Säkerhetsledning – en systemteknisk tillämpning

Björn Wahlström

Introduktion

Hur kan man styra ett komplicerat system på ett säkert sätt? Den frågan dyker upp i många sammanhang och kan få många svar inom ett område som brukar kallas säkerhetsvetenskap (safety science). De rekommendationer som man vanligen brukar få är att man skall göra en *riskanalys*, man skall bygga upp ett *säkerhetsledningssystem* och man skall se till att den organisation som opererar det komplicerade systemet är en *lärande organisation*. Alla dessa rekommendationer brukar ofta kastas fram, utan att man närmare funderar på hur man i praktiken skall se på styrproblemet. En del forskare har dock i säkerhetssammanhang lyft fram något som man kan kalla *kontrollmetaforen* och som kan tolkas att säkerhetsledning kan behandlas som ett styrproblem (Rasmussen, Svedung, 2000). Jag skall för att illustrera detta här i stora drag gå igenom några av de komponenter som man måste se på närmare för att ge svar på den ovan ställda frågan.

Vad menar man med säkerhetsledning?

När man ser på begreppet säkerhetsledning består det av två ord *säkerhet* och *ledning* som bildar utgångspunkten för vad man försöker göra. Med säkerhet menar man i dagligt tal att man inte behöver vara orolig för olika hot som kan drabba en. Man behöver t.ex. inte vara rädd för vilda djur när man går på en gata i en stad. Däremot kan man istället vara orolig för att bli påkörd av en bil. Man kan visserligen påverka risken att bli påkörd t.ex. genom att alltid använda skyddsväg och aldrig gå mot rött ljus när man går över en gata. Man kan således inse att det går att påverka sin riskbild genom olika åtgärder. Man talar således om risker när man menar hot, som kan drabba en och om säkerhet när man genom olika mot-åtgärder har lyckats göra riskerna tillräckligt små.

Med begreppet ledning, menar man att leda en grupp av människor eller en organisation så att vissa mål uppfylls. Leda och styra är således ekvivalenta begrepp åtminstone då objektet för det som vi försöker styra är människor eller en organisation. När man ser på vad som har skrivits om hur man kan och bör leda organisationer, så kommer man till ett mycket stort område som brukar kallas ledningsvetenskap (management science). Om man sedan ser på vad man inom ledningsvetenskap talar om så är det en blandning av psykologi, ekonomi, sociologi och systemvetenskap, som tillämpas på olika sätt.

Säkerhetsledning har således med risker att göra och hur man bör styra organisationer för att riskerna skall minimeras. När man ser på ett komplicerat system, t.ex. en industrianläggning, ett trafikflygplan eller ett stort fartyg, så kan man skilja mellan risker som uppstår på grund av

att den tekniska delen av systemet felfungerar och de risker som uppstår av att systemet drivs på ett felaktigt sätt. Detta betyder att man skiljer mellan fel i systemet självt och fel som uppstår när man använder systemet. Detta kunde då med en analogi tolkas så att i ena fallet handlar det om en bil som är säker och i det andra fallet om att köra bilen på ett säkert sätt.

När ett nytt system konstrueras behöver man således något slag av system som ser till att konstruktionsprocessen styrs på ett sådant sätt att resultatet, dvs. industrianläggningen, flygplanet eller fartyget, uppfyller de säkerhetskrav som gäller. På samma sätt behöver man för driftprocessen ett annat system som ser till att systemet drivs och underhålls på ett säkert sätt. I båda fallen brukar man tala om ett system för säkerhetsledning, som gör att arbetsprocesser, aktiviteter och uppgifter genomförs på ett sätt som gör att systemet är säkert och att det hanteras på ett säkert sätt. Säkerhetsledning har alltså att göra med hur man styr organisationer och människor så att de sin tur genomför sina uppgifter så att systemet de konstruerar eller opererar inte förorsakar fara.

Säkerhetsledningens komponenter

Vad skall man då kräva att ett system för säkerhetsledning skall innehålla? Först och främst måste man ha en aktivitet som identifierar de *hot* mot säkerheten som en industrianläggning, ett flygplan eller ett fartyg kan utsättas för. Det betyder att man i konstruktionsprocessen identifierar vad som av olika orsaker kan gå fel och vad som då kan inträffa. Det kan t.ex. bli fel på elförsörjningen till viktiga komponenter i systemet, vilket då kan få olika konsekvenser. Man kan då i konstruktionsprocessen *avlägsna* möjligheterna till fel, *hindra* att de uppstår eller *lindra* deras konsekvenser. Detta betyder att man först måste göra en *riskanalys* som identifierar möjliga fel och hur ofta de kan väntas inträffa och sedan ändrar konstruktionen på så sätt att risken kan anses tillräckligt liten.

På samma sätt kan man för systemets driftsfas försöka identifiera vad som kan gå fel, för att sedan vidta åtgärder för hindra att felen uppstår, göra felen mera sällsynta eller lindra de konsekvenser de kan få. För att hindra fel att uppstå kan man t.ex. genom förebyggande underhåll byta komponenter redan innan de går sönder, för att göra felen mera sällsynta kan man använda komponenter med högre kvalitet och för att lindra konsekvenserna av ett fel kan driftpersonalen företa olika motåtgärder. För att göra en riskanalys måste man känna sitt system, så att man vet vilka hot som finns och hur de kan motverkas. Detta betyder i systemtekniskt språkbruk att man har en modell som på ett rimligt sätt avbildar den verklighet man försöker styra.

En konstruktionsprocess kan aldrig vara fullständig i den meningen att inga brister i systemets konstruktion mera finns när det tas i drift. Bristerna kan förorsakas av förbiseende eller okunskap hos konstruktörerna, som gör att någon farlig situation inte identifierats eller åtgärdats på ett riktigt sätt. Man kan således vänta sig att driftpersonalen åtminstone någon gång ställs inför en hotfull situation, som är svår att hantera på ett adekvat sätt. Man kan också tänka sig att problem uppstår för att de instruktioner som driftpersonalen har inte är ändamålsenliga. Detta betyder att ett system för säkerhetsledning måste ha aktiviteter som samlar de *erfarenheter* man får under driften och analysera dem för att identifiera möjliga

brister. För att undvika framtida problem bör man sedan göra *ändringar* som avlägsnar bristerna i systemet eller instruktionerna.

Ett system för säkerhetsledning bör dels innehålla de *krav* man ställer på processer, aktiviteter och uppgifter och dels de *instruktioner* som säkrar att processerna, aktiviteterna och uppgifterna utförs på ett riktigt sätt. Det inte räcker emellertid inte med att en instruktion finns, utan man måste också på något vis säkerställa att den är riktig och att den faktiskt följs. För att säkerställa att den är riktig kan man använda sig av något slag av *simulator*, mot vilken man testar sina instruktioner. Då måste man visserligen först säkerställa att simulatorn ger en riktig beskrivning av hur systemet uppför sig i olika situationer. För att säkerställa att drift- och underhållspersonal följer de instruktioner som definierats kan man göra en jämförelse mellan instruktionerna och hur arbeten görs i verkligheten, dvs. man gör en *auditering* av arbetsprocesserna.

När det gäller verksamheter där säkerheten är en kritisk faktor, är det vanligt att samhället inrättar en *myndighet* som får uppgiften dels att ställa krav på verksamheten och dels att övervaka att kraven är uppfyllda (Wahlström, 2007). Myndighetstillsynen kan för organisationen ses som ett yttre av samhället upprätthållet system, som på samma sätt som organisationens eget system för säkerhetsledning strävar efter en hög säkerhet. Säkerhetsledningen och de dokument som beskriver hur säkerhetsledningen realiseras kan ses som styrsystem som implementerar målet säkerhet. Jag skall därför nedanför mera i detalj granska de förutsättningar som måste gälla för att en styrning skall fungera.

Systemteknikens tre problem

På en mycket generell nivå kan man tala om ett system **S**, som styrs av en ingång **u** och som genererar en utgång **y**. Man kan då särskilja mellan systemteknikens tre problem (Wahlström, 1994). För det första har man en mängd ingångs- utgångspar $(\mathbf{u}_i,\mathbf{y}_i)$ för $i\in\{1, ... ,N\}$ och man söker en modell **M**, som på bästa sätt avbildar systemet **S**. Man kan säga att detta problem är att *modellera* systemet **S**. För det andra har man en ingång $\mathbf{x}_j$ och en modell **M** av systemet **S** och man söker ett sätt att beräkna den utgång $\mathbf{y}_j$, som systemet väntas ge när ingången $\mathbf{x}_j$ appliceras. Man kan säga att detta problem är att *simulera* systemet **S**. För det tredje har man en önskad utgång $\mathbf{y}_k$ och en modell **M** av systemet **S** och man söker ett sätt att beräkna den ingång $\mathbf{x}_k$ man skall applicera för att systemets utgång skall vara så nära $\mathbf{y}_k$ som möjligt, dvs. man söker ett sätt att *styra* systemet. Detta är det egentliga styrproblemet och vi kan se att det tredje problemet förutsätter att vi lyckats lösa de två första.

En komplikation av modelleringsproblemet är att vi måste ta hänsyn till det *tillstånd* systemet befinner sig i när vi applicerar en styrning. Med tillstånd menar vi en storhet som integrerar allt som tidigare har hänt systemet fram till en tidpunkt t=0, så att man kan tala om ett begynnelsetillstånd $\mathbf{x}_0\in\mathbf{X}$, som tillsammans med en styrning $\mathbf{u}(t)$ för $t\in(0,T]$ genererar en entydig trajektorie $\mathbf{x}(\mathbf{x}_0,\mathbf{u}(t))$ i tillståndsrummet **X**. Varje deltrajektorie $\mathbf{x}(\mathbf{x}_\tau,\mathbf{u}(t))$ för $0<\tau<T$ och $t\in(\tau,T]$ är då också en del av denna trajektorie. Ett exempel är att se på en bil som kör på en väg. Tillståndet för bilen kan karakteriseras av den väg den kört och den hastighet den har.

Styrningen som påverkar tillståndet är trycket på gasen eller på bromsen, som bestämmer den momentana hastigheten och som i sin tur bestämmer den väg som tillryggalagts.

Bilexemplet visar på att vi förenklar det verkliga systemet, bilen, så att vi endast är intresserade av bilens tillryggalagda väg och momentana hastighet. I verkligheten har bilen naturligtvis betydligt flera tillstånd som kan karakteriseras av ålder, märke, kondition etc. För att mera noggrant förstå hur en bil rör sig längs en väg, bör man även ta med tillståndet hos föraren och vägen. Det att man begränsar sig till bara hastighet och väg, betyder då att man för tillfället inte är intresserad av de andra tillståndskomponenterna. Syftet med modellen förmedlar alltså det tillstånd vi är intresserade av.

Tillståndsbegreppet är i säkerhetssammanhang viktigt, eftersom man kan tänka sig en uppdelning av tillståndsrummet i tre icke överlappande delar, dvs. $\mathbf{X}= \mathbf{X}_d \cup \mathbf{X}_o \cup \mathbf{X}_g$, där $\mathbf{X}_d$ är tillstånd som kan karakteriseras som osäkra (dåliga), $\mathbf{X}_g$ är tillstånd som kan anses säkra (goda) och $\mathbf{X}_o$ är tillstånd som inte tillhör någon av de tidigare mängderna (oavgörbara). Man kan då tala om säkerhetsledningens två problem, antingen är systemet i den säkra regionen och man vill hålla det där eller så har det kommit i den osäkra eller oavgörbara regionen och man vill komma tillbaka till den säkra regionen. De två problemen kan formuleras på följande sätt, 1) $\mathbf{x}_\tau \in \mathbf{X}_g$ och man söker sådana styrningar $\mathbf{u} \in \mathbf{U}_g(\mathbf{x}_\tau)$ så att trajektorien $\mathbf{x}(\mathbf{x}_\tau,\mathbf{u}(t))$ håller sig inom $\mathbf{X}_g$ och 2) $\mathbf{x}_\tau \in \mathbf{X}_d \cup \mathbf{X}_o$ och man söker sådana styrningar $\mathbf{u} \in \mathbf{U}_g(\mathbf{x}_\tau)$ så att trajektorien $\mathbf{x}(\mathbf{x}_\tau,\mathbf{u}(t))$ så snart som möjligt återförs till $\mathbf{X}_g$. Man ser att det skulle vara värdefullt att på något vis kunna karakterisera de tre delarna av tillståndsrummet $\mathbf{X}$.

Beslut och styrning

Det kan i det här sammanhanget vara på sin plats att i korthet reda ut skillnaden mellan enskilda beslut och styrningen av en process. Ett enskilt beslut kan ses som ett slag av optimering. Man har ett antal alternativ $A=\{a_1, \ldots, a_m\}$, som man skall välja mellan och man gör en bedömning $B=\{b_1, \ldots, b_m\}$, av vad de kommer att leda till i form av nytta för beslutsfattaren. En rationell beslutsfattare väntas då välja det beslut beslutsalternativ a_k, som har egenskapen $b_k \geq b_i$ för alla $b_i \in \{1, \ldots, m\}$. En komplikation är här att beslutsfattaren kanske inte känner den väntade nyttan för alla beslutsalternativ. Beslutsfattaren kan då ge sig tid att närmare reda ut vad de olika beslutsalternativen kan väntas leda till och vad då nyttan av utfallet kan vara. Tyvärr kan en sådan strategi ofta leda till beslutsförlamning snarare än till optimala beslut.

Beslutsfattare måste alltså i en situation välja ett beslut som är tillräckligt bra hellre än att försöka hitta det bästa beslutet. Här har forskning visat att människan verkar ha två olika beslutssystem, ett som gör besluten snabbt, men som ibland kan ta fel och ett annat som gör noggranna avvägningar, men som fungerar långsamt. Detta betyder att man måste skilja mellan beslut som kan göras med god tid och beslut som görs i realtid, dvs. sådana där situationen förändras kontinuerligt. Praktiskt betyder detta att man för realtidsbeslut måste vara väl förberedd t.ex. genom långvarig träning eller genom att använda detaljerade instruktioner. Beslut som görs med det långsamma och eftertänksamma systemet kan då

användas för att se till att det finns metoder och verktyg, som säkerställer att tillräckligt bra realtidsbeslut kan göras.

När man talar om styrning menar man vanligen till varandra kopplade beslut som sker i realtid. En form av styrning är visserligen att man vid olika närliggande tidpunkter gör justeringar så att det styrda systemet anpassar sig till den för handen varande situationen. I bilexemplet kan man säga att realtidsbeslut eller styrning sker då man vrider på ratt och trycker på gas eller broms och att den långsamma men eftertänksamma typen av beslut t.ex. görs då man bestämmer vilket bilmärke man vill köpa.

Fyra nödvändiga villkor för att styra

Vi har nu kommit så långt att vi kan tala om nödvändiga villkor för att styrproblemet skall vara möjligt att lösa (Zadeh, Desoer, 1963). Om inte de nödvändiga villkoren är uppfyllda, så måste man gå tillbaka antingen till sin modell eller till de mål man vill uppnå. Det första villkoret, som egentligen är uppenbart, är att man vet vad man vill. Om man inte har ett mål som man vill uppnå med sin styrning, så kan resultatet knappast bli bra. Alltså det första villkoret är att man har definierat en *målfunktion*. Målfunktionen kan konstrueras på många olika sätt. Ett sätt är att röra sig från A till B på snabbaste tid, ett annat kan vara att en sådan förflyttningen skall ske med en så liten ansträngning som möjligt.

Ett andra krav är att man har en rimligt riktig *modell* av det system man önskar styra. Om man inte har den ringaste uppfattning om hur systemet reagerar för olika input, kan man knappast nå sina mål. En systemmodell behöver inte vara speciellt raffinerad, men huvudsaken är att den med de valda begränsningarna speglar systemets beteende på ett riktigt sätt. Den modell man söker kan hittas på många olika sätt. Ett sätt är att använda sig av olika orsak–verkan förklaringar, som finns tillgängliga för olika situationer. Forskare menar t.ex. att den tidiga människan använde sig av berättelser (narratives) för att förstå sin omvärld och för att i den agera på ett ändamålsenligt sätt.

Ett tredje krav på en framgångsrik lösning på ett styrproblem är att systemet man vill styra är *observerbart*. Detta krav har egentligen att göra med den modell man använder för sitt system och de tillståndskomponenter man är intresserad. Observerbarhet betyder att man kan följa med hur systemets tillstånd ändras med tid, så att man kan ställning till de styråtgärder som behövs i den för handen varande situationen.

Det sista kravet för en framgångsrik lösning på ett styrproblem är att systemet man vill styra är *styrbart*. Detta kanske kan ses som en tautologi, men så är det inte. För att ett system skall vara styrbart, så måste vi ha möjligheter att påverka systemets tillstånd i en önskad riktning. I bilexemplet är det uppenbart att vi har det. Vi kan med gas och broms välja den hastighet med vilken bilen rör sig, vilket gör att vi kan styra både hastighet och väg. Nedanför skall jag kort diskutera begreppet säkerhetskultur, som på senaste tid använts mycket i säkerhets-sammanhang. Problemet här är att säkerhetskultur är en modell som knappast kan anses varken observerbar eller styrbar.

Modelleringens problem

När man bygger en modell av ett system så är det vad man är intresserad av, som ger den första avgränsningen av modellen. Man gör då först en åtskillnad mellan system och omgivning. Denna avgränsning är i många avseende godtycklig, men man brukar ofta försöka göra den på så sätt att systemets interaktion med omgivningen är så liten som möjligt. Nästa steg i att bygga en modell att lyfta fram de detaljer av systemet man är speciellt intresserad av att undersöka. Detta sker vanligen så att man väljer de tillståndskomponenter man är intresserad av och lämnar bort alla andra. Om man t.ex. vill bygga en modell av ett flygplan, så är man kanske intresserad av hur det rör sig i rummet, vilket då betyder att man behöver sex rumskoordinater (x, y, z, ϕ, φ, ψ) med avseende på vilka man ser hur väg och hastighet förändras beroende av de krafter som påverkar flygplanet. Detta ger en betydligt mera komplicerad modell än bilexemplet ovan, men lämnar också här mycket av det verkliga systemet obeaktat.

En modell är alltid en förenkling av verkligheten och man kan säga att förenklingen är modellens både styrka och svaghet. Modellen gör att man kan koncentrera sig på det man önskar studera och lämna bort allt det andra. Modellen bör dock vara tillräckligt komplicerad för att inte vara trivial, men inte så komplicerad att den blir ohanterlig. Viktigt med en modell är att man är medveten om när de förenklingar man har gjort inte mera kan anses giltiga.

Modellen är en nödvändig komponent för att man skall kunna lösa styrproblemet. I och med att man har valt bort flera av systemets tillståndsvariabler i sin modell, så betyder det att man begränsar sig till att styra de tillståndsvariabler man har i sin modell. Modellen skall således vara både observerbar och styrbar för att den skall vara användbar. Om den inte är det får man välja sin modell på något annat sätt. Ett sätt att få en hanterbar modell, är att bestämma sig för om man vill modellera antingen en systemhelhet på ett övergripande sätt eller gå ner i mindre delar av systemet för att få en större detaljrikedom.

Speciellt när man vill studera säkerhetsledning inser man att inte alla aktiviteter i och kring en industriprocess, ett flygplan och ett stort fartyg är lika viktiga för säkerheten. Detta faktum har adresserats med principen om *ett anpassat förhållande till säkerheten*, som i all enkelhet betyder att man skall sätta mera resurser på det som är viktigt för säkerheten än man sätter på det som är mindre viktigt. I praktiken betyder detta att man måste ha en god uppfattning om vilka händelsekedjor och styrningar som är viktiga för säkerheten. Denna uppfattning tas fram i en *riskanalys* där man går igenom händelsekedjor som kan representera hot mot säkerheten, så att man kan installera styråtgärder som gör att hoten kan undvikas. Riskanalysen kan ses som en modell av hur systemet uppför sig i vissa väl definierade situationer.

Systemet vi försöker styra

Om vi nu antar att systemet vi försöker styra är en stor industrianläggning, ett trafikflygplan eller ett stort fartyg inser man genast att systemet har många mycket olika komponenter. Inom säkerhetsvetenskaperna skiljer man ofta mellan delsystemen *människa*, *teknik* och *organisation* (MTO). Tyvärr är också denna uppdelning alltför grov för att man skall kunna

ge konkreta förslag för hur systemen skall konstrueras och drivas. Om man t.ex. ser på trafikflygplanet, så är det beroende av flera olika organisationer, som alla agerar med sina egna uppgifter och system, för att flygplanet skall kunna genomföra en säker flygning från en stad till en annan. Ett trafikflygplan byggs upp i flera olika konstruktionsprocesser där flygplanets delsystem (flygkropp, motorer, kommunikationsutrustning, etc.) konstrueras. Driftprocessen kommer i sin tur att behöva olika delsystem såsom piloter, flygledning, flygfält, underhåll, osv.

Så länge man begränsar styrproblemet till det tekniska systemen, så har man av tradition goda metoder och verktyg för att bygga sina modeller. När man i stället är intresserad av hur människor i en organisation hanterar styrproblemet blir det betydligt svårare. Visserligen kan man kan ibland begränsa sig till gränssnittet M-T och då tala om ergonomi och de krav man kan ställa på ett tekniskt system för att det skall vara hanterbart. Ett steg svårare blir det när man vill ta med O-systemet och gränssnitten T-O och O-M. För gränssnittet T-O kan en ansats vara att t.ex. ställa krav på att organisationen har funktioner för drift, underhåll, teknikstöd och säkerhetsledning, som alla har de resurser som behövs för det arbete de gör. En liknande ansats kunde vara att för gränssnittet O-M t.ex. kräva att organisationen skall ha ett ledningssystem som beskriver ansvar och befogenheter och den utbildning personer i olika befattningar skall ha.

En ytterligare komplikation är att människorna i en organisation kontinuerligt måste kommunicera med varandra och med det tekniska systemet. Detta kan ske i tal och skrift och det kan ske elektroniskt från kontor eller kontrollrum. När man studerat olyckor visar det sig nämligen ofta att nödvändig information inte har nått fram till de personer som gör beslut i kritiska situationer. Detta anser vi att kan beaktas med att man till MTO-modellen fogar en fjärde komponent *information* (Rollenhagen, 2005). Detta gäller i synnerhet styrsystemen, eftersom tillståndsinformation alltid måste förmedlas från det ställe där den samlas till kontrollalgoritmer och styrelementen. När man ser på I-systemet kan man tänka sig ett tillstånd bildat av den information som samlas in i olika media och de sökalgoritmer som finns för att hitta relevant information.

Tillgängliga styrmetoder

Vart och ett av de fyra MTOI-systemen har sina egna interna styrningar, som måste fungera för att säkerheten skall kunna tillfredsställas. Dessutom måste det finnas styrningar i gränssnitten mellan de fyra systemen. Om man t.ex. ser på T-systemet så har man vanligen ett övergripande styrsystem som sköter koordineringen av olika tekniska delsystem, som sedan vart och ett har sina egna styrsystem. Bland dem finns också de skyddssystem, som har till uppgift upptäcka att en förflyttning till ett osäkert tillstånd har skett och som då initierar en lämplig motåtgärd. På flygplan kan t.ex. ett sådant system vara att sänka nosen och dra på mera gas om läge och hastighet på planet indikerar en fara för stallning. Man brukar också använda så kallade förreglingar som i vissa situationer hindrar kontrollrumsoperatörerna att göra ingrepp som kan innebära risk.

För M-systemet får man tillämpa helt andra styrningar. Man kan använda sig av befallningar eller instruktioner, men här ställs man inför ett problem. För att en befallning skall bli utförd krävs en chef–medarbetar relation. Detta innebär ett slags kontrakt där en person underställer sig en annan mot något slag av ersättning. Här behövs alltså modeller av sociala relationer för att på ett riktigt sätt kunna representera de styrningar som sker i systemet. M-systemet styrs också av instruktioner på många olika nivåer ända från samhällets lagar och förordningar till enkla handlingsinstruktioner och checklistor. Man inser också att det inte räcker med att bara ersätta en gammal instruktion med en ny för att en uppgift skall utföras på ett nytt sätt.

När man ser på hur styrningar exekveras i O-systemet får man igen ta in nya begrepp. För det första har man att göra med ansvar och befogenheter, vilket betyder att man får skilja mellan olika grupper av personer och de uppgifter de utför. Man måste således modellera organisationsstrukturen för att se vilka arbeten olika grupper ansvarar för och vilka befogenheter de har i kritiska situationer. Man brukar förutsätta att organisationen som driver ett system har ett odelbart ansvar för säkerheten, vilket då uppfattas som att den högsta chefen i organisationen fortfarande bär ansvaret, trots att hon eller han har delegerat uppgifter åt sina underordnade. Detta ansvar betyder i princip också att organisationen, dvs. den högsta chefen, ansvarar för att organisationens medlemmar är kunniga och motiverade, samt har alla nödvändiga verktyg och metoder för att utföra sitt arbete. Man brukar ofta säga att en säkerhetsorienterad organisation skall vara en lärande organisation (Wahlström, 2011).

För I-systemets interna styrningar är det en fråga om hur man på lämpligt sätt kan säkra att i de data som samlas är riktiga och hur denna datamängd sedan skall integreras för att ge relevant information åt viktiga styrsystem. I gränssnittet I-M är det igen viktigt att se till att information som behövs i en speciell situation är lätt att hitta.

Ett vanligt sätt att sköta informationsinsamling och -hantering är att definiera ett antal nivåer där en informationsförädling sker när man från en lägre nivå flyttar sig till en högre. På den lägsta nivån har man då enkla mätningar som förmedlar värdet på någon tillståndskomponent. Detta kan ske t.ex. till en operatör via ett visarinstrument eller till en automatisk krets som alarmerar om ett gränsvärde överskrids. På en högre nivå kombineras information från flera olika delsystem och givare, så att förädlad information kan ges vidare. På den högsta informationsnivån kombineras både kvalitativ och kvantitativ information för att stöda operatörer och ledning i deras beslutsfattande.

Säkerhetsledningens styrproblem

Om vi ser på säkerhetsledningen styrproblem kan man skilja mellan uppgiften att dels försöka identifiera brister i det styrda systemet och korrigera dem och dels att värdera effektiviteten av säkerhetsledningens egna uppgifter. När det gäller att identifiera brister i själva systemet får man inbegripa alla delar av MTOI-systemet och deras styrningar. De aktiviteter som då ingår är som tidigare nämnts riskanalys, erfarenhetsåterföring och ändringshantering. Riskanalysen används huvudsakligen för att se om nykonstruktioner eller ändringar är tillräckligt bra. Erfarenhetsåterföringen används under driften av systemet för att identifiera kvarblivna brister i de system man opererar. Ändringshanteringen syftar i sin tur på att sluta återkopplingen från

erfarenheter till bestående förbättringar i systemen. Här är det speciellt viktigt att en tillräckligt noggrann analys görs så att inte en ändring skapar nya problem.

För att utvärdera säkerhetsledningens effektivitet, kan man granska dessa tre aktiviteter. För en bedömning av riskanalysens effektivitet kan man utgå från den kvalitativa modelleringen av de händelsesekvenser man analyserat. Kan man anse att riskanalysen är täckande, riktig och konsistent? För att den skall vara det bör den ha både bredd och djup, dvs. dels täcka in alla de system som kan ha en påverkan på säkerheten och dels gå ner tillräckligt i detaljer. För den kvantitativa delen av riskanalysen, så bör denna göra en riktig uppskattning av frekvensen av de händelser man väntar sig att skall kunna inträffa och allvarligheten av de konsekvenser man kan vänta sig av olika initierande händelser.

För att utvärdera effektiviteten av erfarenhetsåterföringen kan man se på vilka händelser som tas upp för en mera noggrann analys. Är de för många, så kanske man inte orkar genomföra analysen med den detaljrikedom som skulle behövas, men är de för få kanske man missar viktig information. En händelseanalys börjar med att man etablerar en beskrivning av vad som har hänt. I nästa skede av analysen frågar man *varför* i flera led. Varför fungerade inte de skydd som borde ha funnits, varför reagerade inte operatörerna, varför var instruktionen felaktig osv? Viktig här är att förstå att det egentligen inte finns något absolut kriterium för var man skall stanna i sin analys. Då svaren har etablerats så går det vanligen att urskilja ett mönster, man kan t.ex. identifiera tekniska system som har felfungerat, styrsystem som inte fungerat som det var tänkt eller felaktiga och uteblivna ingripanden. I det sista steget kan man sedan närma sig frågan om vad som borde ändras för att inte samma händelse skall inträffa på nytt.

Förslag till ändringar i något av MTOI-systemen förs över till ändringshanteringen. En effektiv ändringshantering börjar vanligen med att man samlar ihop relaterade förslag för att se om de pekar mot gemensamma underliggande brister som borde korrigeras. Då går det kanske att med att helhetsgrepp lösa flera problem samtidigt. Nästa steg är att utarbeta ett preliminärt lösningsförslag, som sedan kan analyseras mera i detalj. I och med att en detaljerad konstruktion har tagits fram, kan man detaljplanera hur den skall införas. En ändring av tekniska delsystem kräver vanligen att de tas ur drift medan ändringen görs och sedan testas efter att ändringen har gjorts. En ändring av organisationen kan kräva t.ex. att befattningsbeskrivningar ses över och att specifika utbildningsinsatser genomförs.

Styrning av säkerhetskultur

Säkerhetskultur fördes in i säkerhetsvetenskapen efter olyckan i Tjernobyl 1986 (IAEA, 1991). Begreppet väckte omedelbar entusiasm och många projekt startades för att definiera vad man menar med säkerhetskultur. Om man idag från den akademiska diskussionen försöker ta till sig vad man har hänt under det kvartssekel som gått, kan man konstatera att det knappast finns konsensus i hur begreppet bör tolkas. Om man sedan ser hur industrin (t.ex. kärnkraft, flyg, sjöfart) tagit till sig begreppet kan man konstatera att alla anser att säkerhets-kultur är viktig och att man bör anstränga sig för att upprätthålla en god säkerhetskultur. Man har också utvecklat olika frågescheman, med vilka man försöker göra mätningar av säkerhets-

kulturen. Man har gjort statistiska analyser av resultaten och har den vägen identifierat ett antal faktorer som kan karakterisera god säkerhetskultur. Också säkerhetsmyndigheterna i en del länder reagerar ibland med påpekandet "dålig säkerhetskultur" i de granskningar som görs.

I diskussionen om säkerhetskultur har man sällan eller aldrig gjort någon djupgående analys av styrbarhetsproblematiken. Om man vill använda säkerhetskultur som en modell för att styra säkerhet borde man ha något slag av relation mellan säkerhetskultur och den säkerhets-prestation som ett system förmår prestera. Redan på denna nivå finns det stora svårigheter. Här kommer bl.a. akademikernas oförmåga in att komma överens om vilka komponenter som skall räknas in i begreppet säkerhetskultur och och vad som behövs för att en säkerhetskultur skall kunna anses god.

Man kan visserligen tänka sig att man försöker styra mot en god säkerhetskultur som ett värde i sig självt, men då bör man fortfarande ha en idé om hur man kan påverka säkerhetskulturen och hur man kan observera resultaten. En ansats till tillstånd kunde vara att man ser på de begrepp man vanligen brukar associera med säkerhetskultur, dvs. attityder, beteenden, föreställningar och värden. Dessa begrepp går dock inte att använda direkt, eftersom de måste sättas i relation till varandra och till händelser, objekt och situationer. En annan svårighet är att man för att kunna tala om en säkerhetskultur hos en organisation måste göra något slag av integrering över organisationens medlemmar. Hur skall denna göras, lika över alla, i förhållande till säkerhetsrelaterade uppgifter personerna gör eller på något annat sätt? Nästa fråga är vad man sedan kan göra för att påverka säkerhetskulturen. Det vanliga är att föreslå något slag av upprycknings-projekt, som då predikar vikten av säkerhet och illustrerar med bilder av hur illa det kan gå. Här kunde man kanske tala om metoderna, skrämma, hota och muta, men det är tvivelaktigt om sådana metoder kan användas i detta sammanhang.

Vi ser alltså att kraven på modell, observerbarhet och styrbarhet blir svåra att uppfylla för begreppet säkerhetskultur. Hur är det då med en målfunktion? För att konstruera en mål-funktion är det kanske tillräckligt om man kan anta att ett antal utbildade specialister gör intervjuer och observationer och den vägen gör en subjektiv bedömning av säkerhetskulturen på någon lämpligt vald skala. Här uppstår det två svårigheter. Den ena svårigheten är att en kännedom om experternas bedömningsgrunder kan antas påverka de mätresultat man får. Den andra svårigheten uppstår om bedömningsgrunderna inte är kända, för att detta kan göra det enkelt för de bedömda att förklara dåliga resultat med att experterna inte har förstått de svar de har fått och de situationer de observerat.

I och med att det uppstår problem i att försöka styra säkerhet genom säkerhetskultur eller att styra säkerhetskultur som ett inneboende värde, kan man fråga på vilket sätt begreppet säkerhetskultur kunde vara användbart. Min uppfattning är att det skulle vara fel att helt döma ut begreppet, eftersom det har rönt ett stort intresse och har blivit väletablerat. En möjlighet kunde vara att i gruppdiskussioner om säkerhet använda säkerhetskultur som ett samlande begrepp på mycket som kan gå rätt eller fel. Genom att var och en i diskussionen definierar hur hon eller han förstår begreppet och illustrerar med situationer där man kan se exempel på god eller dålig säkerhetskultur, så lyckas man ofta stimulera till upplysande diskussioner, som bl.a. förmedlar en insikt i hur envar på sitt sätt bidrar till en god säkerhet.

Några kvarvarande problem

När man ser på de begränsning som innefattas i ett ledningssystem, kan man se att kanske den största svårigheten uppstår i att modellera sitt system. Det är många komponenter som på något vis kan påverkar hur en händelsekedja kommer att utveckla sig. Vilka bör man ta med och vilka kan man lämna bort? Det är inte heller sagt att man känner alla de påverkans-mekanismer som kan uppträda och hur de påverkar i olika situationer. Speciellt när man försöker modellera människor och organisationer är det inte ens sagt att det finns någon vedertagen teori för hur interaktioner på en mikronivå genererar beteenden på en makronivå. Allt detta gör att varje modell av helheten måste bli mycket grov.

Till detta kommer några resultat från matematiskt teori, som bl.a. visar att ett instruktions-system aldrig kan bli fullständigt och att man aldrig a priori kan säga om ett visst system kommer att nå ett visst tillstånd eller inte. Vidare vet man att vissa olinjära system uppvisar ett kaotiskt beteende, vilket gör att en förutsägelse om deras framtida beteende endast kan var giltigt för en mycket kort tid. Allt detta visar att det också i deterministiska system finns osäkerheter, som är svåra att hantera (Wahlström, Rollenhagen, 2012).

För att få en riskbedömning bör man kunna ge sannolikhetsbedömningar av hur ofta ett identifierat hot kan väntas bli realiserat. För att kunna ge en sådan borde man ha en modell av fördelningsfunktionen. Här har normalfördelningen använts flitigt, vilket är motiverat i många fall. Studier av bl.a. finansmarknader har emellertid demonstrerat att en normalfördelning kan ge mycket stora underskattningar av osannolika händelser. Till detta tillkommer dessutom svårigheten att empiriskt bestämma en sannolikhetsfördelning. Man kanske aldrig kan få en tillräckligt lång observationsperiod för att man med ett visst mått av säkerhet skall kunna säga något om sannolikhetsfördelningen.

När man ser på dessa problem kan man inte frigöra sig från uppfattningen att det bland lekmän och varför inte också bland specialister, ofta finns en alltför stor övertro till riktigheten av de modeller man använder. Det är ofta också så att en mycket detaljerad modellering av det tekniska systemet inte försvarar sin plats i en bedömning av helhetsrisker, om man inte har en i stort sett lika god modell av de människor och de organisationer som hanterar det tekniska systemet. I detta sammanhang har begreppet resilience engineering förts fram som ett komplement till klassisk säkerhetsteknik. I begreppet ingår tanken, att man i systemen skall bygga in en bättre återhämtningsförmåga, så att systemens olika delar lättare kan kompensera för störningar och normal variabilitet som alltid uppträder.

Slutsatser

Till slut vill jag föra fram några synpunkter jag tycker blir uppenbara, när man försöker tillämpa kontrollmetaforen på begreppet säkerhetsledning. Först och främst det att man kan identifiera sitt problem (modellering, simulering, styrning) är redan till en stor hjälp. Vill man med sin modell bara förstå och beskriva eller vill man också ha den som hjälp för att styra sitt system? Om man vill styra så är det tillrådligt att gå igenom de fyra nödvändiga villkoren för en framgångsrik styrning. Om något av villkoren inte är uppfyllda, så bör man försöka ändra

på sin modell. Sedan är också tanken att särskilja mellan de fyra olika MTOI-systemen värd att uppmärksamma, eftersom systemen är mycket olika till sin karaktär och därför kräver olika typer av modeller och styrningar. Idén att begränsa sin modell till det man för ögonblicket är intresserad av, kan också vara till stor hjälp när man försöker hitta något som är hanterbart, men i alla fall kan ge vettiga svar på de frågor man vill ställa. Till sist tror jag att tanken om tre distinkta regioner i systemets tillståndsrum kan vara till stor hjälp när det gäller att skapa styralgoritmer som förmår hålla systemen inom regionen av säkra tillstånd.

När man ser styrning av säkerhet mera generellt, så tror jag att det är viktigt att inse att det alltid kommer att finnas brister i vår förståelse av system och omvärld. Detta har också förts fram inom ett koncept som kallas resilience engineering (Hollnagel et al., 2006). Vi skall naturligtvis försöka modellera våra system så bra som möjligt, men vi måste alltid vara beredda på överraskningar av sådant som vi inte visste. Samtidigt måste vi ha en förmåga att ta till oss de erfarenheter som kan samlas både från det egna systemet och från andra liknande system. Detta betyder bl.a. en öppenhet för intryck från omvärlden. Eftersom det verkar finnas en övertro på vår förmåga att ge förutsägelser när det gäller risk, så kan det vara på sin plats att åtminstone de som arbetar inom området säkerhet undviker att komma med alltför självsäkra påståenden av typen "systemen är absolut säkra" eller "vi har tänkt på allt".

För att kunna argumentera för att använda ett system som för med sig risker, bör man kunna argumentera för att samhällets helhetsnytta är betydligt större än det riskbidrag som systemet ger. För att kunna göra detta måste man kunna ge något slag av kvantitativ riskbedömning, som är försvarbar även i det fall att en olycka har hänt. Här får man t.ex. argumentera för att ett modernt samhälle förutsätter att vissa tjänster såsom kraftförsörjning och transporter fungerar, vilket då betyder att man kan tolerera olyckor och tillbud under förutsättning att de sker tillräckligt sällan. Om vi lyckas ta till oss de erfarenheter som hela tiden skapas i världen, borde det med nuvarande kommunikationer vara möjligt att bygga upp de lärande system, som många inom området säkerhetsteknik frågar efter (Rollenhagen, Wahlström, 2013).

Referenser

Hollnagel E., Woods D.D., Leveson N., 2006. Resilience engineering: Concepts and precepts, Ashgate.

IAEA, 1991. Safety Culture, INSAG-4, International Atomic Energy Agency, Vienna.

Rasmussen J., Svedung I., 2000. Proactive risk management in a dynamic society, Swedish Rescue Services Agency, Karlstad, Sweden.

Rollenhagen, C. 2005. Säkerhetskultur, RX Media, Stockholm.

Rollenhagen, C., Wahlström, B. (2013). Ledning av säkerhetskritiska organisationer, en introduktion, Studentlitteratur AB, Lund.

Wahlström B., 1994. Models, modelling and modellers; an application to risk analysis, European Journal of Operations Research (EJOR), Vol.75, Issue 2.

Wahlström B., 2007. Reflections on regulatory oversight of nuclear power plants, Int.J.Nuclear Law, 1, No. 4.

Wahlström B., 2011. Organisational learning – reflections from the nuclear industry, Safety Science 49, 65–74.

Wahlström, B., Rollenhagen, C. Safety management – A multi-level control problem. Safety Sci. (2013), http://dx.doi.org/10.1016/j.ssci.2013.06.002.

Zadeh L., Desoer C., 1963. Linear systems theory, McGraw Hill, New York.

Om författaren

Björn Wahlström (Djurholmsvägen 2, 22920 Brändö, bjorn@bewas.fi) föddes den 22 april 1944 i Jakobstad, Finland. Han avlade sin diplomingenjörsexamen vid Tekniska högskolan i Helsingfors 1967 med regleringsteknik som huvudämne. Han fortsatte sina studier vid samma högskola och avlade 1971sin licentiatexamen med systemteori som huvudämne och matematik som biämne. Björn anställdes vid Statens tekniska forskningscentral (VTT) 1971. År 1985 utnämndes han till professor och laboratoriechef för VTTs elektrotekniska laboratorium. Under åren 1989-91 var Björn tjänstledig från VTT för att arbeta på International Institute for Applied Systems Analysis i Laxenburg utanför Wien i Österrike. Från 1994 fram till sin pensionering i januari 2008 innehade han en forskningsprofessur i systemteknik på VTT. Under sin yrkeskarriär har Björn deltagit i flera arbetsgrupper inom IAEA och OECD/NEA. Han var koordinator for EU-projekten ORFA och LearnSafe, som under åren 1998–2004 undersökte inverkan av ledning och organisation på kärnkraftens säkerhet. Han har skrivit mer än 300 artiklar inom områdena systemteknik, simulering, kontrollsystem, kärnkraft, kontrollrumsplanering, MTO-frågor, organisation och ledning, riskanalys samt teknologiplanering och innovationsprocesser. Efter sin pensionering utför Björn konsultuppdrag genom sin egen firma Oy Bewas Ab.