Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Författare: Tomas Lackman

Forskning

2011:24

Utredning och kartläggning av tillfällen då människan räddat och förbättrat en situation där automatiken inte räckt till eller fungerat fel

Rapportnummer: 2011:24 ISSN:2000-0456
Tillgänglig på www.stralsakerhetsmyndigheten.se

SSM perspective

Bakgrund

Inom kärnkraftsindustrin införs ofta automatiska lösningar i syfte att förbättra riskfyllda situationer och arbetsmoment. Ökad automation innebär en förändrad roll för människan i många system. Det finns ett behov av ytterligare förståelse för vilken påverkan den ökade användningen av automation får på människans möjligheter att agera när problem uppstår.

ÅF har fått i uppdrag att beskriva vilken/vilka som är den/de bakomliggande filosofierna inom kärnkraftsindustrin. Detta innebär en litteraturgenomgång och en beskrivning av state-of-the-art. Utifrån denna har också beskrivits hur människans roll ser ut och hur människan påverkas enligt de automationsfilosofier man identifierat som de rådande.

Syfte

Syftet med uppdraget var att öka kunskapen inom området automation och dess påverkan på människans förutsättningar att agera på ett säkert sätt.

Resultat

ÅF har genomfört en litteraturstudie och beskrivit en aktuell bild över rådande automations-filosofier och på vilket sätt människan påverkas av olika nivåer av automation. De har även kartlagt och beskrivit tre händelser inom kärnkraftsindustrin där människan ingripit och räddat eller förbättrat en situation där automatiken inte räckt till eller fungerat fel.

De händelser som studerats i rapporten visar att människan är en av de vitalaste skyddsfunktionerna i djupförsvaret. För att upprätthålla en hög säkerhet bör det således vara stort fokus på att vårda och upprätthålla förmågan hos människan att rädda dylika situationer. I de studerade händelserna har det funnits möjlighet för människan att ingripa då automatiken fungerat fel eller inte haft tillgång till kraftförsörjning i form av el eller tryckluft. Det bör eftersträvas att människan alltid har möjlighet att ingripa i de fall automatiken inte fungerar.

Behov av ytterligare forskning

I rapporten tar författaren upp möjliga alternativ till fortsatt forskning. SSM ser flera av dessa som intressanta men har i dagsläget inte för avsikt att beställa ytterligare forskning inom området.

Projekt information

Kontaktperson SSM: Per Chaikiat
Referens: SSM 2010/2663

Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Författare: Tomas Lackman
ÅF, Stockholm

2011:24

Utredning och kartläggning av tillfällen då människan räddat och förbättrat en situation där automatiken inte räckt till eller fungerat fel

Rapportnummer: 2011:24 **ISSN:**2000-0456
Tillgänglig på www.stralsakerhetsmyndigheten.se

Denna rapport har tagits fram på uppdrag av Strålsäkerhetsmyndigheten, SSM. De slutsatser och synpunkter som presenteras i rapporten är författarens/författarnas och överensstämmer inte nödvändigtvis med SSM:s.

SSM 2011:24

Innehåll

Bilagor

Sammanfattning

Ökad automation innebär en förändrad/minskad roll för människan i många system. Det finns ett flertal filosofier som ligger bakom automationsförfarandet inom olika industrier, vilka sträcker sig från att automatisera allt i så lång utsträckning som möjligt, via att försöka att få en jämn fördelning mellan människa och maskiner, till att endast stötta människan i enstaka arbetsmoment.

Strålsäkerhetsmyndigheten har gett ÅF i uppdrag att beskriva vilken/vilka som är den/de bakomliggande filosofin/-erna inom kärnkraftsindustrin. Uppdraget innefattar även en kartläggning av händelser där människan räddat en situation eller behövt ingripa för att automatiken inte räckt till, samt en analys av dessa händelser med fokus på att dra lärdomar avseende vilken automationsfilosofi som är lämpligast för att uppnå en hög säkerhet.

I rapporten redovisas tre händelser där människan räddat en situation då automatiken inte fungerat som tänkt: Vandellos, Spanien 1989, Schweiz 1996, och Forsmark 2006. Dessa händelser visar att människan är en av de vitalaste skyddsfunktionerna i djupförsvaret och för att upprätthålla en hög säkerhet bör det således vara stort fokus på att vårda och upprätthålla förmågan hos människan att agera i dylika situationer.

Händelserna påvisar också den potential som finns att förstärka djupförsvaret genom att till fullo utnyttja människans unika förmåga att tänka intuitivt och kreativt, och genomföra åtgärder utan tillgång till externa kraftkällor eller uppgjorda procedurer.

Denna förmåga att rädda situationer påverkas dock av automationsnivån, t.ex. på så sätt att för hög automationsnivå kan leda till bristande situationsmedvetenhet, medan för låg automationsnivå kan leda till alltför hög mental belastning för operatörerna. För att undvika erosion av människans förmåga att ingripa bör förändringar i automationsnivån på kärnkraftverken alltid åtföljas av en analys av påverkan på människan.

För att bättre kunna avgöra effektivitet hos de metoder som finns för bedömning av automationens påverkan på människa föreslås att dessa metoder testas på konkreta frågeställningar inom kärnkraften, i några fallstudier.

Eftersom olyckor består av såväl latenta och direkta orsaker, föreslås studier av också mer vardagliga ingripanden från operatörer för att korrigera automatiska funktioner. Sådana ingripanden i ett tidigt skede kan i det stora hela också visa sig vara viktiga för djupförsvaret om det görs en djupare analys.

Summary

In many systems an increased level of automation implies an altered role for the human. Behind the introduction of new automation lies different automation philosophies which stretches from trying to use as much automation as possible to adding automation only as a support to human tasks in specific situations.

The Swedish Radiation Safety Authority has assigned ÅF-engineering to describe the current automation philosophies within the nuclear industry. The assignment also includes a survey of events in which human involvement was necessary in order to save a situation in which the automation has not been sufficient. The survey also include an analysis of these events focusing on which automation philosophy/level of automation is most appropriate for obtaining a high level of safety.

In the report three events are described in which human involvment has been crucial for the successful outcome of the situation; Spain 1989, Switzerland 1996, Forsmark/Sweden 2006. These events shows that the human is one of the most vital parts of the defense in depth, hence a strong focus should be given to looking after and maintaining human abilities in order for her to be able to act safely in such situations.

The events also show potential enhancement of the defense in depth through making the most of the unique human abilities of intuitive and creative thinking and acting without access to external sources of power or prearranged procedures.

These abilities are affected by the levels of automation, e.g. a too high level of automation can lead to a lack in situation awareness whilst a too low level can lead to too high levels of mental workload for the operators. To avoid degradation in human abilities to safely intervene, changes in automation levels at nuclear power plants should always be preceded by an analysis of its effect on the human in the situation at hand.

In order better determine the efficiency of existing methods for assessing the effects of automation on human operators case studies of nuclear specific cases of automation are suggested.

Since accidents has its origins in latent as well as in direct causes another suggestion for future studies is to look at tasks that operators carry out to correct automatic functions in their everyday work. Such operator interventions in an early stage may also be of great importance for the defense in depth if studied more closely.

1. Inledning

Ökad automation innebär en förändrad/minskad roll för människan i många system. Det finns ett flertal filosofier som ligger bakom automationsförfarandet inom olika industrier, vilka sträcker sig från att automatisera allt i så lång utsträckning som möjligt, via att försöka att få en jämn fördelning mellan människa och maskiner, till att endast stötta människan i enstaka arbetsmoment.

Strålsäkerhetsmyndigheten (SSM) har gett ÅF i uppdrag att beskriva vilken/vilka som är den/de bakomliggande filosofin/-erna inom kärnkraftsindustrin. Detta innebär en litteraturgenomgång och en beskrivning av state-of-the-art. Utifrån denna beskrivs hur människans roll ser ut och hur människan påverkas enligt de automationsfilosofier man identifierat som de rådande. Av denna beskrivning framgår hur bl.a människans förståelse av bakomliggande processer påverkas/ändras, på vilket sätt detta kan ha betydelse vid säkerhetskritiska händelser och vilken påverkan filosofin i förlängningen har på människans möjligheter att ingripa vid händelser då tekniken fallerar.

Uppdraget innefattar även en kartläggning av tre händelser där människan räddat en situation eller behövt ingripa för att automatiken inte räckt till.

Till detta beskrivs översiktligt de krav som kan komma att bli nödvändiga att ställa på framtida utrustning då automatiken inte fungerar, beaktande operatörernas höga stressnivåer vid sådana situationer.

Området är stort och innehåller mycket outforskad mark, varför förslag på fortsatta problemområden utgör en del av slutsatserna av arbetet.

Litteraturstudien över automationsfilosofi har utförts genom att söka på olika kombinationer av uttryck relaterat till automation och human factors i databaserna Science Direct och Google Scholar, samt i IAEA:s katalog. Det material som redovisas i denna rapport är baserat på de mest refererade och utifrån frågeställningen mest relevanta artiklarna.

Mycket av den litteratur som är publicerad inom området är av generell karaktär, och inte branschspecifik för kärnkraften utan har kanske snarare sitt ursprung inom flygindustrin och liknande. Denna rapport är därför också förhållandevis generell i sin beskrivning av automationsfilosofier, utan att gå in i detalj kring hur specifika funktioner på kärnkraftverken är automatiserade.

Händelser där människan räddat en situation eller behövt ingripa för att automatiken inte räckt till har identifierats genom att söka bland publikationer på SSMs hemsida och genom att diskutera med personer engagerade i utbildning och erfarenhetsåterföring nationellt och internationellt inom kärnkraftsbranschen för att med hjälp av dem få förslag på illustrativa exempel.

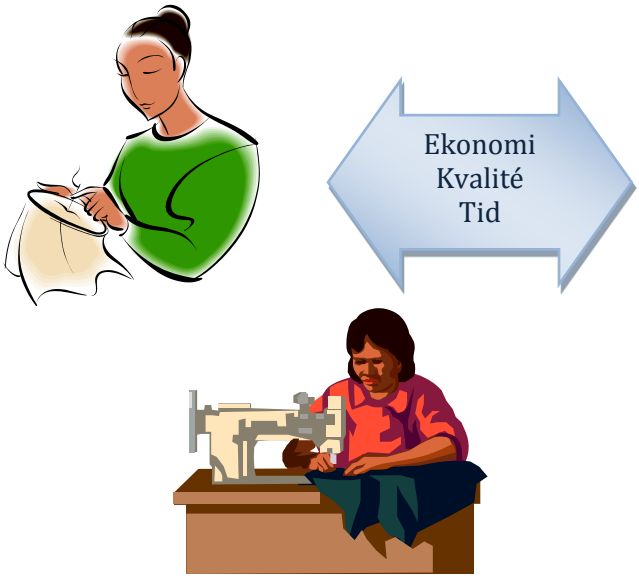
2. Automationsfilosofier

I detta avsnitt definieras först vad som avses med begreppen automation och automationsfilosofi. Detta följs av en kort beskrivning av de generella drivkrafterna bakom automatisering i produktionssystem. Sedan följer en beskrivning av krav och riktlinjer avseende automationsprinciper från IAEA, samt ett exempel från svensk kärnkraft. Därefter beskrivs vilken inverkan olika automationsprinciper har på människans roll och vilken påverkan detta har på människans förutsättningar att hantera en situation där automationen inte räcker till.

Automation har definierats som en anordning eller ett system som utför en funktion som helt eller delvis skulle kunna ha utförts av en människa (Parasuraman et al, 2000). Valet av vilka funktioner som skall utföras av maskin respektive människa kan ske på flera sätt. I denna rapport används begreppet automationsfilosofi för den bakomliggande tanken bakom detta val.

Alltsedan människan började använda de första redskapen har teknikutvecklingen lett till att automationsgraden successivt ökat. Detta har å ena sidan förenklat människans liv på många sätt, men samtidigt lett till att vissa kunskaper gått förlorade.

Idag är *ekonomi, kvalité och tid* starka drivkrafter inom de flesta verksamheter. Dessa tre faktorer är också i många fall den bakomliggande drivkraften bakom valet mellan automation och människa.



Genom att automatisera uppgifter som tidigare utförts av en människa är det möjligt att minska personalkostnader. I detta fall påverkas valet mellan maskin och människa av faktorer som installations- och driftskostnader å ena sidan, och lönekostnader å andra sidan. Ur det ekonomiska perspektivet är

det uppgifter som utförs sällan och är komplicerade att automatisera, som lämnas till den mänskliga operatören.

Eftersom en och samma maskin kan arbeta 24 timmar om dygnet sju dagar i veckan innebär automation i många fall en möjlighet att öka repeterbarheten i ett arbetsmoment och på så vis uppnå en jämnare kvalité. Automatiserade maskiner kan i många fall utformas för att genomföra arbeten med en precision som en människa inte kan klara. I andra fall, t.ex. då uppgiften kräver kreativitet och problemlösning, är det svårt att med hjälp av automation uppnå en kvalité som motsvarar det mänskliga utförandet.

I jämförelse med en dator är en människas förmåga att på kort tid samla in och bearbeta data begränsad. Muskelstyrkan och snabbheten hos en människa är också begränsad i jämförelse med maskinernas. Genom en automatiserad process kan arbetsmoment genomföras på kortare tid, och produktiviteten öka.

Vid sidan om drivkrafterna ekonomi, tid och kvalité påverkas valet av automatisering även av faktorer som *säkerhet, arbetsmiljö och ergonomi*.

Inom verksamheter med en hög risk, såsom kärnkrafts-, flyg- och processindustrin är säkerheten överordnad ekonomi, tid och kvalité. Inom dessa branscher styrs valet av om en uppgift ska utföras av en människa eller maskin också av vilken lösning som ger en minimal eller åtminstone acceptabel risk.

2.1. Internationella riktlinjer inom kärnkraftsbranschen

Inom kärnkraftsbranschen avgörs valet att automatisera en funktion istället för att låta en människa utföra den utifrån vad som bedöms ge den högsta säkerheten. IAEA publicerar både krav och allmänna råd avseende automationsfilosofi. Kraven finns publicerade i ”Safety of Nuclear Power Plants: Design”, IAEA Safety Standard Series (2000) och de allmänna råden i ”Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook”, IAEA (1999).

Dessa krav och riktlinjer är i huvudsak inriktade på säkerhetskritiska funktioner. Driftsfunktioner, som inte har betydelse för säkerheten är inte reglerade på samma sätt.

De krav som är gällande kan sammanfattas enligt följande:

- Anläggningen ska vara användarvänlig, bland annat på så vis att konsekvensen av möjliga mänskliga fel ska vara begränsad.
- Vidare anges att det skall finnas en tydlig distinktion mellan vilka funktioner som skall skötas av operatören och vilka funktioner som ska skötas av det automatiska systemet.
- Människan i systemet har två roller: dels systemhanterare, dels utrustningsoperatör. I rollen som systemhanterare ska hon få tillgång till den information som behövs för att kunna över-

vaka att automatiska säkerhetsfunktioner utförs som de ska. I rollen som utrustningsoperatör ska hon få tillgång till nödvändig information för att kunna initiera säkerhetsfunktioner.

- Kraven på det automatiska säkerhetssystemet är att hantera förutsedda scenarier på egen hand, utan ingripande från människan i det korta perspektivet. Syftet med detta är att skapa rådrum för operatören (30 min), och på sätt bland annat undvika förhastade slutsatser och ogenomtänkta ingripanden.
- Under rådrumstiden ska operatören dock ha möjlighet att följa åtgärder och effekter av det automatiska säkerhetssystemet.

Ursprunget till filosofin bakom dessa krav kan spåras i de incidenter som inträffat inom branschen, och den samlade driftserfarenheten från kärnkraftsverk runt om i världen. Mycket av denna internationella erfarenhet som ligger till grund för IAEAs krav avseende balansen mellan människa och maskin finns samlade i ”The Role of Automation and Humans in Nuclear Power Plants” (IAEA, 1992). I denna rapport redovisas vilka automationsfilosofier som varit rådande under utvecklingen av den moderna kärnkraften i olika länder.

Boettcher (IAEA, 1992) anger att det efter händelserna vid TMI och Tjernobyl funnits en tendens att öka automatiseringen och att begränsa operatörernas möjligheter att stoppa de automatiska säkerhetsfunktionerna. Den bakomliggande drivkraften bakom ökad automatisering i detta fall är att det annars finns en risk att operatörerna agerar på ett oförutsett sätt, vilket kan leda till oförutsedda scenarion.

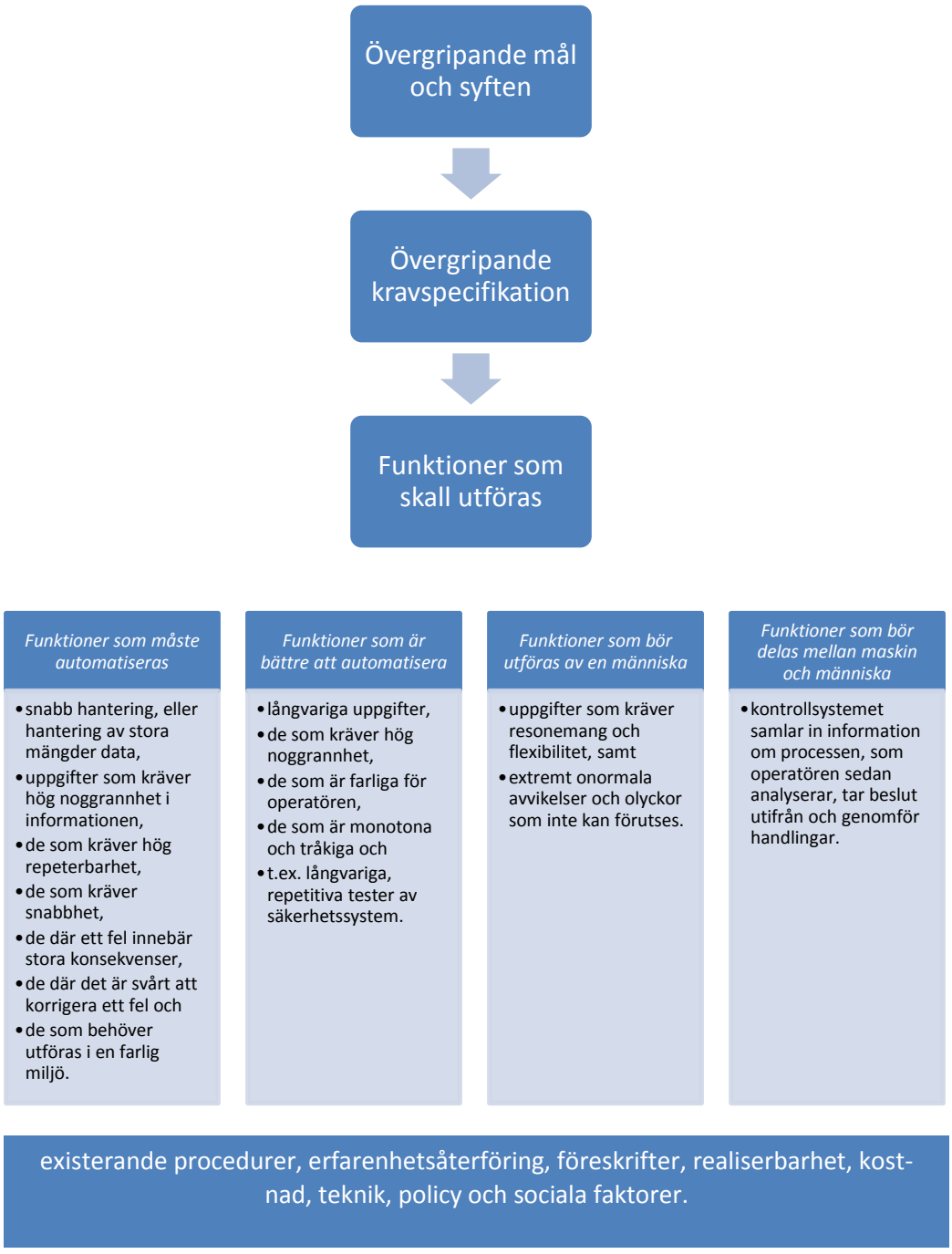
En annan faktor som drivit på automatiseringen är teknikutvecklingen. De ursprungliga verken var byggda med stora säkerhetsmarginaler och kördes med konstant kraftproduktion (IAEA, 1999). Dessa äldre verk har moderniserats för att levererar högre effekt, och med större möjlighet att variera effektuttaget. För att uppnå detta krävs en ökad automatisering i kontrollsystemen.

En tidig metod för att allokera uppgifter mellan människa och maskin under kärnkraftsutvecklingen var att använda en så kallad Fitts list, efter Fitts et al (1951). Enligt denna metodik allokeras en uppgift till en människa alternativt maskin utifrån vilka starka sidor som människor respektive maskiner har. Fitts list i Tabell 1 anger starka och svaga sidor hos människor respektive maskiner.

Tabell 1. Fitts lista över starka och svaga egenskaper

Människa	Maskin
+ En kanal	+ Flera kanaler
- Begränsad kapacitet att hantera information	+ Hög kapacitet
- Dålig på beräkningar	+ Utmärkta beräkningsfunktioner
- Begränsad tillförlitlighet	+ Hög tillförlitlighet kan åstadkommas
- Begränsad repeterbarhet för snabba hög-precisionsarbeten	+ Hög tillförlitlighet och kontinuerliga funktioner
+ Långsam nedbrytning av funktion	- Plötslig förlust av funktion - Redundans nödvändig
+ Bra långsiktigt minne i vissa fall	+ ”Obegränsad” minneskapacitet
- Relativt dåligt kortminne	+ Snabb åtkomst till minne
+ Bra på att korrigera egna fel	- Behöver ett separat system för att korrigera fel
+ Mönsterigenkänning kan förenkla komplexa problem	+ Behöver i många fall exakt programmering för att känna igen en situation, numer finns dock avancerade mönsterigenkänningssystem
+ Klarar lösa arbetsbeskrivningar, flexibel	+ Hög repeterbarhet, behöver en exakt arbetsbeskrivning
+ Kan generalisera och göra induktiva beslut	- Effektiv inom snäva ramar
+ Kan hantera stor arbetsbelastning under kortare perioder	+ Robust mot stor arbetsbelastning, om den är konstruerad för det

Den senaste metodiken som föreslås i IAEAs allmänna riktlinjer, baseras till största del på IAEAs rapport från 1992. Först identifieras övergripande mål och syften. Utifrån dessa identifieras en övergripande kravspecifikation för systemet. Därefter identifieras de funktioner som skall utföras. Dessa funktioner allokeras sedan i ett första steg enligt följande schema:



Faktorer som tas hänsyn till vid allokeringen inkluderar: existerande procedurer, erfarenhetsåterföring, föreskrifter, realiserbarhet, kostnad, teknik, policy och sociala faktorer.

Den första allokeringen utvärderas sedan med avseende på procedurer, personal, utbildningsbehov, gränssnittsfrågor och i en analys av operatörernas arbetsbeskrivning. Därefter modifieras allokeringen eventuellt för att bättre matcha systemets behov, och uppnå en optimal lösning ur ett systemperspektiv.

En fallgrop som författarna noterat med denna allokering av uppgifter till människan är att uppgifter riskerar att fördelas till människan av bekvämlighet och ekonomiska skäl, i de fall det är svårt att specificera eller automatisera en uppgift.

2.2. Exempel från svensk kärnkraft

För att undersöka vilken automationsfilosofi som gäller vid svenska kärnkraftverk har ett stickprov i form av ett studiebesök genomförts hos ett kärnkraftsverk i Sverige

Från verket deltog Manager Electrical and I&C Engineering och Senior I&C Engineer vid besöket. Dessa har båda lång erfarenhet av styrsystem i kärnkraftverk och var båda med vid moderniseringen av styrsystemet vid en av kärnkraftsverkets reaktorer. En telefonintervju med MTO-funktionen vid verket genomfördes också.

Avseende säkerhetsfunktioner är de flesta funktioner, med några få undantag, helautomatiserade utan möjlighet för operatören att ingripa. Exempelvis är säkerhetsfunktionen för att isolera en reaktor genom att stänga ventilerna näst intill helautomatiserad. Operatören har viss möjlighet att ingripa, men endast om vissa villkor avseende mätvärden på givare är uppfyllda. Valet under vilka omständigheter som operatören kan ingripa är styrt i föreskrifter från myndigheter, och ifrågasätts normalt inte av verken. Under senare tid är uppfattningen att myndighetskraven på automatisering generellt setts öka.

Avseende funktioner som behövs för driften, och som inte är säkerhetsrelaterade, har man vid kärnkraftsverket en konservativ hållning med utgångspunkt att inte automatisera i onödan. Filosofin bakom denna hållning är att man vill undvika risken att operatörerna blir för passiva, och på så sätt tappar i situationsmedvetenhet och riskerar att sätta alltför stor tillit till automatiken.

Vissa funktioner som t.ex. när en turbin ska startas kräver många moment och inhämtande av stora mängder information, vilket ger en alltför stor mental belastning av operatörerna. I sådana fall har man valt att automatisera förloppet för att det helt enkelt fungerar mycket bättre då.

Andra startsekvenser kunde mycket väl också automatiserats, men detta har undvikits för att förhindra att operatörerna passiviseras och i förlängningen förlorar uppmärksamhet på processen och medvetandet om vilken status den befinner sig i.

Utöver denna konservativa hållning i samband med automatiseringar används ytterligare två strategier för att upprätthålla en hög situationsmedvetenhet: rådrumsregeln och simulatorövningar.

Genom den tidigare beskrivna rådrumsregeln, hanteras alla förutsedda händelser automatiserat i 30-minuter så att operatörernas mentala belastning minskas och på så sätt får tillräcklig tid att fatta beslut om eventuella åtgärder.

Genom simulatorträning övas olika scenarion. Detta är ett sätt att förbereda operatörer för olika händelser, vilket ökar deras möjlighet att upprätthålla situationsmedvetandet om något händer.

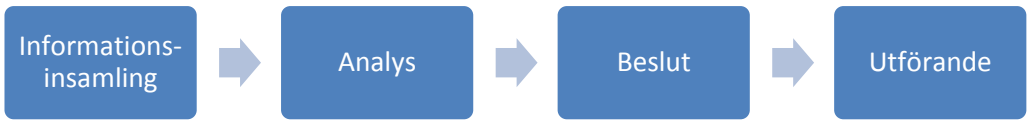
Sammanfattningsvis är man vid kärnkraftsverket nöjd med den automatiseringsgrad man har. Vad som dock har uppmärksammats som problematiskt efter moderniseringen till ett digitalt styrsystem är alla felfunktionslarm som systemet i sig genererar. Dessa larm är inte kopplade till själva processen, utan har istället sitt ursprung i självdiagnosticerande komponenter som givare, olika elektronikkort mm, som kräver en underhållsåtgärd. Dessa larm som ofta inte är akuta har ökat den mentala belastningen för operatörerna.

2.3 Människans roll och påverkan på denna

Fitts list och liknande anger vilka starka och svaga sidor som människor och maskiner har. Människans förmåga är dock inte statisk utan påverkas av den miljö som hon verkar i, och förändras av erfarenhet och utbildning. Valet av automationsgrad bör därför också ta hänsyn till hur människans förmågor påverkas av den valda automationsgraden.

Parasuraman et al (2000) har utvecklat ett system för att beskriva automation och automationsnivåer i fördelningen mellan människa och maskin.

Oavsett om en uppgift löses av en människa eller maskin kan enligt Parasurman et al (2000) funktionen grovt indelas i fyra steg:

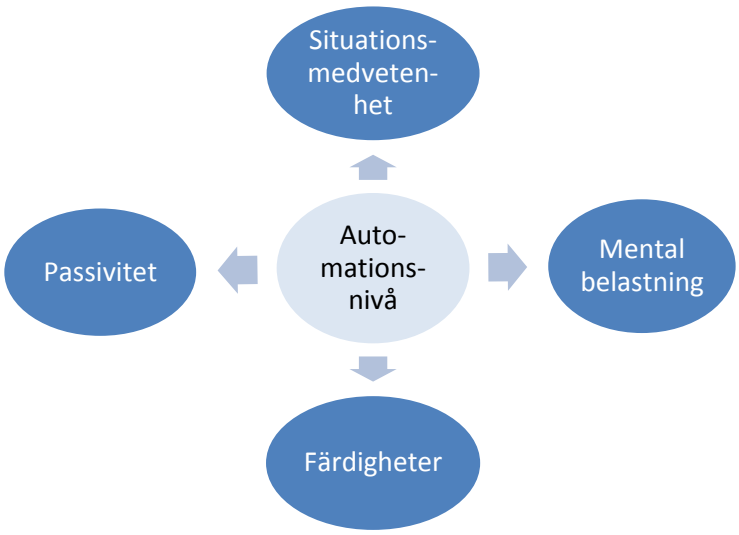


1) insamling av information,
2) analys av informationen,
3) beslut och val av åtgärd, samt
4) utförande av åtgärden.

Beroende på till vilken grad denna uppgift delas mellan människa och maskin, kan automationsgraden indelas i 10 nivåer, från hög automationsgrad (10) till låg automationsgrad (1) enligt följande:

Hög	10	Datorn beslutar allt, agerar autonomt och ignorerar människan
	9	Informerar människan endast om datorn bestämmer så
	8	Informerar människan om informationen efterfrågas, eller
	7	Exekverar automatiskt, och informerar sedan människan, och
	6	Tillåter människan att stoppa exekveringen inom en bestämd tid, eller
	5	Utför den åtgärd som människan godkänner, eller
	4	Föreslår en åtgärd, eller
	3	Föreslår några begränsade åtgärder, eller
	2	Föreslår samtliga möjliga beslut/åtgärder, eller
Låg	1	Datorn ger ingen assistans och människan måste ta alla beslut och genomföra alla åtgärder.

Förutom människans förutsättningar att agera självständigt, påverkas i varje steg av automationen också människans mentala belastning, situationsmedvetenhet, passivitet/förnöjdsamhet och färdigheter av automationsgraden (1-10). Med passivitet/förnöjdsamhet avses i detta sammanhang att operatörerna har en övertro på automatiken och inte längre aktivt bevakar och involverar sig i processen, utan förlitar sig på att systemet sköter sig själv.



Parasuraman nämner några exempel:

- I första automationssteget, *insamling av information*, kan människans *mentala belastning* påverkas positivt av automationen, t.ex. om automationen organiserar information i listor, om den markerar viktig information och genom att grafiskt återge information.

- Negativ påverkan på *mental belastning* kan t.ex. uppstå om det är komplicerat att genomföra åtgärder i det automatiserade systemet, eller om automationen kräver att människan behöver mata in stora mängder data.

- *Människans situationsmedvetenhet* påverkas negativt av högt automatiserade system, eftersom operatören då inte följer med i de förändringar som sker på samma sätt som om man själv är aktiv i processen.

- Automatiserad informationsanalys, såsom integrering av data har en positiv inverkan på *människans situationsmedvetenhet*.

- Graden av *passivitet/förnöjdsamhet* är ytterligare en mänsklig faktor som påverkas av automationsgraden. Om människan har en övertro på automatiken, kan det innebära att fel i automatiken missas. Störst är risken om operatören är engagerad i flera uppgifter samtidigt. Om presentationen av processinformation är högt automatiserad, riskerar operatören att missa annan viktig information om denne inte aktivt eftersöker denna.

- Slutligen riskerar också människans *färdigheter* att påverkas negativt av en hög automationsgrad. Om uppgifter automatiseras kommer människans förmåga att utföra dessa uppgifter sakta men säkert att eroderas.

För att undvika negativ påverkan på människans förmågor har Parasuraman et al (2000) föreslagit en strategi för att identifiera den optimala automationsnivån. Denna tar sin utgångspunkt i vilken automationsgrad som är optimal för människan, dvs:

A. hur påverkas människans förmåga att agera av automationsgraden, och

B. hur tillförlitlig är automationen och hur allvarliga är konsekvenserna av ett felaktigt agerande.

I det första steget bedöms alternativa automationsnivåer med hänsyn till hur de kommer att påverka faktorerna: mental belastning, situationsmedvetenhet, passivitet och förlust av färdighet hos operatörerna.

Den nivå som identifierats som optimal ur ett operatörsperspektiv utvärderas sedan ur ett säkerhetsperspektiv där det tas hänsyn till såväl tillförlitligheten hos det automatiserade systemet, som konsekvensen av ett felaktigt mänskligt eller maskinellt agerande, t.ex. tillföljd av att det uppstår en ny situation som systemet inte är programmerat för.

Händelser som kräver mycket uppmärksamhet, men som inte är speciellt viktiga, kan med fördel automatiseras enligt detta sätt att tänka, eftersom det avlastar operatörens mentala belastning. Händelser, där konsekvensen av ett felaktigt mänskligt agerande är mycket svåra bör också vara helautomatiserade. Detta bör dock endast gälla under förutsättning att alla händelser kan förutses, och det aldrig förväntas att människan ska behöva agera, enligt Parasuraman et (2000).

De flesta experiment som gjorts för att studera hur automationsgraden påverkar människan har gjorts inom flygbranschen. En nyligen publicerad artikel redovisar dock ett experiment som utförts i en kärnkraftssimulators kontrollrumsmiljö, Lin et al (2010).

I det försöket deltog 20 ingenjörsstudenter, som delades in i operatörsgrupper tilldelade varsin uppgift. Varje grupp fick genomföra sin uppgift med två olika automationsnivåer i en kärnkraftssimulator för transient- och olycksscenarier.

Den ena gruppen fick i uppgift att styra reaktorn under en normal driftssituation. En gång med hjälp av ett helautomatiserat system, där operatören i huvudsak endast behöver övervaka processen, och en gång där operatören manuellt behöver manövrera styrstavarnas läge och den interna reaktorpumpens hastighet.

Den andra gruppen fick i uppgift att hantera en onormal situation, där det inkommer fem larm till följd av avvikelser hos reaktorns vätskenivå. Denna uppgift fick också lösas två gånger med hjälp av olika nivåer av automation. I den ena generar datorn ett åtgärdsförslag som sedan initieras av operatören för att sedan utföras enligt en programmerad sekvens. I den andra automationsnivån har operatören möjlighet att välja åtgärder också utöver de som föreslås av datorn.

Samtidigt som försökspersonerna skulle utföra den uppgift de tilldelats, fick de också i uppgift att särskilja två signaler på en intilliggande tavla. Syftet med denna sekundära uppgift var att mäta hur den mentala belastningen påverkas av automationsnivån i en uppgift.

Ett tydligt resultat från den sekundära uppgiften var att den *mentala belastningen* påverkas kraftigt av automationsnivån, eftersom de försökspersoner som manuellt fick kontrollera styrstavarnas läge och den interna reaktor-

pumpens hastighet blev överbelastad och hade svårt att hänga med i den sekundära uppgiften att särskilja signaler på den intilliggande tavlan.

Den lägsta *mentala belastningen* upplevde försökspersonerna då de fick hantera den onormala vätskenivån i reaktorn med hjälp av en dator som föreslog åtgärder åt dem. Det var också då de fick bäst resultat i den sekundära uppgiften.

Avseende *situationsmedvetenhet* gjordes en utvärdering genom att efter försöket ställa frågor till försökspersonerna om utrustningens funktion, trender och andra observationer de gjort. Detta test visade att det var vid försöket då försökspersonerna fick hantera den onormala vätskenivån i reaktorn med hjälp av en dator som föreslog åtgärder åt dem som den bästa *situationsmedvetenheten* uppnåddes. Både de uppgifter som genomfördes manuellt och de som utfördes i helautomatiserade system gav en sämre *situationsmedvetenhet*.

Sammanfattningsvis avseende studien av Lin et al (2010) kan det konstateras att det är bra med automatisering avseende mental belastning om den minskar antalet ingrepp för operatörerna. Det är dock bra om operatörerna tvingas att vara delaktiga i beslutsfattandet, eftersom de då blir mer uppmärksamma på vad som händer och således får en bättre situationsmedvetenhet än om de kan vara helt passiva – såsom i ett helautomatiserat system.

Erfarenheterna från flygbranschen sammanfaller i stort med Lins slutsatser. Sepp Moser som är flygspecialist beskriver i Swiss Engineering (Dec 2010) hur automationsfilosofierna vid Boeing respektive Airbus skiljer sig åt, och på vilket sätt de påverkar piloterna. Enligt Moser, ser Airbus piloten som den svagaste länken i systemet, och försöker utforma systemet så att datorn självständigt utför de kommandon som piloten utfärdar. Boeing, å andra sidan, försöker optimera automatiken, på ett sätt så att piloten hela tiden har kontroll över de sekvenser som utförs, samtidigt som piloten får feedback på hur systemet reagerar t.ex. i form av att styrspaken känns trögare vid vissa manövrar.

Denna skillnad i automationsfilosofi har haft till följd att Airbus-piloterna styr sitt plan enbart genom rationellt beslutsfattande, medan Boeing-piloterna förutom rationellt beslutsfattande, också har möjlighet att ta snabba intuitiva beslut. Moser bedömer att denna möjlighet kan vara livsavgörande i vissa scenarier.

För att stärka sin ståndpunkt redovisar Moser en lista på sex allvarliga incidenter inom flyget under 2009 där kontrollsystemet haft negativ inverkan på händelseförloppet, samtidigt som piloten försökt rädda situationen. Ett exempel är hämtat från en landning på Azorerna i augusti 2009 med en Airbus 320. Vid detta tillfälle landar planet så kraftigt att det studsar upp från landningsbanan. Piloten försöker korrigera, men det automatiska landningssystemet bromsar istället planet så att det återigen faller ned extremt hårt mot landningsbanan och skadas.

Reason (2008) har tittat på människans roll som en räddare i farliga situationer ur ett bredare perspektiv, utan fokus på just automatiserade system. I sin analys har han gjort en genomgång av ett stort antal händelser där människan gjort vad han kallar ”heroiska” räddningar av svåra situationer. Han redovisar händelser från krigssituationer, flygplansincidenter, rymdfart (Apollo 13), sjöfarten (Titanic) och inom kirurgin. Enligt honom är följande ingredienser av betydelse för människans möjlighet att rädda en situation:

- Situationsmedvetenhet
- Rätt person vid rätt tillfälle
- Beslutsstil
- Ledarstil
- Realistisk optimism, man kan inte lyckas om man inte försöker

Valet av personal på plats, deras ledarstil och skapandet av en realistisk optimistisk anda ligger utanför omfattningen av automation och läsaren hänvisas istället till Reason för att läsa mer om detta. Däremot har, som tidigare beskrivits, balansen mellan människa och automation stor betydelse för *situationsmedvetenheten*.

Ytterligare en av Reasons framgångsfaktorer som påverkas av automationsgraden är vilka *beslutsstilar* automationen möjliggör för operatören. Det finns i huvudsak fyra beslutsstilar, beskrivna som: intuitivt, regelbaserat, analytiskt och kreativt tänkande. Genom identifiering av tänkbara scenarier, procedurer och övningar har man inom alla branscher som mål att kunna hantera händelser genom regelbaserat och analytiskt tänkande. Intuition och kreativitet är förknippade med en osäkerhet som man helst vill undvika i hög-risk branscher.

Reason påpekar dock att det i många kritiska situationer inte finns tid för regelbaserat och analytiskt tänkande, utan det krävs snabba intuitiva beslut. Något som människan utrustats med i evolutionen, och som ”oftast” har rätt. I de fall en operatör ställs inför en helt ny situation, finns dessutom inga regler att tillgå utan denne måste förlita sig på kreativ problemlösning.

Här följer nu några scenarion från kärnkraftsbranschen där operatörerna haft möjlighet att ta kontroll och rädda situationen. Syftet med beskrivningen av dessa är att göra en jämförelse mot den ovan beskrivna teorin, och dra generaliserbara lärdomar som kan användas för att öka möjligheten att rädda framtida situationer där automatiken inte fungerar.

3. Händelser där människan räddat en situation eller behövt ingripa för att automatiken inte räckt till

Nedan följer en sammanfattad beskrivning av tre händelser där människan räddat en situation eller behövt ingripa för att automatiken inte räckt till. Händelsen i Vandellos 1990 har hittats hos KSU, där den används som ett exempel i undervisningen. Händelsen i Schweiz 1996 har återgetts av Eberhard Würsch, som är en kollega från Schweiz med lång erfarenhet i branschen. Händelsen vid Forsmark 2006 hör till de mer rapporterade och undersökta inom svensk kärnkraft under den senaste 10-årsperioden, och är också den ett bra exempel på människans roll i systemet.

3.1. Vandellos, Spanien 1989

Denna händelse som finns mer utförligt beskriven i Bilaga 1 sammanfattas här för att visa det sätt som människan räddade situationen på.

Vandellos 1 var en koldioxidkyld och grafitmodererad reaktor på 545 MW_e. Stationen var utrustad med två turbinaggregat med vätgaskylda generatorer. Någon turbinbyggnad fanns inte, utan turbinerna var inneslutna i var sin skyddskåpa under bar himmel.

Den 19 oktober 1989 producerade stationen 400 MW_e, med stabila driftparametrar. Klockan 21.39 gick visaren på det instrument som övervakar turbinvibrationerna utanför skalan. I samma sekund hördes en kraftig explosion och golvet i kontrollrummet skakade. Skiftingenjörens första tanke var att en transformator hade exploderat. Detta hade nämligen inträffat tre gånger under 1989 i Vandellos 2. Från kontrollrummet kunde han emellertid se höga eldflammor svepa över ett turbinaggregat. Reaktorn snabbstoppades automatiskt. Som en extra säkerhetsåtgärd utlöste reaktoroperatören också manuellt snabbstopp.

Explosionen orsakades tillföljd av ett turbinhaveri. Turbinen hade havererat av de kraftiga vibrationer som uppstod efter att några skovlar inuti turbinen lossnat. Dessa vibrationer skjuvade också sönder rörledningar till turbinens smörjolja, som snabbt antändes. De orsakade också skador på generatorn, vilket medförde att vätgas läckte ut och exploderade.

Den explosionsartade branden som följde, smälte stationens rörledningar för tryckluft och de flesta ventiler måste manövreras manuellt eftersom de var luftstyrda. Den förstörde också alla elektriska kablar i berörda utrymmen och kring turbinaggregatet. Eftersom en dörr lämnats öppen strömmade dessutom stora mängder havsvatten från turbinens läckande kylsystem in i reaktorbyggnaden, och orsakade en översvämning.

Sammantaget ledde de skadade tryckluftsledningarna, skadorna på elsystemet och översvämningen till att:

- cirkulationsfläktar stoppade,
- sekundärvattenpumpar förstördes,
- nivåreglering i matarvattentankarna till kylsystemet inte fungerade,
- interna kommunikationssystemet förstördes,
- belysningen kring turbinerna slocknade.

Koldioxidtrycket i primärsystemet steg till 0,4 bar under det värde där ett stort bortfall av kylmedel kunde ha inträffat. Temperaturen steg samtidigt till endast 5 °C under det värde där totalt bortfall av kylningen kunde inträffa.

I kontrollrummet hämtade man sig snabbt från chocken i och med att man konstaterat att styrstavarna gått in. Insatserna koncentrerades på att hålla de två återstående huvudcirkulationsfläktarna i drift. Eftersom varje pneumatisk ventil var försedd med en ratt för manuell manövrering, genomfördes flera manuella justeringar i förbyggande syfte för att parera eventuella fel i automatiken.

Utöver en omfattande brandbekämpningsinsats, vidtogs också vid midnatt massiva åtgärder för att dränera stationen. Detta arbete var avslutat på förmiddagen morgonen därpå, dvs ett halvt dygn efter det att störningen inträffat. I och med detta kunde flera korrigerande åtgärder vidtas som nästa dag resulterade i att resteffektkylsystemet kunde återställas. Härmed började härdens och blockets parametrar stabiliseras mot normala värden.

Efter händelsen uttalades brister i brand/haveriberedskapen. Det konstaterades också att Vandellos 1 inte uppfyllde innebörden i "djupförsvarsprincipen". Ett politiskt beslut antogs 1990 om en nedläggning av blocket.

3.2 Schweiz, 1996

Denna händelse sammanfattas här på svenska, men finns mer detaljerat återgiven i Bilaga 2.

Händelsen inträffade på ett schweiziskt kärnkraftverk med två tryckvattenreaktorer. Efter en störning på det externa elnätet, kopplades de två enheterna bort från nätet för att gå ned till husturbindrift och på så sätt endast producera den effekt som behövs inom respektive anläggning. Sekvensen som ska ta ned reaktorerna till husturbindrift misslyckades dock av olika anledningar, och istället går en av reaktorerna ned till varm avställning.

Kontrollsystemet till den reaktor som befinner sig i varmt avställt läge får nu sin strömförsörjning bakvägen från den reaktor som befinner sig vid husturbindrift, eftersom deras effektuttag är sammankopplade.

De driftansvariga beslutar att återstarta den avställda reaktorn genom att initiera den automatiska startsekvensen. Samtidigt som automatiken startar, ingriper dock en operatör som befinner sig i kontrollrummet och stoppar den automatiska starten. Operatören har nämligen kommit på att det inte går att starta processen från det aktuella läget med den förprogrammerade sekven-

sen. Den automatiska sekvensen innebär nämligen att systemet kopplas bort från sin inkopplingspunkt till elnätet under en viss tid. Eftersom reaktorn i den speciella situationen nu fick sin strömförsörjning bakvägen från den andra reaktorn via denna inkopplingspunkt, innebar detta att enheten hade blivit näst intill strömlös vid varm avställning och naturlig cirkulation om automatiken hade fått fortgå.

Efteråt återställdes reaktorn istället till normal drift genom en manuell återstartssekvens.

Om operatören inte hade ingripit skulle troligen reaktorns reservkraftsförsörjning initierats, och reaktorn hade på så sätt stabiliserats till dess att strömförsörjningen återställts.

Den andra reaktorn som befann sig vid husturbindrift hade också påverkats ifall den automatiska startsekvensen hade fullföljts. Den hade troligen också snabbstoppats och fått sin strömförsörjning från samma reservkraftskälla, som bestod av två dieslar.

Efter händelsen gjordes vissa modifieringar i anläggningen bland annat i syfte att förbättra tillgången till reservkraft vid liknande händelser.

En trolig bidragande orsak till att operatören agerade så rådigt, var att han själv inte vara engagerad i starten utan betraktade det hela från en åskådares position och på så sätt var det troligen mentalt enklare att ifrågasätta de planerade åtgärderna. Det var också en person med tillräcklig erfarenhet och kunskap för att kunna förutse hur den automatiska sekvensen genomförs.

3.3 Forsmark 2006

Händelsen vid Forsmark 2006 finns bland annat beskriven av Analysgruppen (2007), och i två rapporter från Vattenfall (2006).

Forsmark 1 är en kokvattenreaktor med två turbinaggregat, som vid händelsetillfället levererade en full effekt av 990 MW.

Tisdagen den 25 juli, kl 13.20 inträffade en störning som hade sitt ursprung i en kortslutning i 400 kV ställverket utanför Forsmarksanläggningen. Denna genererade en kraftig spänningtransient som hade en kraftig påverkan på kontrollsystemets strömförsörjning, och på så sätt automatikens möjlighet att ha kontroll över reaktorn.

Under händelsen fick reaktorhärden hela tiden tillräcklig kylning och reaktortanken utsattes inte för några onormala belastningar i tryck och temperatur. Det som gör Forsmarksincidenten allvarlig, är istället att reaktorns djupförsvar inte fungerade tillfredställande på så sätt att flera oberoende system slogs ut samtidigt av en och samma spänningtransient.

Det som däremot fungerade väl var operatörernas ingrepp som ledde till att reaktorn kunde stabilseras i ett underkritiskt och stabilt läge.

Det första som hände vid störningen var att ett snabbstopp av reaktorn initierades automatiskt. Den kraftiga spänningtransienten hade dock som effekt att delar av det batterisäkrade växelspänningsnätet slogs ut och att två av de fyra dieseldrivna elgeneratorerna inte kunde startas automatiskt. Detta ledde bland annat till att information från givare ute i anläggningen inte nådde fram till operatörerna i kontrollrummet, bland annat kunde de inte se styrstavarnas läge. Denna avsaknad av information skapade en osäkerhet om snabbstoppet skulle fungera som tänkt, men kunde kompenseras genom olika manuella kontroller.

Efter 22 minuter kopplades strömmen från de två frånkopplade dieselaggregaten slutligen in manuellt, och på så sätt var det möjligt att återfå strömmen till instrumenten, verifiera styrstavarnas läge och fullfölja snabbstoppet. 45 min efter att händelsen inleddes var reaktorn ”säkert underkritisk och driftläget stabilt”.

Efter händelsen genomfördes en så kallad ”Vad hade hänt om?”-analys av SKI och Forsmark. Avseende operatörernas ingripande kan bland annat konstateras att:

- Såväl spänningssättning som andra avhjälpande åtgärder var vid den aktuella situationen beroende av operatörsingripande eftersom automatiken inte fungerade.
- Om alla fyra delsystem hade blivit spänningslösa och inga operatörsingripanden gjorts inom åtta timmar, skulle med stor sannolikhet en härdsmälta inträffat.

I Forsmarks erfarenhetsrapport avseende situationen i kontrollrummet (2006) konstateras att signalbilden i kontrollrummet blev komplicerad och svårtolkad samtidigt som informationsflödet blev omfattande. Med användning av i simulator inövade rutiner och arbetssätt kunde störningen dock hanteras. I denna rapport redovisas också en rad förbättringsförslag, bland annat olika sätt att säkra upp informationsflödet till operatörerna då vissa system blivit utslagna.

4. Diskussion

Som händelserna ovan visar är det än så länge inte möjligt att helt räkna bort människan. Händelser som ligger utanför automatikens kontroll har hänt och kommer hända. I dessa fall kommer vi fortsatt att vara beroende av människans förmåga att rädda situationen. Samtidigt som vi bygger så säkra system som möjligt, bör vi ha i åtanke på vilket sätt som dessa säkra system påverkar människans möjlighet att rädda de situationer som vi inte förutsett eller åtminstone ligger utanför automationens omfattning.

Händelsen i Forsmark visar också att människan är en av de vitalaste skyddsfunktionerna i djupförsvaret, och att det måste vara stort fokus på att vårda och upprätthålla förmågan hos människan att rädda en situation, vid alla förändringar av människans roll.

Två av Reasons (2008) mänskliga framgångsfaktorer för att rädda en situation är *situationsmedvetenhet* och förmåga att använda flera *beslutsstilar*.

För att möjliggöra en hög *situationsmedvetenhet* är det därför viktigt att automationsgraden utformas med detta i åtanke. Lin et al (2010) har visat att situationsmedvetenheten påverkas negativt av automatiserat beslutsfattande, i synnerhet om operatören är helt bortkopplad från såväl analys av informationen som utförande av uppgiften. Lins försök visade dock att för låg automationsnivå också kan försämra situationsmedvetenheten eftersom operatören i det fallet troligen blir alltför upptagen med utföranden för att kunna stanna upp och reflektera över situationen.

Fullständig bortkoppling av människan är således inte önskvärt, utan människan bör istället i möjligaste mån engageras, i synnerhet i beslutsfattande – eftersom denne då tvingas att sätta sig in i och följa med i skeendet. Antalet uppgifter som behöver utföras av en människa behöver dock samtidigt reduceras med hjälp av automation i syfte att minska den mentala belastningen.

För att hitta en optimal automationsnivå, eller åtminstone förhindra att en förändring av automationsnivån leder till att människans förmåga att rädda en situation påverkas i negativ riktning bör förändringar i automationsnivån föregås av en analys av vilken påverkan på människan som den tänkta automationsnivån har.

Den andra av Reasons (2008) framgångsfaktorer som påverkas av automationsgraden är vilka *beslutsstilar* automationen möjliggör för operatören. Som vi såg från fallet Airbus, har piloten där fråntagits möjligheten att genomföra intuitiva åtgärder. Det samma gäller till viss del också inom kärnkraften i vissa länder, där operatören inte kan stoppa en säkerhetsfunktion.

I de händelser som Reason tittat närmare på är det just ofta *intuition och kreativitet* som bidragit till en lyckosam räddning. Det stämmer också bra med den redovisade händelsen i Schweiz, 1996, där en utomstående operatör tack vare en kombination av erfarenhet, intuition och kreativitet lyckades identifiera ett potentiellt problem i den automatiska sekvensen.

För att människan ska kunna ingripa och rädda en situation förutsätts att systemet möjliggör och tillåter mänskliga ingripanden.

Händelsen i Vandellos där operatörerna kunde manövrera ventilerna med hjälp av *handvred*, då tryckluftssystemet var utslaget, är ett illustrativt exempel på ett system som lämnar utrymme för operatören att ingripa om automatiken inte fungerar. Det samma kan sägas om händelsen i Forsmark, där operatörerna hade möjlighet att *manuellt* koppla in dieselaggregaten. I fallet från Schweiz, tillät systemet att den automatiska startsekvensen stoppades för att istället genomföras manuellt. Dessa möjligheter att ingripa är viktiga oavsett om anledning är att åtgärden finns nedtecknad i en instruktion eller om det identifieras som den bästa lösningen på ett oförutsett problem.

För att stärka djupförsvaret bör människans unika förmåga att tänka intuitivt och kreativt, och genomföra åtgärder utan tillgång till externa kraftkällor eller uppgjorda procedurer utnyttjas till fullo, på samma sätt som att fast installerad belysning kan kompletteras med ficklampor, sprinklers med handbrandsläckare, automatventiler med manuella funktioner etc.

Slutsatsen är att det inte finns något egenvärde i att eftersträva ett system som helt utesluter intuitiva och kreativa operatörsingripanden. Avvägningen mellan operatörernas möjlighet att ingripa i en automatiserad sekvens måste dock självklart vägas mot risken associerad med ett felaktigt ingripande, och i vissa fall är det troligen säkrast att låta automatiken i t.ex. säkerhetssystem vara opåverkbar.

Vid såväl händelserna vid Forsmark och Vandellos påpekade operatörer att de upplevt en hög *mental belastning* tillföljd av bland annat alla larm som påkallar deras uppmärksamhet. Alltför hög mental belastning har en tydlig påverkan på människans förmåga att utföra en uppgift, vilket visats av bland annat Lin et al (2010). Vid rätt vald automationsnivå avlastar automationen människan från arbetsamma uppgifter, samtidigt som människan får möjlighet att följa och vara delaktig i beslutsfattandet.

Vid studiebesöket på det svenska kärnkraftverket i studien framstod även där larmhanteringen som ett problem för operatörernas mentala belastning. Installationen av larm som visas i kontrollrummet är en form av automatiserad informationsinsamling där operatören själv inte har möjlighet att påverka vilken information som presenteras. I många sammanhang tas beslut om nya larm med ett ganska snävt problemperspektiv framför sig. Ofta bara med ett specifikt scenario i åtanke. Detta leder till en suboptimering. Om larmsystemet istället utformades med ett helhetsperspektiv, där det tas hänsyn till på vilket sätt en larmfunktion påverkar operatörens förmåga att agera i ett scenario där larmet är irrelevant skulle larmsituationen på det hela kunna förbättras.

Införandet av nya larm till ett kontrollrum, liksom andra förändringar av automationsnivån, bör föregås av en förändringsanalys som tar sin utgångspunkt i på vilket sätt förändringen påverkar människans förmåga att agera.

Denna metodik bör följa de riktlinjer som föreslagits i Parasuramans strategi för att identifiera den optimala automationsnivån, dvs:

A. hur påverkas människans förmåga att agera av automationsgraden, och

B. hur tillförlitlig är automationen och hur allvarliga är konsekvenserna av ett felaktigt agerande.

Om vi tar fallet införandet av ett nytt larm som exempel, är det ofta så att i vissa situationer kommer larmet vara viktigt medan i andra situationer är det oviktigt och kommer endast ha en negativ effekt på operatörens *mentala belastning*. I detta fall handlar det om att värdera positiva respektive negativa konsekvenser mot varandra ur ett helhetsperspektiv. Det vill säga: A) vilken inverkan kommer larmet ha på operatörernas *mentala belastning, situationsmedvetenhet* mm i olika scenarion; och B) hur tillförlitlig är signalen, och vad blir *konsekvensen* om operatören gör fel pga. av att denne inte fått tillgång till larmet.

I fallet med *beslut* om vilka larm som behöver följas upp av en operatör skulle det troligen vara en fördel med ökad automatisering, i form av en automatiserad larmfiltrering/blockering som avlastar operatörernas mentala belastning. Denna larmfiltrering bör dock i så fall inte gå så långt att operatörerna förlorar i situationsmedvetande.

Ett sätt att lösa denna och liknande konflikter där olika scenarion ställer olika krav på automationsnivå är med hjälp av *adaptiv automation*. Om adaptiv automation används kan en uppgift lösas automatiskt i ett fall, medan den i andra fall löses manuellt. Inom flyget finns exempel där uppgifter som normalt sker manuellt löses automatiskt om det är tidskritiskt eller om flyplanet har en viss hastighet. Med fördel kan man också engagera en operatör i denna uppgift att besluta vad som ska ske automatiskt och vad som ska göras manuellt, t.ex. skulle en operatör kunna avgöra vilken nivå på larmfiltrering som ska råda i en viss situation beroende på den egna upplevda mentala belastningen.

Även om utgångspunkten är att bevara människans förmågor, måste vissa system ändå vara helautomatiserade för att garantera säkerheten. I de fall en funktion av drift- och säkerhetsskäl måste vara helautomatiserad, bör simulatorträning användas för att motverka den negativa inverkan som helautomatisering har på operatörers situationsmedvetenhet och risken för passivisering.

Avseende situationer som inte omedelbart är säkerhetskritiska har människans förmågor också troligen stor betydelse. I denna rapport som fokuserat på situationer där människan räddat en situation där automatiken inte fungerat eller räckt till är det förhållandevis allvarliga händelser som studerats. Olyckor består dock av såväl latenta och direkta orsaker, och följer ett händelseförlopp där människan påverkar utvecklingen vid flera tillfällen. I de redovisade händelserna har människan ingripit i ett sent skede, och det är därför som de rapporterats.

Om människan ingriper i ett tidigt skede genom att åtgärda latenta fel i automatiken, eller genom att omedelbart åtgärda ett fel kommer det inte att noteras som en incident. För att ta reda på människans verkliga funktion avseende dess uppgift att vara ”back-up” för automatiken behöver även dessa vardagshändelser studeras närmare.

Normal Operations Safety Survey (NOSS) är en metodik som används i flygindustrin för att proaktivt samla in säkerhetsrelaterad information. En liknande metodik skulle kunna användas för att öka kunskapen om hur operatören bidrar positivt till säkerheten i de situationerna då automatiken inte riktig räcker till.

5. Slutsatser

De händelser som studerats i rapporten visar att människan är en av de vitalaste skyddsfunktionerna i djupförsvaret. För att upprätthålla en hög säkerhet bör det således vara stort fokus på att vårda och upprätthålla förmågan hos människan att rädda dylika situationer.

Denna förmåga att rädda situationer påverkas av automationsnivån. För hög automationsnivå leder lätt till bristande situationsmedvetenhet, medan för låg automationsnivå kan leda till alltför hög mental belastning för operatörerna. Vid en optimal automationsnivå involveras människan i beslutsfattande, medan utförandet av uppgifter i större utsträckning kan lämnas till automationen.

I de studerade händelserna har det också funnits en möjlighet för människan att ingripa då automatiken fungerat fel eller inte haft tillgång till kraftförsörjning i form av el eller tryckluft. Det bör eftersträvas att människan alltid har en möjlighet att ingripa i de fall automatiken inte fungerar. För att stärka djupförsvaret bör människans unika förmåga att tänka intuitivt och kreativt, och genomföra åtgärder utan tillgång till externa kraftkällor eller uppgjorda procedurer utnyttjas till fullo, på samma sätt som att fast installerad belysning kan kompletteras med ficklampor, sprinklers med handbrandsläckare, automatventiler med manuella funktioner etc.

Automationsnivån inom kärnkraftsbranschen har hittills styrts av teknikutveckling och erfarenheter från de allvarliga händelser som inträffat, vilket lett till att flera system idag är helautomatiserade av säkerhets- och driftskäl. För att undvika onödig erosion av människans förmåga att ingripa i en situation då automatiken inte fungerar som tänkt, rekommenderas att fortsatta förändringar i automationsnivån på kärnkraftverken åtföljas av en analys av påverkan på människan liknande den metodik som Parasuraman et al (2000) föreslagit. Denna metodik vore ett tillskott till de riktlinjer som idag finns att tillgå vid automatiseringen av kärnkraftsverk.

I de fall en funktion av drift- och säkerhetsskäl måste vara helautomatiserad, bör simulatorträning fortsatt användas för att motverka den negativa inverka som helautomatisering har på operatörers situationsmedvetenhet och risken för passivisering.

Avseende fortsatt arbete förslås följande:

För att bättre kunna bedöma tillämpbarheten av Parasuramans metodik föreslås att den testas på konkreta frågeställningar inom kärnkraftverken, i några fallstudier.

Olyckor består av såväl latenta och direkta orsaker, och följer ett händelseförlopp där människan påverkar utvecklingen vid flera tillfällen.
För att öka kunskapen om människan som skyddsfunktion föreslås studier av också mer vardagliga ingripanden från operatörer för att korrigera automatiska funktioner. På så sätt kan man bättre se vilken funktion dessa ingripan-

den har för lärandet hos operatörerna, samt få en bättre bedömning människans betydelse som skyddsfunktion i djupförsvaret.

Referenser

Analysgruppen Bakgrund "Forsmarksincidenten den 25 juli 2006" Nummer 5, December 2006, Årgång 19, Reviderad Mars (2007)

Fitts, P.M. et al , Human Engineering for an Effective Air Navigation and Control System, Nuclear Regulatory Commission, Washington D.C. (1951)

Forsmarks Kraftgrupp "Erfarenhetsrapport avseende situation I kontrollrummet under störningen den 25/7 2006" F1-2006-0703, (2006)

Forsmarks Kraftgrupp "Forsmark 1 – Störningsanalys – Bortfall 400 kV samt utebliven dieselstart i A- och B-sub" F1-2006-0699, (2006)

IAEA Safety Standards Series, "Safety of Nuclear Power Plants: Design" Requirements No. NS-R-1 (2000)

IAEA Technical Reports Series No. 387, "Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook (1999)

IAEA TECDOC-668, "The role of automation and humans in nuclear power plants", (1992)

Lin, C.J., Yenn, T-C, Yang, C-W, "Automation design in advanced control rooms of the modernized nuclear power plants", Safety Science 48 (2010), pp 63-71

Moser, S., "Automatisierung für oder gegen der Menschen" i Swiss Engineering, Dec (2010)

Parasuraman, R., Sheridan, T.B. and Wickens C.D., "A Model for Types and Levels of Human Interaction with Automation" in IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans, Vol. 30, No 3., May (2000), pp 286-297

Reason J. "The Human Contribution – Unsafe Acts, Accidents and Heroic recoveries" Ashgate (2008)

http://www.skybrary.aero/index.php/Normal_Operations_Safety_Survey_(NOSS) (Jan, 2011)

BILAGA 1

Följande beskrivning med tillstånd från KSU hämtad ur deras utbildningsmaterial:

Vandellos

Station Vandellos, 1
Start 1972
Typ GCR
Effekt 545 MW_e
Land Spanien
Händelsedatum 19 oktober 1989

Sammanfattning

På kvällen den 19 oktober 1989 gick visaren på instrumentet som övervakar turbinvibrationerna i Vandellos 1 kontrollrum högt utanför skalan. I samma sekund hördes en kraftig explosion och golvet i kontrollrummet skakade. Skiftingenjörens första tanke var att en transformator hade exploderat, vilket hade inträffat tidigare på Vandellos 2. Från kontrollrummet kunde han emellertid se höga eldsflammor svepa över turbinaggregat 2. Reaktorn snabbstoppades automatiskt. 37 skovlar på högtrycksturbinen tillhörande turbinaggregat 2 hade lossnat. De momentant kraftiga vibrationerna på turbinaxeln skjuvade sönder ett antal rör kopplade till turbinen. Bland dessa var tre av fyra ångledningar samt rörledningar till turbinens smörjolja. Smörjoljan antändes snabbt, samtidigt som den rann ner i utrymmen under turbinen. Händelsekedjan kunde bemästras efter det att man fått branden under kontroll efter ca fyra timmar och branden var helt släckt efter ca sju timmar. Efter det att stationen dränerats på vatten kunde en ny pump till restvärmesystemet startas, vilket resulterade i en stabilisering mot normala parametervärden.

Kortfattad beskrivning av blocket

Vandellos 1 är en koldioxidkyld och grafitmodererad reaktor på 545 MW_e netto. Efter 1986 har dock reaktorn endast producerat 400 MW_e på grund av vissa korrosionsproblem. Stationen har två turbinaggregat med vätgaskylda generatorer. Någon turbinbyggnad finns inte, turbinerna är inneslutna i var sin skyddskåpa under bar himmel. Bränslet utgörs av naturligt uran omslutet av ett hölje med kylflänsar. De 15 bränsleelementen laddas ovanför varandra och bildar en bränslekanal. Drygt 3 000 bränslekanaler och 135 styrstavar finns i härden. Bränslet byts kontinuerligt under drift.

Händelsebeskrivning

Den 19 oktober 1989 producerade stationen 400 MW_e, med stabila driftparametrar. I anläggningen denna kväll fanns ett skiftlag på 12 man, och en bemannad centralvakt. Klockan 21.39 gick visaren på det instrument som övervakar turbinvibrationerna utanför skalan. I samma sekund hördes en kraftig explosion och golvet i kontrollrummet skakade. Skiftingenjörens första tanke var att en transformator hade exploderat. Detta hade nämligen inträffat tre gånger under 1989 i Vandellos 2. Från kontrollrummet kunde han emellertid se höga eldflammor svepa över turbinaggregat 2. Reaktorn snabbstoppades automatiskt. Som en extra säkerhetsåtgärd utlöste reaktoroperatören manuellt snabbstopp. 37 skovlar på högtrycksturbinen tillhörande turbinaggregat 2 hade lossnat. De momentant kraftiga vibrationerna på turbinaxeln skjuvade sönder ett antal rör kopplade till turbinen. Bland dessa var tre av fyra ångledningar samt rörledningar till turbinens smörjolja. Smörjoljan antändes snabbt, samtidigt som den rann ner i utrymmen under turbinen. Vid skovelhaveriet skakade turbinen axiellt, vilket bl a resulterade i skador på den vätgaskylda generatorn. Vätgas läckte ut och ett vätgasmoln antändes. Den omfattande branden förstörde all utrustning under turbinaggregat 2. Läckage från en av branden förstörd gummikoppling, tillsammans med brandvatten och vatten från en överfylld tank, medförde att ca 4 000 m^3 vatten fyllde de nedre planen i stationen.

Vid branden smälte dessutom rörledningarna för stationens tryckluft och de flesta ventiler måste manövreras manuellt eftersom de var luftstyrda. Den stigande vattennivån var endast 10 cm från att dränka samtliga hjälpmatarvattenpumpar som garanterar cirkulationsfläktarnas funktion. Koldioxidtrycket i primärsystemet steg till 0,04 MPa (0,4 bar) under det värde där ett stort bortfall av kylmedel kunde ha inträffat. Temperaturen steg samtidigt till endast 5 °C under det värde där totalt bortfall av kylningen kunde inträffa. Skiftingenjören ringde brandkåren i den närbelägna staden Tarragona, och brandstyrkan i Vandellos 2. Han ringde också centralvakten för att be denne informera och kalla in personal till anläggningen. Några av de anställda som befann sig i stationen påbörjade släckningsarbetet genom att från marknivån spruta vatten på brandhärdarna. Branden spred sig i det första skedet huvudsakligen genom att turbinens smörjolja rann ut och sedan långväga vidare via kabelstegar. Deflagrationen av vätgas från generatorns läckande kylsystem initierade också nya brandhärdar. Branden förstörde alla elektriska kablar i berörda utrymmen under och kring turbinaggregat 2. En tjock rök fyllde de nedre planen under turbinerna. I mindre omfattning rökfylldes också reaktorbyggnaden och med vinden kontrollrummet och elbyggnaden. I kontrollrummet hade ett antal fläktar installerats och startats en dryg halvtimme in i händelsen för att avleda röken och förebygga att personalen skulle behöva använda andningsutrustning. Branden förstörde tidigt elkablarna till smörjoljepumparna för två av de fyra turbindrivna cirkulationsfläktarna, vilka följaktligen stoppade på grund av låg nivå i oljesystemet. Tidigt kom bortfall av 48 V-skenor, vilka matar komponenter i regler- och indikeringssystem. Det interna kommunikationssystemet förstördes tämligen omgående, liksom belysningssystemet under och kring turbinerna. Branden resulterade vidare i att rörledningar och ventiler i stationens tryckluftssystem förstördes. Detta var besvärligt eftersom många av stationens ventiler var pneumatiskt manövrerade. Varje pneumatisk ventil var dock försedd med en

ratt för manuell manövrering. Bortfallet av tryckluft innebar att de ventiler som inte skadats av branden endast kunde manövreras manuellt på ort och ställe. Detta skedde dock i begränsad omfattning i den svåra miljö som rådde under det första skedet av störningen. En tillstötande komplikation, med tanke på kylning av reaktorn, var att nivån i hjälpmatarvattentanken tillhörande huvudcirkulationsfläkt 1 respektive 2 var oviss och troligtvis låg på grund av att de pneumatiskt manövrerade ventilerna inte fungerade. Reglerproblemen började en halv timme efter primärhändelsen och kvarstod i ca två timmar, vilket krävde upprepade manuella insatser. Branden förstörde också kablarna till samtliga fyra sekundärvattenpumpar i resteffektkylsystemet. En annan mycket viktig konsekvens av branden blev förstörelsen av en armerad gummikompensator på turbin 2-kondensorns inlopps- respektive utloppsledning. Dessa gummikopplingar har en diameter på två meter. Denna skada förblev oupptäckt under hela händelseförloppet. Den perforerade gummikompensatorn på inloppsledningen tillsammans med det faktum att huvudkylvattenpumparna förblev i drift resulterade i att stora mängder havsvatten strömmade in och vattenfyllde utrymmen under turbin 1 och 2. Operatörerna visste inget om detta havsvattenflöde förrän betydligt senare. Mellan turbin- och reaktorbyggnaderna finns ståldörrar som ska vara stängda. Vid tidpunkten för olyckan var de öppna. Följden blev att stora mängder havsvatten från turbinkondensorns läckande kylsystem rann in i bl.a. reaktorbyggnaden och byggnaden för utbränt bränsle. En annan konsekvens av att dörrarna stod öppna blev att röken spred sig in i reaktorbyggnaden. Då många pneumatiskt manövrerade ventiler låg kvar i fel läge överfylldes tanken för dejoniserat vatten. Utöver dessa vattenläckage tillfördes stationens utrymmen mycket vatten från brandsläckningssystemet. Totalt ca 4 000 m^3 vatten översvämmade blockets nedre plan i reaktor- och turbinbyggnaderna samt i byggnaden för utbränt bränsle. Vattendjupet i botten av reaktorbyggnaden var ca 81 cm efter drygt 4 timmar in i händelsen. Driftpersonalen visste då inte varifrån dessa stora vattenmängder kom. I samband med en radiologisk analys av ett vattenprov konstaterades emellertid att 65 % av vattnet var havsvatten.

Översvämningen förstörde de fyra pumparna i resteffektkylsystemet ytterligare. Elmatningen till dessa pumpar hade redan förstörts av branden. Dessutom förstördes två av de fyra återstående driftdugliga, av totalt åtta, hjälpmatarvattenpumparna till cirkulationsfläktarna. De två resterande pumparna fungerade. Elanslutningarna till dessa motorer var ca 10 cm ovanför vattenytan. Pumparna i byggnaden för utbränt bränsle blev dränkta av översvämningen och vattentemperaturen i bränslebassängen steg till strax under högsta tillåtna värde.

Ungefär fyra timmar in i händelsen bedömdes branden vara under kontroll och drygt två timmar senare var den släckt.

Åtgärder och lärdomar

Det uppskattades att ca 15 m^3 av turbinens smörjolja läckte ut och matade på branden. Uppskattningsvis deltog 50 personer i den direkta brandbekämpningen. I kontrollrummet hämtade man sig snabbt från chocken i och med att man konstaterade att styrstavarna gått in. Nödvändiga telefonkontakter togs snabbt med centralvakten och den externa

brandkåren. Insatserna i kontrollrummet koncentrerades på att hålla de två återstående huvudcirkulationsfläktarna i drift. Vissa ventilmanövrar gjordes manuellt i förebyggande syfte för att parera eventuella fel i automatiken. Massiva insatser vidtogs också vid midnatt för att dränera stationen. Detta arbete var avslutat på förmiddagen morgonen därpå, dvs ett halvt dygn efter det att störningen inträffat. I och med detta kunde flera korrektiva åtgärder vidtas som nästa dag resulterade i att en nyinstallerad pump i resteffektkylsystemet kunde startas med hjälp av nydragna kablar. Härmed började härdens och blockets parametrar stabiliseras mot normala värden.

På en hypotetisk fråga om vad de skulle önska sig om de åter fick uppleva en liknande störningssituation, svarade kontrollrumspersonalen att man främst ville ha arbetsro i kontrollrummet. Stressen ökade markant när operatörernas svängrum krympte på grund av allt folk i kontrollrummet. Skiftingenjören menade att han under störningen saknade:
• mer personella resurser i initialskedet
• bättre och fler kommunikationsmedel (snabbtelefon och högtalarsystem förstördes relativt omgående)
• bättre handlampor med kraftigare ljus.

Alla åtgärder i stationen krävde användning av andningsutrustning. Behovet av tryckluftstuber blev större än vad som någonsin förutsetts. I kombination med utslagning av stationens tryckluftssystem ställdes oväntade krav på mobila luftkompressorer för fyllning av lufttuber. Efter händelsen uttalades brister i brand/haveriberedskapen. Realistiska övningar med myndigheter, brandkår och press hade inte förekommit. Mer utbildning och praktik om den interna haveriberedskapen hade varit önskvärd. Det tog t ex flera timmar innan man fick klart för sig att skiftmedlemmarna hade överlevt utan skador. Det fanns inga rutiner för kontroll av personalen i en liknande situation. Efter Tjernobyl 1986, hade tillsynsmyndigheten ställt krav på kompletteringar och ombyggnader i bl. a. brandsystemet, elsystemet samt systemet för resteffektkylning. Man konstaterade att dessa åtgärder uteblivit. Det konstaterades också att Vandellos 1 inte uppfyllde innebörden i "djupförsvarsprincipen". Ägaren hade beslutat att åtgärda stationen till en kostnad motsvarande ca 1,3 miljarder kronor. Ett politiskt beslut antogs 1990 om en nedläggning av blocket.

BILAGA 2

Schweiz 1996
Introduction

Remark: The following event description is written down from memory. The official event description is not available and the specific moment of intervention is not included in the protocol / event analysis. As the experience during simulator training sessions show, this happens often. Such a moment of perception may become conscious during in depth analysis after the event.
The incident in question happened in a nuclear power plant (NPP) with two units. A load rejection occurred due to an external event. The disturbance happened in the high voltage grid (380kV), a long distance protection circuit opened the dedicated switches. Due to this disconnection a section of the 380kV ring line was switched off. The NPP feeds the produced power exactly into this part. This situation means a load rejection to house load for the NPP. This transient proceeded faulty and incomplete due to internal reasons, the units stabilized after the initial event in an abnormal plant status for house load. One unit remained on house load as expected, the other was shut down to hot zero condition. One RCP of this second unit remained in operation, energized due to power backflow from the other unit.

After situation analysis of the transient and the cause of the event, the restart of the units was organized. It was intended to restart one of the turbine/ generator group (TG) automatically. If this would be performed as planned, the automatic program would have caused an opening of the only one switch, providing power for the house load to the unit. The unit would have shut down again, this time to hot zero condition in natural circulation and almost complete loss of power (station blackout).

Due to the intervention of an operator, this specific problem was recognized, the automatic progress was stopped and the TG was manually synchronized with the grid. The unit was brought up to load preventing an unnecessary additional transient.

1. Event description

A disturbance in the high voltage grid (380kV) caused the activation of the long distance protection circuit. This protection circuit opened the designated switches, shutting down a section of the 380kV grid consisting of 2 independent power lines. The NPP consists of two units, each with two turbine/generator sets. Each generator is usually connected to one of these two lines (i.e. each unit feeds both lines). Both lines were affected by this disturbance, causing loss of offsite power to both units. Normally in such an event, the units were shut down from full power to house load. This time the transient did not completely function as expected. In one unit the TG's remained in operation, providing the house load to the plant and additionally power to the other unit. In the other unit, the TG's tripped, but the main switches remained closed and the plant was fed from the other. The unit stabilized in hot zero load, forced circulation (one RCP still running).

Both plants stabilized in an exceptional status; one plant on house load, additionally feeding the second plant, the other plant on hot shutdown, TG off, one RCP running due to backflow of electric power supply over main transformer and the house load transformer.
After analysis of the status / operation mode of both units, the operation management decided about the proceeding to bring up both units to the grid in to full power. Especially challenging was the situation with the second plant. The main power supply was provided over one path, feeding the unit backwards. First intention for this unit was to start the designated TG automatically. The critical situation aroused with the programmed step to synchronize the TG with the grid.

2 Course of transient without intervention

The critical step of the automatic program normally brings up the turbine to nominal speed for equalizing the frequency and after equalizing the voltage it would close the main switch of the generator. For safety reason this step starts with an open command to the main switch in order to have an unambiguous situation. During normal TG start up this switch is already open and no change of the status would be observed. In this special case opening of this switch would cause a new loss of power, because this line is the most important for the power supply. The reason is this line provides power to the RCP, keeping the reactor in forced circulation. Loss of power to the RCP causes a loss of forced circulation and therefore causes a reactor trip. The reactor would shut down again, this time due to loss of RCP. This new transient would bring the plant to hot zero conditions in natural circulation. And because the designated unit is fed from the first unit, it was unknown what the influences to this unit would be due to the disturbance on the (secluded) grid.

3 Intervention and course of transient

During the startup of the TG set an operator (not directly involved in the actions) recognized this critical step early enough. He was able to communicate his thoughts and findings to the shift supervisor and operation manager. The program was stopped and the situation newly analyzed. After confirmation of the findings the solution was to synchronize the TG manually (i.e. avoiding the protective opening of the main switch). The TG was synchronized, loaded and both units were brought later on to full load without any further disturbances.

4 Conclusions

Automatic programs are compiled for normal situations in the frame of expected plant behavior. Some variations are included, because they could be foreseen. With the appropriate logic control with interlocks the most usual transients could be covered by such a program. The proceeding of the program steps just have to be supervised by responsible operators and shift supervisors.

In cases of unexpected situations or faulty behavior of one or more plant systems the automatic program is not able to handle the transient regularly. At best the program will just stop and alarm the operator. That depends on the situation itself and the interlocks contained in the program. In the worst

case the automatic control system will just follow the programmed steps and driving the plant into an uncontrolled status with unknown effects to the system(s).

In situations which are not in advance included in the frame of possible plant behavior or possible transient evolution the successful handling of the event is depending on meaningful human intervention. With the acquired deep and wide knowledge about the plant, the individual systems and the goal (plant status) to reach only humans are able to cope with any new or unknown situation (situation awareness). Only with the attentive attitude focused on the goal to reach and close supervision of the ongoing transient in order to discover as early as possible any deviation from the expected course of evolution is it possible to prevent an unwanted progress. As the experience demonstrates, it needs an independent thinking ahead of the automated programs with the enquiring attitude "what happens next …", "what, if…" et cetera to be able to intervene in a wrong progressing transient and improve the situation (see also IAEA TECDOC 668, chapter 2.1/2.2).

Baden, 06.12.2010
AF-Colenco Ltd
Nuclear Technology
Eberhard Wyrsch
Senior Expert / Project Manager

2011:24

Strålsäkerhetsmyndigheten har ett samlat ansvar för att samhället är strålsäkert. Vi arbetar för att uppnå strålsäkerhet inom en rad områden: kärnkraft, sjukvård samt kommersiella produkter och tjänster. Dessutom arbetar vi med skydd mot naturlig strålning och för att höja strålsäkerheten internationellt.

Myndigheten verkar pådrivande och förebyggande för att skydda människor och miljö från oönskade effekter av strålning, nu och i framtiden. Vi ger ut föreskrifter och kontrollerar genom tillsyn att de efterlevs, vi stödjer forskning, utbildar, informerar och ger råd. Verksamheter med strålning kräver i många fall tillstånd från myndigheten. Vi har krisberedskap dygnet runt för att kunna begränsa effekterna av olyckor med strålning och av avsiktlig spridning av radioaktiva ämnen. Vi deltar i internationella samarbeten för att öka strålsäkerheten och finansierar projekt som syftar till att höja strålsäkerheten i vissa östeuropeiska länder.

Strålsäkerhetsmyndigheten sorterar under Miljödepartementet. Hos oss arbetar drygt 250 personer med kompetens inom teknik, naturvetenskap, beteendevetenskap, juridik, ekonomi och kommunikation. Myndigheten är certifierad inom kvalitet, miljö och arbetsmiljö.

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96

Tel: +46 8 799 40 00
Fax: +46 8 799 40 10

E-mail: registrator@ssm.se
Web: stralsakerhetsmyndigheten.se