overhaul/laboratory (TI/TA/TL)</li> <li>• Unscheduled test (TU)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Upptäcktsätt - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Kategori</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr> <td>MA</td> <td>16</td> </tr> <tr> <td>MC</td> <td>1</td> </tr> <tr> <td>MW</td> <td>6</td> </tr> <tr> <td>TI</td> <td>8</td> </tr> <tr> <td>TA</td> <td>18</td> </tr> <tr> <td>TU</td> <td>1</td> </tr> <tr> <td>U</td> <td>2</td> </tr> </tbody> </table>	Kategori	Antal händelser	MA	16	MC	1	MW	6	TI	8	TA	18	TU	1	U	2		
Kategori	Antal händelser																		
MA	16																		
MC	1																		
MW	6																		
TI	8																		
TA	18																		
TU	1																		
U	2																		

Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
High voltage battery (V>200) DC System. Uninterrupted power supply for emergency DC system and secondary emergency DC system.	6	FR (Loss of performance, Failure to run)	Design, manufacture or construction inadequacy	Hardware Design	TA (Test during annual overhaul)	CCIII	High / High
<p><b>Händelsebeskrivning:</b></p> <p>Unit 1 of plant X was at refuelling outage. During the 220 V (NIFE cells) Ni-Cd batteries unloading annual test, it was found that the storage capacities of two batteries did not match the requirements. In fact, the minimum voltage was reached before the 60 minutes required: The root cause of deterioration of the Ni-Cd batteries performance is related to a design problem. According to the studies carried out by Y, the defective behavior of the NIFE batteries was due to the carbonation of a particular form of graphite contained in the active material of their positive plate. In the electrolyte, the resulting depletion in charge carriers affects the voltage under discharge conditions, this impact increasing with the inrush current. This peculiar behavior is unacceptable for stationary applications.</p> <p>The event is interpreted as a CCF of two batteries because they were affected by the same design fault so that it is a generic problem. The four others batteries were potentially failed.</p>							

Tabell 3. Exempel på inträffad ICDE-händelse.

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Medium Voltage (50<V<200) DC System. Uninterrupted power supply for emergency DC system and secondary emergency DC system.	2	FS (No voltage/open circuit, Failure to start)	Procedure inadequacy	Operational (maintenance/test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	MC (Monitoring in control room)	CC	High / High

**Händelsebeskrivning:**

On February 1, 1994, Unit 1 was in Mode 5 at 0% power and Unit 2 was defueled while in a refueling outage. It was determined that the Unit 1 and Unit 2 Control Room Make-up and Fuel Handling Building Exhaust dampers were inoperable due to depleted lithium battery back-up power supplies. The cause of this event was the failure to understand that failure of the batteries affected should be covered in the Technical Specification Surveillance Program. A contributing cause was the failure to identify that the method of monitoring battery condition specified in the IEEE Qualification Test Report and subsequently, the vendor manual was not implemented in the as-built configuration of the plant. Immediate corrective actions were taken to replace the batteries and restore the Fuel Handling Building and Control Room Heating, Ventilating and Air Conditioning systems to operability. The Equipment Clearance Order database was modified to address the removal of the battery fuses as part of the Equipment Clearance Order process to prevent the cycling of the hydraulic system and subsequent depletion of the batteries. Additional corrective actions are addressed within the LER.

Licensee failure to understand how batteries affect dampers and failure to incorporate effects into procedures and TS caused the failures.

*Tabell 4. Exempel på inträffad ICDE-händelse.*

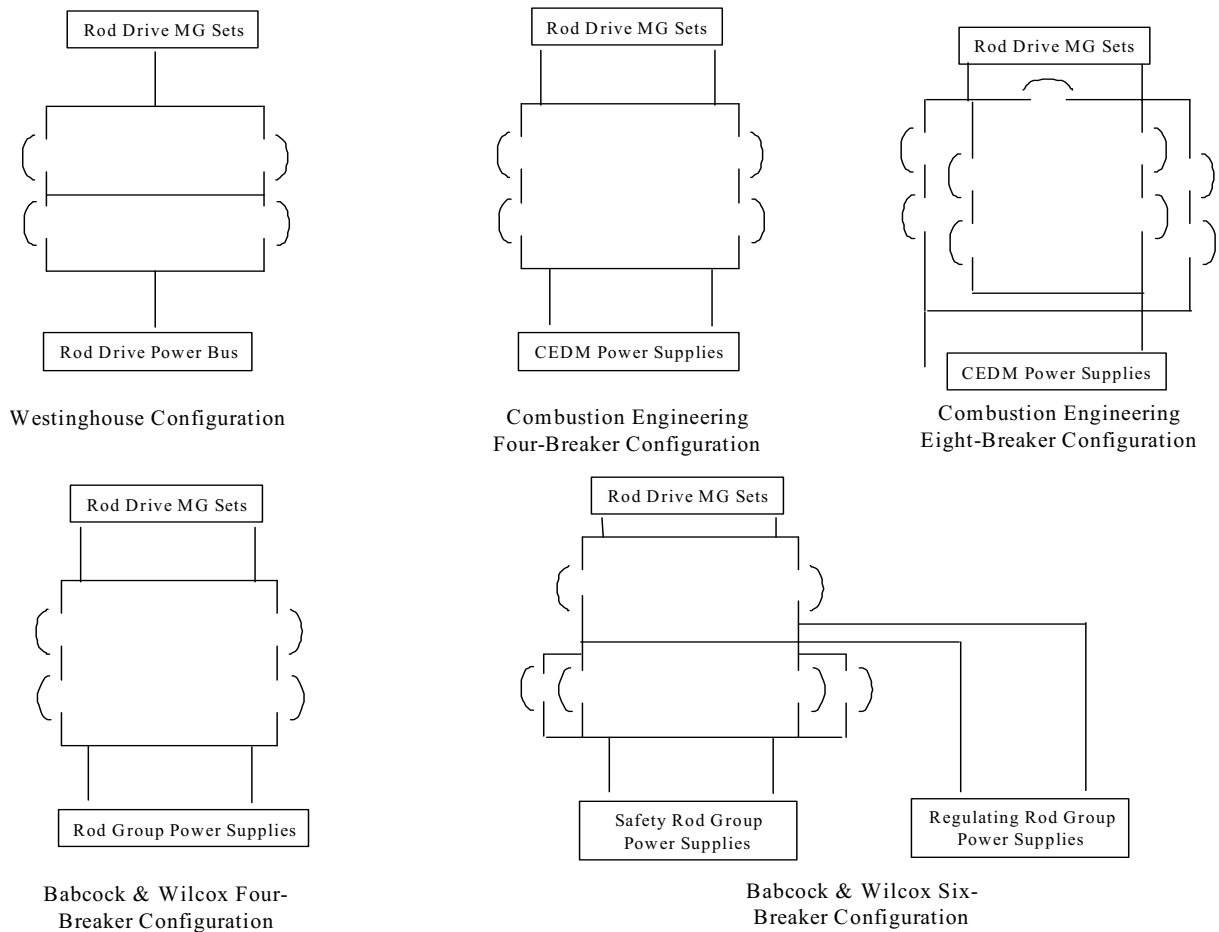
**Vidare läsning**

- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [8].
- Sammanfattande rapport från ICDE [17].

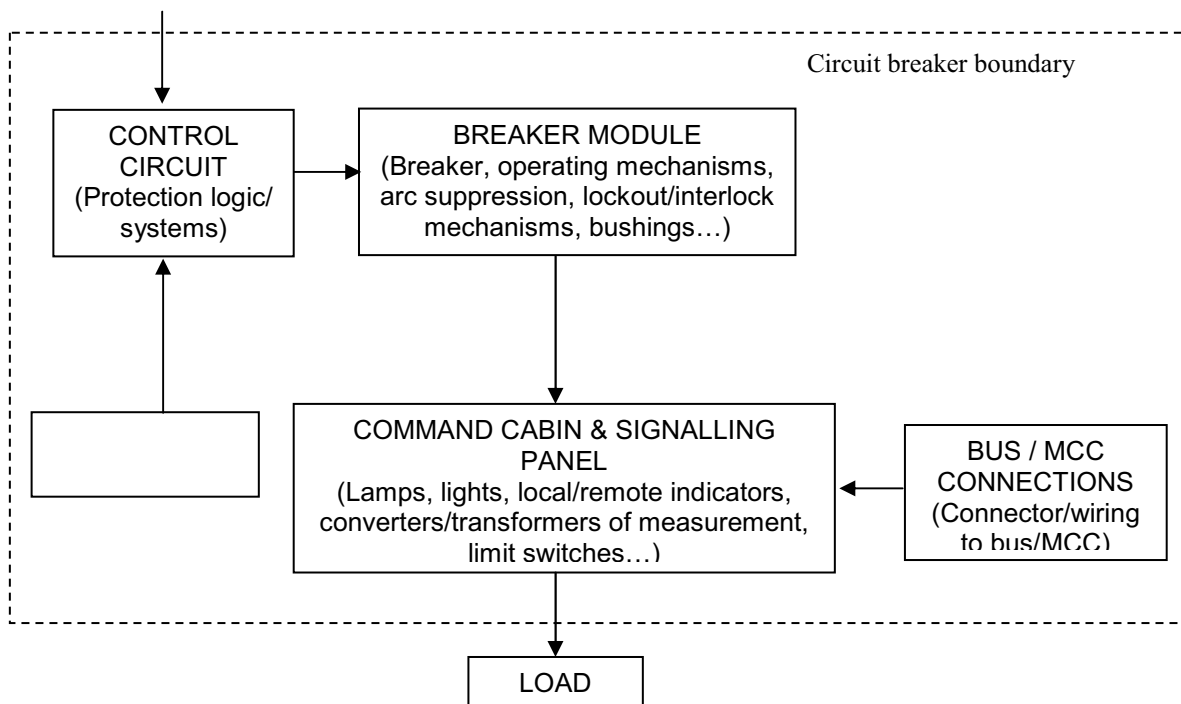
## Bilaga 6: Vägledning – erfarenheter från insamling av CCF-händelser på brytare (BR)

### Komponentgruppen brytare

De brytare som är av störst intresse är sådana som ingår i kraftdistributionssystem och reaktorutlösningssystem (Reactor Trip breakers). Nedan ges exempel på olika typer av utformning och komponentens fysiska gränser.



Figur 1. Exempel på utformning.



Figur 2. Komponentgräns, brytare.

Komponenternas uppgift är att upprätthålla, sluta eller bryta ström i en elektrisk krets efter behov och anses därmed fela när denna uppgift inte kan utföras.

Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

Observerat antal kalenderår	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för såväl nordiska som internationella data är 1983-01-01 – 2004-12-31	2	274,75	1137,09
	3	21,01	34,01
	4	790,83	1989,71
	5		46,01
	6	31,69	200,05
	7		25,99
	8		618,91
	9		84,32
	10		29,01
	11		88,04
	12	47,54	110,56
	13	15,85	15,85
	14		70,02
	15		69,02
	16		3944,78
	17		58,02
	18		29,01
	19		61,02
	20		103,03

	21		16,01
	23		241,02
	24		69,02
	26		16,01
	28		16,01
	29		16,01
	30		32,01
	31		22,01
	32		30,01
	33		16,01
	34		32,01
	35		32,01
	36		48,02
	38		32,01
	40		8,00
	42		16,01
	48		48,02
	51		16,01
	53		16,01
	55		24,01
	56		16,01
	64		25,01
	74		32,01
	78		16,01
	79		16,01
	87		16,01
	99		32,01
	373		196,00
	537		168,00
Totalt		1181,67	9977,71
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		3	107

Tabell 1. Observationsperiod.

### Samlad CCF statistik om BR komponentgruppen

För komponentgruppen finns endast tre händelser i datasamlingen för de nordiska anläggningarna. På grund av detta kommer presenterad statistiken för brytare istället att breddas till att beakta internationella (inklusive nordiska) data.



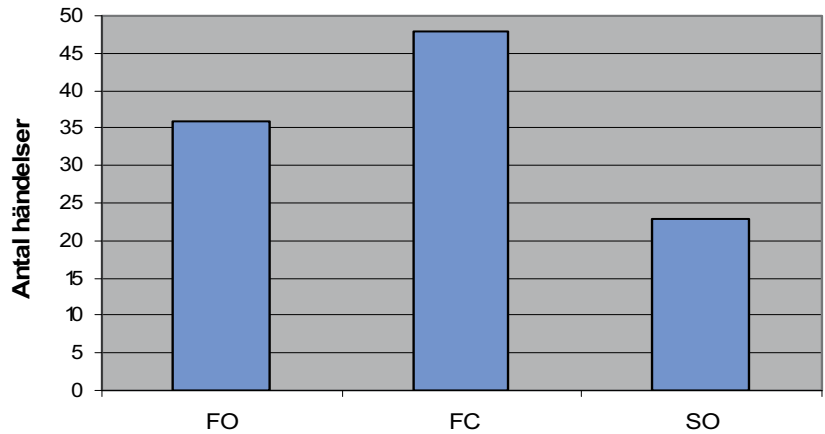
### Felmoder

För komponentgruppen är följande felmoder relevanta i ett PSA perspektiv och därmed tillämpade vid datainsamling inom ICDE.

- FO (Failure to open)
- FC (Fail to close)
- SO (Spurious Operation)

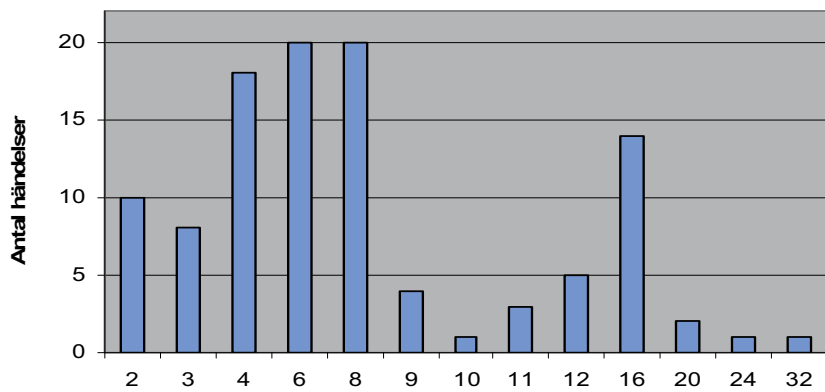
Felmoden FC är vanligast förekommande och står för ca 45%.

Felmoder - internationella data



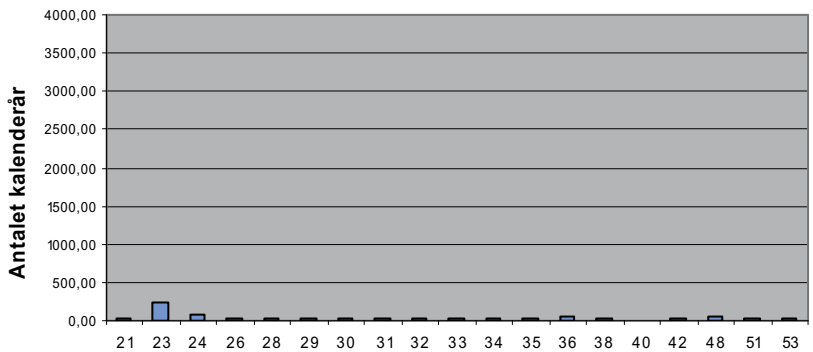
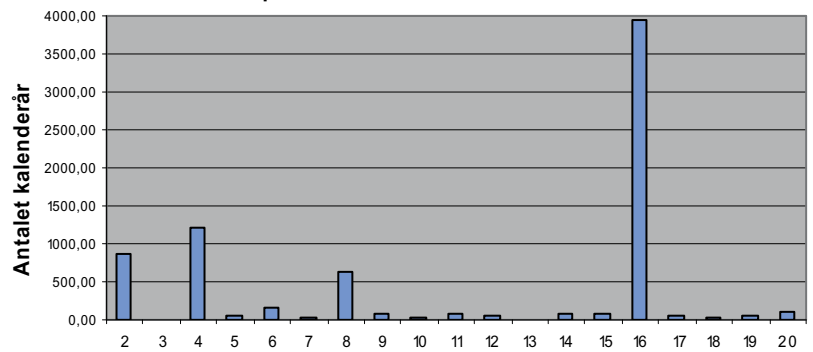
### Påverkade komponent gruppstorlekar

Storlek på exponerad population - internationella data

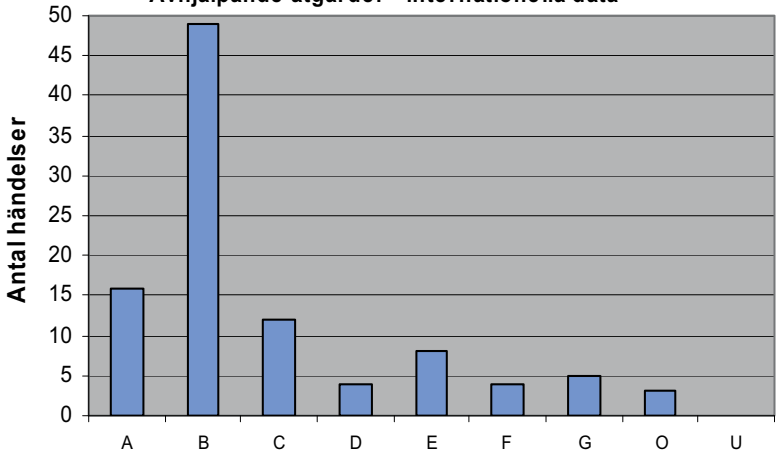
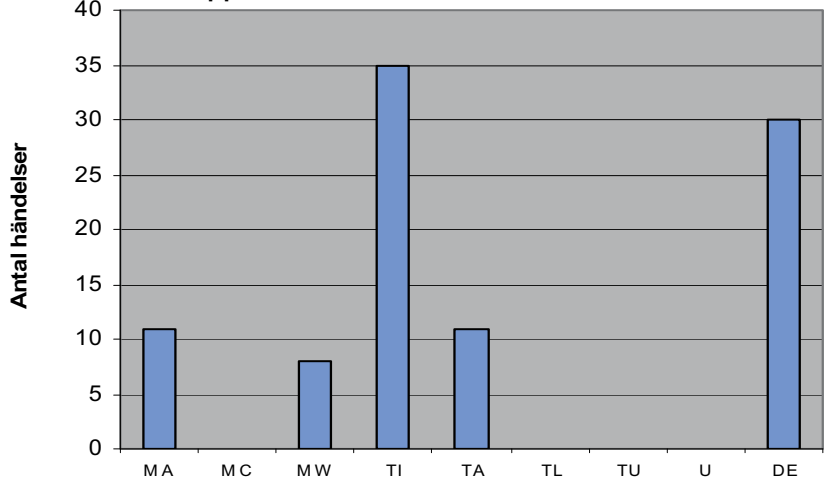


### Ackumulerade kalenderår per komponentgruppsstorlek

Kalenderår per KG-storlek - internationella data



	<table border="1"> <caption>Antalet kalenderår</caption> <thead> <tr> <th>Kategori</th> <th>Antal kalenderår</th> </tr> </thead> <tbody> <tr><td>55</td><td>~100</td></tr> <tr><td>56</td><td>~100</td></tr> <tr><td>64</td><td>~100</td></tr> <tr><td>74</td><td>~100</td></tr> <tr><td>78</td><td>~100</td></tr> <tr><td>79</td><td>~100</td></tr> <tr><td>87</td><td>~100</td></tr> <tr><td>99</td><td>~100</td></tr> <tr><td>373</td><td>~250</td></tr> <tr><td>537</td><td>~200</td></tr> </tbody> </table>	Kategori	Antal kalenderår	55	~100	56	~100	64	~100	74	~100	78	~100	79	~100	87	~100	99	~100	373	~250	537	~200
Kategori	Antal kalenderår																						
55	~100																						
56	~100																						
64	~100																						
74	~100																						
78	~100																						
79	~100																						
87	~100																						
99	~100																						
373	~250																						
537	~200																						
<p><b>Troliga felorsaker</b> De vanligaste identifierade bakomliggande orsakerna för inträffade CCF-händelser hos komponentgruppen brytare är relaterade till hårdvara. Se även kategoriseringen nedan.</p> <ul style="list-style-type: none"> <li>• MTO-relaterade orsaker <ul style="list-style-type: none"> <li>- Operatörsåtgärder, anläggningspersonal</li> <li>- Underhåll</li> <li>- Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)</li> </ul> </li> <li>• Hårdvarurelaterade orsaker <ul style="list-style-type: none"> <li>- Brist i design konstruktion eller tillverkning</li> <li>- Internt (inom komponent)</li> </ul> </li> <li>• Miljöpåverkan, onormal miljö</li> <li>• Tillstånd hos annan komponent</li> <li>• Annat/okänt</li> </ul>	<p><b>Root cause - internationella data</b></p> <table border="1"> <caption>Root cause - internationella data</caption> <thead> <tr> <th>Orsak</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>MTO-orsakade CCF</td><td>~25</td></tr> <tr><td>Hårdvarurelaterade orsaker</td><td>~75</td></tr> <tr><td>Miljöpåverkan, onormal miljö</td><td>~0</td></tr> <tr><td>Tillstånd hos annan komponent</td><td>~2</td></tr> <tr><td>Annan/okänd orsak</td><td>~5</td></tr> </tbody> </table>	Orsak	Antal händelser	MTO-orsakade CCF	~25	Hårdvarurelaterade orsaker	~75	Miljöpåverkan, onormal miljö	~0	Tillstånd hos annan komponent	~2	Annan/okänd orsak	~5										
Orsak	Antal händelser																						
MTO-orsakade CCF	~25																						
Hårdvarurelaterade orsaker	~75																						
Miljöpåverkan, onormal miljö	~0																						
Tillstånd hos annan komponent	~2																						
Annan/okänd orsak	~5																						
<p><b>Kopplingsfaktorer</b> Liksom för identifierade bakomliggande orsaker är även de vanligast förekommande kopplingsmekanismerna relaterade till hårdvara, men nästan lika många av händelserna har kopplingsmekanism relaterad till drift. Se även kategorisering nedan.</p> <ul style="list-style-type: none"> <li>• Miljö (E) <ul style="list-style-type: none"> <li>- Extern miljö</li> <li>- Intern miljö</li> </ul> </li> <li>• Hårdvara (H) <ul style="list-style-type: none"> <li>- Hårdvarudesign</li> <li>- Hårdvarukvalitet</li> <li>- Systemdesign</li> </ul> </li> </ul>	<p><b>Kopplingsmekanismer, i grupp - internationella data</b></p> <table border="1"> <caption>Kopplingsmekanismer, i grupp - internationella data</caption> <thead> <tr> <th>Mekanism</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>E</td><td>~0</td></tr> <tr><td>H</td><td>~55</td></tr> <tr><td>O</td><td>~50</td></tr> </tbody> </table>	Mekanism	Antal händelser	E	~0	H	~55	O	~50														
Mekanism	Antal händelser																						
E	~0																						
H	~55																						
O	~50																						

<ul style="list-style-type: none"> <li>• Drift (O) <ul style="list-style-type: none"> <li>- Driftpersonal</li> <li>- Underhållspersonal</li> <li>- Underhållsprocedur</li> <li>- Underhållsschema</li> <li>- Driftinstruktion</li> </ul> </li> </ul> <p>Vidare är undergruppen ”hårdvarudesign” den klart dominerande inom kategorin ”hårdvara”.</p>																					
<p><b>Avhjäljande åtgärder</b></p> <p>De, tydligt, mest frekventa avhjäljande åtgärden är sådana som är relaterade modifiering av design, enligt kategorisering nedan:</p> <ul style="list-style-type: none"> <li>• Administrative control or a procedure control (A)</li> <li>• Specific maintenance or operational practice (B)</li> <li>• Design modification (C )</li> <li>• Diversity (D)</li> <li>• Functional/spatial separation (E)</li> <li>• Test and maintenance policies (F)</li> <li>• Fixing of component (G)</li> <li>• Other (O)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Avhjäljande åtgärder - internationella data</b></p>  <table border="1" style="display: none;"> <caption>Avhjäljande åtgärder - internationella data</caption> <thead> <tr> <th>Kategori</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>A</td><td>15</td></tr> <tr><td>B</td><td>48</td></tr> <tr><td>C</td><td>12</td></tr> <tr><td>D</td><td>4</td></tr> <tr><td>E</td><td>8</td></tr> <tr><td>F</td><td>4</td></tr> <tr><td>G</td><td>5</td></tr> <tr><td>O</td><td>3</td></tr> <tr><td>U</td><td>0</td></tr> </tbody> </table>	Kategori	Antal händelser	A	15	B	48	C	12	D	4	E	8	F	4	G	5	O	3	U	0
Kategori	Antal händelser																				
A	15																				
B	48																				
C	12																				
D	4																				
E	8																				
F	4																				
G	5																				
O	3																				
U	0																				
<p><b>Upptäcktsätt</b></p> <p>De vanligaste sättet för upptäckt av händelse är ”test during operation”, tätt följt av kategorin ”demand event”. Se även kategorisering nedan. Dessa två kategorier står tillsammans för</p> <ul style="list-style-type: none"> <li>• Monitoring on walkdown (MW)</li> <li>• Monitoring in control room (MC)</li> <li>• Maintenance/test (MA)</li> <li>• Demand event (DE)</li> <li>• Test during operation/annual overhaul/laboratory (TI/TA/TL)</li> <li>• Unscheduled test (TU)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Upptäcktsätt - internationella data</b></p>  <table border="1" style="display: none;"> <caption>Upptäcktsätt - internationella data</caption> <thead> <tr> <th>Kategori</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>MA</td><td>11</td></tr> <tr><td>MC</td><td>0</td></tr> <tr><td>MW</td><td>8</td></tr> <tr><td>TI</td><td>35</td></tr> <tr><td>TA</td><td>11</td></tr> <tr><td>TL</td><td>0</td></tr> <tr><td>TU</td><td>0</td></tr> <tr><td>U</td><td>0</td></tr> <tr><td>DE</td><td>30</td></tr> </tbody> </table>	Kategori	Antal händelser	MA	11	MC	0	MW	8	TI	35	TA	11	TL	0	TU	0	U	0	DE	30
Kategori	Antal händelser																				
MA	11																				
MC	0																				
MW	8																				
TI	35																				
TA	11																				
TL	0																				
TU	0																				
U	0																				
DE	30																				

Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Breaker System type: Low voltage AC (less than 600V - mainly 480V) System sub type: AC Low voltage (up to 600 V)	3	FC (Failure to Close)	D (Design, manufacture or construct- ion inade- quacy)	HC (Hardware Design)	TI	CCD	High
<p><b>Händelsebeskrivning:</b> DC CIRCUIT BREAKER TRIPPED WITH INSUFFICIENT CAUSE</p> <p>10/27/93</p> <p>With Unit 2 shutdown for refueling, during the Loss of Offsite Power (LOSP) B-Train testing, the supply breaker for battery charger 2B (Auxiliary Building) tripped off when sequenced. The charging capability was rendered inoperable but there was no impact to plant operations as the swing charger 'C' could have been aligned manually. The failure was investigated and testing conducted. Current surges following AC breaker closure could sometimes exceed the breaker's instantaneous trip setting. A modification was then made to change the trip settings which required replacing the 150A current sensors with 200A size. This modification still provides proper overcurrent and short protection without adverse effects on system function. Failure is attributed to inadequate engineering design. The amptector current sensors were replaced with a new size of 200A rating. The breaker was retested and verified for proper operation. (This modification was made to the 2A, 2B, and 2C battery charger supply breakers)</p> <p>10/27/93</p> <p>With Unit 2 shutdown for refueling during the loss of site power (LOSP) testing, the supply breaker for battery charger 2A (Aux Bldg) failed to close when sequenced. The charging capability was rendered inoperable by the failure but there was no impact to plant operations as the swing charger 'C' could be aligned manually to this train. A root cause investigation and testing was conducted. Following AC breaker closure the inrush of current could sometimes exceed the breaker's instantaneous trip setting causing the breaker to trip. A modification was made to change the trip settings and the amptector was changed from 150A to 200A size. This modification still provides proper overcurrent and short protection without adverse affects on the system. (Modification was made to the 2A, 2B, and 2C battery charger breakers) Failure is attributed to engineering/design. The 150A amptector current sensor was replaced with a new one of 200A rating and trip settings changed. The breaker was tested for proper operation.</p> <p><b>Tolkning:</b> During the Loss of Offsite Power testing, two battery charger supply breakers would not close when sequenced. Current surges following AC breaker closure could sometimes exceed the breaker's instantaneous trip setting. A modification was then made to change the trip settings which required replacing the 150A current sensors with 200A size. This modification still provides proper overcurrent and short protection without adverse effects on system function. The failures were attributed to inadequate engineering design. The amptector current sensors were replaced. The breakers were retested and verified for proper operation. This modification was made to all three battery charger supply breakers.</p>							

Tabell 3. Exempel på inträffad händelse.

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Breaker System type: High voltage AC (greater than 15kV including off-site power) System sub type: AC Medium voltage (3 - 11 kV)	2	SO (Spurious Operation)	H (Human actions, plant staff)	HS (System Design)	-	CC	High

**Händelsebeskrivning:**

Power level 0%. On 10/21/93, at 1525 hours, the infeed breakers to 1A and 1C 4 Kilo-Volt (KV) buses tripped on an undervoltage (UV) signal, resulting in automatic starting and blackout signal loading of the buses from 1A and 1C Diesel Generators (D/Gs). At approximately 2030 hours (same day), infeed power to the buses from 12 Station Power Transformer (SPT) was restored and the D/Gs were secured and returned to standby. The root cause of this event is electrical shorting within the 4KV switchgear, due to personnel error associated with ongoing relay maintenance activities. The electrical shorting most probably occurred between adjacent terminals on the 12 SPT undervoltage (UV) relay circuit within the B vital bus 12BSD breaker cubicle. As a result of this event, work associated with SPTs and 4KV vital switchgear was reevaluated to ensure minimized plant safety risk. Increased coordination of activities and the importance of exercising caution in the vicinity of 4KV relays was emphasized with key supervisory personnel and workers. A vital bus and switchyard work standdown was imposed by the station General Manager, to allow review of remaining outage-related activities. Station outage management will review scheduling of similar activities to ensure incorporation of lessons learned into future outage schedules.

*Tabell 4. Exempel på inträffade händelse.*

**Vidare läsning**

- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [14].

## Bilaga 7: Vägledning – erfarenheter från insamling av CCF-händelser på säkerhets- och avblåsningsventiler (SRV)

### Komponentgruppen säkerhets- och avblåsningsventiler

Komponenten används för att förhindra övertryck av komponenter och ledningar. Komponentgränsen, inom ICDE, inkluderar lokal instrumentering, kontrollutrustning, kontakter och andra komponentdelar som är specifika för ventilen.

Komponentens uppgift är att öppna då trycket i ett visst system överskrider satt gränsvärde och stänga när trycket har sjunkit under en bestämd nivå. Felande av komponenten definieras som misslyckad operation av komponenten enligt ovan.

Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

Observerat antal kalenderår	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för nordiska data är 1977-05-08 – 2003-12-31	2	80,60	1209,97
	3	54,02	772,60
	4	31,66	668,33
	5		106,36
	6		70,72
	7	54,03	105,38
Observationsperioden för internationella data är 1977-05-08 – 2004-12-31	8		346,07
	9		11,00
	10	69,03	203,08
	11		99,02
	12	86,23	370,32
	13	13,01	25,01
	14	10,0	28,00
	15		75,00
	16	80,027397	551,58
	17		32,01
	18	27,008219	121,03
	19		12,00
	20	95,054795	354,95
	21		54,99
	24		32,01
28		31,51	
30	10	10,00	
104		15,00	
112		28,01	
<b>Totalt</b>		600,66	5333,94
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		38	214

Tabell 1. Observationsperiod.

## Samlad statistik om komponentgruppen

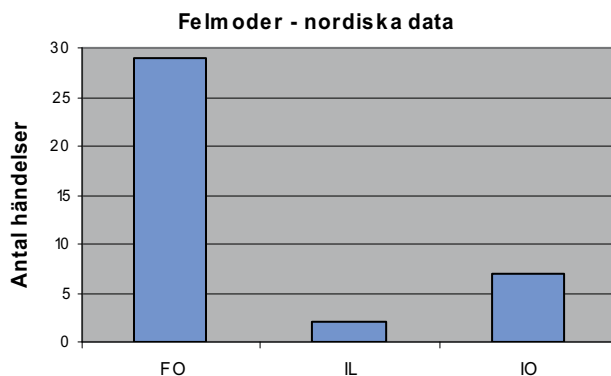
### Felmoder

För komponentgruppen är följande felmoder relevanta i ett PSA perspektiv och därmed tillämpade vid datainsamling inom ICDE.

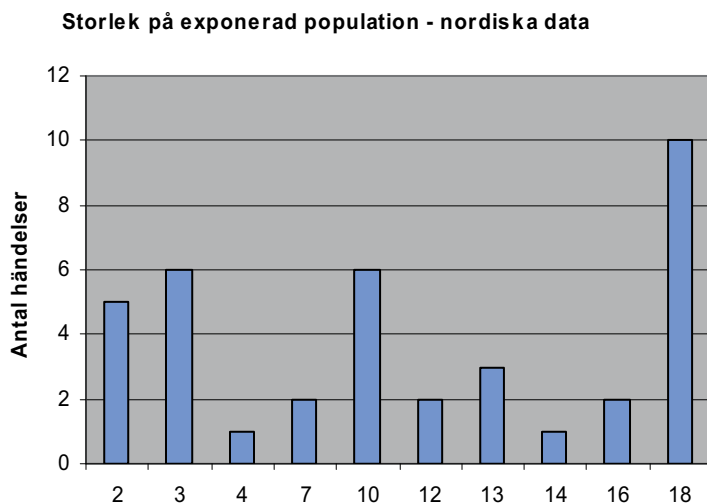
- FO (Failure to open)
- FC (Failure to close)
- IL (Internal leakage)
- IO (Inadvertent opening)
- (Other)

Felmoden FO är den mest förekommande och gäller för ca 76% av händelserna.

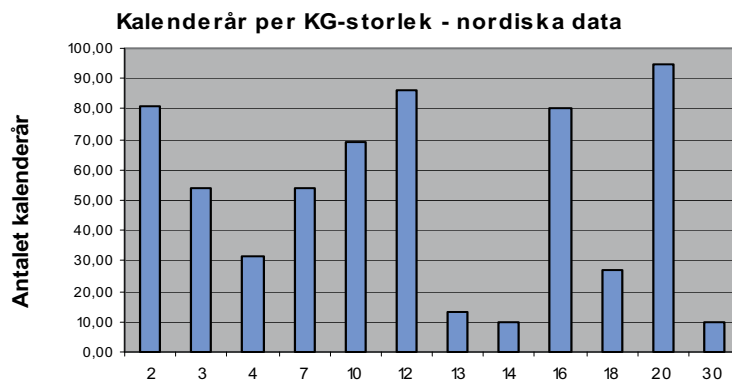
Att FO är den vanligast inträffade felmoden bekräftas även av internationella data där den svarar för ca 73% av händelserna.



### Påverkade komponent gruppstorlekar



### Ackumulerade kalenderår per komponentgruppsstorlek

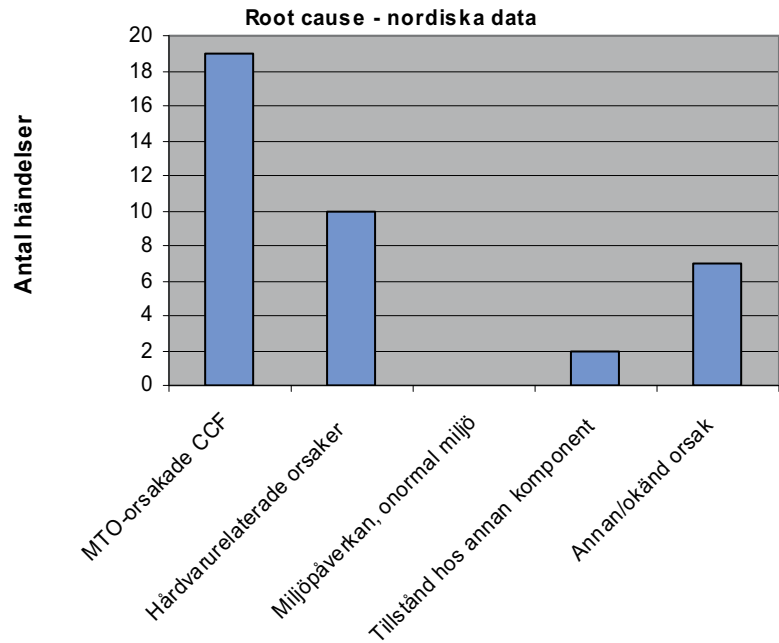


### Troliga felorsaker

För nordiska data är de vanligaste bakomliggande orsakerna relaterade till MTO enligt kategoriseringen nedan:

- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt

För internationella data är däremot hårdvarurelaterade orsaker de mest förekommande, följt av MTO-orsakade händelser.



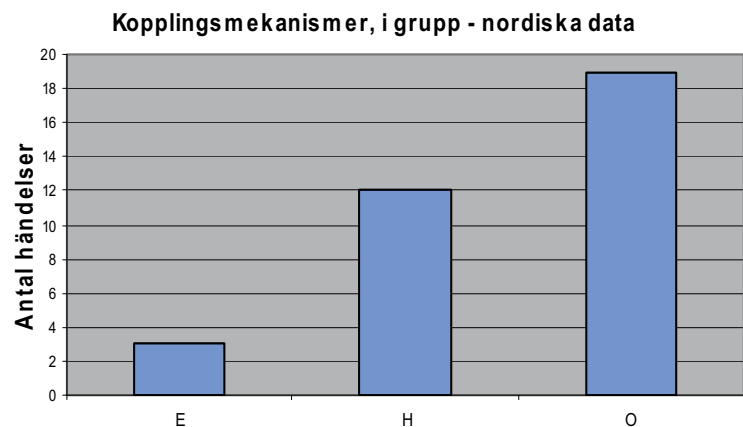
### Kopplingsfaktorer

De mest förekommande kopplingsmekanismerna för komponentgruppen är sådana som är relaterade till drift. Se kategoriindelningen nedan:

- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedur
  - Underhållsschema
  - Driftinstruktion

Fördelningen, där driftrelaterade kopplingsmekanismer är vanligast följt av hårdvarurelaterade och sedan miljörelaterade, gäller även för internationella data.

Vidare, för både nordiska och internationella data, är undergruppen "underhållsprocedur" klart dominerande både inom kategorin "drift" och totalt sett.



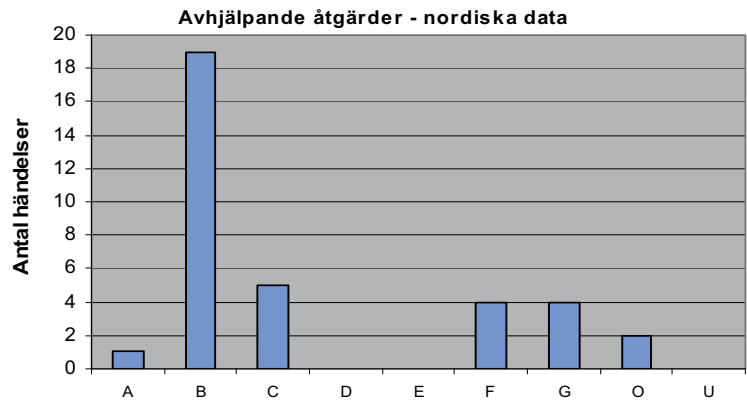


### Avhjälpan åtgärder

Vanligaste vidtagna åtgärderna är sådana som ligger inom ramen för kategorin ”specific maintenance or operational practice” (B), enligt indelningen nedan:

- Administrative control or a procedure control (A)
- Specific maintenance or operational practice (B)
- Design modification (C)
- Diversity (D)
- Functional/spatial separation (E)
- Test and maintenance policies (F)
- Fixing of component (G)
- Other (O)
- Unknown (U)

Ser man till internationella data är däremot ”test and maintenance policies” (F) de vanligaste vidtagna åtgärderna, följt av kategori B.

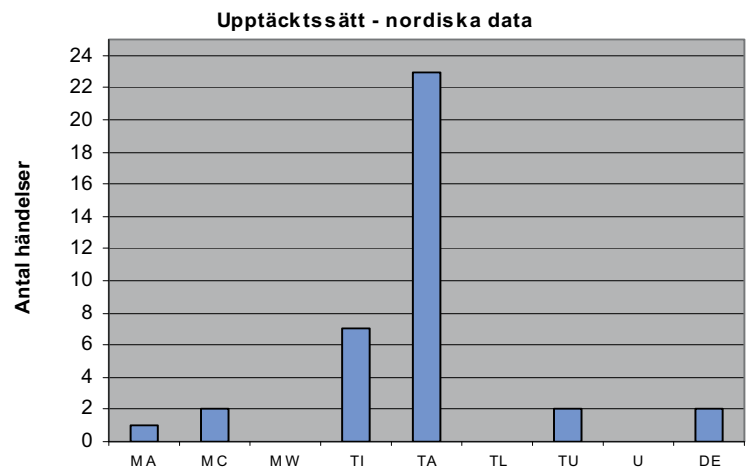


### Upptäcktsätt

Det vanligaste sättet (ca 60% av fallen) händelser upptäckts genom är ”test during annual overhaul” (TA), enligt följande indelning:

- Monitoring on walkdown (MW)
- Monitoring in control room (MC)
- Maintenance/test (MA)
- Demand event (DE)
- Test during operation/annual overhaul/laboratory (TI/TA/TL)
- Unscheduled test (TU)
- Unknown (U)

Denna trend bekräftas även av internationella data där det vanligaste upptäcktsättet är kategori TA, följt av TI.



Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Safety and relief valves System type: Turbine by-pass Component type: PWR steam generator safety valve	8	FO (Failure to open)	H (Human actions, plant staff)	OMF (Maintenance/test Staff)	TI (Test during operation)	CCCCCCCC	High
<p><b>Händelsebeskrivning:</b> On the 09th of April 1997, a unit was at hot shutdown. During a periodical test of control and treatment unit of turbine by-pass to atmosphere, 1 relief valve was unavailable by a default of an electronic circuit board of the line B. To replace the failed card, the line B was made unavailable by closing the 4 isolation valves (to avoid a spurious opening of the relief valves). However, the maintenance operations were carried out by mistake on the line A and all the 4 valves of this line were in fail-safe position, so that, the turbine by-pass to the atmosphere system was not available (8 valves).</p>							

Tabell 3. Exempel på inträffad händelse.

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Safety and relief valves System type: Pressure control (includes primary safety relief valves) Component type: BWR safety valve	14	IO (Inadvertent opening)	H (Human actions, plant staff)	H (Hardware (component part, system configuration, manufacturing quality, installation/configuration quality))	TA (Test during annual overhaul)	CCWWWWW WWWW	High
<p><b>Händelsebeskrivning:</b> At tripping test with I- and TB-chain within 516-test with operation switch in position "0" an alarm appeared at low level in 324 T1. The level in B/C/D-basin was falling. Control showed that the main valves V7 and V8 were open and water from B/C/D-basin was evacuated to the condensation pool. Attempting to close V7 and V8 by help of the respective electrical pilot valves was unsuccessful as the open signal from TB-chain was activated. I and TB-chain was restored when the el. pilot valves was closed. By that the main valves were closed and drainage to B/C/D-basin stopped. Instructions for testing will be updated with reference to operation of the system.</p> <p><b>Tolkning:</b> As a preparation for the 516-test all forced closing valves in the system were put in closed position with help of L/C-switch. Sometime before or during the test a shutdown was performed. The result of this was that the valve 754 V370 was closed. Due to leakage after 754 V370 the operating feed for forced closing of valves 314 V7 and V8 was missing. These valves are pneumatic, spring-opened (pfö) and by that opened.</p>							

Tabell 4. Exempel på inträffad händelse.

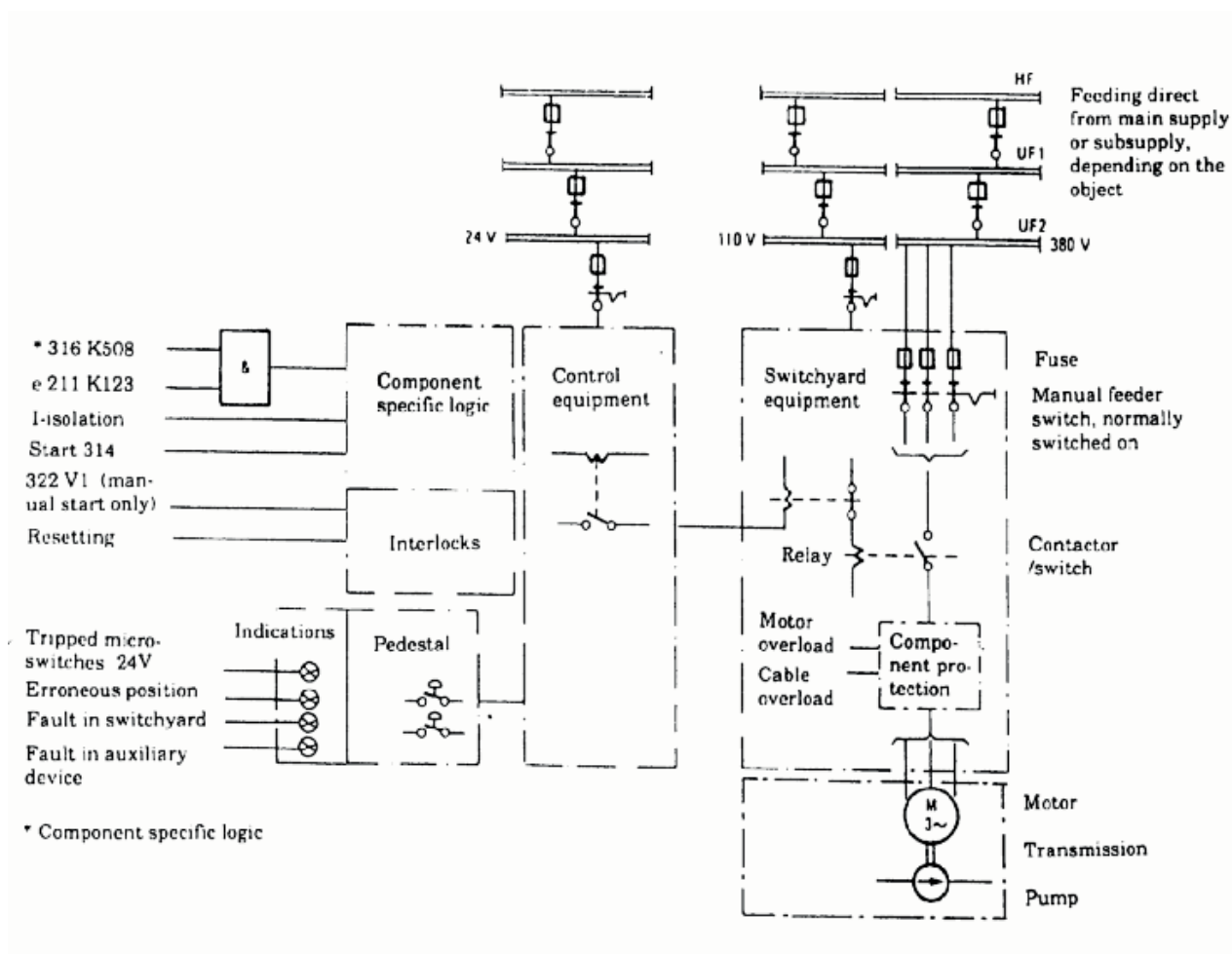
## **Vidare läsning**

- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [13].
- Sammanfattande rapport från ICDE [17].
- Erfarenheter av komponenten i UK [3].

# Bilaga 8: Vägledning – erfarenheter från insamling av CCF-händelser på motordrivna centrifugalpumpar (CP)

## Komponentgruppen Centrifugalpumpar

Komponentgruppen utgörs av de centrifugalpumpar som är motordrivna och används för att etablera flöde till eller från primär- eller servicesystem. Kategorisering av komponentgrupper görs baserat på massflöden och tryckuppsättning (< 75 kg/s, > 75 kg/s, 0.2-2 Mpa, 2-8 Mpa och 8-20 Mpa).



Figur 1. Komponentgräns, centrifugalpumpar.

Komponentens uppgift är att bibehålla vattenmängden i primärsystemet eller upprätthålla kylflöde i primär- sekundär eller i servicesystem. Komponenten anses fela vid utebliven pumpstart eller om drift inte kan bibehållas då det krävs att pumpen tas/är i drift för att möjliggöra flöde.

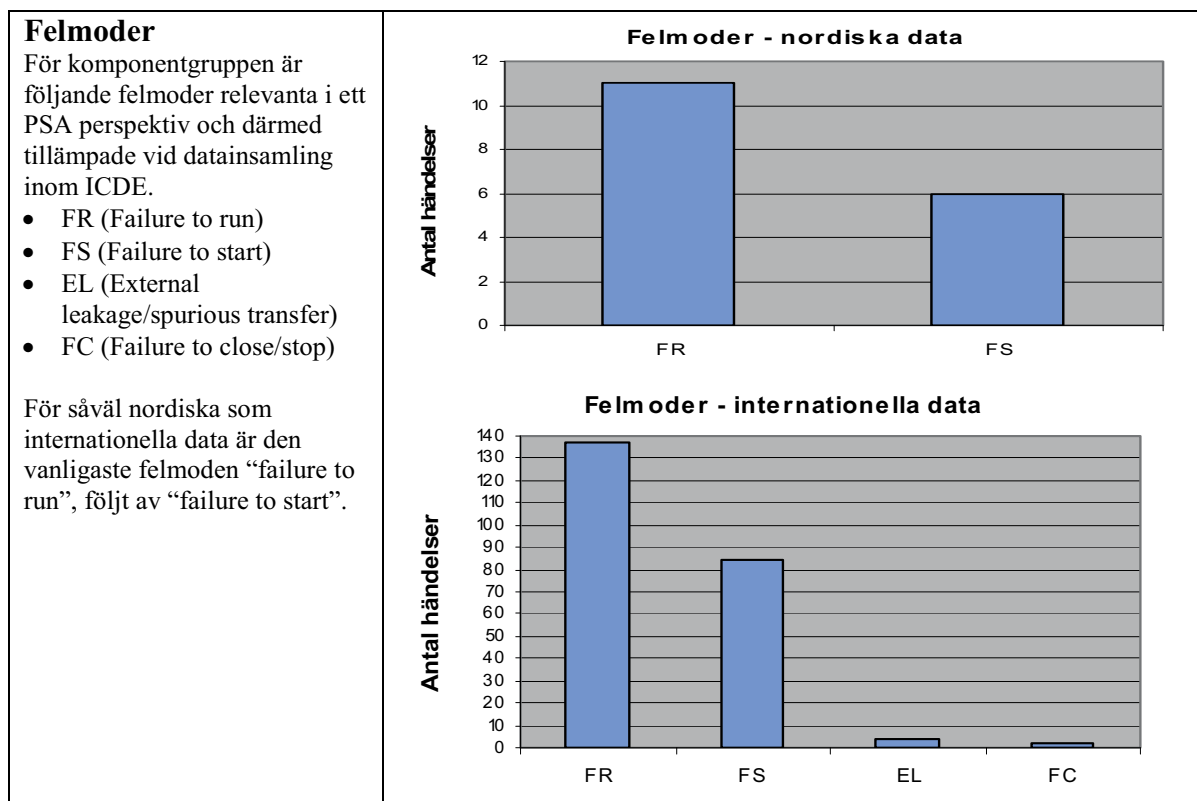
Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

Observerat antal kalenderår	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för nordiska data är 1986-01-01 – 2003-12-31	2	586,88	4114,81
	3	311,25	1829,26
	4	513,04	2551,18
Observationsperioden för internationella data är 1975-10-15 – 2005-06-06	5		150,04
	6	12,01	274,52
	7		18,0
	8		306,14
	9		18,0
	10		6,0
	12		18,0
	Totalt		1423,18
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		17	227

Tabell 1. Observationsperiod.

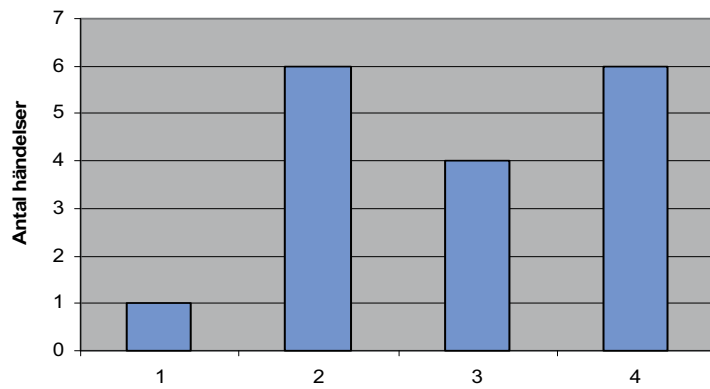
### Samlad CCF statistik om komponentgruppen

Nedan presenteras statistik för såväl nordiska som internationella observationer i ICDE-databasen.

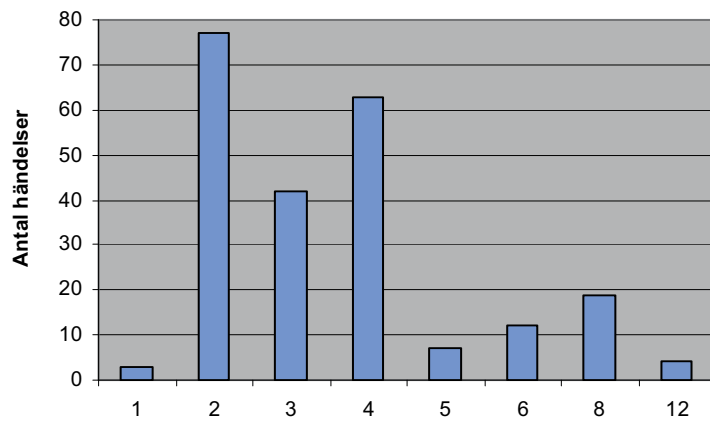


**Påverkade komponent  
gruppstorlekar**

**Storlek på exponerad population - nordiska data**

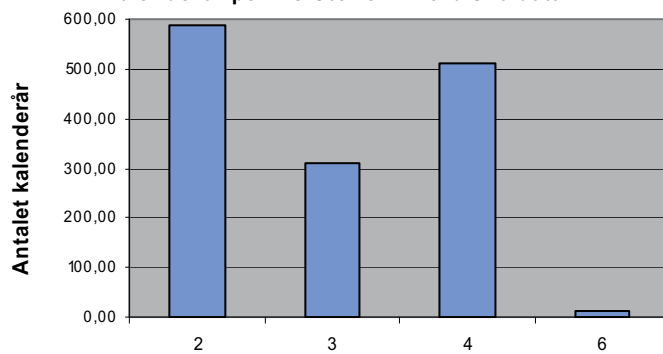


**Storlek på exponerad population - internationella data**

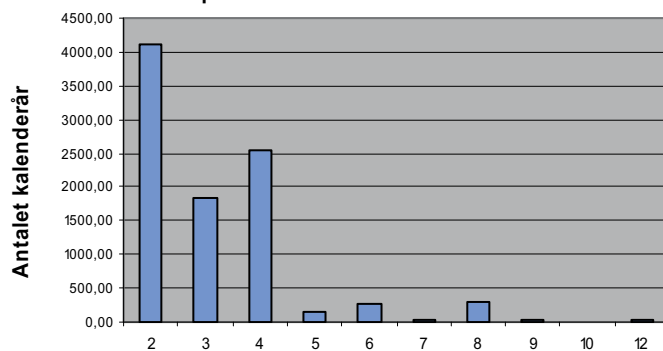


**Ackumulerade  
kalenderår per  
komponentgruppsstorlek**

**Kalenderår per KG-storlek - nordiska data**



**Kalenderår per KG-storlek - internationella data**

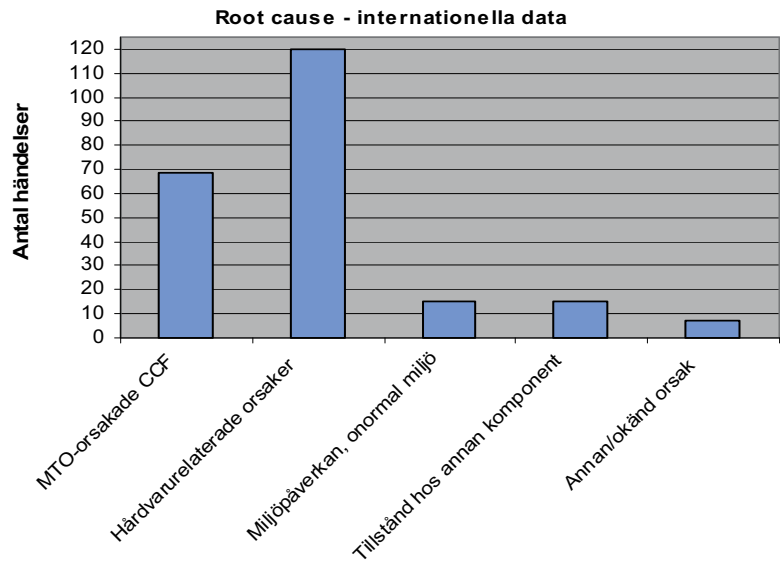
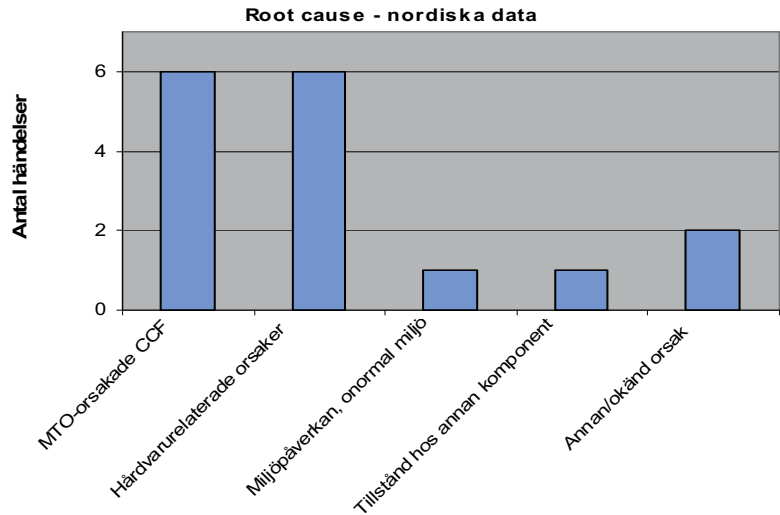


### Troliga felorsaker

Av inträffade nordiska händelser kan lika många kopplas till MTO-relaterade orsaker som till hårdvarurelaterade orsaker, vilka är de vanligaste orsakskategorierna. Se vidare indelningen nedan.

- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt

För internationella data är däremot hårdvarurelaterade orsaker de vanligaste och svarar för ca 53%.



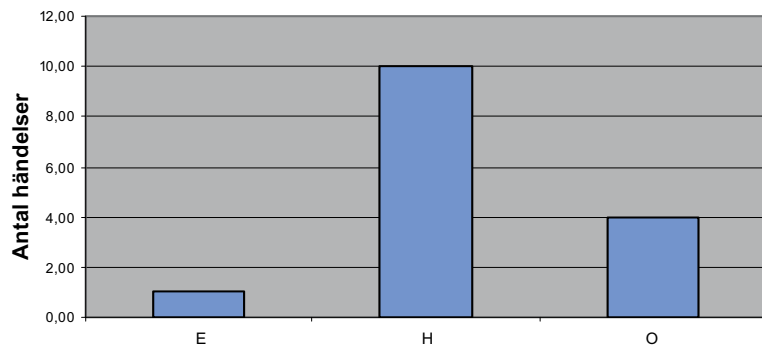
### Kopplingsfaktorer

För nordiska data har ungefär 2/3 av händelserna kopplingsmekanism relaterad till hårdvara, enligt grupperingen nedan:

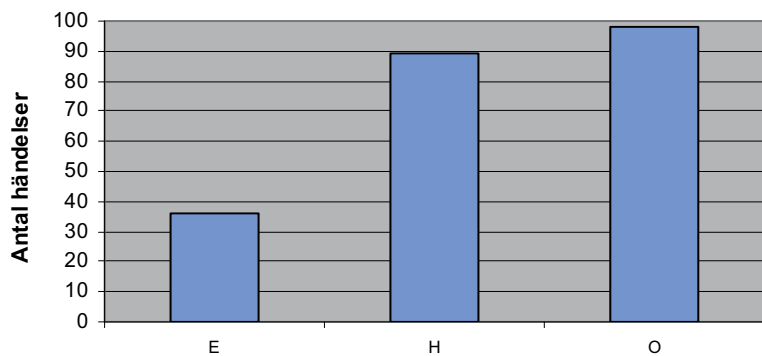
- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedur
  - Underhållsschema
  - Driftinstruktion

För internationella data däremot är kopplingsmekanismer knutna till driftkategorin de vanligaste, följt av hårdvarurelaterade kopplingsmekanismer.

Kopplingsmekanismer, i grupp - nordiska data



Kopplingsmekanismer, i grupp - internationella data



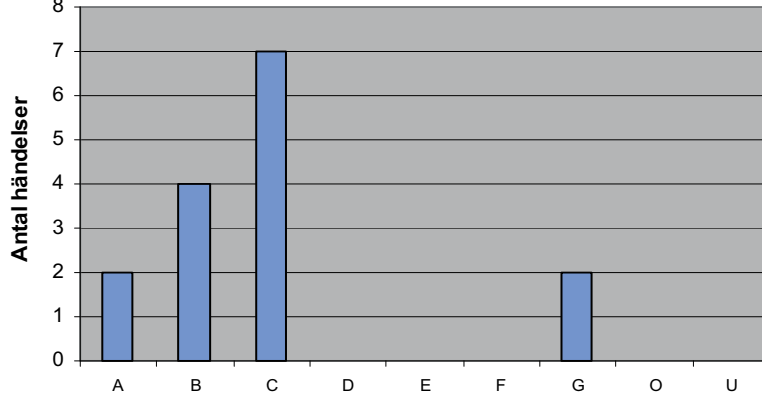
### Avhjälpande åtgärder

För inträffade händelser i Norden är ”design modification” (C) den mest frekvent vidtagna åtgärds-kategorin och svarar för drygt 40% av händelserna. Kategorisering är gjord enligt nedan:

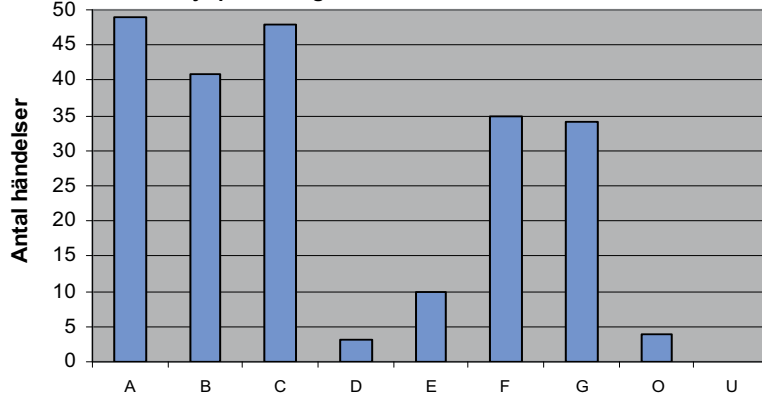
- Administrative control or a procedure control (A)
- Specific maintenance or operational practice (B)
- Design modification (C)
- Diversity (D)
- Functional/spatial separation (E)
- Test and maintenance policies (F)
- Fixing of component (G)
- Other (O)
- Unknown (U)

För internationella data är däremot spridningen betydligt större mellan olika typer av åtgärder som vidtagits vid inträffade händelser.

Avhjälpande åtgärder - nordiska data



Avhjälpande åtgärder - internationella data



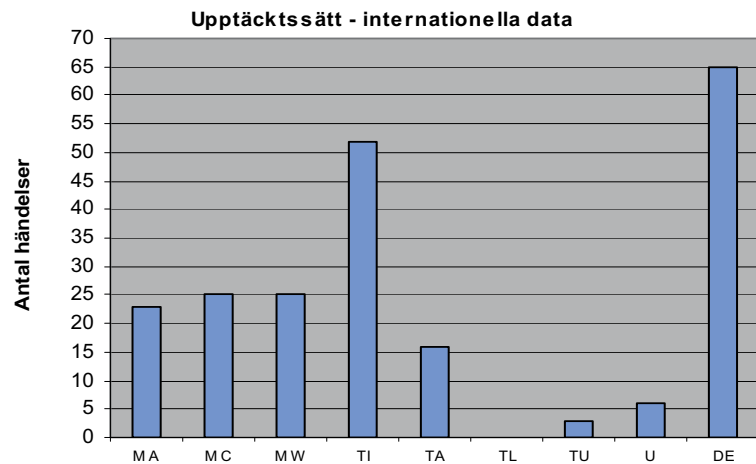
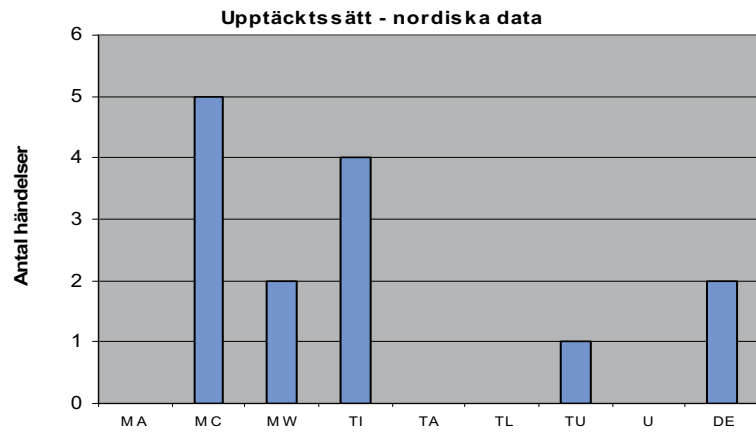


### Upptäcktssätt

För nordiska händelser är vanligaste upptäcktssättet ”monitoring in control room” (MC), följt av ”test during operation” (TI).

- Monitoring on walkdown (MW)
- Monitoring in control room (MC)
- Maintenance/test (MA)
- Demand event (DE)
- Test during operation/annual overhaul/laboratory (TI/TA/TL)
- Unscheduled test (TU)
- Unknown (U)

På internationell basis är däremot det vanligaste upptäcktssättet ”demand event” (DE), följt av kategorin TI.



Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Centrifugal pump System type: Residual heat removal (PWR and BWR out of ECC functions)	2	FS (Failure to start)	H (Human actions, plant staff)	O (Operational, maintenance/test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	DE (Demand event)	CC	High
<b>Händelsebeskrivning:</b> Power level 0%. On October 15, 1995, at approximately 1523 hours, with the plant in a hot shutdown condition, a quality assurance engineer noted that the switches for the containment spray and recirculation pumps were in a trip pullout when the Technical Specifications and plant procedures required the pumps to be operable. Operations filed a 1 hour report to notify the authority that the plant was in a condition not covered by emergency and operating procedures. The plant exceeded 200 degrees F for about 4 hours and 8 minutes in this condition. Immediate corrective action was taken to place the switches in the automatic position and subsequently check other equipment for acceptability. The cause was personnel error due to poor work practice and the contributing causes were personnel error due to poor work practice, management methods and error detection. Corrective actions that were completed include procedural reviews and revisions, an assessment of post shift briefings, an assessment of pre-mode change switch alignment and other checkoffs, a Control Room Supervisor qualification procedure, a training review process, board walkdown instructions, and briefing of crews on the significance of the event. There was no significant effect on the public health and safety due to this event.							

Tabell 3. Exempel på inträffad händelse.

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Centrifugal pump System type: Essential raw cooling or service water	4	FR (Failure to run)	D (Design, manufacture or construction inadequacy)	H (Hardware, component part, system configuration, manufacturing quality, installation/configuration quality)	MC (Monitoring in control room)	CC	Low
<b>Händelsebeskrivning:</b> Failure of a pump in the nuclear service water Plant state: full power operation In the unit control room a signal of the level transmitter of a room in the cooling water pump building occurred on 20.01.1990 (flooding of the room). The local inspection showed a leakage at the gland seal of the nuclear service water pump 4 in connection with a loud noise. High abrasion at the upper sealing element of the shaft enclosing tube results in loosening of the shaft enclosing tube. The pump was stopped and not available during installation of a new one. A similar failure with noise from the lower radial bearing as a result of high abrasion was detected on 18.06.1990 in the redundancy 3 of the nuclear service water. The pump was not available for 6 hours until a new one was installed. Cause for the abrasion was a gap between the lower radial bearing and the shaft enclosing tube permitting sand from the river to get into the grease lubricated radial bearing. The bearing was degraded. For prevention a newly designed shaft enclosing tube was installed. Additionally, the bearings of the nuclear service water pumps have been modified from grease lubricated bearings to siliconcarbide bearings without grease lubrication.							

Tabell 4. Exempel på inträffad händelse.

## **Vidare läsning**

- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [9].
- Arbete genomfört av nordiska arbetsgruppen för CCF-studier (NAFCS) [6].
- Sammanfattande rapport från ICDE [17].

## Bilaga 9: Vägledning – erfarenheter från insamling av CCF-händelser på backventiler (CV)

### Komponentgruppen backventiler

Backventiler används för att etablera eller hindra ett flöde till eller från ett vätskesystem. Komponentens funktion är, förutom det nämnda, att utgöra en villkorsbaserad gräns mellan hög- och lågtryckssektion i ett system under statiska förhållanden. Ventilen är designad så att den öppnar, för att tillåta flöde, när lågtryckssektionen får en tryckökning (t ex vid pumpstart). Det är generellt sett inte möjligt att öppna, stänga eller blockera dessa ventiler men vissa kan dock manövreras med manuell, motor- eller hydraulkraft.

Huvudkomponenten består av själva ventilen. Utöver den ingår även ventilkroppen med interna delar (bricka, fjäder, etc.) samt, om ventilen drivs av extern kraft, ventilstyrningen.

Komponenten anses fela då den inte öppnar eller hålls stängd som respons på direkt differens i systemtryck, eller inte stänger (helt) då differenstrycket försvinner.

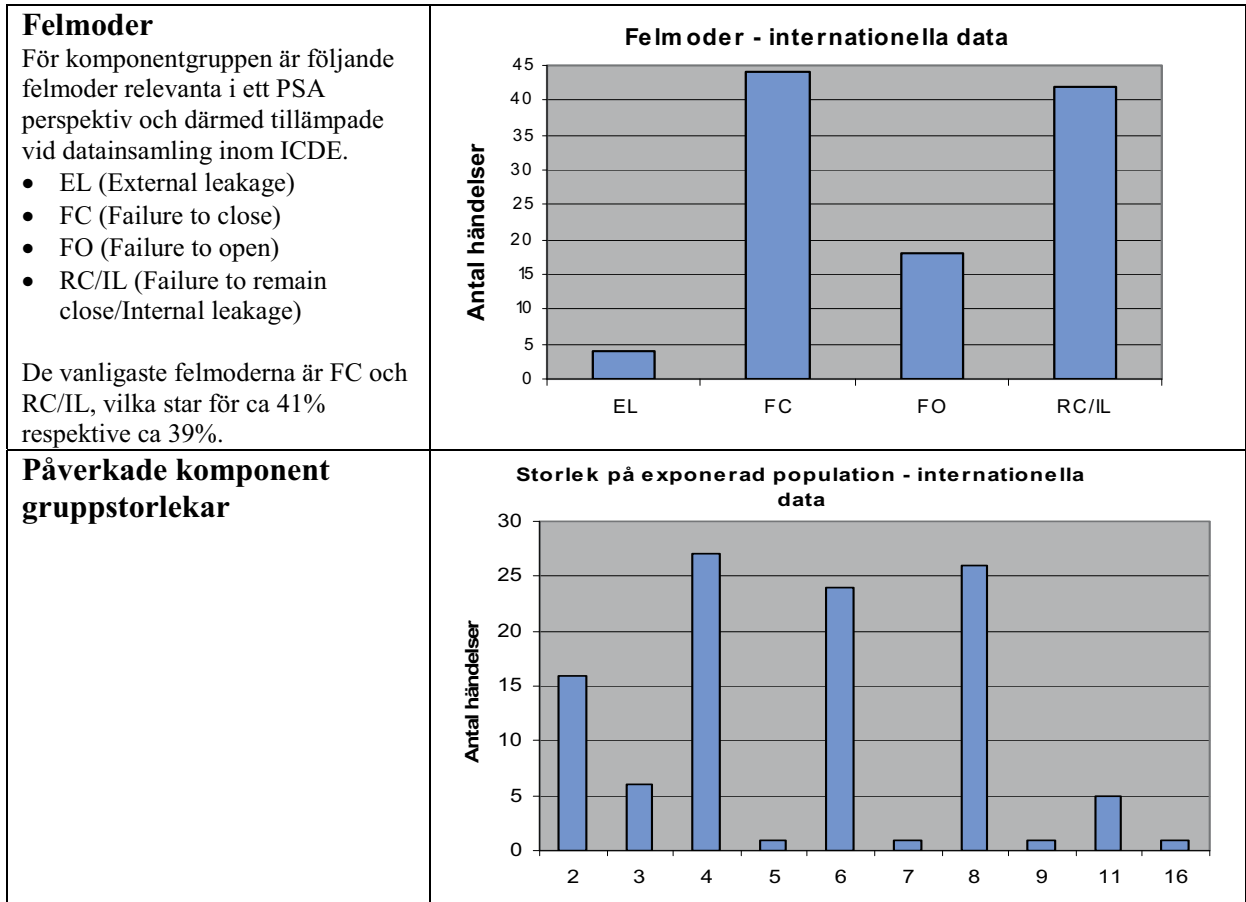
Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

Observerat antal kalenderår	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för nordiska data är 1975-01-01 – 2003-12-31	2	1096,64	2971,96
	3	318,16	1210,32
Observationsperioden för internationella data är 1972-11-01 – 2005-12-01	4	381,19	2917,67
	5		16,00
	6		486,05
	8	64,03	655,12
	9		6,08
	10		10,00
	11	29,02	47,27
	12		10,42
	16		33,02
18		10,00	
Totalt		1889,04	8373,91
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		5	108

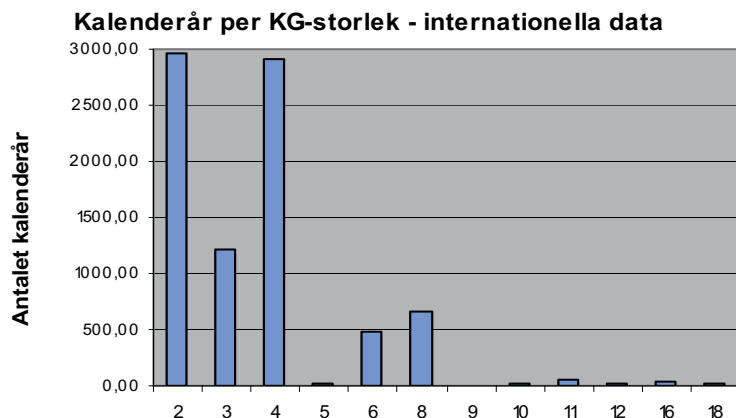
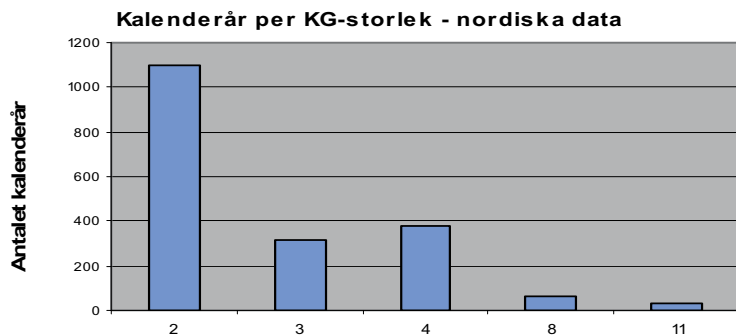
Tabell 1. Observationsperiod

## Samlad statistik om komponentgruppen

För komponentgruppen backventiler finns endast fem nordiska händelser i datainsamlingen. Detta gör att nyttan med presentation av nordiska data blir väldigt liten och i det följande fokuseras presentationen av statistik istället på internationella data.



## Ackumulerade kalenderår per komponentgruppsstorlek

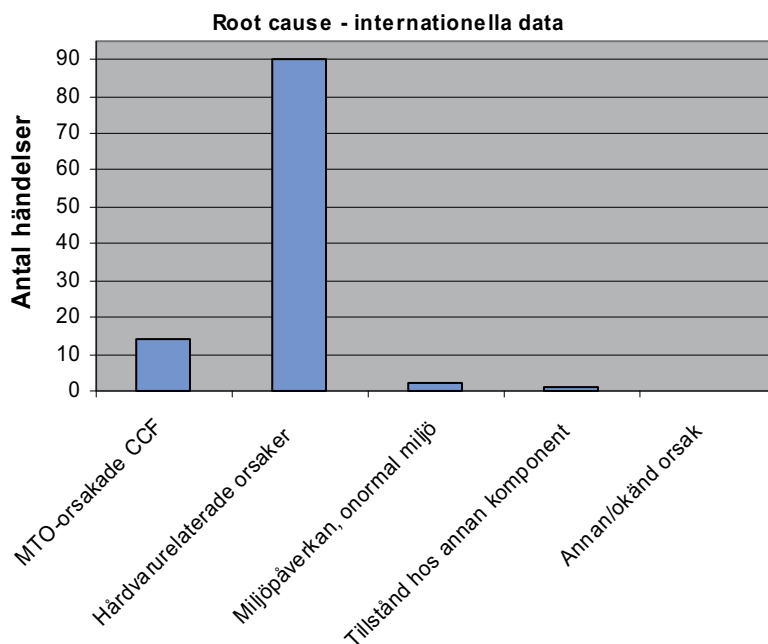


## Troliga felorsaker

De dominerande bakomliggande orsakerna till insamlade händelser är relaterade till hårdvara, vilka svarar för ca 84%. Kategorisering är gjord enligt nedan:

- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt

Såväl inom kategorin ”hårdvarurelaterade orsaker” som totalt sett, är den mest framträdande orsakskategorin ”internt (inom komponent)”.



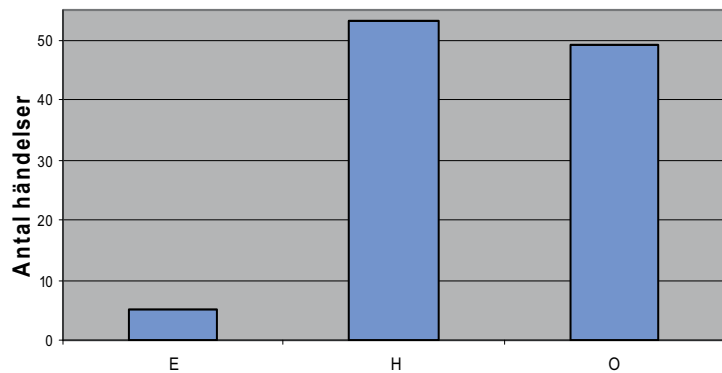
### Kopplingsfaktorer

De vanligaste förekommande (50%) kopplingsmekanismerna är relaterade till hårdvara, tätt följt av driftrelaterade kopplingsmekanismer (46%). Gruppering är gjord enligt nedan:

- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedur
  - Underhållsschema
  - Driftinstruktion

Den enskilt mest frekventa kopplingsfaktorn är dock "Underhållsschema", en kategori inom "Drift".

Kopplingsmekanismer, i grupp - internationella data

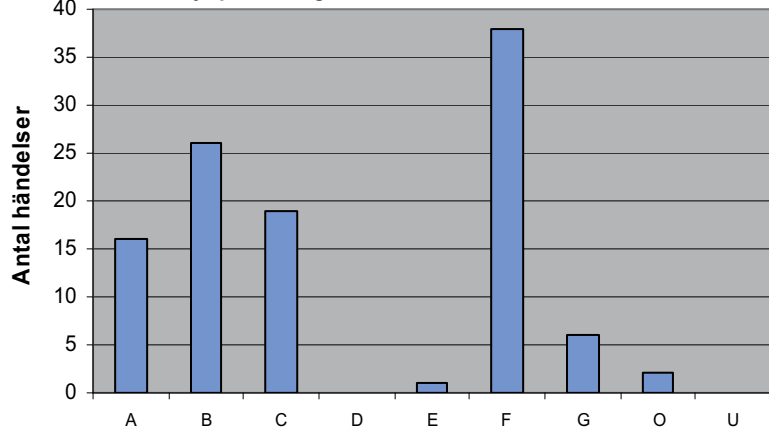


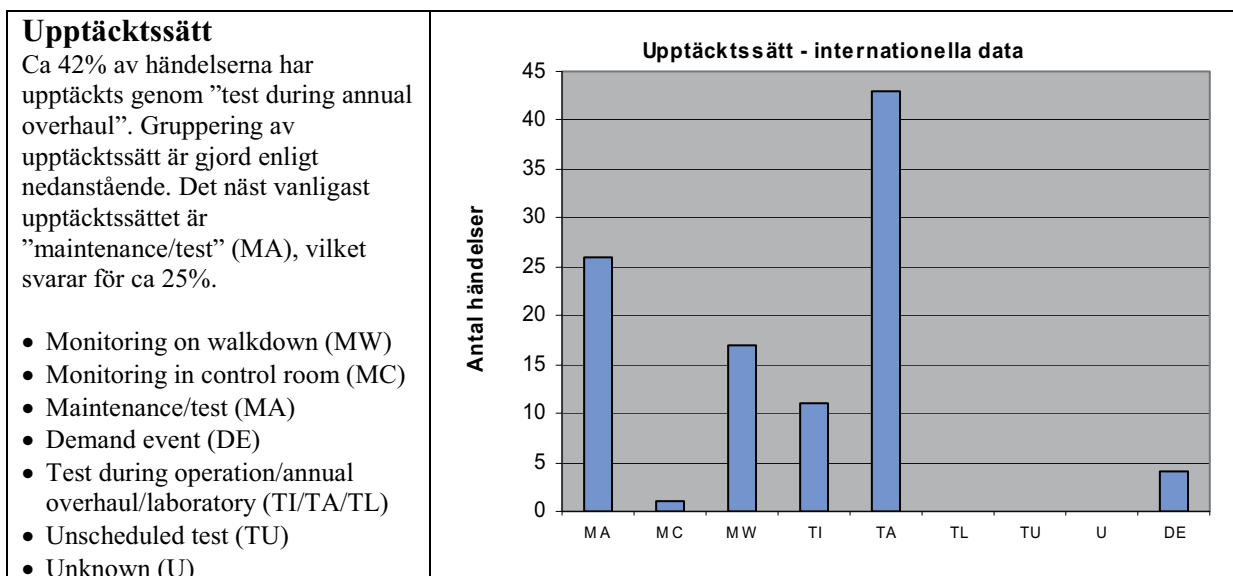
### Avhjälpannde åtgärder

De vanligaste vidtagna åtgärderna ligger inom ramen för kategorin "test and maintenance policies" (F), vilken svarar för ca 35% av händelserna i datainsamlingen. Kategorisering är enligt följande:

- Administrative control or a procedure control (A)
- Specific maintenance or operational practice (B)
- Design modification (C)
- Diversity (D)
- Functional/spatial separation (E)
- Test and maintenance policies (F)
- Fixing of component (G)
- Other (O)
- Unknown (U)

Avhjälpannde åtgärder - internationella data





Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Check valve System type: Emergency core cooling (core spray or RHR, CVCS participation)	2	FC (Failure to close)	D (Design, manufacture or construction inadequacy)	HC (Hardware Design)	TA (Test during annual overhaul)	CC	High

**Händelsebeskrivning:**

Plant state: hot stand-by prior to criticality after refuelling outage  
On recurrent testing a line break of one of the safety injection lines is simulated by opening a motor operated test valve. By this test, the closing function of the medium-operated check valves in the common discharge header of the safety injection system are tested. The test is performed with two of the four high pressure safety injection pumps running. On 8 March 1995, both check valves did not close completely. The non-closure of the check valves lead to strong vibrations which resulted in the breaking off of a 15 mm drain line and a rupture of a second 15 mm drain line. The cause of the non-closure of the check valves was maintenance carried out in 1993 and the fitting of graphite gaskets in 1994 had resulted in such dimensional changes that the piston contacted the cylinder cover before the valve reached its seat. From records it could be demonstrated that the last normal tests were carried out in 1991. There was no requalification program after modifications. Periodic testing instructions did not contain quantitative success criteria.

Tabell 3. Exempel på inträffad händelse.



Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplings- faktor	Upptäckts- sätt	Komponent- degradering, vektor	Tidsfaktor/ faktor för gemensam orsak
Check valve System type: Condensate and feedwater	4	RC/IL (Failure to remain close/ Internal leakage)	D (Design, manufacture or construct- ion inade- quacy)	H (Hardware, component part, system configuration, manufacturing quality, installation/ configuration quality)	MC (Monitoring in control room)	CCCD	High

**Händelsebeskrivning:**

At 99.5% reactor power, 3 out of 4 feedwater swing check valves closed for a short while. The fourth one also began closing. Because the feed-water supply dropped, the reactor pressure vessel level reached the actuating mark for the reactor scram system. The cause of this event was spurious actuation of the reactor-protection-logic in one channel which actuated (opened) 2 out of 4 solenoid pilot valves each per main valve. According to the design this does not lead to a closing of the swing check valves. But through hydraulic effects on opening of the pilot valves the swing check valves closed for a short while.

*Tabell 4. Exempel på inträffad händelse.*

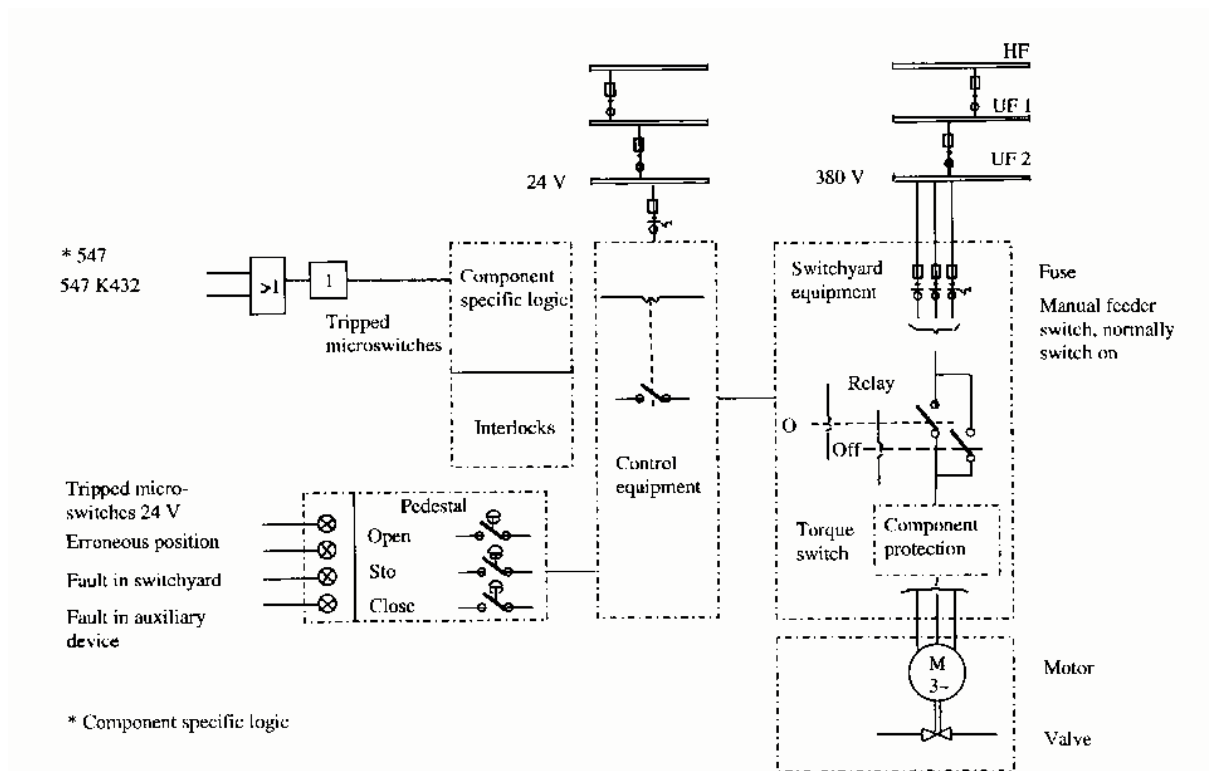
**Vidare läsning**

- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [10].
- Sammanfattande rapport från ICDE [17].

# Bilaga 10: Vägledning – erfarenheter från insamling av CCF-händelser på motormanövrerade ventiler (MOV)

## Komponentgruppen motormanövrerade ventiler

Komponentgruppen utgörs av motormanövrerade ventiler i härdsnödkylsystem som används för att etablera eller hindra flöde till eller från det primära systemet.



Figur 1. Komponentgräns, motormanövrerade ventiler.

Komponentens uppgift är att möjliggöra flöde av vatten till eller förhindra att vatten flödar från primärsystemet vid en LOCA. Komponenten anses fela om öppning uteblir när det krävs att den öppnar för att möjliggöra tillflöde, eller om stängning uteblir när det krävs att den stängs för att förhindra bortflöde.

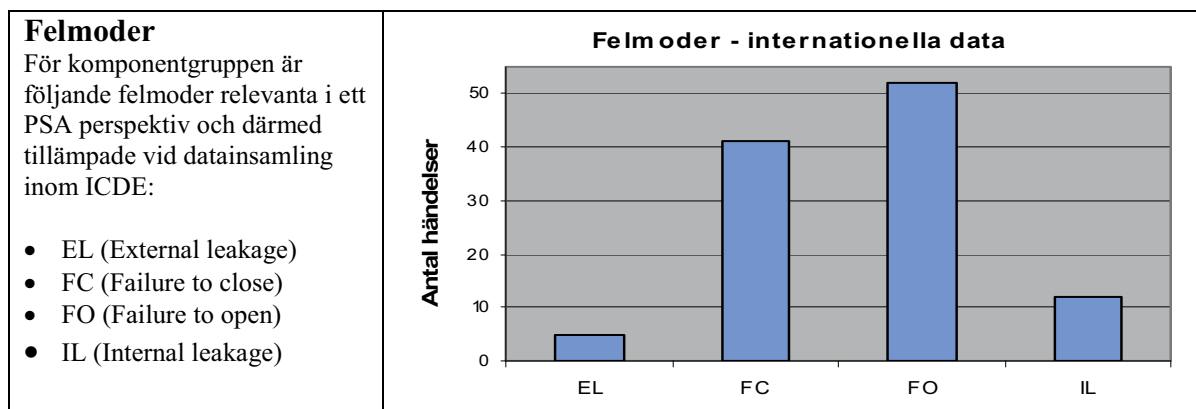
Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

<b>Observerat antal kalenderår</b>	<b>CCCG storlek</b>	<b>Nordiska data</b>	<b>Internationella data (inkl. nordiska)</b>
Observationsperioden för nordiska data är 1980-01-01 – 2003-12-31	2	840,65	3590,05
	3	127,06	294,08
Observationsperioden för internationella data är 1970-03-14 – 2005-12-31	4	397,14	1582,49
	5		6,00
	6	24,01	225,72
	8	24,01	2485,05
	10		6,00
	13		6,00
	14	24,01	30,01
	15		15,00
	16		92,04
	19		10,00
	24	30,02	30,02
<b>Totalt</b>		<b>1466,91</b>	<b>8372,47</b>
<b>Antal observerade CCF-händelser i ICDE-databasen</b>		<b>8</b>	<b>112</b>

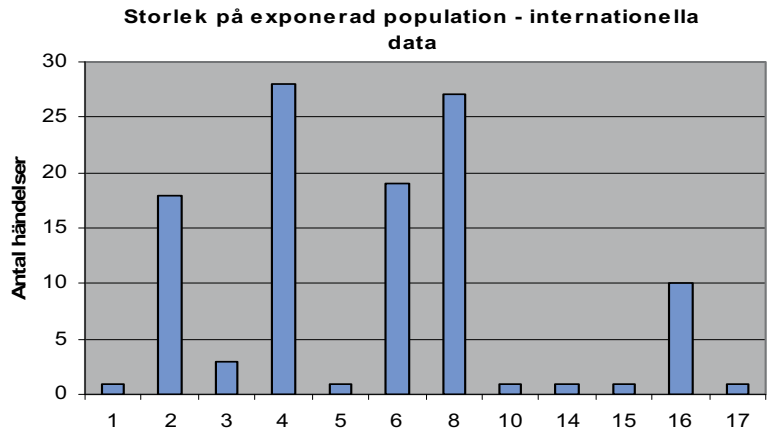
Tabell 1. Observationsperiod.

### Samlad statistik om komponentgruppen

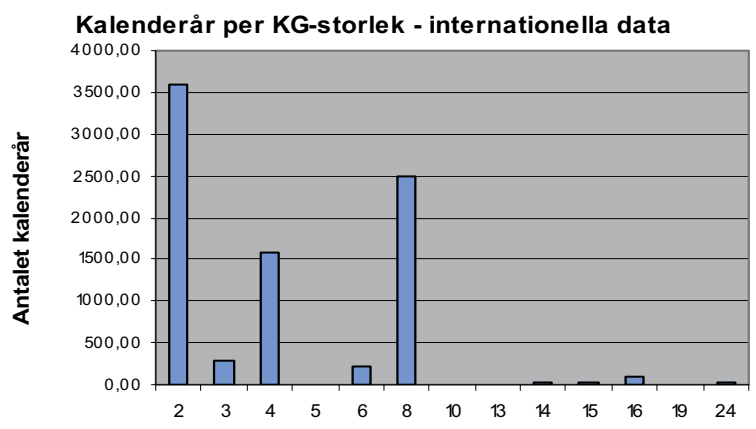
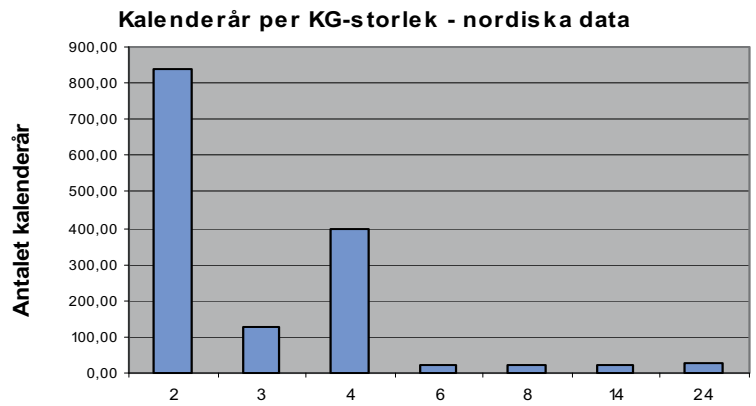
För komponentgruppen finns så fåtal nordiska händelser att det är mer relevant att fokusera på internationella data, vilket därför görs i nedanstående presenterad statistik.



**Påverkade komponent  
gruppstorlekar**



**Ackumulerade  
kalenderår per  
komponentgruppstorlek**

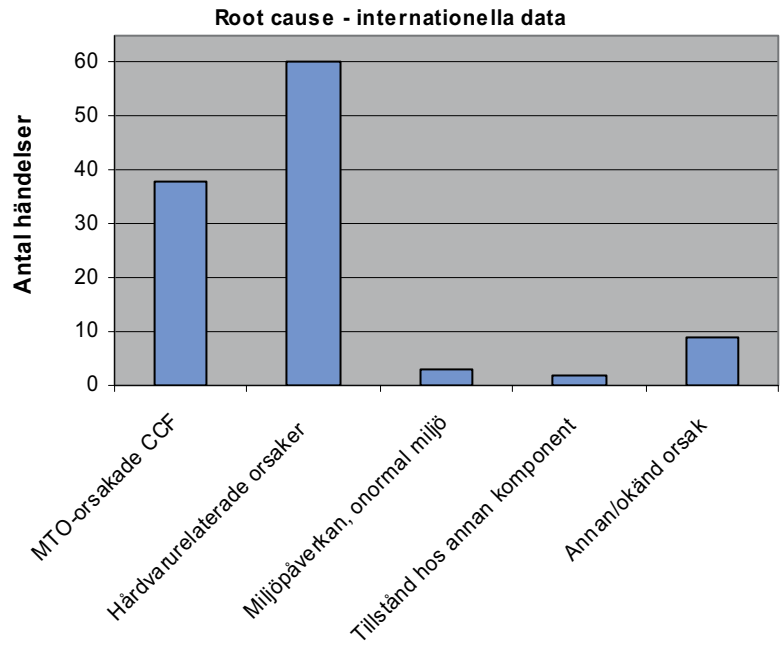


### Troliga felorsaker

De vanligaste felorsakerna är sådan som är relaterade till hårdvara. Gruppering är gjord enligt nedan:

- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt

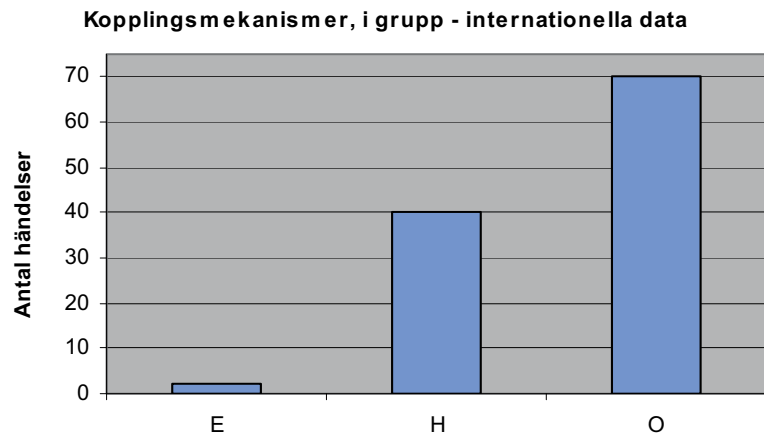
”Brist i design konstruktion eller tillverkning ” och ”internt (inom komponent)” står är lika ofta förekommande och står tillsammans för ca 54% av händelserna. De näst vanligaste felorsakerna är relaterade till MTO och svarar för ca 33%.

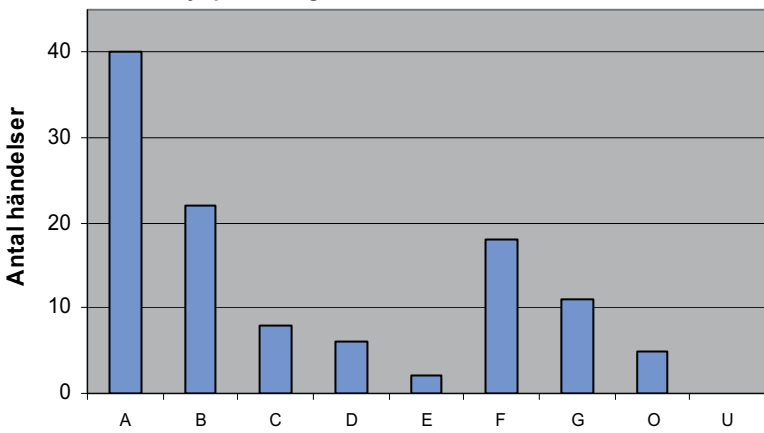
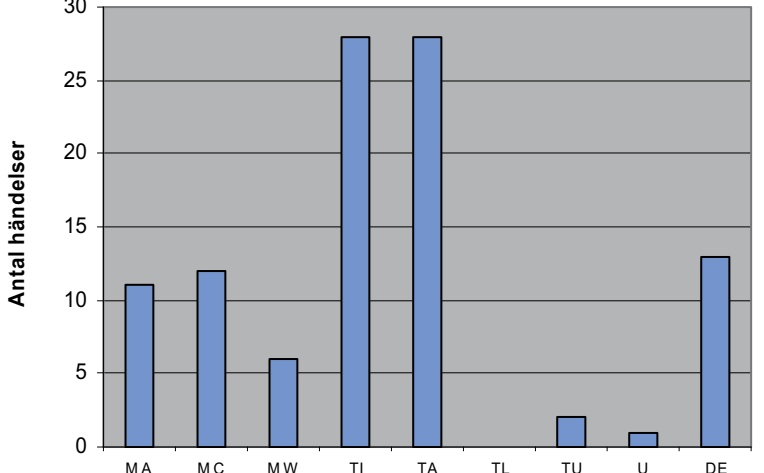


### Kopplingsfaktorer

De flesta händelser (61% av dem) har kopplingsmekanismer kopplade till drift. Därefter, i antal händelser, följer hårdvarurelaterade sådana (ca 37%). Gruppindelning är gjord enligt följande:

- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedure
  - Underhållsschema
  - Driftinstruktion



<p><b>Avhjälpan åtgärder</b></p> <p>De typer av avhjälpan åtgärder som dominerar, i antal, vid inträffade händelser är kopplade till kategorin "administrative control or a procedure control" (A) då de står för ca 35%. Kategorisering är gjord enligt:</p> <ul style="list-style-type: none"> <li>• Administrative control or a procedure control (A)</li> <li>• Specific maintenance or operational practice (B)</li> <li>• Design modification (C)</li> <li>• Diversity (D)</li> <li>• Functional/spatial separation (E)</li> <li>• Test and maintenance policies (F)</li> <li>• Fixing of component (G)</li> <li>• Other (O)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Avhjälpan åtgärder - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Kategori</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>A</td><td>40</td></tr> <tr><td>B</td><td>22</td></tr> <tr><td>C</td><td>8</td></tr> <tr><td>D</td><td>6</td></tr> <tr><td>E</td><td>2</td></tr> <tr><td>F</td><td>18</td></tr> <tr><td>G</td><td>11</td></tr> <tr><td>O</td><td>5</td></tr> <tr><td>U</td><td>0</td></tr> </tbody> </table>	Kategori	Antal händelser	A	40	B	22	C	8	D	6	E	2	F	18	G	11	O	5	U	0
Kategori	Antal händelser																				
A	40																				
B	22																				
C	8																				
D	6																				
E	2																				
F	18																				
G	11																				
O	5																				
U	0																				
<p><b>Upptäcktsätt</b></p> <p>De mest förekommande sätten att upptäcka fel är genom "test during operation" (TI) och "test during annual overhaul" (TA), vilka svarar för ca 25% var. Tillsammans står de därmed för ungefär hälften av händelserna.</p> <ul style="list-style-type: none"> <li>• Monitoring on walkdown (MW)</li> <li>• Monitoring in control room (MC)</li> <li>• Maintenance/test (MA)</li> <li>• Demand event (DE)</li> <li>• Test during operation/annual overhaul/laboratory (TI/TA/TL)</li> <li>• Unscheduled test (TU)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Upptäcktsätt - internationella data</b></p>  <table border="1"> <thead> <tr> <th>Upptäcktsätt</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>MA</td><td>11</td></tr> <tr><td>MC</td><td>12</td></tr> <tr><td>MW</td><td>6</td></tr> <tr><td>TI</td><td>28</td></tr> <tr><td>TA</td><td>28</td></tr> <tr><td>TL</td><td>0</td></tr> <tr><td>TU</td><td>2</td></tr> <tr><td>U</td><td>1</td></tr> <tr><td>DE</td><td>13</td></tr> </tbody> </table>	Upptäcktsätt	Antal händelser	MA	11	MC	12	MW	6	TI	28	TA	28	TL	0	TU	2	U	1	DE	13
Upptäcktsätt	Antal händelser																				
MA	11																				
MC	12																				
MW	6																				
TI	28																				
TA	28																				
TL	0																				
TU	2																				
U	1																				
DE	13																				

Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Motor operated valve System type: Emergency core cooling (core spray or RHR, CVCS participation)	4	FO (Failure to open)	Human actions, plant staff	OF (Operation Staff)	MC (Monitoring in control room)	CCCC	High
<p><b>Händelsebeskrivning:</b>            The unit was at shutdown phase. Shutdown of the plant was necessary due to a leakage at the boron accumulator of the high pressure safety injection line with loss of about 1 m<sup>3</sup> of boron solution. After isolation of the leakage (with plant still at full power) shutdown of the plant began. About two hours later, the four isolation valves of the boron accumulator were locked out in closed position by an order of the head of the technical department. This was done for security reasons to protect the personnel which should refill the accumulator. But in the actual plant state the availability of the high pressure safety injection line was required. This was recognised by the operator. Therefore 13 minutes later the shift supervisor demanded to make the valves available.            About 1h30 later it was decided again to lock out the valves. But the safety engineer disagreed with this decision. 1h40 later after several discussions the representative of the plant director decided that the valves have to be available in the actual plant state.            The causes of the event were that the repair works should begin in a plant state where these works were not permitted. Further, priority was given to the security of the personnel and not to the plant safety. Third, there was confusion about the responsibility within plant management.</p> <p><b>Tolkning:</b>            The event is interpreted as a CCF of the 4 valves in the injection line of the boron accumulator because the valves were two-times unavailable (13 min and 1h40) in a plant state where they had to be available.</p>							

Tabell 3. Exempel på inträffad händelse.

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
Motor operated valve System type: Emergency core cooling (core spray or RHR, CVCS participation)	12	FO (Failure to open)	I (Internal to component, piece part)	H (Hardware, component part, system configuration, manufacturing quality, installation/configuration quality)	TI/MA (Test during operation / Maintenance, test)	CCDDWWW WWWWW	High

**Händelsebeskrivning:**

In the power operation of a unit the motor operated valve (MOV) V304 of the core spray system (323) opened during the periodic test performed on 11 December 2000, but it failed to close. Two teeth were found missing from the pinion. The damaged pinion was replaced with a brass pinion. Other redundant valves were inspected and following cracks were found: V104 – 4 cracks, V204 – 8 cracks (actuator was replaced in August 2000 due to similar pinion failure), V404 – 2 cracks.

Because of the recurrent cases of damage, and after the inadequate quality of the removed bakelite pinions was verified, a decision to replace each pinion with brass ones in all actuators at the component location 323 VX04 at two plant units was made.

The results of the liquid penetrant testings on the pinions of the eight 323 VX04 valves showed a certain number of cracks. The direct cause of the failures in the bakelite pinions were investigated by conducting material technological studies. According to these studies the probable cause of the cracks was nucleation and growth of fatigue type cracks. No ageing type phenomena were observed.

Temporary corrective actions:

The material of the 323 VX04 actuator pinion was changed from bakelite to brass.

Permanent corrective actions:

The instructions and procedures have been changed.

Actuators are replaced with new generation actuators that do not contain any bakelite pinions.

**Tolkning:**

After detailed analysis the event is interpreted as CCF of four valves according to the failed/degraded bakelite pinions of the checked actuators. The failure mechanism and the probable cause of the degradation are the same for the actuators.

*Tabell 4. Exempel på inträffad händelse.*

**Vidare läsning**

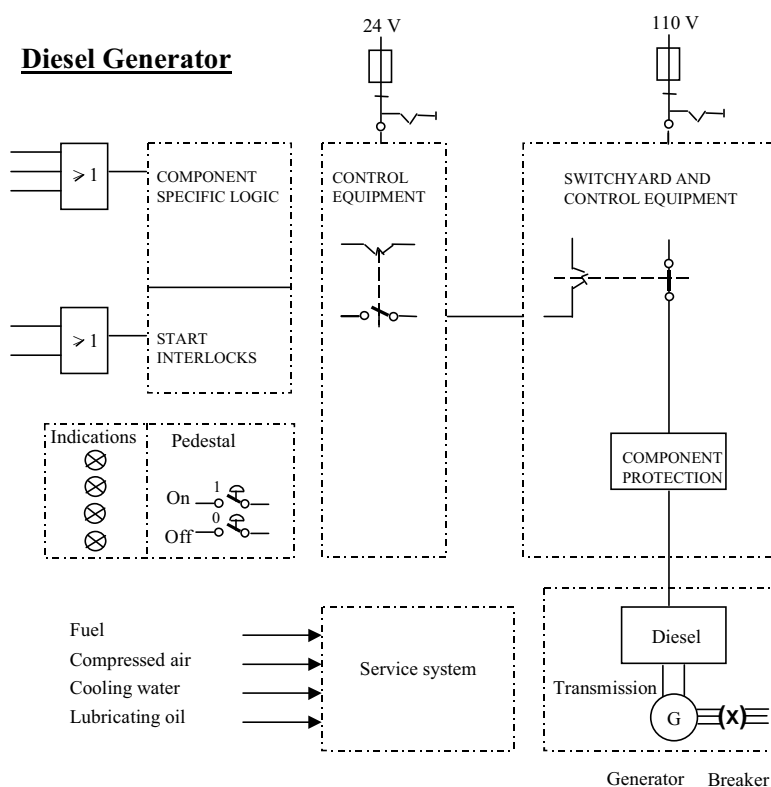
- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [12].
- Arbete genomfört av nordiska arbetsgruppen för CCF-studier (NAFCS) [6].
- Sammanfattande rapport från ICDE [17].



# Bilaga 11: Vägledning – erfarenheter från insamling av CCF-händelser på nödkraftdieslar (DG)

## Komponentgruppen nödkraftdieslar

Nödkraftdieslar är en del av kraftsystemet som ger hjälpkraft vid bortfall av yttre nät för att mata anläggningens säkerhetssystem. Dieselgeneratorer är normalt inte i drift när anläggningen är i effektdrift eller vid avställd anläggning, utan står då i standby. Den fysiska omfattningen av komponentgruppen ges i figuren nedan.



Figur 1. Komponentgräns, nödkraftdieslar.

Komponentens uppgift är dels att starta och ge kraftförsörjning vid LOSP (Loss of Offsite Power), dels att starta och vara redo att kraftmata vid händelse av LOCA. Komponenten anses fela då dessa uppgifter inte kan utföras.

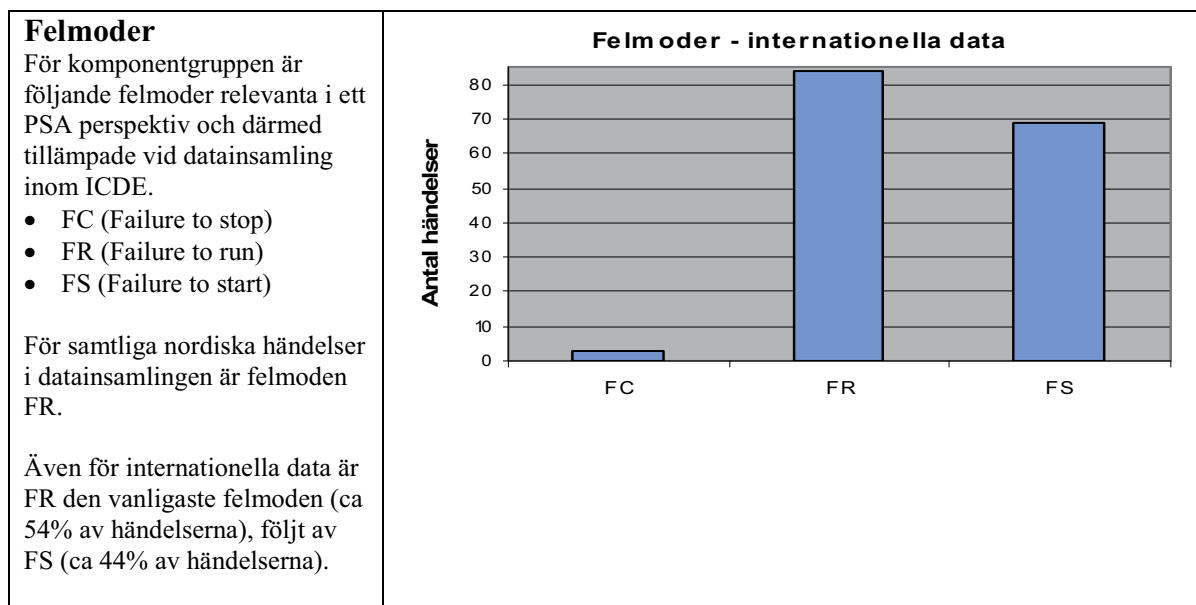
Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

Observerat antal kalenderår	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för nordiska data är 1977-05-08 – 2003-12-31	2	53,09	1606,71
	3		250,98
Observationsperioden för internationella data är 1977-05-08 – 2005-12-31	4	191,39	561,18
	5		76,78
	6		5,00
	8		24,01
Totalt		244,47	2524,65
Antal observerade CCF-händelser i ICDE-databasen		31	156

Tabell 1. Observationsperiod.

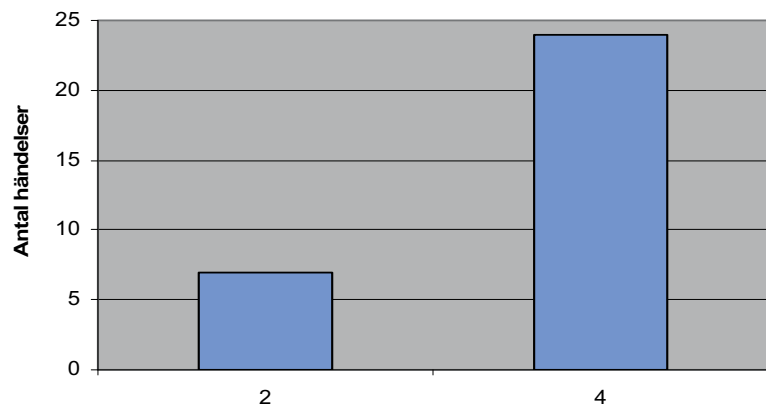
### Samlad statistik om komponentgruppen

20 % av insamlade ICDE-händelser är nordiska händelser. Gällande komponentgruppstorleken 4 svarar nordiska data för ca 34 % av observationstiden i ICDE-databasen.

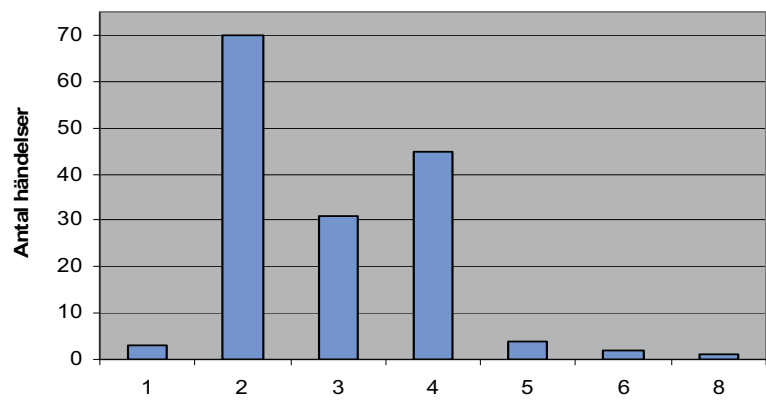


**Påverkade komponent  
gruppstorlekar**

**Storlek på exponerad population - nordiska data**

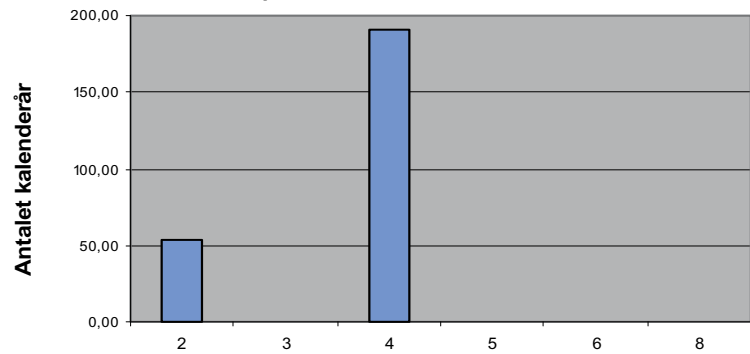


**Storlek på exponerad population - internationella data**

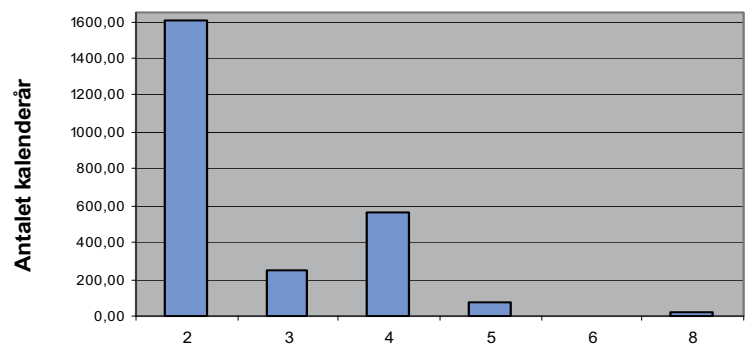


**Ackumulerade  
kalenderår per  
komponentgruppsstorlek**

**Kalenderår per KG-storlek - nordiska data**



**Kalenderår per KG-storlek - internationella data**



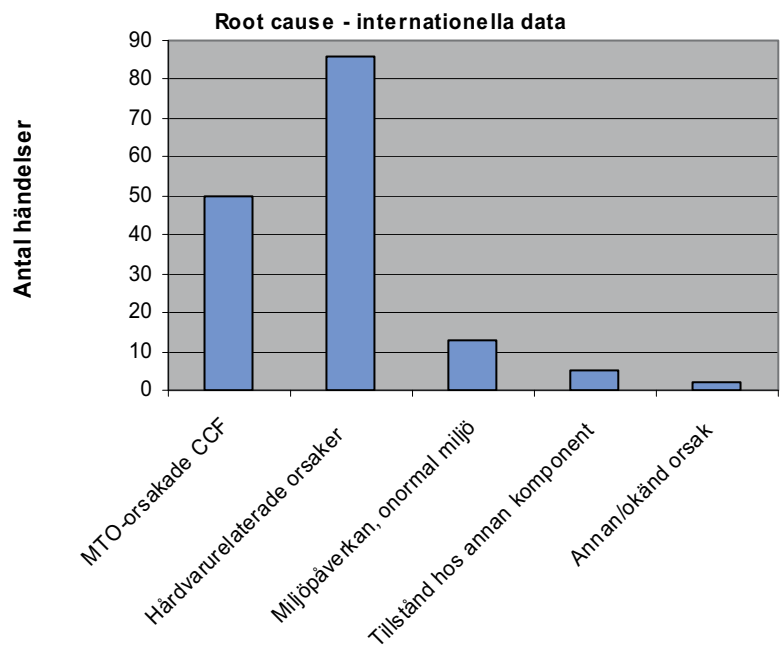
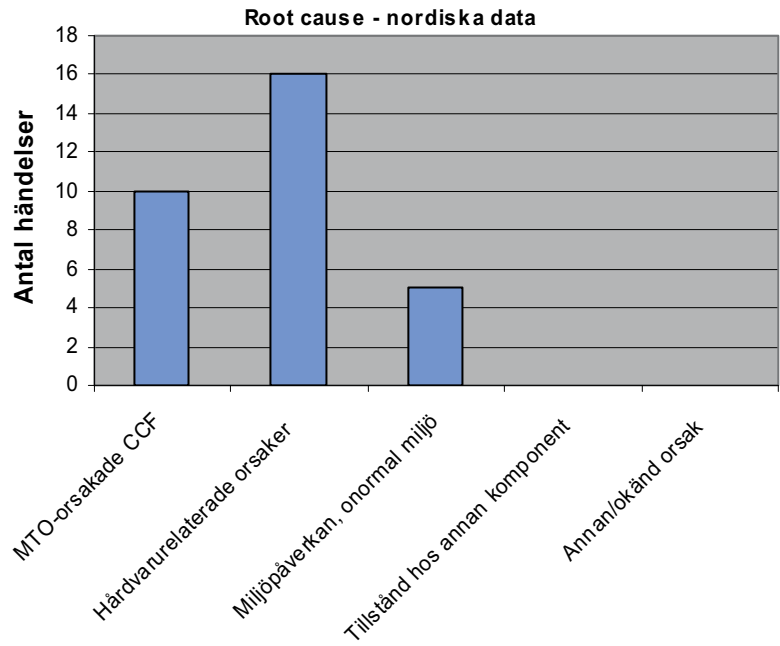
### Troliga felorsaker

För nordiska data är de dominerande felorsakerna knutna till hårdvara, en kategori som svarar för ca 52% av händelserna. Indelning är gjord enligt följande:

- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt

Trenden i de nordiska data, att hårdvarurelaterade orsaker är vanligast, bekräftas av internationella data där orsakskategorin svarar för 55 ca % av händelserna.

Den enskilt mest vanliga felorsaken, för såväl nordiska som internationella data, är ”brist i design konstruktion eller tillverkning” (något mindre än hälften av händelserna).



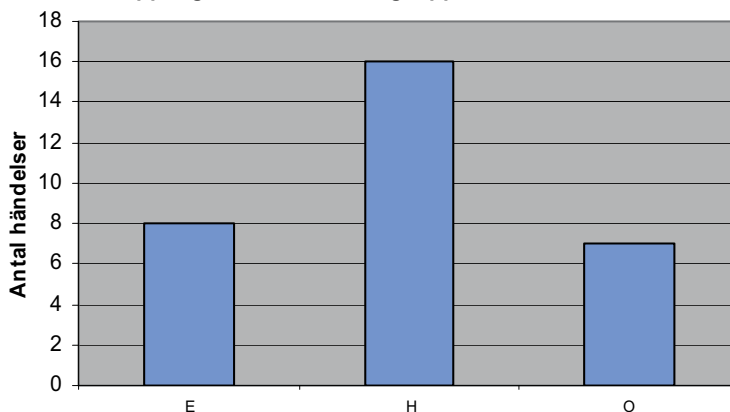
### Kopplingsfaktorer

De flesta nordiska händelser har en hårdvarurelaterad kopplingsmekanism (ca 52 % av händelserna). Detsamma gäller för internationella händelser där kategorin svara för ca 60%. Kategorisering är gjord enligt nedanstående:

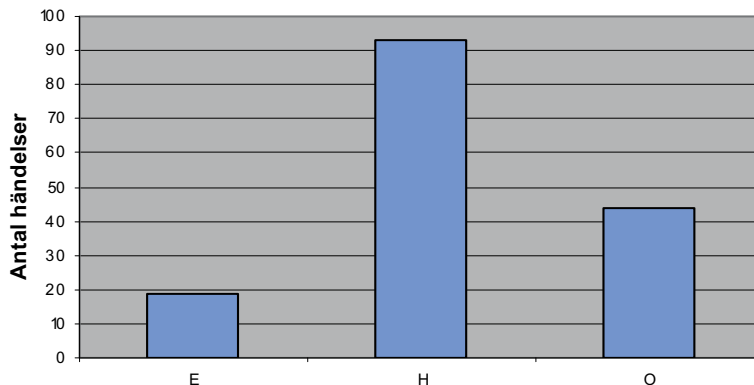
- Miljö (E)
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedur
  - Underhållsschema
  - Driftinstruktion

För nordiska data är dock de enskilda underkategorierna "hårdvarudesign" och "extern miljö" de mest frekventa, vilka står för ca 19 % respektive 16 % av händelserna.

Kopplingsmekanismer, i grupp - nordiska data



Kopplingsmekanismer, i grupp - internationella data



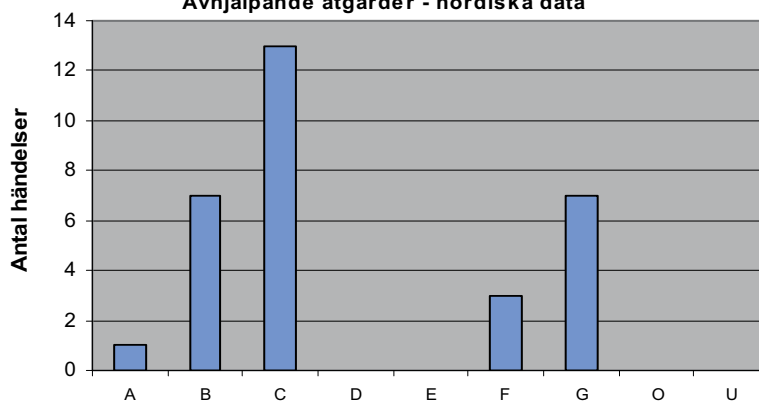
### Avhjälpan åtgärder

Kategorisering av vidtagna åtgärder är gjord enligt följande:

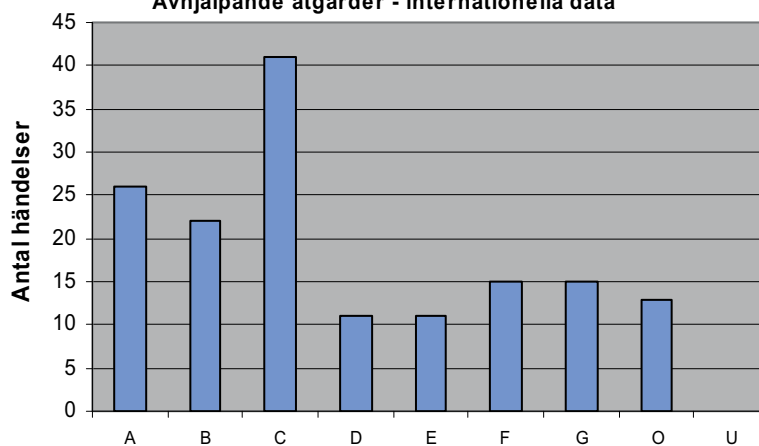
- Administrative control or a procedure control (A)
- Specific maintenance or operational practice (B)
- Design modification (C)
- Diversity (D)
- Functional/spatial separation (E)
- Test and maintenance policies (F)
- Fixing of component (G)
- Other (O)
- Unknown (U)

För både nordiska och internationella data är ”design modification” den vanligaste typen av åtgärd. Kategorin står för ca 42% respektive ca 27 % av händelserna i Norden respektive internationellt. I övrigt, för internationella data, är spridningen ganska stor mellan de olika kategorierna.

Avhjälpan åtgärder - nordiska data



Avhjälpan åtgärder - internationella data

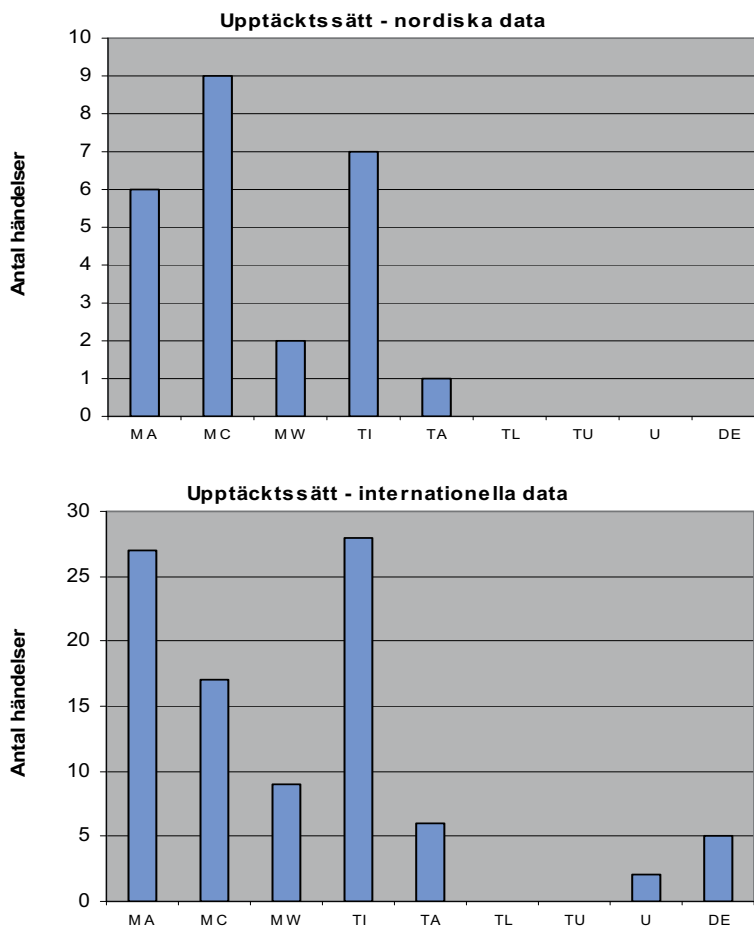


### Upptäcktsätt

De flesta nordiska händelserna är upptäckta genom "monitoring in control room" (MC), "test during operation" (TI) eller "maintenance/test" (MA). Dessa kategorier står för ca 29% respektive ca 23% och ca 19% av händelserna.

- Monitoring on walkdown (MW)
- Monitoring in control room (MC)
- Maintenance/test (MA)
- Demand event (DE)
- Test during operation/annual overhaul/laboratory (TI/TA/TL)
- Unscheduled test (TU)
- Unknown (U)

För internationella data är kategorierna "maintenance/test" (MA) och "test during operation" (TI) de vanligaste, vilka står för ca 18% av händelserna var.



Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffade ICDE-händelser (svenska och/eller utländska).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplings-faktor	Upptäckts- sätt	Komponent- degradering , vektor	Tidsfaktor/ faktor för gemensam orsak
Diesel Generator	4	FS (Failure to start)	H (Human actions, plant staff)	O (Operational, maintenance/ test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	TI/TU	CCII	High

**Händelsebeskrivning:**

At normal start test of the set, didn't the generator of DG210 generate voltage thereby failing to synchronise to the emergency diesel busbar. The diesel generator was declared not operational at 10.26 and the other three diesels were tested. Other failure was detected at DG220, at 11.28 the generator tripped on high voltage.

The reactor power at detection time was 56%. The tech spec requires a cold shut down in then two DG are out of service. Allowable repair time fore one DG is 48 hours. However one hour after the second fault was detected, the first failure was found and repaired. The diesel generator (DG 210) was tested and operational at 12.05. The second DG 220 was declared operational 6 hours later.

DG210 An insufficient torqued screw in a connection block in the field circuit of the generator causing poor connection. The cubicle was changed in October 1996 after a fire.

Circumstances contributing to a failed control by the technician is the fact that the connection block is located lower left corner of the cubicle and the door makes the check difficult.

DG220 The cause was an insufficient torqued screw in a connection block in voltage measuring circuit giving to low voltage to the voltage regulator.

DG230 An insufficient torqued screw in a connection block in the protection circuit's was found during the check. No problem was detected at the earlier test run.

DG240 An insufficient torqued screw in a connection block in the feed circuit for the generator magnetic field was found during the check. No problem was detected at the earlier test run.

The last time the connecting blocks were opened was in 1994.

The blocks are mounted horizontal and opens downwards preventing a accidental closure. In this case the plate didn't fall down. Testing showed a single block needed only half turn of the screw to open and the plate fell down. Mounted together 4 turns needed before the plate fell the friction from the nearby blocks holding the plate.

The use of improper tools could have misled the operator as a wide driver give friction force against the sides of the blocks especially if not hold at a right angle to the screw. The tools were changed before the incident.

Both affected sets were tested 14 respective 7 days before detection at the next test.

No other of the sixteen diesel generators at the plant have had similar problems. For other connection blocks in the unit a test programme applied for the next outage. The procedure for the check after maintenance work was not formalised at the time of the event. Written procedures of checks to do and in which cubicle was the long run corrective action.

**Tolkning:**

Typical misses in maintenance. Even if not the same person torqued the all blocks there is a connection in maintenance procedures, tools and connection block design. The problem with to wide a tool was identified and corrected. Maybe old tools were still in use or an ordinary screwdriver was used. One insufficient torqued connection block have survived 75 tests and the other 15 tests, when fails within 7 days. Vibration or oxidation of contact surfaces could be a contributing factor.

*Tabell 3. Exempel på inträffad händelse.*



Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplings- faktor	Upptäckts- sätt	Komponent- degradering, vektor	Tidsfaktor/ faktor för gemensam orsak
Diesel Generator	2	FS (Failure to start)	H (Human actions, plant staff)	O (Operational, maintenance/ test (M/T) schedule, M/T procedure, M/T staff, operation procedure, operation staff)	MC (Monitoring in control room)	CC	High
<p><b>Händelsebeskrivning:</b></p> <p>Cut signal cable to diesel generators: During the modernizing of the plant, old cables were removed from relay rooms. By accident a cable designed for manoeuvring and indicating the operability of the diesel generators was cut off by a worker affecting both diesel units. The station was in cold shut down mode during outage. When the cable was cut, several alarms occurred affecting the diesel generators. According to Technical Specification one of the two diesels must be operable during current conditions.</p> <p><b>Tolkning:</b> According to Technical Specification one of the two diesels must be operable during current conditions. During the event the busbars were powered by the ordinary grid. In case of an emergency is it possible to manually connect gas turbines to the diesel busbars.</p>							

Tabell 4. Exempel på inträffad händelse.

### Vidare läsning

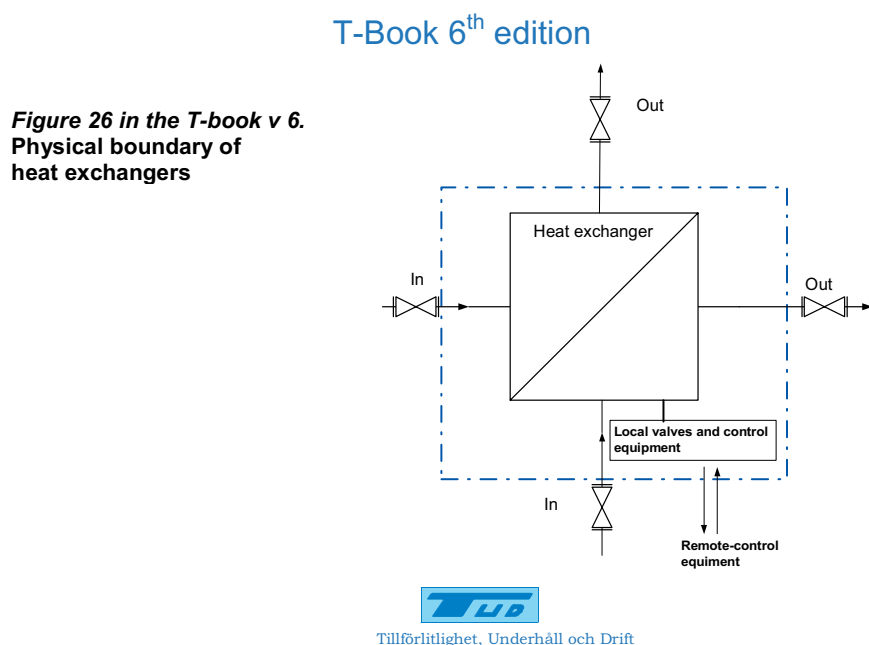
- ICDE General Coding Guidelines [16].
- ICDE Projektrapport för insamling och analys av CCF-data för komponenten [11].
- Arbete genomfört av nordiska arbetsgruppen för CCF-studier (NAFCS) [6].
- Sammanfattande rapport från ICDE [17].

## Bilaga 12: Vägledning – erfarenheter från insamling av CCF-händelser på värmeväxlare (VVX)

### Komponentgruppen värmeväxlare

En värmeväxlare är en enhet, konstruerad för effektiv värmeöverföring från en vätska till en annan, där vätskorna separeras med en solid vägg så att de aldrig blandas. Värmeväxlare används ofta vid kylning, luftkonditionering, rumsuppvärmning och elproduktion där dess typiska funktion är att värma eller kyla.

Komponentgränsen inkluderar själv värmeväxlaren, in och utloppskammare, skal, tuber/plattor, ledningar mellan värmeväxlarens skal och närmaste ventil och lokal ventiler, vilket illustreras nedan.



Figur 1. Komponentgräns, värmeväxlare [22].

Komponenten anses fela då det finns indikering på komponentslitage, mekanisk degradering eller felfungerande och då tillräcklig kylkapacitet inte erhålls vid normalt flöde.

Observationsperiod för insamlade data inom ICDE ges i tabellen nedan.

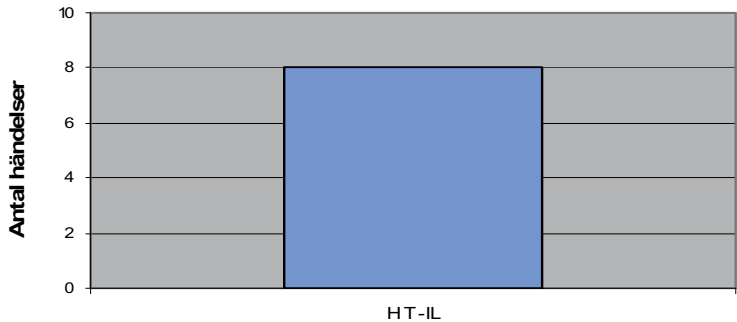
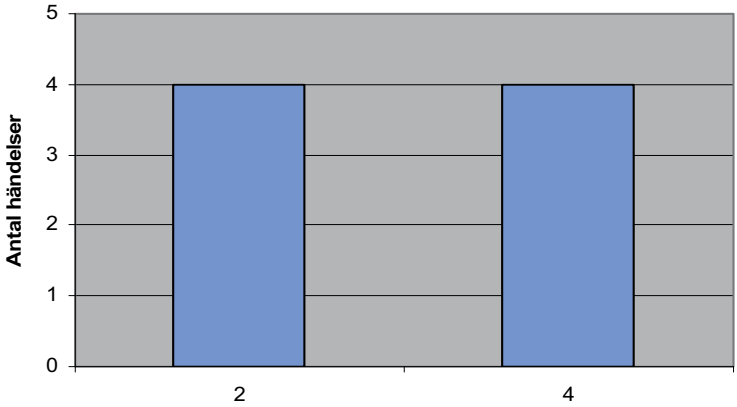
Observerat antal kalenderår	CCCG storlek	Nordiska data	Internationella data (inkl. nordiska)
Observationsperioden för såväl nordiska som internationella data är 1990-01-01 – 2004-12-31	2	-	210,11
	4	-	60,03
	Totalt	-	270,14

<b>Antal observerade CCF-händelser</b>		-	8
--	--	---	---

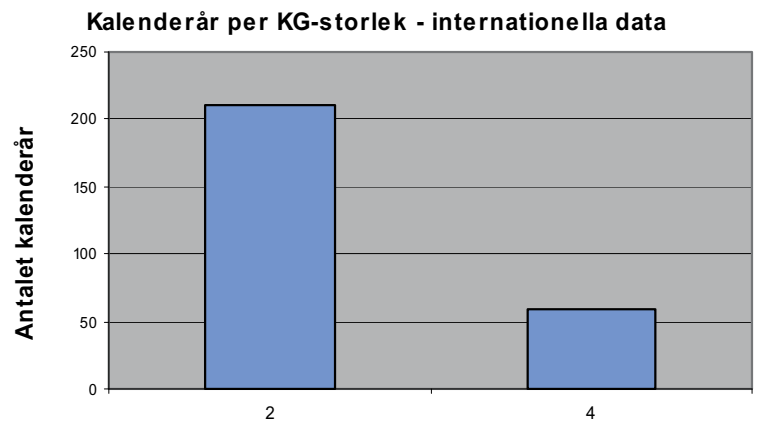
Tabell 1. Observationsperiod.

### Samlad statistik om komponentgruppen

För komponentgruppen, värmeväxlare, finns inga nordiska data i datainsamlingen. I det nedanstående presenteras därför endast internationella data. Även på internationell basis finns dock mycket begränsad mängd data i datainsamlingen, vilket måste beaktas vid tolkning av statistiken för komponentgruppen. Vidare bör det påpekas att av de 8 händelser som finns registrerade förekommer endast komponentdegraderingen "I" ("incipient failure"), dvs fel i begynnande stadie som ännu inte förhindrar komponentfunktionen men kan göra det vid ett påkallat behov.

<p><b>Felmoder</b></p> <p>För komponentgruppen är följande felmoder relevanta i ett PSA perspektiv och därmed tillämpliga vid datainsamling inom ICDE.</p> <ul style="list-style-type: none"> <li>• HT General – Failure of heat transfer (HT)</li> <li>• HT IL – Failure of heat transfer due to internal leakage</li> <li>• HT EL – Failure of heat transfer due to external leakage</li> </ul>	<p style="text-align: center;"><b>Felmoder - internationella data</b></p>  <table border="1"> <caption>Data for Felmoder - internationella data</caption> <thead> <tr> <th>Felmoder</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr> <td>HT-IL</td> <td>8</td> </tr> </tbody> </table>	Felmoder	Antal händelser	HT-IL	8		
Felmoder	Antal händelser						
HT-IL	8						
<p><b>Påverkade komponent gruppstorlekar</b></p>	<p style="text-align: center;"><b>Storlek på exponerad population - internationella data</b></p>  <table border="1"> <caption>Data for Storlek på exponerad population - internationella data</caption> <thead> <tr> <th>Storlek på exponerad population</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>4</td> </tr> <tr> <td>4</td> <td>4</td> </tr> </tbody> </table>	Storlek på exponerad population	Antal händelser	2	4	4	4
Storlek på exponerad population	Antal händelser						
2	4						
4	4						

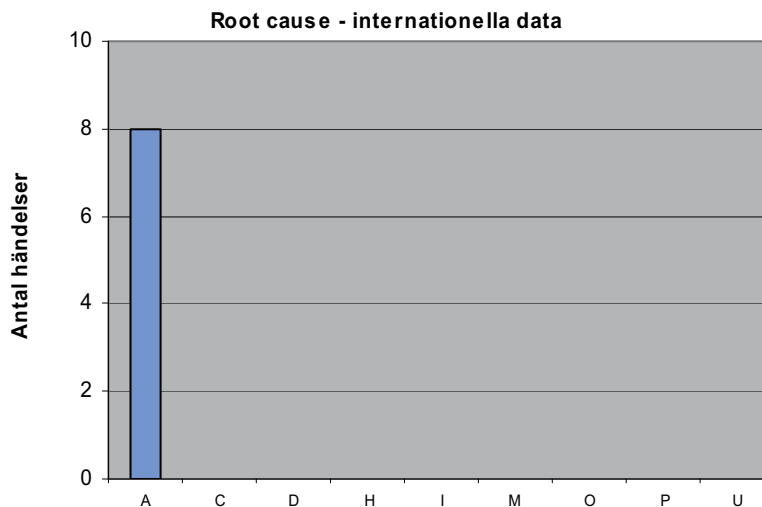
**Akkumulerade  
kalenderår per  
komponentgruppsstorlek**



### Troliga felorsaker

För samtliga rapporterade händelser är felorsaken ”miljöpåverkan, onormal miljö”, enligt följande indelning.

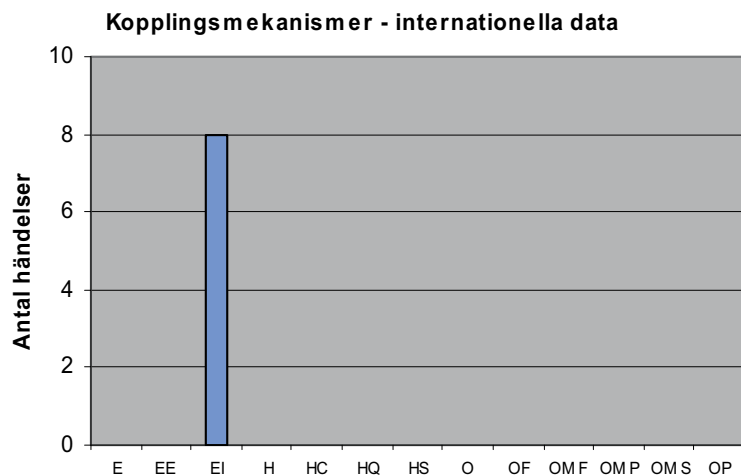
- MTO-relaterade orsaker
  - Operatörsåtgärder, anläggningspersonal
  - Underhåll
  - Brist i instruktioner (tvetydiga, ofullständiga, felaktiga)
- Hårdvarurelaterade orsaker
  - Brist i design konstruktion eller tillverkning
  - Internt (inom komponent)
- Miljöpåverkan, onormal miljö
- Tillstånd hos annan komponent
- Annat/okänt



### Kopplingsfaktorer

Samtliga rapporterade händelser har klassificerats att ha kopplingsfaktorn ”intern miljö”, enligt kategoriseringen nedan.

- Miljö (E )
  - Extern miljö
  - Intern miljö
- Hårdvara (H)
  - Hårdvarudesign
  - Hårdvarukvalitet
  - Systemdesign
- Drift (O)
  - Driftpersonal
  - Underhållspersonal
  - Underhållsprocedur
  - Underhållsschema
  - Driftinstruktion



<p><b>Avhjälpan åtgärder</b> För samtliga rapporterade händelser är genomförd korrigerande åtgärd ”design modification”, enligt följande indelning.</p> <ul style="list-style-type: none"> <li>• Administrative control or a procedure control (A)</li> <li>• Specific maintenance or operational practice (B)</li> <li>• Design modification (C)</li> <li>• Diversity (D)</li> <li>• Functional/spatial separation (E)</li> <li>• Test and maintenance policies (F)</li> <li>• Fixing of component (G)</li> <li>• Other (O)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Avhjälpan åtgärder - internationella data</b></p> <table border="1"> <thead> <tr> <th>Åtgärd</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>A</td><td>0</td></tr> <tr><td>B</td><td>0</td></tr> <tr><td>C</td><td>8</td></tr> <tr><td>D</td><td>0</td></tr> <tr><td>E</td><td>0</td></tr> <tr><td>F</td><td>0</td></tr> <tr><td>G</td><td>0</td></tr> <tr><td>O</td><td>0</td></tr> <tr><td>U</td><td>0</td></tr> </tbody> </table>	Åtgärd	Antal händelser	A	0	B	0	C	8	D	0	E	0	F	0	G	0	O	0	U	0
Åtgärd	Antal händelser																				
A	0																				
B	0																				
C	8																				
D	0																				
E	0																				
F	0																				
G	0																				
O	0																				
U	0																				
<p><b>Upptäcktsätt</b> Samtliga rapporterade händelser har upptäckts genom ”maintenance / test”, enligt följande indelning.</p> <ul style="list-style-type: none"> <li>• Monitoring on walkdown (MW)</li> <li>• Monitoring in control room (MC)</li> <li>• Maintenance/test (MA)</li> <li>• Demand event (DE)</li> <li>• Test during operation/annual overhaul/laboratory (TI/TA/TL)</li> <li>• Unscheduled test (TU)</li> <li>• Unknown (U)</li> </ul>	<p style="text-align: center;"><b>Upptäcktsätt - internationella data</b></p> <table border="1"> <thead> <tr> <th>Upptäcktsätt</th> <th>Antal händelser</th> </tr> </thead> <tbody> <tr><td>MA</td><td>7</td></tr> <tr><td>MC</td><td>0</td></tr> <tr><td>MW</td><td>0</td></tr> <tr><td>TI</td><td>0</td></tr> <tr><td>TA</td><td>0</td></tr> <tr><td>TL</td><td>0</td></tr> <tr><td>TU</td><td>0</td></tr> <tr><td>U</td><td>0</td></tr> <tr><td>DE</td><td>0</td></tr> </tbody> </table>	Upptäcktsätt	Antal händelser	MA	7	MC	0	MW	0	TI	0	TA	0	TL	0	TU	0	U	0	DE	0
Upptäcktsätt	Antal händelser																				
MA	7																				
MC	0																				
MW	0																				
TI	0																				
TA	0																				
TL	0																				
TU	0																				
U	0																				
DE	0																				

Tabell 2. Parameterstatistik.

Nedan ges exempel på inträffad ICDE-händelse (utländsk).

Hjälpssystem / komponent	Storlek på exponerad population	Felmod	Uppskattad, trolig felorsak	Kopplingsfaktor	Upptäcktsätt	Komponentdegradering, vektor	Tidsfaktor/faktor för gemensam orsak
System type: Moderator and auxiliaries (PHWR,...) Component type: HE tube	2	HT-IL (Failure of heat transfer due to internal leakage)	A (Abnormal environmental stress)	EI (Environmental Internal)	MA (Maintenance / test)	II	High

**Händelsebeskrivning:**

Soon after the PNGSB Moderator HXs were put into service they began to fail - the tube material was Incoloy 800 (I-800). Based on eddy current testing and metallurgical examination it was determined that all failure mechanism were caused by under deposit crevice corrosion (lake water being on the shell side of the HXs). In 1985, I-825 was considered the best material and the adopted strategy was to replace all Mod. HXs as soon as possible and then undertake another HX replacement in approx. 10 years. In 1985, U5 and U6 HXs were replaced with I-825 bundles. However, at the end of 1985 it was recommended that the tube bundles for U7 and U8 be replaced with tube bundles manufactured from Sanicro 28 material. Subsequently, the tube bundles of U7 and U8 Mod. HXs were replaced with Sanicro 28 bundles in 1986 and 1987 respectively. Eddy current testing undertaken between 1991 and 1993 found more pitted tubes on the I-825 tubes than on the Sanicro 28 bundles. It was decided that for all subsequent Mod. HX replacements titanium SB-338 Gr. 2 would be used. Between 1994 and 1997 all Mod. HXs, i.e., 5-32110-HX1,2; 6-32110-HX1,2; 7-32110-HX1,2 and 8-32110-HX1,2, were replaced with the titanium tube bundles with tube removal being based on the results of eddy current testing - which was performed on every Mod. HX. For these titanium bundles the current strategy is to inspect U5 HX1 at a frequency of 4 to 6 yrs. Since these last replacements there has been no degradation/failures, with no discernible defects in the last inspection undertaken in 2005.

Tabell 3. Exempel på inträffad ICDE-händelse.

**Vidare läsning**

- ICDE Projektrapport för insamling och analys av CCF-data för komponenten (draft Ralph Nyman, under utveckling) [15].

## Bilaga 13: Identifierade svenska CCF-händelser i ICDE-projektet

I följande avsnitt listas de svenska CCF-händelser som finns identifierade i ICDE-projektet, uppdelat per komponentgrupp. I de fall RO-nr finns i ICDE-databasen anges det i kolumnen ”Event code”, vilket kan nyttjas för vidare läsning av respektive händelse i annan databas.

Se bilaga 1 för tolkning av parametrarnas kodning. Se bilaga 3-12 för information om aktuella felmoder, och tolkning av koder för dessa, för respektive komponenttyp.

### Batterier (BA)

Inga svenska händelser har observerats eller finns registrerade i ICDE-databasen.

### Brytare (BR)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
101152	Sweden\SE-4\3.EB\ODS2\Empty	15698	RO-R1-92/ 015	F0	4	4	CIII	M	OMF	H	B	H	MA



## Centrifugalpumpar (CP)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
3067	Sweden\SE-7\3.BG\CP-HL-Int	3139	R4-RO22-93/R3-RO08-94	FS	3	3	DDW	D	H	H	C	H	TI
3101	Sweden\SE-3\3.BB\CP-MS-SB	3104	RO-02-96/015	FS	2	2	CW	D	HC		B	H	TI
3133	Sweden\SE-6\3.BB\CP-MS-SB	3096	B1-89/30	FR	2	2	DD	A	E	H	G	H	MC
3183	Sweden\SE-3\3.BE\CP-LL-SB	15759	RO-O2-2002/007_012	FS	1	2							
3331	Sweden\SE-10\3.DD\CP-LL-SB	15175	RO R4-98/019	FR	4	4	DDWW WW	D	HC	H	C	H	MA/MW
3425	Sweden\SE-2\3.BG\CP-LL-SB	3032	RO 1-B18/88	FS	2	2	CC	H	O	H	B	H	MC
3497	Sweden\SE-4\3.DD\CP-LL-Int	3121	R1-RO48-93/R1-RO54-93	FR	3	3	IIW	I		M	G	L	MW
3550	Sweden\SE-6\3.BG\CP-LL-SB	3119	B2-91/19	FR	2	2	CC	D	HS	H	C	H	MW
3593	Sweden\SE-7\3.CB\CP-LL-Int	3074	R4-RO026-91	FR	4	4	CCCC	P	O	H	B	H	MC
3593	Sweden\SE-7\3.CB\CP-LL-Int	3092	R4-RO015-94	FR	4	4	CCWW	C	H	H	C	H	TI
3593	Sweden\SE-7\3.CB\CP-LL-Int	3128	R4-RO024-95	FR	4	4	CCWW	H	H	H	A	H	MC
3593	Sweden\SE-7\3.CB\CP-LL-Int	3138	R3-RO014-93/R4-RO012-93	FR	4	4	CCWW	U	H	H	C	H	MC
3682	Sweden\SE-5\3.CA\CP-LL-Int	3069	R2-RO013-90	FS	3	3	CCC	H	O	H	A	H	DE
3794	Sweden\SE-6\3.DD\CP-LL-SB	3065	B2-94/59	FR	3	3	IIW	D	HC	M	C	H	TU
3815	Sweden\SE-3\3.BG\CP-LL-SB	3097	RO-O2-96/043	FS	2	2	CC	H	O	H		H	TI

## Styrstavar och drivdon (CRDA)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
1800	Sweden\SE-2\3.AB\CRDA\1	15851	O1-RO-005/96, -007/96	FCI-M-H/S	3	112	CCC	I	O	H	G	H	DE
1801	Sweden\SE-4\3.AB\CRDA\1	15852	R1-RO-007/95, -011/95	FCI-M-H/S	2	157	CC	M	OMS	M	G	M	DE
1801	Sweden\SE-4\3.AB\CRDA\1	15853	R1-RO-005/94	FCI-M-H/S	2	157	CC	M	OMS	H	G	H	TI
1801	Sweden\SE-4\3.AB\CRDA\1	15854	R1-RO-002/99, -012/99	FCI-B-H/S	2	157	II	D	HC	H	C	M	DE
1801	Sweden\SE-4\3.AB\CRDA\1	15855	R1-RO-001/98, -005/98, -038/98, -040/98, -045/98	FCI-M-H/S	5	157	DDDDD	D	HC	H	C	H	TI
1801	Sweden\SE-4\3.AB\CRDA\1	15856	R1-RO-008/93	FCI-H-H/S	7	157	CCCD DDD	P	OMP	H	F	H	TU/DE
1802	Sweden\SE-6\3.AB\CRDA\1	15857	B1-RO-014/90	FCI-M-H/S	2	109	CC	I	HC	H	G	H	TI
1802	Sweden\SE-6\3.AB\CRDA\1	15858	B1-RO-006/90	FCI-M-H/S	2	109	CC	I	HC	H	G	H	TI
1802	Sweden\SE-6\3.AB\CRDA\1	15859	B1-RO-017/90	FCI-M-H/S	2	109	CC	I	HC	H	G	H	TI
1803	Sweden\SE-8\3.AB\CRDA\1	15860	B2-RO-007/93	FCI-M-H/S	5	109	CCCCC	D	HC	H	C	H	TI
1804	Sweden\SE-3\3.AB\CRDA\1	15861	O2-RO-020/87	FCI-M-H/S	2	109	CC	H	OP	H	B	H	MC
1804	Sweden\SE-3\3.AB\CRDA\1	15862	O2-RO-019/87, -026/88	FCI-H-H/S	34	109	CCIIIIIIII IIIIIIIIII IIIIIIII	D	HQ	H	C	H	DE
1804	Sweden\SE-3\3.AB\CRDA\1	15863	O2-RO-010/85, -016/87	FCI-H-H/S	2	109	CC	D	HQ	H	C	L	DE
1804	Sweden\SE-3\3.AB\CRDA\1	15864	O2-RO-012/88, -013/88, -014/88, -015/88	FCI-M-H/S	9	109	CCCD DDDD	I	HC	M	G	H	DE
1804	Sweden\SE-3\3.AB\CRDA\1	15865	O2-RO-037/88, -039/88, -042/88, -002/89, -007/89	FCI-M-H/S	6	109	CCCCCC	D	HC	H	C	H	TI
1804	Sweden\SE-3\3.AB\CRDA\1	15866	O2-RO-016/93	FCI-M-H/S	2	109	CD	D	HC	H	C	H	DE
1804	Sweden\SE-3\3.AB\CRDA\1	15867	O2-RO-029/99, -030/99, -008/00	FCI-M-H/S	5	109	CCCD	I	HC	M	G	H	DE
1805	Sweden\SE-9\3.AB\CRDA\1	15868	F1-RO-020/94	FCI-M-H/S	2	161	CC	D	EI	H	C	H	DE
1805	Sweden\SE-9\3.AB\CRDA\1	15869	F1-RO-012/93, -016/93, -021/93, -025/93	FCI-M-H/S	4	161	CCCC	D	EI	H	C	M	DE
1805	Sweden\SE-9\3.AB\CRDA\1	15870	F1-RO-025/90, -030/90	FCI-M-H/S	2	161	CC	D	EI	H	C	L	DE
1806	Sweden\SE-11\3.AB\CRDA\1	15871	F2-RO-015/88, -025/88	FCI-M-H/S	2	161	CC	I	EI	M	G	L	TI/DE
1806	Sweden\SE-11\3.AB\CRDA\1	15872	F2-RO-019/91, -023/91	FCI-M-H/S	4	161	CCCC	D	EI	H	C	H	DE
1806	Sweden\SE-11\3.AB\CRDA\1	15873	F2-RO-020/00, -001/01, -004/01	FCI-M-H/S	3	161	III	D	HC	H	C	L	TI
1806	Sweden\SE-11\3.AB\CRDA\1	15874	F2-RO-008/86, -010/86	FCI-M-H/S	2	161	CC	I	EI	H	G	L	DE

## Backventiler (CV)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
6195	Sweden\SE-10\3.BB\CKV Swing	6017	R4 Ro87/16	FC	2	2	CD	I	EI	H	C	H	MA
6223	Sweden\SE-5\3.CA\CKV Lift\3	6036	R2 Ro13/98	FC	3	3	CCC	M	OMP	H	B	H	
6223	Sweden\SE-5\3.CA\CKV Lift\3	15180	RO R2-00/15	FC	3	3	CCI	D	EI	H	G	H	TA
6235	Sweden\SE-5\3.BG\CKV Swing	6077	R2 Ro97/22	FC	11	11	DIWWW WWWWW	D	HC	H	C	H	MA
6256	Sweden\SE-3\3.BE\CKV Lift	6069	RO-O2-1997/025	RC/IL	2	2	DW	D	HQ	H	G	H	TI/MA

## Diesलगeneratorer (DG)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
9057	Sweden\SE-10\3.EF\DG	9001	R4-RO-034/89-R0-040/89	FR	4	4	IWW	D	H	H	C	L	MW/TI
9048	Sweden\SE-11\3.EF\DG	9065	F2-RO-008/92-RO-01092	FR	4	4	CDIW	D	HC	H	C	H	MW/MA
9145	Sweden\SE-12\3.EF\DG	9098	RO-O3-94/004	FR	4	4	DIWW	M	OMP	H	B	L	TI
9041	Sweden\SE-14\3.EF\DG	9016	F3-RO-014/89	FR	4	4	IWWW	D	H	L	C	empty	TA
9207	Sweden\SE-2\3.EF\DG	9004	RO-O1-94/016	FS	2	2	CC	H	O	H	G	H	MC
9207	Sweden\SE-2\3.EF\DG	9039	RO-O1-90/027	FR	2	2	II	D	HQ	H	G	H	TI
9207	Sweden\SE-2\3.EF\DG	9069	RO-O1-94/010	FS	2	2	CW	D	HQ	H	G	H	MC
9207	Sweden\SE-2\3.EF\DG	9101	RO-O1-91/19	FR	2	2	DI	D	HC	H	C	H	DE
9138	Sweden\SE-4\3.EF\DG	15176	RO R1-00/017	FR	4	4	IIIIIIII	H	HS	H	F	H	MW
9139	Sweden\SE-5\3.EF\DG	9100	R2-RO-013/97-R0-014/97	FS	4	4	CCII	H	O	H	F	H	TU/TI
9147	Sweden\SE-6\3.EF\DG	9078	RO-B1-93/022	FR	2	2	CI	H	OF	H	A	H	MC
9147	Sweden\SE-6\3.EF\DG	9085	RO-B1-86/033	FR	2	2	DI	D	HC	H	C	H	MA
9083	Sweden\SE-7\3.EF\DG	9050	R3-RO-003/89-R0-009/89	FR	4	4	IWW	D	H	H	C	L	MW
9083	Sweden\SE-7\3.EF\DG	9081	R3-RO-032/89	FR	4	4	IIII	D	H	L	C	empty	MA
9083	Sweden\SE-7\3.EF\DG	9083	R3-RO-043/94	FR	4	4	CIII	D	HC	L	C	L	TI
9119	Sweden\SE-8\3.EF\DG	9013	RO-B2-91/005	FR	2	2	CI	I	HQ	H	F	H	MA
9143	Sweden\SE-9\3.EF\DG	15177	RO F1-00/010	FR	4	4	IIIIIIII	M	HS	H	B	H	MC

## Nivåmätning (LM)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
16833	Sweden\SE-2\3.IN\7\LM-DTM-MELS	15394	RO-01-93/006	FS	2	2	CC	H	OMP	H	F	H	MA
101104	Sweden\SE-4\3.IN\7\Empty\TMS	15691	R1-RO-023/95	FR Low	6	6	CIWWWWW	I	H	H	B	H	MC
101105	Sweden\SE-4\3.IN\7\Empty\TMS	15690	R1-RO-023/95	FR Low	6	6	CIIIII	D	H	H	B	H	MC
101108	Sweden\SE-4\3.IN\7\Empty\TMS	15693	R1-RO-029/01	FR Low	3	3	DIII	M	OMF	H	F	H	MC
101129	Sweden\SE-4\3.IN\7\Empty\TMS	15692	R1-RO-029/01	FR Low	4	4	DIII	M	OMF	H	F	H	MC
101129	Sweden\SE-4\3.IN\7\Empty\TMS	15694	R1-RO-004/1992	IO	4	4	CDWW	O	HS	H	B	H	MA/MC
101155	Sweden\SE-9\3.IN\7\LM-DTM-M\TMS	15695	RO-98/009	IO	4	4	CIWW	I	O	H	B	H	MC/MA
101203	Sweden\SE-14\3.IN\9\LM General\ELS	15696	RO 1991/03	IO	36	36	CCIIWWWWW WWWWWWW WWWWWWW WWWWWWW WWWWWWW W	I	OMF	H	B	H	MC
101203	Sweden\SE-14\3.IN\9\LM General\ELS	15697	RO 94/014	IO	36	36	CIIIWWWWW WWWWWWW WWWWWWW WWWWWWW WWWWWWW WWWWWWW	D	H	H	C	H	MC

## Motormanövrerade ventiler (MOV)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
12682	Sweden\SE-10\3.BG\MOV Gate	12023	R4 RO 82/05	FO	2	14	CC	P	OP	H	A	H	MC
12171	Sweden\SE-12\3.AF\MOV Ball	15758	RO-O3-2002/008	FO	2	4	D	M	OMF	H	B	H	MA
12171	Sweden\SE-12\3.AF\MOV Ball	15760	RO-O3-2002/008	FO	4	4	CCII	M	OMF	H	B	H	TA
12478	Sweden\SE-3\3.BG\MOV Gate	12070	RO-O2-89/015	FO	4	4	CIWW	H	HQ	H	G	H	MA
12573	Sweden\SE-5\3.BE\MOV Gate	12035	R2 RO 88/08	FO	2	6	CI	P	OMP	H	B	H	MA/DE
12574	Sweden\SE-7\3.DD\MOV Gate	12047	R3 RO 81/21	FO	2	8	DD	P	OMP	H	B	H	TI
12477	Sweden\SE-8\3.FG\MOV Gate	12009	RO-B2-91/008	FO	2	2	CI	I	HC	H	C	H	MC

## Säkerhets- och avblåsningsventiler (SRV)

CCC Group Id	Name	CCF Event Id	Event Code	Failure Mode Id	Number Of Exposed Components	Group size	Component Impairment Vector	Root Cause Id	Coupling Factor Id	Shared Cause Factor Id	Corrective Actions	Time Factor Id	Detection
15261	Sweden\SE-10\3.AF\SV-PIB	15087	R4 Ro99/07	IO	3	3	DDD	H	OMP	H	B	H	TA
15261	Sweden\SE-10\3.AF\SV-PIB	15121	R4 Ro98/21	IO	3	3	DDD	H	OMP	H	B	H	TA
15486	Sweden\SE-10\3.BH\SV-SG\B	15020	R4 Ro95/12	FO	18	18	DDDDWWW WWWWWWW WWWWWWW	H	OMP	H	B	H	TA
15486	Sweden\SE-10\3.BH\SV-SG\B	15141	R4 Ro96/20	FO	18	18	DDDDWWW WWWWWWW WWWWWWW	H	OMP	H	B	H	TA
15487	Sweden\SE-11\3.AF\SV\A.1	15156	F2 Ro96/25	IO	14	14	CCWWWWW WWWWWWW WW	H	H	H	A	H	TA
15325	Sweden\SE-14\3.AF\SV\A.2b	15122	F3 Ro95/10	FO	16	16	CCCWWWW WWWWWWW WWW	C	OMF	H	empty	H	TA
15325	Sweden\SE-14\3.AF\SV\A.2b	15128	F3 Ro99/1	FO	16	16	CCWWWWW WWWWWWW WWWWW	U	U	H	F	H	MA
15355	Sweden\SE-2\3.AF\SV\A.1	15044	O1-1992/027	FO	4	16	CCWW	M	OMP	H	O	H	TA
15355	Sweden\SE-2\3.AF\SV\A.1	15053	O1-97/037	FO	12	16	CDDWWWWW WWWWWWW	U	Empty	H	F	H	TA
15112	Sweden\SE-3\3.AF\SV\A.1	15035	O2-96/010	FO	7	20	CCWWWWWWW	U	Empty	H	C	L	TI
15112	Sweden\SE-3\3.AF\SV\A.1	15104	O2-1992/031	FO	13	20	CCWWWWWWW WWWWWWW	P	OMP	H	F	H	TA
15188	Sweden\SE-5\3.AF\RV-POIE	15178	RO R2-01/012	IL	3	3	DDW	O	OMP	H	O	empty	TA
15188	Sweden\SE-5\3.AF\RV-POIE	15179	RO R2-00/012	IL	3	3	DDD	O	OMP	H	B	H	TA

15462	Sweden\SE-5\3.BH\SV-SG\B	15073	R2 Ro95/25	FO	18	18	DDDDDDDD DDDDDDDD DD	H	OMP	H	B	H	TA
15462	Sweden\SE-5\3.BH\SV-SG\B	15076	R2 Ro97/21	FO	18	18	DDDDDDDD DDDDWWW WWW	H	OMP	H	B	H	TA
15462	Sweden\SE-5\3.BH\SV-SG\B	15119	R2 Ro99/11	FO	18	18	DDDDDDDD WWWWWWW WWW	H	OMP	H	B	H	TA
15462	Sweden\SE-5\3.BH\SV-SG\B	15153	R2 Ro96/28	FO	18	18	DDDDDDDD WWWWWWW WWW	H	OMP	H	B	H	TA
15462	Sweden\SE-5\3.BH\SV-SG\B	15170	R2 Ro98/10	FO	18	18	DDWWWWW WWWWWWW WWW	H	OMP	H	B	H	TA
15502	Sweden\SE-6\3.AF\SV\A.1	15019	B1-1989/026	IO	7	20	IWWWWW	C	HC	H	empty	H	MC
15502	Sweden\SE-6\3.AF\SV\A.1	15127	B1-1998/021	FO	13	20	DDDDWWW WWWWWWW	I	HC	H	C	H	TA
15258	Sweden\SE-7\3.AF\SV-P\B	15012	R3 Ro98/29	IO	3	3	DDW	H	OMP	H	B	H	TA
15258	Sweden\SE-7\3.AF\SV-P\B	15055	R3 Ro99/13	IO	3	3	DDW	H	OMP	H	B	H	TA
15427	Sweden\SE-7\3.BH\SV-SG\B	15120	R3 Ro95/14	FO	18	18	DDDDDDDD DDDDDDDD DD	H	OMP	H	B	H	TA
15427	Sweden\SE-7\3.BH\SV-SG\B	15142	R3 Ro99/08	FO	18	18	DDWWWWW WWWWWWW WWW	H	OMP	H	B	H	TA
15427	Sweden\SE-7\3.BH\SV-SG\B	15144	R3 Ro98/13	FO	18	18	DDDDDDDD DDDDDDWW WWW	H	OMP	H	B	H	TA
15623	Sweden\SE-8\3.AF\SV\A.1	15038	B2-1991/018	FO	13	20	CDWWWWW WWWWWWW	M	Empty	N	F	H	TA

## Värmeväxlare (HE)

Inga svenska händelser finns registrerade i ICDE-databasen. Datainsamlingen har nyligen påbörjats.

[www.ski.se](http://www.ski.se)

**STATENS KÄRNKRAFTINSPEKTION**  
Swedish Nuclear Power Inspectorate

**POST/POSTAL ADDRESS** SE-106 58 Stockholm

**BESÖK/OFFICE** Klarabergsviadukten 90

**TELEFON/TELEPHONE** +46 (0)8 698 84 00

**TELEFAX** +46 (0)8 661 90 86

**E-POST/E-MAIL** [ski@ski.se](mailto:ski@ski.se)

**WEBBPLATS/WEB SITE** [www.ski.se](http://www.ski.se)