Larmsystem i Forsmark

Olle Andersson
Forsmarks Kraftgrupp AB
ÖSTHAMMAR

Föreliggande uppsats identifierar översiktligt dagens kravbild avseende larmsystem i kärnkraftverk. Uppsatsen beskriver också larmsystemet i Forsmark 3. I ett diskussionsavsnitt värderas kravbilden ur ett MTO-perspektiv. I diskussionsavsnittet finns också en värdering av F3:s larmsystem i perspektiv av den identifierade larmbilden.
Uppsatsen är framtagen inom kursen:

Erfarenhetsåterföring och olycksfallsutredning i komplexa system.

IDP-Instituitionen, Mälardalens Högskola, November 2002.

Sammanfattning

I denna uppsats har kravbilden avseende larmsystemens utformning i kärnkraftverk översiktligt analyserats. Detta arbete har skett genom litteraturstudier. En slutsats av dessa studier är att existerande kravbild är i grunden teknisk men den beaktar också ergonomi och människans kognitiva förmåga. Däremot beaktas bara i begränsad omfattning arbetets organisation. Det är författarens uppfattning att man måste ta hänsyn till arbetets organisation vid en värdering av larmsystemens effektivitet vid olika driftlägen. Det är också väsentligt att beakta hur kontrollrumsarbetet är organiserat vid principiella förändringar i den tekniska utformningen av larmsystemet och på motsvarande sätt måste larmsystemets tekniska utformning beaktas vid principiella förändringar av arbetssättet i kontrollrummet.

Den identifierade kravbilden har stämts av mot det larmsystem som finns i block 3 vid kärnkraftverket i Forsmark (F3). Vid denna värdering har arbetssättet vid olika driftlägen beaktats. Författarens uppfattning är att F3:s larmsystem väl uppfyller de i guider, normer och standarder ställda kraven och att den tekniska utformning både uppfyller krav på god ergonomi och är i god harmoni med hur arbetet är organiserat. Oaktat detta finns det alltid utrymme för förbättringar och några rekommendationer lämnas i rapportens diskussionsavsnitt.

Författaren riktar ett stort tack till alla som inspirerat och hjälpt till med faktaunderlag. Ett särskilt tack riktas till Lennart Strandberg för värdefulla kommentarer och kritisk granskning.

Inledning

Konstruktion av nya kärnkraftverk och ombyggnader i befintliga anläggningar styrs idag i hög grad av normer och standarder. Bakgrunden till detta är att normer och standarder är ett bra verktyg för att på ett ordnat sätt att, ofta med bred internationell bas, ta tillvara erfarenheter från tidigare misstag eller positiva erfarenheter från bra konstruktioner och lösningar. Inträffade olyckor (Three Mile Island, Tjernobyl mfl.), expanderad bransch och ökad internationalisering har varit pådrivande faktorer i arbetet med att förändra synen på människans roll i komplexa tekniska system som kärnkraftverk och för utvecklingen av normer och standarder inom detta område. En översiktlig beskrivning av utvecklingen ges i en tidigare uppsats av författaren [1] där även begreppet MTO (Människa-Teknik-Organisation) och Human Factors beskrivs.

Bakgrund till nuvarande kravbild

Larmsystemen i kärnkraftverk är en del av anläggningarnas Instrument och kontrollsystem (I&C-system). De utgör också en del av gränssnittet mellan operatörerna och de tekniska systemen, dvs. en del av det på engelska så kallade Human–Machine–Interface, HMI. I den översiktliga litteraturstudie[1] som genomförts inom ramen för denna uppsats har bara ett fåtal normer och standarder identifierats som explicit behandlar larmsystemen. De krav finns är i huvudsak behandlade som en del i antingen normer och standarder för kärnkraftverkens I&C-system eller i normer och standarder för HMI.

Som framgår av [1] och inledningen till flera standarder har olyckan vid kärnkraftverket Three Mile Island utanför staden Harrisburg i USA, som inträffade i mars 1979, se appendix 3, haft stor betydelse som starthändelse för arbeten som syftar till att förbättra samspelet mellan Människa och Tekniska system inom kärnkraftindustrin. Merparten av de normer och standarder som har betydelse för utformningen av HMI-gränssnittet i kärnkraftverk tillkom under 80-talet som en direkt följd av det fokus på Human Factors som TMI-olyckan innebar. Tyngdpunkten i denna utveckling låg naturligt i USA, dels var det där olyckan inträffade, dels har USA sedan den civila kärnkraften började etablerats varit ledande när det gäller utveckling av normer och standarder allmänt. Många andra länder, däribland Sverige, har i huvudsak tillämpat amerikanska normer och standarder vid nykonstruktionen och vid om- och tillbyggnader. Den här bilden var gällande till mitten av åttiotalet då internationella standardiseringsinstitut på allvar tog sig an kärnkraftens speciella behov. Ett exempel är International Electrotechnical Commission (IEC) som i mitten av 80-talet kom ut med några standarder av stor betydelse för introduktionen av datorer i säkerhetstillämpningar, t.ex. IEC-60880 och senare IEC 964 [2] som behandlar specifikations- och konstruktionsprocessen för kontrollrum. Även Internationella Atom Energi Organet (IAEA) är mycket aktiva och pådrivande när det gäller att omsätta övergripande säkerhetskrav vid konstruktion av I&C-system och HMI. IAEA har dels gett ut grundläggande standarder och normer samt dels ett antal mer fritt skrivna och tolkande handböcker och rapporter med backgrundsmaterial.

Förutom de arbeten som legat till grund för ovan beskrivna utveckling har ett omfattande forskningsarbete bedrivits av OECD inom ramen för The OECD Halden Reactor Project vid Institutt for Energiteknik i Halden Norge. En översiktlig beskrivning av var man inom OECD/HRP står beträffande forskningen inom området ”alarmsystem” är redovisad i Rappor-

[1] Forsmarks Normbibliotek samt en inventering av normer för kontrollrumsutformning som genomfördes inom Vattenfall 1989 [3].

ten ”Recommendations to Alarm Systems and Lessons Learned on Alarm System Implementation”[4].[2] I USA har forskning skett bl.a. vid Brookhaven National Laboratory och andra institut och universitet. Forskningen i Sverige och övriga norden har kanske inte varit så fokuserad på larmsystem men inom området MTO och kognitiv psykologi har forskningen varit omfattande. Detta arbete beskrivs översiktligt i [1].

Kravbild

I detta avsnitt beskrivs sammanfattat och översiktligt några regelverk och standarder som är av betydelse för utformningen av larmsystem.

Svensk lagstiftning

Den svenska lagstiftning, främst SKI:s föreskrift SKIFS 1998:1 [5], innehåller idag inga egentliga tekniska krav. I 2:a kapitlet 3§, punkt 6, finns dock ett övergripande och allmänt krav *att personalen ges de förutsättningar som behövs för att kunna arbeta på ett säkert sätt*. I 3 kapitlet 3§ anges dessutom att *konstruktionslösningarna skall vara anpassade till personalens förmåga att på ett säkert sätt hantera anläggningen samt de driftstörningar och haverier som kan inträffa*. Sedan en tid bedriver SKI ett arbete som skall leda fram till ett antal tekniska ”råd”, allmänna råd till föreskriften om säkerheten i kärntekniska anläggningar, nuvarande SKIFS 1998:1. Dessa allmänna råd skall vara vägledande för hur de svenska kärnkraftanläggningarna bör vara utformade för att möta en internationell kravnivå och som är acceptabel för fortsatt drift en bra bit in på 2000-talet. Dessa råd berör även larmsystemens utformning.

En annan föreskrift[3] som man måste beakta när det gäller datorbaserade larmsystem är Arbetsmiljöverkets föreskrift om "Arbete vid bildskärm". Föreskriften är allmän och gäller alla typer av bildskärmsarbeten. Föreskriften berör dock inte utformningen av larmsystemet som sådant utan mer HMI.

Kommande allmänna råd till SKI:s föreskrift om säkerhet i vissa kärntekniska anläggningar

Utgående från paragrafen i föreskriften som anger att konstruktionslösningar skall vara anpassade till personalens förmåga kommer de nya "allmänna råden" att innehålla ett antal råd som berör kontrollrumsutformning och, inte minst viktigt, råd för hur kontrollrumsarbetet bör vara organiserat. För larmsystemets utformning och arbetets organisation i perspektiv av larmsystemets uppgifter är det primärt följande aspekter som råden tar upp[4]::

Rådrum

Med rådrum avses en konstruktionslösning där anläggningens automatiska funktioner gör att inga Inledande Händelser[5] som kräver aktivering av reaktorskyddssystemet medför krav på omdelbara operatörsingrepp. Vid konstruktionen av Forsmarksreaktorerna har denna så kalla-

[2] Vissa rapporter som ges ut av OECD/HRP i Halden är bara tillgängliga för medlemmar i projektet.
[3] Arbetarskyddsstyrelsens Författningssamling, AFS 1998:5, Arbete vid bildskärm.
[4] Observera att de råd som behandlas inte är exakt citerade utan är sammanfattade och att larmsystemets uppgift är särskilt belyst även om detta system inte nödvändigtvis är omnämnt i rådet.
[5] Med Inledande händelser (Postulated initiating event) avses alla de händelser som medför aktivering av reaktorns skyddssystem eller som medför att reaktoreffekten automatiskt regleras ner för att parera för turbinanläggningen förmåga att kunna ta emot den ånga som produceras i reaktorn.

de rådrumsregel tillämpas och tidsgränsen för operatörsingrepp har där ansatts till ca 30 minuter. Oaktat automatiken är det väsentligt att operatörerna får sådan information att de får en insikt i händelseförloppet och anläggningens status. En viktig aspekt är att operatörerna skall få tid för eftertanke innan konstruktionen ställer krav på manuella ingrepp.

Larmsystemets viktigaste uppgift under ”rådrumstiden” är att signalera till operatörerna att en Inledande Händelse inträffat och vilken denna är. Larmsystemet är direkt olämpligt att använda för operatörerna i deras arbete med att följa händelseförloppet och för att bilda sig en uppfattning om anläggningens status.

Operatörsroll
Allmänt bör anläggningen vara så konstruerad att operatörerna kan övervaka och ingripa när anläggningens automatik inte ger avsedd verkan. Behov av sådana ingrepp bör så långt som möjligt ha förutsätts och vara styrda av instruktioner.

För att tillfredställa ovanstående krav måste alla larm vara kopplade till en instruktionsstyrd aktivitet.

Gränssnittet mellan operatörerna och processen
Gränssnittet mellan operatörerna och processen bör vara konstruerat så att operatörerna ges ändamålsenlig, tillförlitlig och samlad information, tillräcklig för att effektivt kunna övervaka anläggningen och dess driftklarhet. Operatörerna skall dessutom kunna fatta beslut inom tillgänglig tid samt dessutom skall operatörerna få återkoppling på automatiska och manuella åtgärder. Ett lämpligt sätt att utforma larmpresentationen är mönsterigenkänning.

En tolkning av detta råd är att larmsystemet skall vara utformat så att operatörerna med hjälp av larmens placering och typ av presentation (dator, larmslits i panel etc.) får ledning till vilken säkerhetsbetydelse ett larm har och var ett fel finns i anläggningen.

Utvärdering av kontrollrum
I de allmänna råden kommer det att ställas krav på utvärdering av ändamålsenligheten av kontrollrummet och dess olika funktioner, inklusive larmsystemet. Dessutom ställs krav på att ergonomiska och andra förhållanden i samspelet människa-teknik-organisation specificeras och beaktas.

IAEA

Safety Guides
I IAEA:s Safety Standards Series avseende Design[6] behandlas larmsystemets utformning översiktligt i grunddokumentet [6] och mer i detalj i den Safety Guide som berör ”Instrumentation and Control Systems” [7]. I [6] finns ett antal övergripande ”skall-krav” dels i ett avsnitt som behandlar Human Factors och dels i ett avsnittet om I&C. Kraven avseende Human factors innebär sammanfattat:

- ”Operatörsvänlig” och ergonomiskt vettig konstruktion som minimerar risken för att operatörerna skall göra fel. HMI skall vara konstruerat så att operatörerna får tillräcklig och relevant information i alla driftlägen.

[6] Med Design avses i detta sammanhang alla delmoment från idé till driftklar anläggning.

- Systematisk arbetssätt vid konstruktion (se IEC och EUR nedan) inklusive verifiering och validering. Kontrollrumspersonalens olika arbetsuppgifter skall särskilt beaktas.
- ”Rådrumsregeln” skall beaktas.

Kraven avseende I&C-systemets utformning understryker vikten av att det finns tillräcklig instrumentering i kontrollrummet för att operatörerna skall kunna övervaka för säkerheten viktiga parametrar och anläggningens status med betoning på övervakning av säkerhetssystemens status de fysiska barriärernas[7] inegritet. Larmsystemets uppgift är att uppmärksamma operatörerna på avvikelser.
I guiden [6] som behandlar I&C finns ett avsnitt som explicit behandlar larmsystemets utformning. Sammanfattat innebär kraven:

- Larmsystemets uppgift är att göra operatörerna uppmärksamma på att de kan behöva vidta åtgärder för att förhindra ett förlopp som kan hota säkerheten, inklusive att manuellt initiera reaktorskyddsfunktioner, t.ex. att manuellt snabbstoppa reaktorn.
- För säkerheten viktiga larm skall kunna särskiljas. Några olika tekniska lösningar är exemplifierade: Prioritering och filtrering samt gruppering t.ex. genom placering eller ljud- och/eller ljusdifferentiering.

I övrigt ställs ett antal ergonomiska krav avseende larmlampor, blink, kvittering, ljudsignaler etc.

Guiden understryker dessutom att lösningar för att förhindra att operatörerna blir överlastade med larm vid störningar inte får leda till att operatörernas möjlighet att identifiera och lokalisera (bestående) fel går förlorad. Guiden understryker också vikten av att larmsystemet utformas i samklang med underliggande krav på operatörernas arbetsuppgifter.

TECDOC[8]
Förutom i de mer förpliktigande säkerhetsguiderna ges råd och anvisningar i många andra IAEA-dokument. Ett exempel är TECDOC 1252 ”Information integration in control rooms and technical offices in NPP:s” [8]. I denna rapport finns ett relativt omfattande avsnitt med vägledning om utformningen av larmsystem. Förutom övergripande krav anges följande sex konstruktionskrav som förutsättningar för ett ”bra” larmsystem:

1 *The “dark screen” principle is important for obtaining an alarm system that only calls the operator’s attention when something is wrong. This should be the main principle when designing the alarm system. No alarms should be presented when a process part is in a normal state without failures. During normal changes of the process, a number of parameters are changing. As long as the variations are normal with respect to the state of the process, no alarms should be presented. The main goal is to avoid information overload and unnecessary distractions in all states of the process.*

2 *The presentation of alarms should comply with the overall principles defined for the MCR information system and the other workplaces defined.*

3 *Alarms should be readable from a reasonable distance in the MCR. If overview alarms are used, it should be possible to identify them from all locations in the MCR.*

[7] Med fysiska barriärer avses normalt: bränslekapsling, reaktortank, inneslutning och i vissa fall sekundärinneslutning. Se INSAG-10 ”Defence in Depth in Nuclear Safety”.
[8] Se www.iaea.org avseende de olika dokument som IAEA ger ut och deras inbördes hierarki. Från IAEA:s Web-site kan dessutom de flesta TECDOC laddas ner. Övriga publikationer måste beställas.

4 *The alarm system should provide direct guidance to the spatial location of the process section, plant system, etc. in alarmed condition. This can be done, for instance, by a direct reference in a text message for accessing the right format.*

5 *Conventional and screen-based alarms should be presented consistently.*

6 *Alarm acknowledgement should be possible from all locations where alarms are presented. It should be possible to acknowledge alarms in process pictures, alarm lists and from control panels. Acknowledgement should only be performed once for each alarm, even if it is presented at several places. All operators who have access to the alarms should be able to acknowledge the ones pertinent to their process systems.*

NRC[9]/USA

Författaren har inte identifierat en samlad hierarkiskt och tydligt uppbyggd kravbild avseende larmsystem, likartad den som finns t.ex. i IAEA:s guider. Några explicita krav avseende larmsystem finns exempelvis inte i den överordnade kravbilden i den amerikanska kärnkraftlagstiftningen[10]. På lägre nivå, i de ”Process and Guidelines, NUREG” som NRC utgivit, finns dock såväl övergripande som detaljerade tekniska krav väl dokumenterade. Man måste dock beakta att NUREG inte utgivits med syftet att vara guider vid konstruktion (Design) utan syftet är att de skall användas av NRC vid granskning av lösningar, ändringar etc. som kraftindustrin tillställt NRC för godkännande. I praktiken, och kanske särskilt utanför USA, har dock NUREG blivit en sorts defaktostandards även vid nykonstruktion och ändringar. Ordet ”krav” skall i det nedanstående läsas med detta i åtanke. Med sitt upplägg lämpar sig NUREG bra att använda som checklista när man skriver kravspecifikationer, vid konstruktionsgranskning eller vid verifierings- och valideringsaktiviteter (V&V).

Med den modell för tillämpning som redovisats ovan finns ett antal NUREG som kan användas vid olika faser i utvecklingen för av larmsystem och för V&V aktiviteter. De viktigaste NUREG är identifierade och kommenterade i rapporter som togs fram av Carl Rollenhagen 1993 [9] samt i FKA:s första handledning i ergonomi [10]. En av de centrala NUREG som då identifierades var NUREG 700 [11]. Denna guide har sedan dess reviderats varvid två andra, för utformningen av larmsystem viktiga guider inarbetades. Den reviderade NUREG 700 utkom i juni 1996 och inkluderade då bl.a. mycket av det som ingår i NUREG/CR 5908 ”Advanced Human-System Interface Design Review Guide” [12] och NUREG/CR 6105 ”Human Factors Engineering Guidance for the Review of Advanced Alarm System” [13] samt NUREG 711 ”Human Factors Engineering Programme Review Model [14]. Genom revideringen av NUREG 700 har alla den kunskap och erfarenhet som fanns dokumenterad i USA vid mitten av 90-talet integrerats i en sammanhållen guide. NUREG 700 rev1 [15] består av två delar, en ”Process guideline” och en ”Reviewers Checklist”, vardera delen består av ca 500 sidor inklusive appendix och bilagor.

Behandling av larmsystem i NUREG 700 rev 1.

Inledning, sammanfattning och ”executive summary” i NUREG 700 rev 1 behandlar övergripande krav avseende Human Factors mm. på motsvarande sätt som dessa krav är behandlade i IAEA:s dokumentation. Avsnitt 4 i NUREG 700 rev 1 innehåller omfattande ergonomiska

[9] Nuclear Regulatory Commission
[10] 10CFR50 (Code of Federal Regulation), Appendix A General Design Criterion (GDC)

och tekniska detaljkrav explicit för larmsystem. Dessa krav är listade på rubriknivå i appendix 1. Vid läsning av kraven är det högst väsentligt att tänka på att ett larmsystem inte behöver ha alla de funktioner som finns medtagna. Syftet är att ange vad som krävs om larmsystemet har angiven funktion. Eftersom NUREG 700 rev1 är så pass omfattande och heltäckande är den av central betydelse och måste beaktas i arbeten som berör kontrollrumsutformning och HMI.

NUREG 700 rev1 är en av de standarder och guider som legat till grund för de instruktioner som idag styr den ergonomiska utformningen av förändringar och kompletteringar i kontrollrummen i Forsmarksanläggningarna, TIGER [16].

Andra amerikanska normer och standarder

Det finns även standarder utgivna av andra institutioner t.ex. av Institute for Electrical and Electronic Engineering, IEEE, som behandlar utformningen av larmsystem och HMI men ingen av dessa har så central roll som NUREG 700 rev1. En annan NUREG som inte direkt behandlar I&C och HMI men som ändå är av central betydelse är NUREG 800, Standard Review Plan (SRP). NUREG 800 är det dokument som en ny kärnkraftsanläggning i USA skulle granskas mot. SRP används idag som referensdokument och checklista på motsvarande sätt som NUREG 700 rev. 1.

IEC

Inom IEC:s tekniska kommitté TC45 (WG8) har ett arbete pågått för att ta fram en ny standard som riktas direkt mot utformningen av larmsystem: IEC 62241 (draft version) - Alarm information display

Tidigare IEC-standarder som mer eller mindre utförligt behandlar alarmsystem är:

- IEC 964 Design for Control Romm of NPP:s [2]
- IEC 61772 NPP Main Control Room – Application of Visual Display Units (VDU) [17]
- IEC 643 Application of Digital Computers to Reactor I&C [18]

Av dessa har IEC 964 och IEC 61772 ingått i litteraturstudien för denna uppsats. Standarden IEC 643 är indragen av IEC, den publicerades redan 1979. Den innehåller dock en del grundläggande krav varför den också bedömts vara av betydelse för IEC:s fortsatta arbete med den nya standarden, IEC 62241.

IEC 964

I IEC 964 [2] är krav avseende HMI-utformningen samlade. Standarden anger också en metodik, funktionsanalys, för hur man kommer fram till vilka arbetsuppgifter kontrollrumspersonalen skall ha för att kraftverket skall drivas och fungera som avsett. Standarden anger också vilka konstruktionskrav detta medför samt hur HMI behöver organiseras för att effektivt stödja operatörerna. Standarden anvisar dessutom metodik för verifiering och validering (V&V) av HMI. Krav och metodik baseras på ”Human engineering” principer, dock utan att närmare ange var dessa principer är baserade på för "vetenskaplig grund".

Tillika med NUREG 700 rev 1. och IAEA:s guideböcker tar IEC 964 upp arbetsuppgiftsanalys och avstämning av om operatörerna har förmågan att kunna lösa tilldelade arbetsuppgifter. Analysen av operatörerna förmåga inkluderar såväl det tekniska stöd som HMI kan ge och operatörernas kognitiva förmåga. I guiden berörs larmsystemets utformning dels i ett särskilt avsnitt i huvudtexten, dels finns mer detaljerade ”tekniska” anvisningar i ett appendix. Sammanfattat utgör kravbilden en delmängd men en bra sammanfattning av kraven i NUREG 700 rev 1.

IEC 61772

Standarden [17] ger detaljerad teknisk och ergonomisk vägledning när det gäller användningen av bildskärmar i kontrollrum. Standarden kan sägas utgöra en mer detaljerad fortsättning på IEC 964. Beträffande användning av bildskärmar för presentation av larm sägs bland annat:

- Av tillgänglighetsskäl kan det vara lämpligt att presentera viktiga larm både i panel och på bildskärm.
- Vid störningar (förväntade händelser, se ovan) bör både redundans och diversifiering i (larm) presentationen beaktas så att operatörerna inte går miste om väsentlig information p.g.a. ett singulärt fel i presentationssystemet.
- Enbart färg får inte användas som informationsbärare.[11]
- Standarden ger ergonomisk vägledning för hur alfanumerisk information, t.ex. larmlistor skall vara utformade samt hur larm skall presenteras i andra typer av bilder.

Se även vad som sagts tidigare om Arbetsmiljöverkets föreskrift om "Arbete vid bildskärm".

European Utility Requirement (EUR)

Ett arbete som idag och framöver kommer att få stor betydelse är European Utility Requirements [19]. EUR är en allmän europeisk specifikation för ett nytt kärnkraftverk. Som framgår av titeln är EUR ingen norm eller guide, men då kraven är allmänt hållna (kan exempelvis tillämpas för såväl kokar- som tryckvattenreaktorer) och är skrivna med medverkan av alla Europas betydande elkraftproducenter har de fått normativ status. Specifikationen har tagits fram av ett 10-tal europeiska kraftverksägare och andra organ som står kraftindustrin nära. Electricité de France (EdF) har varit och är ledande i arbetet, men alla europeiska länder med kärnkraft är representerade i arbetet. Forsmarks Kraftgrupp AB (FKA) har representerat Sverige och författaren har ingått i den arbetsgrupp som arbetat fram den senaste utgåvan av specifikationerna för I&C.

EUR består av 4 delar ”volymer” där de egentliga kraven avseende reaktorsystem finns i volym 2. I volym 2 ingår även krav avseende ”Instrument and Control and Man-Machine Interface” (I&C och MMI). I&C- och MMI-avsnittet utgör kapitel 10 i volym 2 och i den senaste utgåvan, revision C, innehåller kapitel 10 följande avsnitt:

1. Introduktion.
2. Allmänna principer för I&C

[11] Detta krav kan innebära svårigheter vid presentation av okvitterade larm och kvarstående fel i samma lista.

3. Identifiering av vilka personalkategorier etc. som samverkar med, eller utnyttjar, I&C-systemet.
4. Krav på funktionsanalys mm.
5. Funktionella krav på systemets utformning.
6. Tekniska krav.
7. Krav vid implementering.

EUR-kraven avseende I&C/HMI är i hög grad baserade på IEC-standarder, där IEC 964 spelar en central roll för exempelvis avsnitt 4, krav på funktionsanalys mm. Det enda avsnitt i Det som är innovativt i EUR är kravbildens logiska uppbyggnad och att man i ett separat avsnitt (avsnitt 3) så tydligt identifierar alla som behöver utnyttja och samverka med I&C-systemet. Det är självklart logiskt, att för att kunna analysera alla olika användares arbetsuppgifter och krav på stöd från I&C-systemet, så måste alla användare först identifieras. Då avsnitt 2 innehåller hänvisning om var process- och miljökrav samt alla andra överordnade krav som exempelvis bemanningskrav finns kan man konstatera att hela kapitlet har en attraktiv logisk uppbyggnad uppdelad i fyra steg:

⇒ Identifiera förutsättningar enligt avsnitt 1 (övergripande), 2 (funktionellt) och 3 (användare).
⇒ Analysera och tilldela funktioner enligt metodik anvisad i avsnitt 4.
⇒ Konstruera med hänsyn till analysresultat och EUR:s explicita krav. Dessa krav är angivna i avsnitt 5 (funktionellt) och 6 (tekniskt).
⇒ Utför arbetet, inklusive V&V, enligt de anvisningar och metodik som anges i avsnitt 7.

I avsnittet med tekniska krav finns några övergripande krav och kommentarer som anger hur man anser att arbetet i kontrollrummet skall organiseras och som därför styr kraven vid konstruktion av larmsystemet. Exempel:

Requirement:
Alarm are used for attracting the operators attention to unexpected events, especially to disturbances regarding process control and plant behaviour, requiring an operators reaction (corrective action, need for other personnel's support).

Comment:
The knowledge of the operator's tasks is a basic element to be taken into account in the design of alarms, so that alarms and other information are correctly directed to the appropriate staff. The operator must not be distracted from his main task. In particular attention is drawn to the I&C failures which necessitate a specific analysis to detect those to be considered as real alarms and those to be considered as information directed to the maintenance staff and only to be displayed to the operator at his request.

De tekniska kraven är i övrigt i överensstämmelse med vad som finns i andra normer och krav. EUR hänvisar dessutom till relevanta IEC-standarder, som IEC 964 och IEC 61772.

Kravbilden ur ett forskningsperspektiv

OECD Halden Reactor Project

OECD/HRP har under lång tid bedrivit ett omfattande forsknings- och utvecklingsarbete avseende larmsystem. Det är nog inte fel att säga att OECD/HRP varit banbrytande och ledande när det gäller tekniska lösningar för larmundertryckning, prioritering, filtrering, larmpresentation på bildskärmar etc. OECD/HRP har idag utmärkta hjälpmedel för att kunna bedriva denna typ av forskning och utveckling, dels en forskningsreaktor, dels på bildskärmar simulerade kontrollrum, dels ett virtuell relity (VR) laboratorium där olika kontrollrumsdesigner kan testas utan kostsamma investeringar för varje experiment.

Att redovisa hela OECD/HRP:s arbete och alla resultat från forskning och experiment som berör larmsystem är inte möjligt i denna uppsats. I huvudsak har endast två rapporter ingått i litteraturstudien men författaren har tidigare tagit del av och läst flera andra rapporter utgivna av OECD/HRP. Författaren har dessutom haft förmånen att utbyta många tankar kring larmsystemens utformning med bl.a. Öivind Berg och Andreas Bye. Dessa samtal har varit mycket givande och utbildande för författaren.

OECD/HRP rapport HWR-308 [20] identifierar larmsystemets funktioner avseende att uppmärksamma operatören, att informera operatören samt att ge vägledning om och bekräfta vidtagna åtgärder. Rapporten ger sammanfattat följande rekommendationer:

1. *Alarms should be structured to alert, inform, guide and confirm,*
2. *with removal of unimportant alarms and repetitive alarms cause by noise,*
3. *alarms should be filtered or assigned a dynamic priority,*
4. *ideally no alarms should be presented in normal operation,*
5. *some 'key' alarms should be identified, which warn of conditions of direct threat,*
6. *the key alarms should not be suppressed or filtered,*
7. *two to four levels of priority should be used,*
8. *the chronological order of alarms raised should be displayed.*

Denna kravbild överensstämmer i allt väsentligt med den som finns i andra standarder och guider samt med vad som står i NUREG 700 rev 1. och EUR.

I OECD/HRP rapport HWR-354 [2] sammanfattar Haldenprojektet mycket av den kunskap man samlat under den tid forskning och utveckling av larmsystem skett i Halden. Baserat på denna kunskap har 43 rekommendationer formulerats. Rekommendationerna speglar OECD/HRP nuvarande ståndpunkt beträffande hur ett ”bra” larmsystem skall vara utformat. I appendix 2 redovisas en lista med de 43 rekommendationerna, på rubriknivå översatta till svenska. Rekommendationerna är baserade på en rapport skriven för det Norska Petroleum Direktoratet. Rapporten [21] är tillgänglig för medlemmarna i OECD/HRP.

En kritisk synpunkt på HRP-354 är att den enbart sätter fokus på larmsystemet som enda operatörshjälpmedel för operatörerna vid en störning. I inledningen till rapporten sägs:

The main purpose of an alarm system is to alert the operator if an abnormal situation is about to develop, and to assist him in identifying and correcting the situation.

Most existing alarm systems fulfil their purpose reasonably well if the abnormal situations is a small disturbance. Also, in case of a large disturbance, most existing alarm systems will alert the operator as it should, and many systems will draw his attention to a certain process area. However, if the effect of the root cause is rapidly spreading throughout the plant, the operator is drowned in very many alarms. He gets little help in determining the status of the plant and trying to understand what is happening, as alarms are coming from virtually all parts of the plant. Actually, in many plants it is required that an alarm shall always be acknowledged, and the acknowledgement of a large number of alarms arriving during a short time may absorb a substantial working capacity that could have been spent in a more productive way at such a critical moment. Rather than an alarm-system assisted recovery, you may have an alarm system assisted catastrophe. Most alarm systems therefore fail exactly when they are most strongly needed.

Det första stycket i denna text är oantastlig. Av det andra stycket får man dock intrycket att larmsystemet är den enda informationskällan för operatörerna. Så är inte fallet. Vid en störning finns andra informationskällor som operatörerna inte bara kan, utan skall använda sig av för att bedöma anläggningens säkerhet.

Larmsystemet i Forsmark 3 (F3)

Bland annat i systembeskrivningarna (FSAR[12]) och F3 Kontrollrumsfilosofi [22] beskrivs kraftverkets kontrollrum, arbetets organisation samt larmsystemets utformning. I kontrollrumsfilosofin anges bland annat följande avseende arbetet i kontrollrummet:

- Centrala kontrollrummet (CKR) är i alla driftlägen, inklusive efter ett haveri, driftoperativ ledningscentral.
- Att centrala kontrollrummet är driftoperativ ledningscentral innebär att all verksamhet i driftutrymmen, såväl drift-, underhålls-, ändrings-, bevaknings- och räddningsverksamhet, skall kunna övervakas, ledas och styras härifrån.
- Analys av missöden, haverier eller störningar skall vara möjlig med den information som är tillgänglig i centrala kontrollrummet.
- Vid anläggningens ursprungliga konstruktion och vid ändringar har den så kallade 30-minutersregeln beaktats vilket innebär att alla åtgärder, som krävs inom 30 minuter efter en händelse som kan leda till signifikant utsläpp av radioaktiva ämnen är och skall vara automatiserade.

I F3, och i alla andra svenska kärnkraftverk, styrs operatörernas arbete av drift- och störningsinstruktioner. Dessa instruktioner är verifierade i fullskalesimulatorer. I de svenska kokarreaktorerna (konstruerade och byggda av ASEA-Atom) tillämpas dessutom "rådrumsregeln", se ovan.

[12] FSAR=Final Safety Analysis Report, Säkerhetsredovisning. I FSAR finns dels en allmän del och dels detaljerade systembeskrivningar.

Larmsystemets utformning

Se bild 1 och 2.

Larmsystemet i F3 är i princip oförändrat sedan driftsättningen 1985. Innan kontrollrummet färdigställdes genomfördes utvärderingar baserade på ”walk and talk through” i en mock-up. Principerna dokumenterades i två rapporter [23] och [24]. I samband med provdriften av anläggningen, före och efter laddning, utvärderades arbetet i kontrollrummet, dels av kraftverkets egen personal, dels av SKI. Dessa utvärderingar påverkade både arbetets organisation och larmsystemets utformning. De förändringar som tillkom bestod bl.a. av införandet av stora analoga visarinstrument för visning av för säkerheten väsentliga mätvärden, datoroberoende larm för reaktornivå, datoroberoende presentation av att styrstavarna är i sitt inneläge mm. Även den del av larmsystemet som är realiserad i blockdatorsystemet förändrades, bl.a. tillkom möjligheten att flytta larm mellan två olika kvarstående fellistor, se nedan. Dessa förändringar är baserade på en analys dokumenterad i en rapport [25].

Larmsystemets operatörsgränssnitt utgörs teknisk och funktionellt av följande funktioner:

- **Larmslitsar.** Matta, vita plastlock med ingraverad svart text. Vid larm tänds lampor bakom plastlocket som blinkar tills larmet är kvitterat och som lyser med fast sken så länge felet består. Larmslitsarna är placerade överst i korntrolltavlorna (särskilt fält) och i pulpeterna. I kontrolltavlornas larmslitsar visas endast larm med säkerhetsbetydelse och larm som har betydelse för anläggningens driftklarhet.
- **Bildskärmsbaserade listor.** Dels en okvitterad larmlista där larm som enbart visas via datorsystemet presenteras tills larmet kvitterats, dels en kvarstående fellista där alla felsignaler anslutna till blockdatorn och i stort sett alla fel som signaleras i kontrolltavlornas och pulpeternas larmslitsar presenteras så länge feltillståndet är bestående, dels en händelselista där alla larm och statusförändringar presenteras. Listorna är separata och instruktionsstyrt och uppvalda på vissa bildskärmar. Listorna kan dessutom presenteras på valfri annan bildskärm.
- **Brandlarmssystem.** Vid brandlarm signaleras detta i reaktoroperatörens pulpet varefter (normalt) reaktoroperatören behöver förflytta sig till brandlarmssystemet, som är placerat vid sidan om det utrymme där operatörerna har sina arbetsplatser. Detta är acceptabelt eftersom automatiska brandisoleringsfunktioner och för vissa utrymmen även släckningsinsatser startas automatiskt samtidigt som kraftverkets egen brandstyrka larmas.
- **Ljudsignal.** Vid ett nytt tillkommande larm ljuder en ljudsignal. Signalen är gemensam för alla larm i kontrollrummet.
- **Ledlampstablå och ”storbildsskärmar”.** När ett nytt larm kommer ”leds” operatören till det panelavsnitt, pulpetsektion eller datorsystem (exklusive brandlarmssystemet) där larmet finns och skall kvitteras. Detta sker genom en särskild ”ledlampstablå”. Ledlampstablån är placerad ovanför ett av de centrala panelavsnitten i kontrollrummet och därmed synlig från operatörernas arbetsplatser och vissa av de angränsande utrymmena. Intill ledlampstablån finns en "storbildskärm" som med stora tecken, läsbara på långt avstånd, visar identiteten för de fem senaste kvarstående felen. Presentationen visas en viss tid och raderas därefter. Vid larm kan operatören således inte bara se var larmet kommit utan också vilken identitet larmet har. Med denna information kan ett larms allvarlighetsgrad avgöras. Ledlampstablån är bara användbar vid ”lugn drift” då larmfrekvensen är låg. Vid en störning saknar ledlarmstablån och "storbildsskärmen" funktion.

- **Larm från lokala kontrollrum** presenteras som separata samlingslarm i det centrala kontrollrummet. I många fall registreras och ingår enskilt larm från lokalt kontrollrum i blockdatorsystemets händelse- och kvarstående fellista. Larmstatus i vissa lokala kontrollrum kan även visas på särskilda statusbilder. Avfallsanläggningen och brandlarmsystemet kan i vissa avseenden ses som ”lokala kontrollrum” trots att brandlarmsystemet finns i det centrala kontrollrummet och att avfallsanläggningen kan övervakas, se nedan, och i vissa fall även manövreras från det centrala kontrollrummet.
- **Avfallsanläggningen** i F3 manövreras från ett lokalt kontrollrum men vissa manövrar och övervakning kan ske från en särskild bildskärm i det centrala kontrollrummet. Detta datorsystem är vad avser okvitterade larm och händelseregistrering i princip lika det centrala blockdatorsystemet. Larmlistan är dock inte uppdelad på en okvitterad lista och en kvarstående fellista.

Vid ett nytt tillkommande larm indikeras detta antingen med blinkande lampor i en larmslits eller visas som ett okvitterat larm i listan för okvitterade larm i blockdatorsystemet. Samtidigt som detta sker ges också en ljudsignal. Larm från det lokala kontrollrummet i F3:s avfallsanläggning presenteras också i det centrala kontrollrummet och signaleras på motsvarande sätt som larm i blockdatorsystemet.

Operatören kvitterar larmet, antingen genom att trycka på en kvitteringsknapp i larmat panel- eller pulpetavsnitt eller genom kvittering i det centrala datorsystemet. Om larmet kommer från avfallsanläggningen sker kvittering i detta systems arbetsstation. Brandlarm kvitteras också separat i brandlarmssystemet. Utan att kvittera larmet kan ljudsignalen tystas från valfri plats i kontrollrummet.

Larm för säkerhetsfunktioner

Utlöst säkerhetsfunktion, t.ex. snabbstopp, signaleras med larmlampor i reaktoroperatörens pulpet. Vid utlöst säkerhetsfunktion övergår arbetet till så kallade ”Första kontroller”, se nedan. Vilket eller vilka villkor som utlösts visas i respektive säkerhetskontrolltavla.

Om en del i en säkerhetsfunktion blir blockerad, dvs. förhindrad att fullgöra sin funktion exempelvis p.g.a. fel, larmas detta via särskilda larmlampor (”röda lampor”). Dessa är placerade i en separat larmslits som finns ovanför var och en av de fyra säkerhetskontrolltavlorna.

Ur säkerhetssynpunkt viktiga larm som hör ihop med ett visst kontrolltavelavsnitt visas i ett särskilt fält i aktuellt kontrolltavelfält. Larm i pulpeter är grupperade efter funktion.

Viktiga säkerhetsparametrar: Nivå och tryck i reaktortanken samt reaktoreffekten visas på stora instrument, placerade bredvid ledlampstablån och avläsbara från de flesta platser i kontrollrummet. Denna information visas också i säkerhetskontrolltavlor och i reaktorpulpeten.

Alla viktiga feltillstånd (exklusive vissa typfel och ställverksfel) som larmas med lampa i larmslits presenteras också som kvarstående fel i blockdatorns lista för kvarstående fel. Händelsen, dvs. övergången från felfritt till felande status och tvärtom, registreras i blockdatorsystemets händelselista.

Övriga larm

Övriga processlarm visas som nytillkomna larm i den okvitterade larmlistan i blockdatorsystemet.

Brandlarm visas och hanteras i brandlarmssystemet.

Larm från avfallsanläggningen presenteras i det lokala kontrollrummet i avfallsanläggningen och i en särskild terminal i det centrala kontrollrummet.

Blockdatorsystemets listor

Blockdatorsystemet innehåller tre helt separerade listor som kan visas oberoende av varandra på blockdatorsystemets bildskärmar.

- **Händelselista.** Alla händelser, larm så väl som statusförändringar registreras i den tidsordning de inträffar och presenteras i en händelselista. I denna lista kan operatören sortera och selektera ut den information han är intresserad av. Listan används för att följa ett händelseförlopp, t.ex. vid ett prov och för analys mm. Listan är grön.
- **Okvitterad larmlista.** Larm som inte signaleras i larmslits, som inte tillhör brandlarmssystemet eller avfallsanläggningen (undantaget samlingslarm från bägge systemen) presenteras i blockdatorsystemet i en okvitterad larmlista. Listan innehåller bara okvitterade larm, dvs. larmet tas bort från listan direkt vid kvittering. Vid normal drift är listan tom eller innehåller ett fåtal ännu okvitterade larm. Listan är röd.
- **Kvarstående fellista.** Feltillstånd som är kvarstående visas i en kvarstående fellista. Så snart feltillståndet upphör tas meddelandet bort från bildskärmens lista. Listan innehåller i stort sett alla feltillstånd, oavsett om dessa larmats via kontrolltavlor, pulpeter eller blockdatorsystemet. Undantag är vissa feltyper och feltillstånd i brandlarmssystemet och i avfallsanläggningen. Dessa feltillstånd hanteras i respektive system (undantaget samlingslarm från respektive systemen). Denna lista är gul.

Om operatörerna vet att ett feltillstånd kommer att vara bestående en längre tid kan han överföra denna information till en “Kvarstående fellista B”. Denna lista övervakas normalt inte kontinuerligt varför ett försvinnande feltillstånd från denna lista signaleras till operatörerna som ett okvitterat larm. Operatörerna kan fritt flytta feltillståndsmeddelanden (kvarstående fel) fram och tillbaka mellan listorna.

Arbetssätt vid normal respektive störd drift

Normal drift

Under normal drift görs operatörerna (reaktor- och turbinoperatör) uppmärksamma på tillkommande larm genom ljudsignal, tänd lampa i ledlampstablån, visning av identitet på ”storbildsskärm", blinkande larmslitslampa eller tillkommande okvitterat larm i blockdatorns okvitterade larmlista. Vid brandlarm erhålls tänd larmslits i reaktoroperatörens pulpet och samlingslarm i blockdatorn varefter larmet måste hanteras i brandlarmssystemet.

Efter kvittering och om feltillståndet inte har upphört förblir larmslitsen tänd och en rad tillkommer i blockdatorns kvarstående fellista. Grundprincipen i kontrollrummet är att ingen larmslits skall vara tänd och inget fel skall finnas i kvarstående fellistan. Hur de fel som uppkommer skall hanteras framgår av de systemvisa störningsinstruktionerna. I många fall kan det kräva underhållsinsatser för att undanröja ett feltillstånd. Underhållsinsatserna kan kräva mer eller mindre lång tid att åtgärda. Tiden beror av säkerhetsbetydelse, åtkomlighet, personalresurser, reservdelar, etc. Om operatören vet att en felavhjälpande åtgärd kommer att ta lång tid kan han flytta över det kvartstående felet till lista B.

Den okvitterade larmlista är normalt tom eller innehåller kortvarigt ett fåtal ej kvitterade larm. Den kvarstående fellistan innehåller normalt upp till en sida (~ 30) fel. Att denna lista innehåller så pass många fel beror dels på att många av felen kan kräva insatser av underhållspersonal dels på att olika arbeten i anläggningen kan kräva ingrepp som signaleras som ett feltillstånd.

Åtgärd och respons på tillkommande larm är styrt av instruktioner. Om ett fel uppstår i en säkerhetsfunktion krävs självfallet att detta feltillstånd prioriteras framför ett mer trivialt fel i ett driftsystem. Prioritering av larmen sker dels genom signaleringen: Placering i tavlor och pulpeter, t.ex. ”röda lampor” för signalering av blockerad säkerhetsfunktion, och dels genom de åtgärdsdirektiv som anges i störningsinstruktioner på anläggnings- och systemnivå,

Larmsystemets användning vid störd drift

Vid en störning ändras arbetsmönstret i kontrollrummet. Under ledning av skiftingenjören genomförs ”första kontroller” som innebär avläsning och rapportering av vilken typ av störning som inträffat samt hur anläggningens avställning skett och sker. Under detta förlopp – används inte larmsystemet utan övervakning sker genom observation av ett antal väsentliga parametrar som tryck, nivå, styrstavsläge etc. Arbetet i kontrollrummet följer en i förväg upplagd strategi som finns angiven i Övergripande störningsinstruktioner. Syftet är att klarställa:

- Barriärernas integritet.
- Reaktorskyddssystemets verkställighet av sina funktioner.
- Tillförsel av kylmedel till reaktorn.
- Driftklarhet för aktuell värmesänka (kondensor eller kondensationsbassäng)
- Etc.

I huvudsak sker detta arbete genom avläsning av parametrar i pulpeter och kontrolltavlor samt undantagsvis i blockdatorsystemet. Anläggningens automatik ger normalt ett rådrum på ca 30 minuter innan något ingripande fordras. Baserat på avläst information ges dock operatörerna möjlighet till ingripande enligt de övergripande störningsinstruktionerna. Larmsystemet har i detta skede en underordnad roll.

När störningsförloppet är passerat och anläggningen i säkert läge avseende tryck, nivå och effekt samt att kylning är etablerad finns det anledning för operatörerna att "scanna" igenom den kvarstående fellistan i blockdatorsystemet för att se om något feltillstånd avviker från vad som är normalt i detta tidsläge efter en störning. Detta arbete kräver god anläggningskunskap och erfarenhet eftersom det kan innebära genomgång av ca 10 sidor av fel.

Den okvitterade larmlistan kan innehålla flera hundra larm även vid en förhållandevis ”enkel” störning. Denna lista är därför inte användbar vid och under ett störningsförlopp. När ett säkert driftläge etablerats kvitteras larmen därför ”bort” sidvis genom en särskild sidkvitteringsfunktion.

Diskussion

Normer och standarder värderade ur ett MTO-perspektiv

Vid studier av guider, normer och standarder som berör larmsystem kommer man relativt snart till slutsatsen att de tekniska kraven för dessa system är detaljerat och väl beskriven. När standarder från olika årtal läses parallellt kan man se att de tekniska kraven är baserad på den teknik som varit tillgänglig. Man har trots detta i hög grad tagit hänsyn till ergonomiska krav och krav som har sitt ursprung i människans kognitiva förmåga[13]. NUREG 700 rev 1. är i högre grad frikopplad från tillgänglig teknologi och anger krav som skall tillämpas OM funktionaliteten finns. Guiden anger dock inte alltid att en viss funktionalitet SKALL tillämpas. Rekommendationerna i OECD/HRP:s sammanfattande rapport [4] är också frikopplade från existerande teknologi men anger mer en total idealbild av ett state-of-the-art larmsystem än vad man kan läsa ut ur NUREG 700 rev 1. Ingen av dessa dokument eller andra guider, normer och standarder som ställer krav på larmsystem beaktar HUR arbetet i kontrollrummet är organiserat för att på bästa sätt utnyttja larmsystemet och andra informationskällor för att på det sättet kompensera för ”tekniska och ergonomiska” brister som inte kan lösas med idag tillgänglig teknik.

I guider, normer och standarder som anger och beskriver HUR I&C-system och HMI skall utformas (t.ex. IEC 964 och EUR) finns element som behandlar metodik för hur arbetets organisation skall analyseras. Det saknas dock någon form av sammanknytning mellan denna METODIK och omhändertagande av resultaten vid utformningen av SÅVÄL arbetssätt som teknisk utformning.

Ytterligare en sak som noterats är att ingen av de studerade standarderna, normerna eller guiderna behandlar larmsystem med uppdelad presentation av okvitterade larm och kvarstående fel. Termen "alarm" används sammantaget för både okvitterade larm och kvarstående fel. Även OECD/HRP behandlar dessa skilda signaltyper som ett begrepp.

Slutsatser:

- Vid användning av guider, normer och standarder är det viktigt att beakta arbetssätt och arbetets organisation i kontrollrummet. Det bästa vore om detta var beaktat redan från början i guider, normer och standarder.
- Vid användning av guider, normer och standarder är det viktigt att beakta att dessa dokument inte skiljer på okvitterade larm och kvarstående fel. Det vore önskvärt om så vore fallet.

OECD Halden Reactor Project kommer att ta i drift en ny kokarreaktorsimulator år 2002. Denna simulator, HAMBO, är baserad på Forsmark 3. Halden får då tillgång till en simulator

[13] Se t.ex. Engineering Psychology and Human Performance. Christopher D. Wickens och Justin G. Hollands, Prentice Hall, New Jersey, USA, 1999, ISBN 0-321-04711-7

med delad larmpresentation (okvitterade larm och kvarstående fel). Förhoppningsvis kan detta tillsammans med kunskap om det arbetssätt som F3 använder vid störningar ge positiva inspel till den viktiga forskning som OECD/HRP bedriver.

Värdering av larmsystemet i Forsmark 3.

1998 gjordes en detaljerad genomgång [26] av hur väl F3:s larmsystem uppfyller NUREG 700 rev 1. Slutsatsen är att det inte finns några principiella stora avvikelser. Förutom ett antal mindre avvikelser identifierades, dock två förbättringsförslag:

- Larmsystemet saknar funktionalitet för att på ett bra sätt göra operatörerna observanta på att en ny störning inträffat, överlagrat ett tidigare störningsförlopp.
- Larmfunktionen är inte driftlägesstyrd. Det innebär exempelvis att "röda lampor" signalerar fel i en säkerhetsfunktion som är urdrifttagen eller som naturlig följd av inträffad händelse.

Baserat på analysen från 1998 och egen värdering är det författarens uppfattning att F3:s larmsystem acceptabelt bra uppfyller kraven i NUREG 700 rev 1 och rekommendationerna i OECD/HRP:s rapport HPR-354 [4].

Vid en ytlig genomgång av inträffade händelser har ingen händelse hittats där larmsystemet skulle ha bidragit signifikant eller skulle ha varit den direkta orsaken till någon allvarlig händelse. Ingen händelse har heller hittats där brister i larmsystemet skulle på ett avgörande sätt har förvärrat ett händelseförlopp. Missmatch mellan larmtexter och texter i störningsinstruktioner eller brister i larmtexter och störningsinstruktioner har dock lett till missförstånd och felhandlingar vid något tillfälle.

I hela Forsmark, dvs. inkluderande Forsmark 1 och 2, vars larmsystem byggts om och tekniskt närmats den lösning som finns i F3, finns dock ett antal händelser som kan härledas till brister i larmsystemens utformning.

- Skilda presentationssätt och begrepp i blockdator och brandlarmssystem har lett till att väsentliga fellarm från brandlarmssystemet missats. I dagsläget är denna brist svår att bygga bort då det skulle kräva utbyte av antingen brandlarmssystemet eller blockdatorsystemen. En sådan åtgärd kan inte motiveras ur kostnad/nytta synpunkt. Genomförd åtgärd är utbildning.
- Avsaknad av regler i F1 och F2 mellan larm som riktas till operatörerna och underhållslarm ledde, vid driftsättning efter installation av ny I&C, att larmsystemets funktionalitet till stor del gått förlorad. I någon mån kvarstår dessa brister men ett åtgärdspaket är initierat.
- Tidigare saknades vissa statuslarm från säkerhetssystem i F1 och F2, motsvarande F3:s ”röda lampor”. På grund av detta har man vid något tillfälle missat att någon funktion inte varit driftklar innan man gått vidare med uppstart av anläggningen efter avställning.

Rekommendationer

Den stora mängden larm under avställningar, exempelvis p.g.a. provning och ombyggnader, ökar risken att en störning inte uppmärksammas omedelbart. Viktiga parametrar och signaler döljs då många larm och signaler genereras i provningssyfte.

1. Någon form av operatörsstyrd möjlighet till blockering av larm från en sub och/eller funktion bör övervägas.
2. Driftlägesstyrd blockering av larm som är en normal följd av inträffad händelse bör också övervägas.

Under en större störning är det svårt att upptäcka en ny störning p.g.a. att händelse-, larm-, kvarstående fellista snabbt fylls och att många larm blinkar i kontrollrummet.

3. Larmlogiken och presentationen bör ses över med syfte att underlätta för operatörerna att se och identifiera en ny, överlagrad störning under ett sedan tidigare initierat störningsförlopp.

Många larm i kontrollrummet är "onödiga". När man stoppar en pump kommer kanske ett larm om lågt flöde. Detta är självklart, stoppas pumpen upphör flödet. Detta larm är onödigt. Genom "smart" filtrering av larm kan många sådana onödiga larm filtreras bort.

4. En larmfiltreringsfunktion bör övervägas som filtrerar bort "onödiga" följdlarm.

Larmsystemen innehåller sannolikt larm som inte är av betydelse för operatörerna men som kan vara väsentliga för underhållspersonalen. Larmsystemens texter kan innehålla fel och avvika mot texter i instruktioner och FSAR. Rutiner och regler måste finnas för larmens utformning, vem som är mottagare och för periodiska genomgångar mot instruktioner och FSAR.

5. Blockvisa regelverk behöver etableras som anger vad som skall larmas och hur texter mm. skall se ut och vilken information de skall innehålla.
6. Rutiner behöver etableras för periodisk genomgång av larmtexter mm. för avstämning mot instruktioner och FSAR.

Referenslista

[1] Andersson Olle, MTO-Tillämpning inom svensk kärnkraftindustri. Linköpings Universitet LiTH-IKP-I-263, HT 2000.

[2] Design for Control Rooms of Nuclear Power Plants, IEC 964, International Electrotechnical Commission, 1989.

[3] Rollenhagen Carl, Inventering av normer för kontrollrumsutformning, Vattenfall Rapport PT-89/93.

[4] Sörenssen Aimar et.al, OECD Halden Reactor Project, Report HPR-354, Recommendations to Alarm Systems and Lessons Learned on Alarm System Implementation, november 2001

[5] Statens Kärnkraftinspektions författningssamling, SKIFS 1998:1, Statens Kärnkraftinspektions föreskrifter om säkerheten i vissa kärntekniska anläggningar, beslutade i augusti 1998.

[6] IAEA Safety Standards Series, Safety of Nuclear Plants: Design, No. NS-R-1, Wien september 2000.

[7] IAEA Safety Standards Series, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, No. NS-G-1.3, Wien mars 2002.

[8] IAEA TECDOC 1252, Information Integration in Control Rooms and Technical Offices in Nuclear Power Plants, Wien, november 2001.

[9] Rollenhagen Carl, Inventering av normer för kontrollrumsutformning, Rapport PT-89/93, Vattenfall AB, september 1993.

[10] Rollenhagen Carl och Andersson Olle, Handledning i ergonomi FRIDA, FQ-Rapport 95/30, Forsmarks Kraftgrupp AB, augusti 1995.

[11] Guidelines for Control Room Design Reviews, Division of System Technology, NUREG 0700, U.S. Nuclear Regulatory Commission, 1981.

[12] O'Hara .J.M. et.al., Advanced Human-System Interface Design Review Guideline, NUREG/CR 5908, Brookhaven National Laboratory, 1994.

[13] O'Hara J.M. et.al., Human Factors Engineering Guidance for the Review of Advanced Alarm System, NUREG/CR 6105, Brookhaven National Laboratory, 1994.

[14] Human Factors Engineering Program Review, NUREG 0711, Division of System Technology, U.S. Nuclear Regulatory Commission, 1994.

[15] Human-System Interface Design Review Guidelines, NUREG 0700 Rev. 1, Division of System Technology, U.S. Nuclear Regulatory Commission, juni 1996.

[16] TIGER

[17] Nuclear Power Plants – Main Control Room – Application of Visual Display Units (VDU), IEC 61772, International Electrotechnical Commission, 1995.

[18] Application of Digital Computers to Nuclear Reactor Instrumentation and Control, IEC 643, International Electrotechnical Commission, 1979.

[19] Generic Nuclear Island Requirements, EUR, Volume 2, Chapter 10 Instrument & Control and Man-Machine Interface, Part 1 &2, European Utility Requirements for LWR Nuclear Power Plants, Revision C, April 2001, © 2001 Brittish Energy/plc, Desarrollo Tecnológico Nuclear, S.L., Electricité de France, Fortum & Teollisuuden Voima OY, NRG, SOGIN, Tractebel, UAK, Vattenfall/FKA, Verband der Elekrizitätswirtschaft – VDEW-e V.

[20] Bye Andreas et.al., OECD Halden Reactor Project, Report HPR-308, An Integrated Aalarm System – A Consept Study, 1992

[21] Veland Ö et.al., OECD Halden Reactor Project, Report HPR-679, Useful and Usable Alarm Systems: Recommended Properties, 2001.

[22] Ljungblad Anders et.al., Forsmark 3 – Kontrollrumsfilosofi, F3-Rapport 98/14, Forsmark, januari 1998.

[23] Ingemarsson Karl-Fredrik, Forsmark3 – Bildskärmsanvändning i kontrollrum, KF-Rapport 384/84, Forsmark 1984.

[24] Ingemarsson Karl-Fredrik et.al., Forsmark 3 – Processdatorns roll i kontrollrimsarbetet, KF-Rapport 369/84, Forsmark 1984.

[25] Andersson Olle, Forsmark 3 – Blockdator Händelsehantering, kvarstående fellista, kravspecifikation, KF-Rapport 208/85, Forsmark 1985.

[26] Strandberg Lennart, Forsmark 3 – Utvärdering av alarmsystem F3 kontrollrum, F3-Rapport 98/9, Forsmark 1998.

APPENDIX 1

NUREG 700 rev.1

Human-System Interface Design Review Guidelines, Section 4 Alarms

Krav på rubriknivå (fritt översatta och i vissa fall kompletterade från kravtexten av författaren):

4.1	Allmänna riktlinjer
4.1-1	Bildskärmsbaserade larmmeddelanden.
4.1-2	Funktionalitet vid uppgradering av larmsystem.
4.1-3	Avstämning mot övergripande HMI-krav.
4.1-4	Tillämpning av riktlinjer för granskning av konstruktionen av HMI.
4.1-5	Validering av larmsystem.
4.2	Krav på vad som skall generera larm.
4.2-1	Definition av vilka händelser som skall generera larm.
4.2-2	Tidsaspekter att beakta vid larmning.
4.2-3	Krav avseende ”onödiga” larm, t.ex. ”klapprande reläer”.
4.2-4	Krav på att det inte skall finnas några larm vid normal drift.
4.3	Larmhantering och larmreducering.
4.3-1	Krav på att tillförsäkra operatörernas informationsbehov vid störning med högt larmflöde.
4.3-2	Krav avseende larmreducering (bl.a. krav på validering av valda principer).
4.3-3	Krav på (teknisk) validering av larmsignaler, t.ex. felmärkning vid givarfel.
4.3-4	Krav på filtreringsfunktioner.
4.3-5	Krav på separation mellan larm och händelseregistrering (statusförändringar).
4.3-6	Krav på att kunna identifiera ”utlösande händelse” vid utlösning av reaktor-skyddssystemet.
4.3-7	Krav vid driftlägesstyrd larmhantering.
4.3-8	Krav på hur samma larm men med olika betydelse i olika funktioner skall be-handlas.
4.3-9	Krav på behandling av följdlarm i de fall logik finns för sådan behandling.
4.3-10	Krav på identifiering av oförväntade larm (förutsatt att det finns logik för sådan funktionalitet).
4.3-11	Krav på identifiering av uteblivet förväntat larm (förutsatt att det finns logik för sådan funktionalitet).
4.3-12	Krav på transparens och enkelhet i larmlogik.
4.3-13	Krav på att operatörerna skall kunna analysera ingångssignaler som ger larm.
4.4	Larmprioritering och larmundertryckning
4.4-1	Kriterier för prioritering.
4.4-2	Krav avseende antal prioritetsnivåer.
4.4-3	Krav på åtkomst till undertryckta eller blockerade larm.

4.4-4 Larmfiltrering

4.5 Presentation och visning av larm.

4.5.1 Allmänna riktlinjer för larmpresentation.
4.5.1-1 Presentationsfunktioner
4.5.1-2 Koordinering och samfunktion mellan larmning och händelsehantering.
4.5.1-3 Presentation av prioriterade larm inklusive detaljerad larminformation.
4.5.1-4 Rumsorienterad larmvisning som är synlig för operatörerna oberoende av arbetsplats.
4.5.1-5 Grafik.
4.5.1-6 Kodning.
4.5.1-7 Särskilda krav avseende larmsystem som betjänar fler än ett kärnkraftblock.

4.5.2 Visning av högprioriterade larm
4.5.2-1 Viktiga/betydelsefulla larm
4.5.2-2 Samtidig presentation av högprioriterade larm
4.5.2-3 Kodning av prioritet

4.5.3 Visning av larmstatus
4.5.3-1 Separation mellan kvitterade, kvarstående larm och okvitterade larm.
4.5.3-2 Tillkommande larm.
4.5.3-3 Varselpåkallande av tillkommande nya larm.
4.5.3-4 Kvarstående fel.
4.5.3-5 Larm vid återgång till normalstatus.

4.5.4 Krav avseende larmsystem som betjänar fler än ett kärnkraftblock.
(Ej tillämpligt i Sverige)

4.5.5 Larmmeddelande.
4.5.5.1 Innehåll i larmmeddelande.
4.5.5.1-1 Larminformationens innehåll.
4.5.5.1-2 Larmtexternas utformning.
4.5.5.1-3 Information om från vilken givare eller annat ursprung som larmet har.
4.5.5.1-4 Information om prioritet.
4.5.5.1-5 Börvärden.
4.5.5.1-6 Parametervärden.
4.5.5.1-7 Information om omdelbara operatörsåtgärder sfa ett larm.
4.5.5.1-8 Information om referens till instruktioner.
4.5.5.1-9 Information om referens till annat panelavsnitt, bildskärm eller pulpetsektion.

4.5.5.2 Format
4.5.5.2-1 Format för larmslits.
4.5.5.2-2 Format för bildskärmspresentation och utskrifter.

4.5.6 Kodningsmetoder
4.5.6.1 Allmänt
4.5.6.1-1 Krav avseende lätthet att tolka kodade meddelanden (t.ex. regler för förkortningar).
4.5.6.1-2 Krav avseende metod för kodning, t.ex. färg.

4.5.6.1-3 Krav avseende antal kodningsregler/principer.
4.5.6.1-4 Krav på minimum av komplexitet vid kodning.

4.5.6.2 Ljussignalering.
4.5.6.2-1 Ljussignalering för viktiga larm.
4.5.6.2-2 Redundans vid ljussignalering (blink, konstrastskillnad etc.).
4.5.6.2-3 Blinkfrekvens.
4.5.6.2-4 Ljusstyrka vid halvgenomskinliga larmslitsar.
4.5.6.2-5 Ljusstyrka vid presentation via bildskärm.
4.5.6.2-6 Krav avseende identifiering av färgkodning.
4.5.6.2-7 Krav avseende rumsligt kodade larm (t.ex. viktiga larm på särskild plats).
4.5.6.2-8 Undertryckning av visuell kodning.

4.5.6.3 Ljudsignalering.
4.5.6.3-1 Ljudsignalering för viktiga larm.
4.5.6.3-2 Kodning av ljudsignaler.
4.5.6.3-3 Krav avseende åtskillnad mellan olika kodade ljudsignaler.
4.5.6.3-4 Ljudsignaler för separation av larmstatus.
4.5.6.3-5 Krav på om påminnelsesignal vid automatisk ”larmtystning” efter viss tid.
4.5.6.3-6 Kvittens av ljudsignal (återställning för att tysta larmet)
4.5.6.3-7 Interferens mellan olika ljudsignaler.
4.5.6.3-8 Information om var man ”tystar”/kvitterar viss ljudsigal.
4.5.6.3-9 Ljudstyrka.
4.5.6.3-10 Krav att ljudsignalen skall ha avsedd verkan (att uppmärksamma operatörerna om ett feltillstånd) samtidigt som det inte skapar irritation eller plåga.
4.5.6.3-11 Manuell avstängning respektive möjlighet att justera ljudstyrkan.
4.5.6.3-12 Ljudkälla
4.5.6.3-13 Krav på åtskillnad mellan olika typer av ljudsignaler.
4.5.6.3-14 Krav avseende antal olika ljudsignaler.
4.5.6.3-15 Frekvens.
4.5.6.3-16 Pulskodning.
4.5.6.3-17 Krav avseende antal frekvensmodulerade signaler.
4.5.6.3-18 Krav avseende grundfrekvens för frekvensmodulerade ljudsignaler.
4.5.6.3-19 Ljudmönsterkodning.
4.5.6.3-20 Krav avseende vid kodning genom sammansatta ljudsignaler (frekvens, modulering etc.)
4.5.6.3-21 Intensitetskodning.

4.5.7 Organisation av larmpresentation.
4.5.7.1 Rumslig organisation.
4.5.7.1-1 Funktionell gruppering av larm.
4.5.7.1-2 Separation av funktionella grupper.
4.5.7.1-3 Gruppidentifiering.
4.5.7.1-4 Koordinering vid larmslitsar med flera nivåer och/eller kolumner.
4.5.7.1-5 Antal enskilda larm per larmslitsgrupp.
4.5.7.1-6 Logisk placering av larmslitsar.
4.5.7.1-7 Logisk placering beroende av parameter (tryck, temperatur etc.).
4.5.7.1-8 Benämning av larmslitsgrupper.

4.5.7.2 Larmlista

4.5.7.2-1 Listning enligt prioritet
4.5.7.2-2 Möjligheter att sortera i larmlistan.
4.5.7.2-3 Tomma rader.
4.5.7.2-4 Bildväxling och scrollning
4.5.7.2-5 Krav avseende hantering av ”full larmlista” (overflow).

4.6 Manöverorgan
4.6.1 Allmänna krav
4.6.1-1 Typer av manöverorgan (knappar för tystning av larm etc.).
4.6.1-2 Kodning av manöverorgan.
4.6.1-3 Konsistent utformning av manöverorgan.
4.6.1-4 Separation mellan manöverorgan för slitsar och för bildskärmar.
4.6.1-5 Krav avseende operatörernas möjlighet till otillbörlig påverkan på larmsystemet (t.ex. permanent ”tystning”).
4.6.1-6 Presentation av tillkommande larm vid bildskärmspresentation.

4.6.2 Larmtystningsfunktion.
4.6.2-1 Generell larmtystningsfunktion.
4.6.2-2 Manuell larmtystning.

4.6.3 Larmkvittering
4.6.3-1 Följdfunktion vid kvittering (larmtystning, färgändring etc.).
4.6.3-2 Placering av kvitteringsdon.
4.6.3-3 Kvittering av larmmeddelande.

4.6.4 Återställningsfunktion
4.6.4-1 Krav att återställa larmsystemet i ”okvitterat” läge när larmet försvunnit.
4.6.4-2 Krav avseende manuell återställningsfunktion
4.6.4-3 Krav avseende automatisk återställningsfunktion.
4.6.4-4 Krav avseende placering av återställningsfunktion.

4.7 Karaktäristik för automatiska och dynamiska förändringar av larmsystemets funktion (t.ex. automatisk blockering av larm från avställd anläggningsdel).
4.7-1 Krav avseende automatisk omkonfigurering av larmsystemet (t.ex. sfa driftläge).
4.7-2 Operatörsstyrd omkonfigurering.
4.7-3 Kvittering av omkonfigurering.
4.7-4 Operatörsstyrda larmgränser eller börvärden.
4.7-5 Krav avseende påverkan av operatörsstyrda larmgränser eller börvärden avseende existerande larm.
4.7-6 Övervakning av operatörsstyrda larmgränser eller börvärden.
4.7-7 Krav avseende driftlägesstyrda börvärden.

4.8 Tillförlitlighet, provning, underhåll och felhantering.
4.8.1 Tillförlitlighet.
4.8.1-1 Konstruktionskrav avseende tillförlitlighet.
4.8.1-2 Tillgänglighet avseende bildskärmar.
4.8.1-3 Krav avseende dubbla signallampor i larmslitsar.
4.8.1-4 Felmoder för blinkdon.

4.8.2 Provning.

APPENDIX 1

HRP-354

Recommendations to Alarm Systems and Lessons Learned on Alarm System Implementation

Nedan redovisas på rubriknivå de 35 rekommendationerna som finns i HRP-354 (fritt översatta och i vissa fall kompletterade av författaren):

1. Konstruktionen av larmsystem skall uttryckligen beakta ergonomiska faktorer och människans förmåga.

2. Larmsystemet skall konstrueras för alla driftlägen som kan förekomma.

3. Operatörerna skall dels övas och utbildas i larmsystemets handhavande, dels skall operatörerna ha erforderligt instruktionsstöd för att kunna hantera larmsystemet effektivt.

4. Larmsystemets konstruktion skall baseras på en larmfilosofi (jämför kontrollrumsfilosofi).

5. Larmsystemet skall vara erforderligt dokumenterat samt rutiner och ansvar skall vara tydligt avseende underhåll och utveckling.

6. Det skall vara enkelt för processpecialister att kunna bygga in och underhålla ”kunskap och intelligens” i systemet. Exempel är larmundertryckning och filtrering.

7. Funktionella krav skall anges och vara tydliga. Detta gäller inte bara larmsystem utan I&C allmänt. En av de viktigaste förutsättningarna för att åstadkomma bra systemlösningar är att lägga ner stor omsorg vid framtagningen av funktionsspecifikationer. Bra vägledning finns i IAEA:s TECDOC 1066.

8. Det skall finnas administrativa rutiner för åtkomst till larmsystemet. Vidare skall det finns system för att dokumentera förändringar i systemet.

9. Larmsystemet skall vara feltolerant.

10. Larmsystemets responstid skall inte överstiga 2 sekunder. Tiden mäts från förändring på givarens ingång tills statusförändringen visas i larmsystemet.

11. Säkerhetskritiska larm skall kunna identifieras. Statusinformation och larm från säkerhetskritiska funktioner skall presenteras separerat från annan larminformation och informationen skall alltid finnas tillgänglig och visas.

12. Statusinformation om larmsignaler, t.ex. blockeringar, skall vara enkelt åtkomliga för säkerhetskritiska larm.

13. Varje larm skall kräva en operatörsåtgärd.

14. Larmsystemet skall kunna hantera alla typer av larm från processen, inklusive derivataförändringar, komponentfel etc.

15. Larmsystemet skall kunna generera grupplarm.

16. Alla gränsvärden skall vara baserade på processens krav och de skall vara noggrant dokumenterade under hela larmsystemets livscykel.

17. Det skall vara möjligt för operatörerna att ändra vissa larmgränser.

18. Det skall vara möjligt att filtrera signaler.

19. Larmsignalens korrekthet skall vara möjlig att kontrollera om detta är processtekniskt möjligt. Ett exempel på sådan kontroll är att larm om högt flöde är falskt om pumpen som ger flödet är stoppad.

20. Det skall vara möjligt att sortera, välja ut och gruppera larm.

21. Det skall vara möjligt att undertrycka vissa larm.

22. Larmsystemet skall undertrycka larm istället för att filtrera larmen. Syftet är att ingen information skall gå förlorad.

23. Algoritmer och principer för larmundertryckning skall vara kända av operatörerna.

24. Det skall vara möjligt att prioritera larm.

25. Prioritering skall ske utifrån larmens säkerhetsbetydelse och allvarlighetsgrad.

26. Larm skall prioriteras utifrån den tillgänglig åtgärdstid.

27. Prioritering skall ske på ett sådant sätt att larmsystemets funktion i olika driftlägen inte påverkas negativt.

28. Principerna för prioritering skall vara dokumenterade.

29. Det skall finnas en särskild bildskärm för larmpresentation (main alarm display).

30. Särskilt viktiga larm skall visas på en översiktsbild som alltid är uppvald. Larmen skall åtskiljas genom placering.

31. Det skall finnas en larmlista och en händelselista.

32. Larm skall vara integrerade i processbilder.

33. Det skall vara möjligt att välja listpresentation.

34. Larmprioriteten skall framgå av någon form av kodning.

35. Ljudsignal skall avges vid varje nytt, tillkommande larm.

36. Visuell signal skall visas för varje nytt, tillkommamde larm.

37. Larmtexter skall vara informativa och lätta att förstå.

38. Larmtexterna skall vara lätta att läsa.

39. Nödvändig larminformation skall finnas tillgänglig vid varje arbetsplats.

40. Varje larm skall kräva kvittering.

41. Det skall vara möjligt att ta bort larm från larmlistan.

42. Det skall vara enkelt och gå snabbt att navigera i larmbilder.

43. Det skall finnas störningsinstruktioner för övervakning och åtgärder vid alla kända störningsförlopp. Dessa instruktioner skall vara kända för operatörerna.

APPENDIX 3

Beskrivning av TMI-olyckan i Harrisburg

(Informationen är baserad på en text i publikationen BAKGRUND, Nr 7 1988 samt en artikel av Christer Viktorsson i NUCLEUS 3-4/1999)

I gryningen den 28 mars 1979 stoppades alla turbiner och ordinarie matarvattenpumpar i block 2 i kärnkraftstationen Three Mile Island, nära staden Harrisburg i Pennsylvania, USA. Detta var inget onormalt.
Därefter följde en hel serie händelser av karaktären ”olyckliga omständigheter”. Resultatet blev en totalförstörd reaktor och en uppmärksamhet från allmänhet och press utan motstycke. Långt efter olyckan och förmodligen ännu efter 20 år, är namnen TMI, Three Mile Island och Harrisburg förknippade med föreställningen om att det var en katastrofal olycka som inträffade med stora skador i omgivningen. Sanningen är att de radioaktiva utsläppen var så låga att de helt saknar betydelse ur hälsosynpunkt. Ingen person blev heller skadad av radioaktiva utsläpp.
De tekniska skyddsnäten förhindrade att det blev en olycka med konsekvenser för omgivningen. För befolkningen i närheten av anläggningen blev dock de psykologiska konsekvenserna allvarliga och detta saknar inte betydelse när man skall förklara allmänhetens inställning till kärnkraften.
Händelsen initierade en mängd stora och omfattande utredningar om haveriets förlopp och orsaker. Flera av dessa behandlade mänskligt beteende i komplicerade tekniska processer, vid haverier och under stress. En av de amerikanska utredningarna (den så kallade Kemenykommissionen) riktade stark kritik mot bl.a.:

- Utformningen av driftpersonalens instruktioner
- Operatörernas utbildning
- Kontrollrummets utformning
- USA:s kärnkraftinspektions (NRC) tillsynsverksamhet

Den svenska reaktorsäkerhetsutredningen konstaterade att en del av kritiken gällde specifikt amerikanska förhållanden: relationen mellan kärnkraftföretagen och tillsynsmyndigheten är exempelvis annorlunda än i Sverige. Operatörsutbildningen i USA nådde inte heller upp till den svenska nivån. De svenska kontrollrummen har redan från början haft en mer överskådligt utförande.
Icke desto mindre ansåg reaktorsäkerhetsutredningen att flera åtgärder med anknytning till samspelet *människa – maskin* borde vidtas också i Sverige. Det gällde bl.a. utbildning, processövervakning samt förbättringar av driftrutinerna.
Därutöver ville man införa ännu flera skyddsnät för att lindra konsekvenserna av eventuella haverier (filtrerad tryckavlastning).
I huvudsak genomfördes alla de åtgärder som reaktorsäkerhetsutredningen föreslagit under 80-talet.
Grundorsaken till den stora uppmärksamhet som begreppet människa – maskin fick i utredningen var de tidigare nämnda ”olyckliga omständigheterna”. Personalen gjorde före och under olycksförloppet flera grundläggande fel, beroende på brister i arbetsdisciplin, utbildning och tillgängliga instruktioner. Utöver detta hade kontrollrummet och instrumenteringen stora brister vilket gav möjligheter till misstolkningar och försvårade för personalen att ”göra rätt”.