

Innehållsförteckning

Sammanfattning	7
Läsanvisningar	7
1. Bakgrund	8
2. Några grundläggande begrepp	9
2.1. Verifiering, validering och ackreditering	9
2.2. Risk	11
2.3. Trovärdighet	11
3. Verifiering, validering och ackreditering	12
3.1 Modellerings- och simuleringsprocessen.....	12
3.2 Verifierings-, validerings- och ackrediteringsprocessen.....	13
3.3 Metoder och tekniker för verifiering och validering - en översikt.....	14
4. Riskteori	16
4.1 Historiskt perspektiv	16
4.2 Kvantifiering av risker	16
5. Riskanalys generellt	17
5.1 Hur genomförs en riskanalys?	17
5.1.1 Vilka riskhändelser kan uppstå och vilka följder kan dessa få?	17
5.1.2 Vad kan orsaka riskhändelserna?.....	18
5.1.3 Hur troligt är det att riskhändelserna inträffar (risktalet)?	19
5.1.4 Vilka är riskbärare?.....	20
5.1.5 Vilken nytta kan systemet ge?	20
5.2 Metodik för att genomföra en riskanalys	21
5.2.1 Preliminary Hazard Analysis –PHA	21
5.2.2 Failure Modes and Effect Analysis (FMEA).....	21
5.2.3 Felträdsanalys	21
5.2.4 Händelseträdsanalys.....	23
5.2.5 Hazard and operability analysis (HAZOP)	23
6. Riskanalys för simuleringsmodeller	24
6.1. Jämförelse mellan tekniska system och simuleringsmodeller	24
6.2. Varför bör en riskanalys genomföras inför utveckling av en simuleringsmodell?.....	25
6.3. Hur genomförs riskanalysen?	25
6.3.1. Vilka riskhändelser kan uppstå?	25
6.3.2. Vilka följder kan riskhändelserna få?	26
6.3.3. Vad kan orsaka riskhändelserna?.....	27
6.3.4. Hur troligt är det att riskhändelserna inträffar (risktalet)?	28
6.3.5. Vad kan göras för att nedbringa risktalet och/eller minska omfattningen av konsekvensen av riskhändelserna?	28
6.4. Hur kan riskanalysen ligga till grund för inriktning av V&V- aktiviteterna?	28

7. ITOP-metoden: En struktur för inriktning av V&V-aktiviteter	29
8. Exempel: Riskanalys av en modell för ett autonomt samverkande robotsystem	30
8.1. Bakgrund.....	30
8.2. Val av modell.....	30
8.3. Beskrivning av modellen	31
8.4. Genomförande av riskstudien	32
8.4.1. Metodik för riskanalysen	32
8.4.2. Vilka riskhändelser kan uppstå?	35
8.4.3. Vilka följder kan riskhändelserna få?	36
8.4.4. Vad kan orsaka riskhändelserna?.....	37
8.4.5. Hur troligt är det att riskhändelserna inträffar?.....	38
8.4.6. Hur bör V&V-aktiviteterna inriktas utifrån resultatet av riskanalysen?	39
8.5. Vad kom ut av riskstudien?	39
9. Generella slutsatser.....	40
10. Fortsatt arbete.....	41
11. Referenser.....	42

Sammanfattning

Användningen av simuleringsmodeller ökar alltmer inom militär verksamhet. Samtidigt har modellerna blivit alltmer komplexa, vilket lett till att det idag kan vara svårt att få ett grepp om modellernas trovärdighet.

Verifiering, validering och ackreditering av simuleringsmodeller är en process som syftar till att öka tillförlitligheten hos simuleringsmodeller och att ge användaren av en modell information om dess lämplighet för ett givet syfte samt om vilken tilltro han kan sätta till modellen. Denna process bidrar även till att fel och ofullständigheter ofta upptäcks tidigt under utvecklingsprocessen, vilket kan vara av betydande ekonomiskt intresse.

För att avgöra hur stora resurser som skall avsättas till verifierings- och valideringsarbete bör man ställa sig frågor som

- Vilka riskhändelser är förknippade med felaktigheter i modell eller data eller felaktigt användande av densamma?
- Vilka konsekvenser kan dessa riskhändelser få?
- Hur mycket kan vi nedbringa sannolikheten för att riskhändelserna inträffar?

Genom att kartlägga riskerna med en simuleringsmodell och på ett strukturerat sätt beskriva vad som gjorts för att undvika eller reducera dessa, ges även kund/användare en insyn i modellens trovärdighet.

Denna rapport syftar till att belysa frågor om hur en riskanalys genomförs samt hur ett riskperspektiv kan ligga till grund för inriktningen av verifierings- och valideringsaktiviteter samt utgöra ett underlag vid bedömningen av dessa resursers omfattning. Ett exempel ges rörande en forskningsmodell av ett autonomt samverkande robotsystem.

Läsanvisningar

Kapitel 2 och 3 riktar sig till läsare med ringa kunskap inom modellering och simulering. I kapitel 2 ges en förklaring av använda begrepp och i kapitel 3 ges en sammanfattning av M&S- och VV&A-processerna samt en översikt över V&V-tekniker. Kapitel 4 ger en historisk tillbakablick på riskteorin samt tar upp några allmänna frågor rörande riskkvantifiering. I kapitel 5.1 tar vi upp vilka frågor en riskanalys generellt syftar till att belysa, och ger i kapitel 5.2 exempel på några vanliga använda metoder för detta. I kapitel 6 betraktar vi riskanalysprocessen speciellt för simuleringsmodeller, och i kap 8 genomför vi denna för en modell av ett autonomt samverkande robotsystem. Kapitel 7 beskriver en metodik för framtagning av den information som ligger till grund för ett ackrediteringsbeslut. I kapitel 9 ges några generella synpunkter som robotstudien lett fram till och i kapitel 10 kommenteras framtida arbete inom området.

1. Bakgrund

Det är en genomgående trend att världens försvarsmakter alltmer använder sig av modeller och simuleringar som stöd för sin verksamhet.

Det finns flera skäl till denna ökade efterfrågan på simuleringsmodeller. Den tekniska utvecklingen på datorområdet har givit nya möjligheter även inom modellering och simulering. Exempelvis har teknik för distribuerad interaktiv simulering gjort det möjligt att samköra flera olika modeller, som är utvecklade på olika håll och för olika syften, i en och samma simulering på geografiskt skilda datorer. Man kan därigenom koppla samman simuleringsmodeller på olika nivåer, simulatorer och mänskliga beslutsfattare. Simuleringsmodeller har dessutom kort svarstid och stor flexibilitet och kan även användas för att studera framtida systemvarianter. Detta tillsammans med minskade ekonomiska ramar har lett till att simuleringsmodeller allt oftare används dels för att ersätta mer konventionella metoder och dels för att undersöka komplicerade komplexa förlopp som annars ej kunnat studeras p.g.a. risker för både människor och miljö. Inom Försvarsmakten (FM) utnyttjas simuleringsmodeller vid såväl studier och analys som utbildning och träning. Simuleringsmodeller används också i materielanskaffningsprocessen och som planeringsinstrument.

Den tekniska utvecklingen har medfört en kraftigt ökad komplexitet hos simuleringsmodellerna. Det kan idag vara i det närmaste omöjligt för någon, inkluderande modellutvecklaren, att ha kontroll över alla delar av en modell och kunna garantera att dessa är korrekta. Beställare och användare av modellerna har naturligtvis ännu svårare att få ett grepp om vilken tilltro de kan sätta till modellerna. Hur vet vi då att de modeller som vi utvecklar och utnyttjar inom försvaret verkligen fångar de egenskaper som vi är ute efter att beskriva och hur vet vi att modellerna är användbara för sina syften?

Verifiering, validering och ackreditering av simuleringsmodeller är en process som syftar till att öka tillförlitligheten hos simuleringsmodeller och att ge användaren av en modell information om dess lämplighet för ett givet syfte samt om vilken tilltro han kan sätta till modellen. Denna process bidrar även till att fel och ofullständigheter ofta upptäcks tidigt under utvecklingsprocessen, vilket kan vara av betydande ekonomiskt intresse.

Hur stora resurser som bör avsättas för verifierings- och valideringsarbete är beroende av tillämpningens art och syfte.

Det arbete som beskrivs i denna rapport har genomförts inom FM-projektet "Verifiering, validering och ackreditering av simuleringsmodeller" som ett första steg i att öka vår insikt inom området riskanalys av simuleringsmodeller genom att belysa frågor om hur en riskanalys genomförs samt hur ett riskperspektiv kan ligga till grund för inriktningen av verifierings- och valideringsaktiviteter samt utgöra ett underlag vid bedömningen av dessa resursers omfattning.

2. Några grundläggande begrepp

2.1 Verifiering validering och ackreditering

Innan vi förklarar innebörden av begreppen verifiering och validering och skillnaden mellan dessa ger vi en enkel förklaring av modellering och simulering.

Med en *modell* avses en fysikalisk, matematisk eller på annat sätt logisk representation av ett system, enhet, fenomen eller process.

En *konceptuell modell* är en redogörelse för kundens/användarens och modellutvecklarens gemensamma uppfattning om modellens innehåll och interna representationer.

Simulering är att experimentera med en modell över tiden.

De definitioner som anges nedan för verifiering, validering och ackreditering, följer Department of Defense (DoD) Directive 5000.59 och är de som används i ”VV&A Recommended Practices Guide” [RPG2000].

Validering är en process som avgör till vilken grad en modell eller simulering är en god representation av verkligheten med hänsyn till modellens syfte.

Verifiering är en process som avgör om en modellimplementation representerar utvecklarens specifikationer. Man talar också om verifiering av kravuppfyllnad, d v s kontroll av att kundens kravspecifikation är uppfylld.

Verifiering görs således mot ett dokument, såsom modellutvecklarens specifikation eller kundens kravspecifikation. Validering däremot görs mot verkligheten.

Förenklat brukar man säga att validering handlar om att bygga rätt modell,



medan verifiering handlar om att bygga modellen rätt.

På basis av verifierings- och valideringsresultaten kan sedan ett ackrediteringsbeslut fattas.

Ackreditering är ett officiellt bemyndigande att en modell får användas i ett visst syfte.

I fortsättningen kommer modellering och simulering att förkortas M&S, verifiering validering och ackreditering att förkortas VV&A och verifiering och validering att förkortas V&V.

Mycket förenklat kan man säga att en M&S-process ser ut på följande sätt:

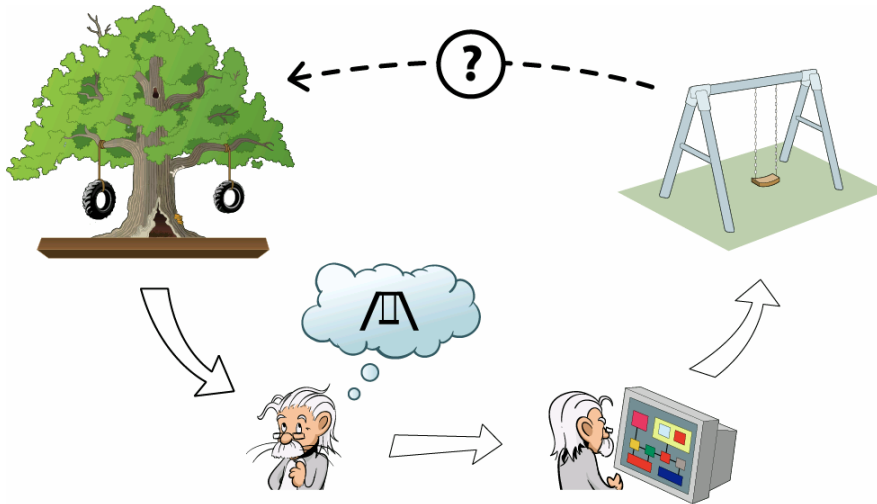


Bild 1: Förenklad M&S-process

Trädet representerar en del av verkligheten. Vi är intresserade av att avbilda den del av verkligheten som utgörs av en gunga. Vi gör oss då en mental bild (en konceptuell modell) av hur denna gunga skall avbildas (vilka funktioner som skall finnas med) och dokumenterar den i en konceptuell modellbeskrivning. När vi är nöjda med den konceptuella modellen och den är ordentligt validerad mot verkligheten överför vi denna till en datormodell. Detta arbete måste ordentligt verifieras mot den konceptuella modellen så att det sker på ett korrekt sätt. När vi sedan kör den färdiga gungmodellen skall resultaten valideras mot uppträdandet hos gungan i verkligheten med avseende på de egenskaper som är av intresse.

Parallellt med begreppet VV&A förekommer beträffande data begreppet VV&C (verifiering, validering och certifiering).

Verifiering av data fastställer att data som produceras överensstämmer med en specifikation.

Validering av data fastställer att data är en god representation av verkligheten.

Certifiering av data är en process som fastställer att data är lämpliga för en viss tillämpning.

Med begreppet *oberoende V&V* avses det VV&A-arbete som utförs av någon eller några andra än modellutvecklingsgruppen. En hel del tester av modellen görs som en naturlig del av modellutvecklingsarbetet, men för modeller som ska användas i mer omfattande sammanhang, där det ställs större krav på modellens validitet, är det viktigt att ha en VV&A-process oberoende av modellutvecklingsprocessen

2.2 Risk

I dagligt tal förknippas risker vanligen med händelser som av en individ eller grupp uppfattas ha ett negativt värde. Ibland används riskbegreppet i betydelsen sannolikheten för att en negativ händelse kommer att inträffa. För att skilja dessa tolkningar åt används i detta dokument begreppen riskhändelse och risktal.

Med *riskhändelser* avses slumpmässiga eller osäkra händelser, vars konsekvenser är av negativt värde.

Med *risktal* avses sannolikheten för att en riskhändelse skall inträffa.

En *riskälla* är en specificerad omständighet som leder fram till en specificerad önskad händelse eller effekt.

Riskbärare är den individ eller grupp av individer som upplever risken.

Om den önskade konsekvensen kan ha varierande storlek brukar ”risk” ange den på något sätt sammanvägda sluteffekten.

2.3 Trovärdighet

För att bedöma en modells trovärdighet bör man ställa följande frågor:

- Är modellen korrekt?
- Är data korrekta och representerar verkligheten?
- Har modellen använts korrekt?
- Har lämpliga scenarier valts?
- Har resultaten tolkats korrekt?
- Om det finns till modellen samverkande enheter, har dessa använts korrekt?

Hur trovärdig en modell behöver vara är beroende av tillämpningens art och syfte. Ofta skall simuleringsresultaten utgöra ett underlag för någon typ av beslutsfattande. Trovärdighetskravet beror då på två aspekter: de konsekvenser ett felaktigt beslut kan leda till samt hur stor inverkan simuleringsresultaten har på beslutet.

Högre krav på trovärdighet medför ökade modellutvecklingskostnader men även ökad användbarhet av modellen. Efter att ha uppnått en viss nivå på trovärdigheten ger oftast fortsatta ansträngningar större kostnader än vinster. Var denna nivå ligger varierar dock från fall till fall beroende på tillämpningens art och syfte.

3. Verifiering, validering och ackreditering

Innan vi går in på riskanalysen ges för den mindre insatte läsaren en översikt över vad M&S- och VV&A-processerna innebär samt en orientering över metoder och tekniker som verifiering och validering kan grunda sig på.

3.1 Modellerings- och simuleringsprocessen

För att beskriva VV&A-processen är det lämpligt att först titta på huvuddragen i M&S – processen, d v s den process av modellerings- och simuleringsåtgärder som leder fram till en simuleringsmodell (se bild 2 nedan).

För överskådlighetens skull har inte iterationer i processen ritats ut, men iterering mellan faserna i processen förekommer i hög grad. Ändras något i en fas måste iterationer i arbetsprocessen beröra också tidigare faser. De olika färgerna på bilden antyder olika aktörer

Processen initieras av att en användare definierar ett problem som han behöver få löst och specificerar krav som inringar användarens syfte. Det är viktigt att man har en klar definition av problemet, eller av vilka frågor man vill besvara, innan man använder sig av M&S. Därefter bestämmer man angreppssätt. Är M&S bästa tillvägagångssättet för att lösa problemet och/eller ska man använda sig av icke-M&S-metoder. Om man väljer att använda sig av M&S måste man specificera krav på simuleringsmodellen. Därefter väljer man alternativ d.v.s. finns redan en befintlig modell som är lämplig att använda utan modifieringar, skall man modifiera en befintlig modell eller behöver man utveckla en helt ny modell.

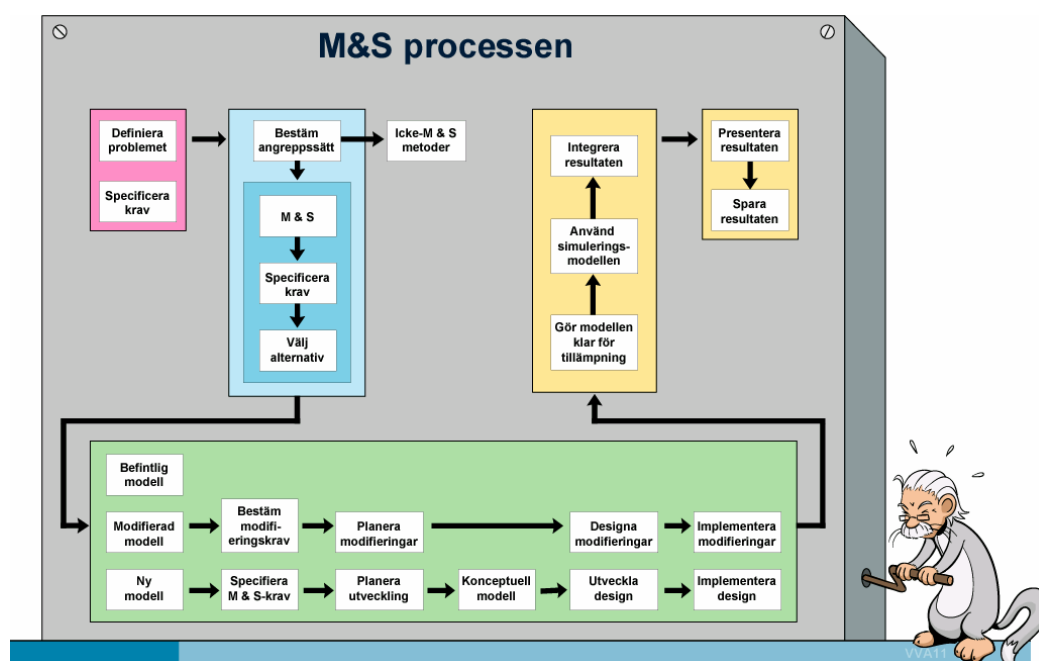


Bild 2: M&S-processen

Om man använder en befintlig modell är det viktigt att man skaffar sig god kunskap om modellen, så att man vet vilka antaganden och begränsningar som ligger till grund för modellen.

Ska modellen modifieras krävs förståelse för hur de tänkta modifieringarna påverkar modellen. Modifieringsprocessens utvecklingssteg är: bestäm modifieringskrav, planera modifieringar, designa modifieringarna och implementera dem.

Vid utvecklandet av en ny modell måste detaljerade krav på simuleringsmodellen specificeras (exakt vad vill man att modellen ska göra). M&S-utvecklingen planeras och en konceptuell modell utvecklas. Denna är grunden för det fortsatta arbetet och det är viktigt att användaren och utvecklaren är överens om den konceptuella modellen innan man går vidare till nästa fas i utvecklingsarbetet. Simuleringsmodellen skall därefter designas och implementeras.

Ett viktigt steg är sedan att försä modellerna med lämpliga data. Först därefter är modellen klar att användas och resultaten presenteras.

3.2 Verifierings-, validerings- och ackrediteringsprocessen

I VV&A-processen ingår följande steg

Definition av VV&A-krav:

När väl ett beslut tagits huruvida ärvd modell, modifierad modell eller helt ny modell skall utnyttjas för aktuell tillämpning måste krav definieras mot vilka VV&A-arbetet skall kunna värderas.

Initiering av VV&A-planering

De planer som skall tas fram fokuserar på att identifiera VV&A-aktiviteter som passar ihop med M&S-plan, krav och resurser.

VV&A av problemkrav

Det är viktigt att validera de krav som ställts upp vid problemdefinitionen, så att simuleringen kommer att behandla rätt problem.

V&V av den konceptuella modellen

Detta är ett mycket viktigt steg och såväl den konceptuella modellen som V&V-arbetet måste dokumenteras. Dokumentationen visar varför (eller varför inte) antaganden, algoritmer, tillgängliga data o s v kan förväntas vara en acceptabel representation av systemet för den tänkta applikationen.

V&V av design

M&S-designen verifieras mot den konceptuella modellen.

V&V av implementationen

När väl implementeringen av designen har resulterat i kod skall denna kontrolleras för att minska risken för programmeringsfel.

V&V för hela tillämpningen

För att kontrollera att den kompletta modellen är tillräckligt noggrann för den aktuella tillämpningen jämförs den med känt eller förväntat uppträdande hos det system den skall representera.

Acceptansvärdering

Acceptansvärdering är det slutliga steget innan beslut kan tas om ackreditering av modellen för ett givet syfte. I detta steg granskas informationen som samlats upp under V&V-arbetet med modellen.

3.3 Metoder och tekniker för verifiering och validering – en översikt

En modell kan bevisas vara inkorrekt, men det ligger i sakens natur att den sällan kan bevisas vara helt korrekt. Man utför därför olika tester på modellen för att försöka belysa dess trovärdighet (eller icke-trovärdighet). Varje misslyckat försök att påvisa brister stärker modellens trovärdighet.

Kärnfrågan i V&V-processen är att välja metoder baserade på vetenskaplig grund som på ett mångsidigt och korrekt sätt belyser modellens giltighet och utesluter så många fel som möjligt.

Metodik för ackreditering tas inte upp som ett särskilt ämne, eftersom det är verifierings- och valideringsarbetet som ligger till grund för ackrediteringen.

Vid *verifiering* utnyttjas metodik för kontroll av att alla antaganden och algoritmer är konsistenta med den konceptuella modellen samt att kodimplementationen av den konceptuella modellen har utförts på ett korrekt sätt.

Validering bör ses som en holistisk process där det samlade resultatet från många olika testmetoder ligger till grund för utsagor om modellens validitet. Metoderna för att jämföra en modell med verkligheten kan indelas i empirisk validering, teoretisk validering och övrig validering.

Empirisk validering baserar sig på någon form av data och är av den typ som vanligtvis förknippas med den matematiska/naturvetenskapliga vetenskapstraditionen.

Teoretisk validering rymmer metoder för test av modellens analytiska stringens, analys av att modellavgränsningar är relevanta och jämförelser av modellen med andra validerade modeller.

Till övrig validering hör metoder i stil med att utnyttja expertbedömningar, att göra jämförelser med doktrin, att göra jämförelser med andra modeller som har osäker valideringsgrad samt att jämföra med andra informationskällor.

V&V-teknikerna brukar man indela i fyra kategorier: informella, statistiska, dynamiska och formella. Användning av matematisk och logisk formalism i varje kategori ökar från informell till formell teknik och därmed också komplexiteten.

Informella V&V-tekniker

Informella tekniker grundar sig på mänskligt förnuft och subjektivitet utan någon sträng matematisk formalism. Som exempel kan nämnas granskning av dokumentationen för modellen eller subjektiva bedömningar av huruvida modellen och dess resultat verkar rimliga.

Statiska V&V-tekniker

Statiska tekniker används av modellutvecklarna och kontrollerar statisk modelldesign och källkod. För detta ändamål finns många automatiska verktyg som kan utnyttjas av vilka simuleringspråkets kompilator är ett. För utnyttjandet av de statiska teknikerna krävs ingen maskinexekvering av modellen. Exempel på statiska tekniker är semantisk analys, som kontrollerar att modellutvecklarens specifikationer är riktigt översatt till kod, och syntaxanalys som ombesörjs av programspråkets kompilator för att försäkra att mekanismerna i språket tillämpas korrekt.

Dynamiska V&V-tekniker

Dynamiska V&V-tekniker kontrollerar modellens uppträdande under exekveringen. Vanligen införs ytterligare kod i modellen för att få information om förloppet under exekveringen.

Ett exempel är ”Comparison testing” som används när flera modeller som representerar samma system finns tillgängliga. De olika modellerna körs med samma indata och därefter sker jämförelser av utdata. Finns det skillnader i utdata avslöjar detta problem med noggrannheten hos någon eller några av modellerna. Andra exempel är ”debugging”, som är en iterativ process för att upptäcka fel i programkoden, och ”felinsättning” som innebär att man sätter in ett fel eller en brist i modellen och observerar när modellen producerar det förväntade felaktiga uppträdandet.

Formella V&V-tekniker

Formella V&V-tekniker baseras på formella matematiska bevis för korrektheten och är de mest effektiva V&V-åtgärderna. Tyvärr kan dagens tekniker för formella bevis av korrekthet inte användas för något mer komplexa M&S-tillämpningar, men de kan utgöra en grund för andra V&V-tekniker.

För en utförligare beskrivning av V&V-teknikerna hänvisas till [RPG2000].

4. Riskteori

4.1 Historiskt perspektiv

I vårt dagliga liv fattar vi ständigt beslut om risker. De flesta av dessa beslut fattar vi utan att vara medvetna om det, därför att vi uppfattar den negativa konsekvensen som acceptabel. Det är först när vi upplever konsekvensen av en händelse tillräckligt negativ som vi medvetet gör en riskbedömning.

Tidigare i historien har riskbedömningar och hantering av risker byggts på generationers samlade erfarenheter [Grimvall 1998].

Genom industrialiseringen infördes ny teknik av vilken man saknade erfarenhet. Detta ledde till inträffande av olyckor, som kunde drabba många samtidigt. För att hantera riskerna fick man kombinera de få olycksdata man hade med kalkyler, vilket var början till dagens riskanalys.



Idag införs stora komplexa system i snabb takt och de negativa konsekvenserna om något går fel kan vara förödande, medan risken för olyckor per system och år vanligtvis är mycket liten [Thedéen 1981]. Vidare har systemen snabb genomslagskraft, vilket medför att långvarig erfarenhet från drift saknas i början. Detta gör det svårt att erhålla skattningar av risker grundade på empiriska dataserier. Kärnkraften är ett exempel på detta, och det var också i och med kärnkraftsdebatten som riskforskningen kom igång på allvar.

Andra områden där riskteorin har haft stor betydelse är inom spelteori och inom försäkringsmatematik. Här kan riskteorin byggas upp på matematiskt statistiska grunder och riskhändelserna kan direkt mätas i ekonomiska vinster och förluster. Vidare är riskbärarna själva de som fattar besluten och även de som får den eventuella vinsten. Med tekniska system är situationen betydligt mer komplicerad, vilket ytterligare försvårar riskanalysen och riskhanteringen.

4.2 Kvantifiering av risker

Som tidigare nämnts (kap. 2.2) bygger risknivån på två storheter ”omfattningen av konsekvenserna för riskhändelser” och ”sannolikheten för att dessa inträffar”. Ett vanligt använt mått på risknivån är produkten av dessa båda storheter. Detta mått förutsätter att vi lyckas kvantifiera de båda ingående storheterna vilket inte alltid är fallet.

En annan svårighet vid beräkning av risknivån enligt ovan kan vara att värdera risken när risksannolikheten är väldigt liten, medan konsekvensen är oerhört stor. Ibland kan en riskhändelse uppfattas så allvarlig att vi väljer att inte bygga ett sådant system för att vi inte kan garantera säkerheten. Just för kärnkraft har detta varit föremål för diskussion.

Om en beräknad risk skall bedömas som acceptabel är också beroende av hur vi bedömer nyttan av det system vars användning kan leda fram till denna riskhändelse. Nyttan värderas genom en s.k. nyttoanalys. Stora risker med små vinster undviks, medan små risker med stora vinster eftersträvas. Här är det viktigt att skilja på de två olika storheterna i den beräknade risknivån. Nyttan kan vara så stor i förhållande till

de negativa konsekvenserna att vi är benägna att acceptera mycket stora risktal dvs. också ett stort riskvärde. I andra fall kan nyttan vara för liten i förhållande till den möjliga negativa konsekvensen för att vi ska vara beredda att acceptera någon positiv risksannolikhet.

5. Riskanalys generellt

5.1 Hur genomförs en riskanalys?

Omfattningen av en riskanalys är beroende av tillämpningens art och syfte, men kunskap om det aktuella systemet är alltid en förutsättning för att genomföra en bra riskanalys.

En riskanalys går i grova drag ut på att besvara följande frågor:

- Vilka riskhändelser kan uppstå?
- Vilka följder kan dessa händelser få och hur svåra är dessa?
- Vad kan orsaka dessa riskhändelser (riskkällan)?
- Hur troligt är det att dessa riskhändelser inträffar (risktalet)?
- Vilka är riskbärare?
- Vad kan göras för att nedbringa risktalet och/eller minska omfattningen av konsekvensen av riskhändelserna?

5.1.1. Vilka riskhändelser kan uppstå och vilka följder kan dessa få?

För att identifiera riskhändelser och orsaker krävs stor kunskap om systemet och hur det skall användas.

Riskanalysen kan utföras på olika sätt beroende på tillämpningens art. Ett sätt kan vara att börja nedifrån genom titta på tillståndet för varje komponent i ett tekniskt system och kombinera dessa olika tillstånd för att se vilka fel på det övergripande systemet som kan uppkomma för olika kombinationer på komponentnivå. Ett annat sätt är att börja uppifrån med en specifik riskhändelse (topphändelsen) som vi vill analysera och avgöra vad som kan leda fram till denna, genom att bryta ned den i delhändelser som i sin tur bryts ned i ytterligare delhändelser, tills vi når den lägsta nivån av händelser.

Vid nedbrytning i delhändelser blir en högre händelse en tänkbar konsekvens av en lägre händelse t.ex. radioaktivt utsläpp är en konsekvens av reaktorhaveri. Det är viktigt att rama in riskstudien så att topphändelsen väljs på ett relevant sätt.

”Människor blir sjuka” kan ha betydligt fler orsaker än radioaktiva utsläpp, varför detta inte är en topphändelse i riskanalysen för ett kärnkraftverk, utan en negativ konsekvens av en sådan topphändelse.

För varje riskhändelse identifieras vilka konsekvenser denna kan leda till och omfattningen av dessa kvantifieras. [MIL-STD-882C 1993] grupperar omfattningen av skadan i fyra nivåer: katastrofal, kritisk, marginell och försumbar. En riskfaktors svårighetsgrad är även beroende av vem eller vad som drabbas t.ex. skada på människor, skador på miljön eller ekonomiska förluster. Kvantifieringen av skadans

omfattning är en subjektiv bedömning som grundas på ett antal kriterier. De kriterier som föreslås i MIL-STD-882C redovisas i tabell 1 nedan.

Impact Levels	CATASTROFIC	CRITICAL	MARGINAL	NEGLIGIBLE
Impact Categories				
Personnel Safety	Death	Permanent partial disability	Injury resulting in 1 or more lost work days	Minor injury with no lost work days
Equipment Safety	Major equipment loss; broad-scale major damage	Small-scale major damage	Broad-scale minor damage	Small-scale minor damage
Environmental Damage	Irreversible and severe damage	Reversible damage \$200K<loss<\$1M	damage \$10K<loss<\$200K	Damage <10K nor violating laws or regulations
Occupational Illness	Severe and broad scale	Severe or broad scale	Minor and small scale	Minor or small scale

Tabell 1: Criteria for determining impact severity. [MIL-STD-882C, 1993]

Det kan även vara aktuellt att t.ex betrakta risken för stora ekonomiska förluster. En mer detaljerad version finns i [MIL-STD-8882D, 2000]

5.1.2 Vad kan orsaka riskhändelserna?

Som tidigare nämnts kan man för att finna orsaker till riskhändelser gå tillväga på olika sätt. Ett sätt är att bilda en händelsekedja baserad på olika kombinationer av komponentfel, ett annat är att bryta ned en specifik riskhändelse i delhändelser så långt som möjligt.

Orsaker till riskhändelser kan vara av olika karaktär:

- a) Kända orsaker som kan undanröjas
- b) Kända orsaker som till del kan kontrolleras
- c) Kända orsaker som vi inte kan påverka (t.ex. naturfenomen)
- d) Orsaker vi kan ana, men inte har en tillräckligt tydlig bild av (t.ex. terroristattacker)
- e) Orsaker vi ej förutsett (p.g.a. försummelse, avsaknad av kunskap/erfarenhet, ej förutsägbara).

Ett syfte med riskanalysen är att identifiera och analysera orsaker av typ a) och b) och genom att vidtaga tillräckliga säkerhetsåtgärder förhindra att motsvarande riskhändelser inträffar, respektive minska omfattningen av dem. För orsaker av typ c) är det viktigt att belysa vilka konsekvenser dessa kan leda till och analysera vad som kan göras för att nedbringa dem. Typ d) kan t.ex. vara terroristattacker, trots att vi är medvetna om att sådana kan inträffa, kan de alltid ta sig uttryck vi inte förutspått. För riskhändelser med mycket allvarliga konsekvenser måste dessa orsaker finnas med i

analysen. Riskanalysen går naturligtvis även ut på att minimera orsaker av typ e), men det är viktigt att man är medveten om att dessa händelser ofta existerar.

5.1.3 Hur troligt är det att riskhändelserna inträffar (risktalet)?

Sannolikheten att en riskhändelse inträffar kan beskrivas på olika sätt, beroende på riskfaktorns art: t.ex.

förväntat antal gånger den inträffar under systemets livstid
 ” ” ” ” ” per enhet i en population
 ” ” ” ” ” per tidsenhet
 ” ” ” ” ” per antal händelser.

MIL-STD 882C grupperar sannolikheten i fem kategorier:

- frequent
- probable
- occasional
- remote
- improbable

och föreslår riktlinjer för hur man skall välja lämplig kategori. Tabell 2 nedan tillhandahåller dessa riktlinjer i termer av hur många gånger händelsen inträffar under systemets livstid och per antal enheter i en population.

Probability description	Likelihood of occurrence over lifetime of an item	Likelihood of occurrence per number of items
Frequent	Likely to occur frequently	Wildely experienced
Probable	Will occur several times in life of item	Will occur frequently
Occasional	Likely to occur some time in life of item	Will occur in several items
Remote	Unlikely but possible to occur in life of item	Unlikely but can reasonably be expected to occur
Improbable	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur but possible

Tabell 2: Probability levels [MIL-STD-882C 1993]

Då vi kvantifierat såväl omfattning som risktal återstår att kombinera dessa till en risknivå. Flera olika tabeller för detta presenteras i MIL-STD-882C varav tabell 3 nedan är ett exempel. Dessa tabeller måste dock utformas för varje enskilt fall med avseende på den specifika tillämpningen.

Level of impact	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
Frequency				
FREQUENT	high	high	medium	low
PROBABLE	high	high	medium	low
OCCASIONAL	high	medium	low	low
REMOTE	medium	medium	low	low
IMPROBABLE	medium	low	low	low

Tabell 3 Risk assessment matrix [MIL-STD-882C 1993]

Dessutom finns en osäkerhet i själva riskanalysen som bör uttryckas.

5.1.4 Vilka är riskbärare?

För vissa tillämpningar kan det också vara betydelsefullt att identifiera vilka olika grupper som kan påverkas av dessa riskhändelser.

5.1.5 Vilken nytta kan systemet ge?

På samma sätt som man identifierar riskhändelser och deras negativa konsekvenser, identifieras nyttoeffekter och deras positiva påverkan. Även i detta fall analyseras sannolikheten att dessa effekter uppnås. Nyttan kan t.ex. innebära ekonomiska vinster eller förbättrad hälsa. Bortsett från typen av nyttoeffekt är det även här viktigt att definiera kriterier enligt vilka nyttoeffekterna kan rankas eller kategoriseras efter graden av påverkan.

[Muessig1997] illustrerar detta genom att klassificera nyttoeffekterna som:

- Effectiveness of major system
- Morale and welfare
- Operating cost reductions

och graden av påverkan som:

- Revolutionary
- Significant
- Marginal
- Negligible

5.2 Metodik för att genomföra en riskanalys

För att genomföra en riskanalys finns ett antal olika metoder att tillgå. Nedan följer en kort sammanfattning av de mest använda analysmetoderna för tekniska system [Rausand 1991].

5.2.1 Preliminary Hazard Analysis –PHA (Grovanalys)

Grovanalys genomförs under tidig designfas genom att lista upp riskhändelser förbundna med de olika elementen i systemet. För varje sådan riskhändelse beskrivs möjliga orsaker till, effekter av och omfattning av potentiella olyckor. Vidare beskrivs möjliga förbättringar eller förebyggande åtgärder. Syftet med analysen är att riskhändelserna skall kunna elimineras eller reduceras vid konstruktionen av systemet..

5.2.2 Failure Modes and Effect Analysis - FMEA

FMEA var en av de första systematiska metoderna för att analysera fel i tekniska system. Den utvecklades i slutet av 50-talet för att identifiera och analysera problem som kunde uppstå p.g.a. fel i militära system. Metoden har senare vidareutvecklats och använts inom olika områden

FMEA utförs under konstruktionsfasen med syfte att förbättra delar eller egenskaper hos systemet för att uppfylla uppställda säkerhetskrav.

Delmål i analysen är bl. a. att

- Identifiera möjliga feltillstånd till varje enkel komponent i ett tekniskt system
- Bestämma orsaker till felen
- Bestämma felens inverkan på systemet som helhet

En vidareutvecklad variant av denna metod där man även bedömer omfattningen av de olika feleffekterna kallas FMCEA. Dessa metoder är enkla att utföra, men förutsätter ingående systemkunskap och kunskap om under vilka betingelser systemet skall operera.

5.2.3 Felträdsanalys

Felträdsanalysmetoden utvecklades av Bell Telephone Laboratories 1962 och är idag den mest använda analysmetoden för risk- och säkerhetsanalyser.

Ett felträd kan uppfattas som ett logiskt diagram som illustrerar sambandet mellan en oönskad händelse i ett system och orsakerna till denna händelse. Orsakerna kan inkludera miljöfaktorer, mänskliga felhandlingar, normala händelser (som förväntas inträffa under systemets livstid) och rena komponentfel. Ett felträd består av symboler som visar tillståndet för komponenterna (ingångstillstånd) i systemet, och sambandet mellan dessa ingångstillstånd och systemets tillstånd (utgångstillståndet). De grafiska symbolerna som visar sambandet kallas logiska portar (se bild 3 nedan). Utgången av en logisk port är bestämd av ingångstillstånden.

När vi skall definiera felträdet utgår vi från topphändelsen. Därefter identifieras fel som kan vara direkta orsaker till topphändelsen. Dessa fel knyts samman med topphändelsen via en logisk port. Vi arbetar oss så successivt ned till ingångshändelserna på komponentnivå.

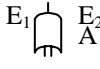



	Symboler	Betydelse
Logiska portar	”ELLER”-port 	Utgångshändelsen A inträffar om minst en av ingångshändelserna E_i inträffar.
	”OCH”-port 	Utgångshändelsen A inträffar endast om alla ingångshändelser E_i inträffar.
Ingångs-tillstånd		Symbol för komponent i feltillstånd
Tillstånds-beskrivning		Verbal tillståndsbeskrivning i rektangeln

Bild 3: Logiska portar [Rausand 1991]

Följande exempel är hämtat ur [Bedford 2001] och illustrerar en process i en kärnkraftsreaktor. Systemet har två sensorer S_1 och S_2 som oberoende av varandra kan upptäcka en onormal temperatur. De skickar en elektrisk signal till en elektrisk ”ELLER”-port A, som skickar en signal till de båda skyddsenheterna P_1 och P_2 om endera sensorn ger en signal. Skyddsenheterna och ”ELLER”-porten får ström från strömkällan E_1 , medan sensorerna får ström från strömkällan E_2 . Felträdet i bild 4 nedan beskriver topphändelsen ”skyddssystemet fungerar ej” i termer av fel i bashändelserna

En felträdsanalys kan vara kvalitativ, kvantitativ eller bägge delarna beroende på analysens omfattning och mål. Ett möjligt resultat från en felträdsanalys är en lista över möjliga kombinationer av miljöfaktorer, mänskliga felhandlingar, normala händelser och komponentfel som medför att den oönskade händelsen inträffar. Genom att uppskatta sannolikheten för inträffandet av händelser på lägre nivåer kan en skattning av sannolikheten för inträffandet av topphändelsen erhållas.

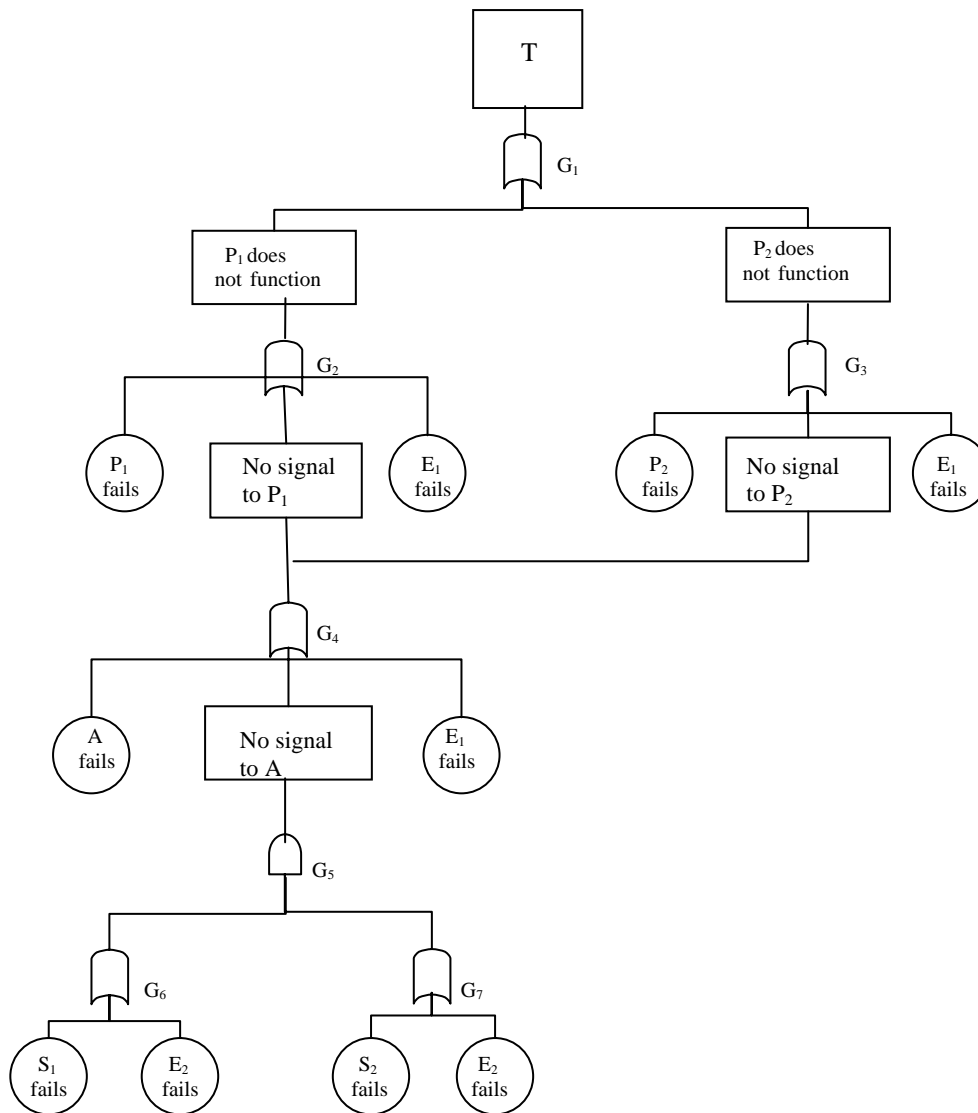


Bild 4: Felträd för reaktorskyddssystem [Bedford 2001]

5.2.4 Händelseträdsanalys

Ett händelseträd är ett logiskt diagram som visar möjliga händelsekedjor som följer efter en initierande kritisk händelse. Den initierande händelsen kan vara ett fel i en teknisk enhet eller en mänsklig felhandling. Händelseanalyser ingår i de flesta större riskanalyser. Denna analysmetod användes bl.a. under arbetet med de amerikanska kärnkraftssäkerhetsanalyserna på 1970-talet [Rasmussenrapporten 1974].

5.2.5 Hazard and operability analysis (HAZOP)

Denna metod används vanligen i samband med projektering av en processanläggning, antingen som en fullständig riskanalys eller som en förstudie för mer detaljerade studier på vissa kritiska processavsnitt. Metoden kan även användas under senare faser.

HAZOP är en formell, systematisk och kritisk granskning av de olika delarna i en processanläggning. Avsikten med analysen är att identifiera möjliga säkerhetsmässiga eller operationella problem som kan uppstå under drift eller underhåll av anläggningen. Analysen genomförs av en handfull ämnesspecialister i form av en serie "brain storming" möten. Denna metod ställer stora krav på erfarenhet hos gruppledaren för att vara framgångsrik.

6. Riskanalys för simuleringsmodeller

6.1 Jämförelse mellan tekniska system och simuleringsmodeller

Simuleringsmodeller, till skillnad från tekniska system, har sin grund i matematik och logik och inte i fysiska lagar. Mjukvaran åldras inte och mjukvarufel som rättats kommer inte att orsaka samma fel igen. Å andra sidan är en simuleringsmodell en tankeprodukt och inte en fysikalisk produkt, vilket gör att möjligheten att introducera osäkerheter i systemet under utvecklingen är större än för icke-mjukvarusystem. Det kan hända att simuleringsmodellen inte på ett adekvat sätt representerar det verkliga systemet, att indata till modellen inte är lämpliga eller korrekta, att utdata kan vara bristfälliga eller feltolkade etc.

[Hofmann 2001] tar upp frågan om svårigheten att modellera mänskligt beslutsfattande och påpekar att nuvarande kunskap om människans psykologi inte är tillräcklig för att kunna modellera beteendet hos våra egna militära ledare för att inte tala om fiendens. Detta är ett viktigt område inom militär modellering, eftersom mänskligt beslutsfattande finns dolt i nästan alla elementära stridsprocesser.

Allt detta påverkar värdering och risker associerade med simuleringsmodeller.

Då vi står inför en situation att avgöra om vi ska använda oss av M&S och i så fall i vilken omfattning, bör vi ställa oss frågor som

- Vad är kostnaden för att utveckla modellen?
- Vilken nytta kommer kunden/användaren att ha av simuleringsmodellen?
- Vilka riskhändelser är förknippade med felaktigheter i modell eller data eller felaktigt användande av densamma?
- Hur stor säkerhet kan vi uppnå i resultaten från simuleringsmodellen?

Verifiering och valideringsaktiviteter utförs för att upptäcka felaktigheter i modellen och därmed reducera riskerna, men även för att samla information för att kunna värdera riskerna med användning av modellen. Vilka riskhändelser och risksannolikheter vi är beredda att acceptera är beroende av modellens syfte.

Först när vi analyserat riskhändelserna och bedömt om risktalen för dessa kan nedbringas till en acceptabel nivå, samt vägt nyttan mot kostnaderna och riskerna bör beslut om användning av M&S fattas.

6.2 Varför bör en riskanalys genomföras inför utveckling av en simuleringsmodell?

Det finns flera goda grunder för att genomföra en riskanalys inför utvecklingen av en simuleringsmodell:

- De krav på trovärdighet en kund/användare ställer på en simuleringsmodell är beroende av vilken ”risk” han är villig att acceptera, vilken är beroende av tillämpningens art och syfte. Om denna risk inte är klart specificerad och kvantifierad är kraven på trovärdighet svåra att formulera. Dessa i sin tur är en grund för värdering av V&V-resultaten.
- Genom att kartlägga riskerna med en simuleringsmodell och beskriva vad som gjorts för att undvika eller reducera dessa, ges även kund/användare en insyn i modellens trovärdighet.
- Resultatet från en riskanalys är också en viktig utgångspunkt för en bedömning av V&V-resursernas omfattning.
- Resultatet från en riskanalys bör också kunna vara en god grund för inriktningen av V&V-åtgärderna. För att belysa denna fråga har inom projektets ram genomförts ett examensarbete där en forskningsmodell för ett autonomt samverkande robotsystem analyserades ur ett riskperspektiv (se kap. 8)

Riskenivån är således grunden för att bestämma typ, kvalitet och djup på den information som behövs för att stödja ett ackrediteringsbeslut.

Den process som beskrivits under kap.5.1 (Hur genomförs en riskanalys?) är till stor del tillämpbar även på simuleringsmodeller.

6.3 Hur genomförs riskanalysen

6.3.1 Vilka riskhändelser kan uppstå?

Med *riskhändelser* för en simuleringsmodell avses de negativa konsekvenser som användning av en modell kan leda till på grund av brister och felaktigheter i modell eller data samt på grund av felaktig användning av modellen. Riskhändelser för själva modellutvecklingsprojektet i form av att projektet blir försenat eller inte håller sig inom tilldelade resurser tas inte upp här.

Vad är det då som kan gå fel vid M&S användning?

En simuleringsstudie kan leda till tre olika typer av felaktiga resultat.

1. Simuleringsresultaten förkastas fast de i själva verket är tillräckligt trovärdiga.
2. Oriktiga simuleringsresultat accepteras som om de var tillräckligt trovärdiga.
3. Simuleringsstudien löser fel problem. (t ex då det uppställda problemet inte helt omfattar det verkliga problemet).

Första fallet, (som brukar benämnas *Model Builder's Risk*) medför en onödig ökning av modellutvecklingskostnaden, medan andra fallet, (*Model User's Risk*) kan få allvarliga följder om kritiska beslut skall fattas på basis av simuleringsresultaten. Den tredje typen av misstag kan leda till att simuleringsstudiens resultat blir irrelevanta oavsett hur förtjänstfullt simuleringsstudien i övrigt genomförs.

VV&A-aktiviteterna fokuserar på att minska dessa risker så mycket som möjligt och att upptäcka fel så tidigt som möjligt i modellutvecklingscykeln. Att korrigera fel som upptäckts i senare faser är betydligt dyrare och mer tidskrävande.

Det vi i första hand kommer att betrakta i fortsättningen är fel av typ 2, eftersom det är dessa fel som kan ge upphov till de allvarligaste riskhändelserna.

För att kunna identifiera riskhändelser måste ändamålet med simuleringsmodellen klargöras. Ofta används simuleringsmodeller som någon form av beslutsunderlag. Det kan vara frågan om operativa beslut eller beslut rörande planering, materielanskaffning, inriktning e.d. Även träningsmodeller kan leda till felaktiga beslut p.g.a. felaktig inläring. Hur stor påverkan simuleringsresultaten har på beslutet kan variera från att ha en ganska perifer inverkan till att vara helt avgörande. Felaktigheter i en simuleringsmodell som används i forskningssyfte kan t.ex. ha ekonomiska och tidsfördröjande effekter, medan simuleringsmodeller som ligger till grund för operativa beslut kan få betydligt mer ödesdigra konsekvenser.

Riskhändelserna kan indelas på basis av olika indelningsgrunder t.ex.

- Riskhändelser som skapas av en aktiv motståndare kontra de som bara inträffar slumpartat (t.ex. väderberoende)
- Riskhändelser vars risksannolikhet går att nedbringa om man har kunskap om faktorerna kontra de som ej kan nedbringas hur mycket forskning man än gör.
- Accepterbara respektive icke-accepterbara riskhändelser

En första ansats bör vara att identifiera oacceptabla riskhändelser, för att avgöra om risktalen för dessa kommer att kunna nedbringas till en acceptabel nivå. Först därefter är det möjligt att fatta beslut om man skall gå vidare med simuleringsprojektet.

Därefter görs en mer omfattande identifiering av riskhändelser. Även här gäller att det är viktigt att vara medveten om att sällan alla möjliga riskhändelser identifierats.

Riskanalysen genomförs ej endast som en förstudie till en simuleringsmodell, utan bör fortleva under hela modellutvecklingsprocessen. Dels kan det finnas en tidsdimension med i bilden - ett riskmedvetande kan växa fram under processen, och dels kan inte en total riskanalys av modellen göras innan den är färdigutvecklad.

6.3.2 Vilka följder kan riskhändelserna få?

På samma sätt som för tekniska system indelas konsekvenserna av riskhändelser i ett antal kategorier: skador på människor och/eller miljö, ekonomiska förluster etc. Konsekvensen av fel i en simuleringsmodell som skall fungera som beslutsunderlag är även beroende av vilken påverkan simuleringsmodellen har på beslutet. Följande fyra utfall kan erhållas:

- beslutet korrekt och modellen rätt
- beslutet korrekt och modellen fel
- beslutet fel och modellen rätt
- beslutet fel och modellen fel

Det vi vill uppnå är förstås första fallet, medan vi vill undvika det fjärde fallet. Man bör även ställa sig frågan varför ett felaktigt beslut fattas på basis av korrekta simuleringsresultat eller tvärtom. Är trovärdigheten för modellen inte ordentligt belyst?

Konsekvenserna kan också vara av olika karaktär såtillvida att vissa konsekvenser uppenbaras genast, medan andra visar sig med tiden. I vissa fall kanske felaktigheter får så små konsekvenser att de aldrig uppdagas.

I vissa sammanhang kan felaktigheter leda till konsekvenser som innebär ett akut kritiskt tillstånd, medan andra kan leda till långsiktiga reaktioner. I det senare fallet kan man hinna korrigera modellen innan tillståndet blir kritiskt. Mindre kritiska aspekter kan också med tiden bli kritiska om de inte åtgärdas.

6.3.3 Vad kan orsaka riskhändelserna?

Riskhändelser som uppkommer på grund av felaktiga simuleringsresultat kan orsakas av brister och felaktigheter i modell eller data samt på grund av felaktig användning av modellen. Dessa orsaker kan brytas ned i mer detaljerade feltyper till lämplig nivå.

Bild 5 nedan visar ett generellt felträd för simuleringsmodeller med endast "ELLER"-portar.

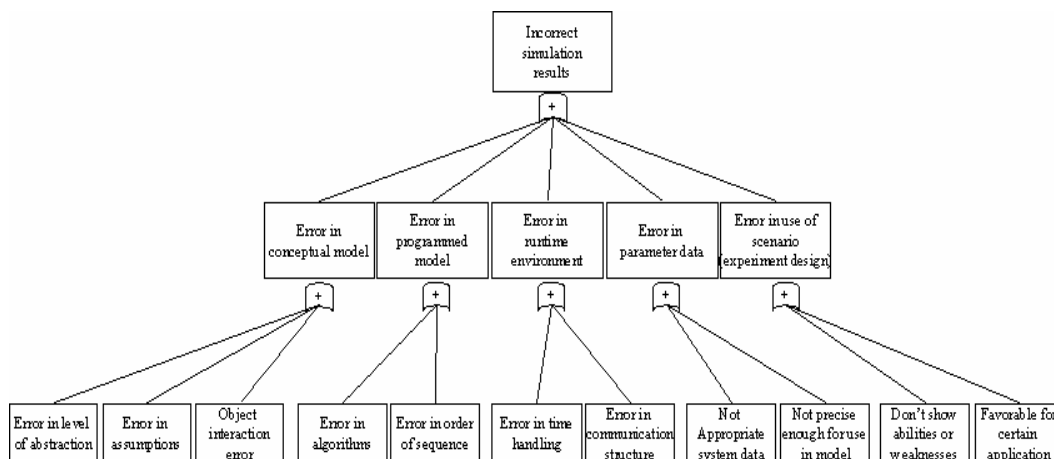


Bild 5: Felträd för simuleringsmodeller [Eliasson 2002]

Tophändelsen "inkorrekta simuleringsresultat" kan brytas ned i delhändelser "fel i den konceptuella modellen", "fel i den programmerade modellen" o.s.v., vilka i sin

tur kan brytas ned i delhändelser. Fel i den konceptuella modellen kan t. ex. bero på ”olämplig abstraktionsnivå” eller ”felaktiga antaganden”.

Därtill kommer fel i användningen av modellen, som kan bero på bristande kunskap om antaganden och begränsningar som ligger till grund för modellen.

6.3.4 Hur troligt är det att riskhändelserna inträffar (risktalet)?

För att avgöra hur troligt det är att felaktigheter i en simuleringsmodell leder till felaktigt beslut, måste den inverkan simuleringsresultaten har på beslutet uppskattas. För att kvantifiera risktalen för olika typer av fel i simuleringsresultaten tillgrips olika metoder beroende på felkategori. Bedömningen av hur stor risken är för olika typer av fel i den konceptuella modellen kan baseras på expertbedömningar. För att uppskatta risktalen för olika typer av implementationsfel kan en sammanställning av tidigare erfarenheter vara till nytta – var brukar det gå snett och hur ofta.

På samma sätt som för tekniska system är det lämpligt att indela risktalen i storleksklasser, men för simuleringsmodeller är det inte fråga om hur ofta ett fel inträffar utan med hur stor sannolikhet t. ex. låg, medium, hög.

6.3.5 Vad kan göras för att nedbringa risktalet och/eller minska omfattningen av konsekvensen av riskhändelserna?

Då vi genomför en riskanalys för vi fram så mycket som möjligt av osäkerheter och tänkbara negativa konsekvenser som användningen av simuleringsmodellen kan leda till. Att inom givna ekonomiska ramar med denna analys som grund inrikta V&V-aktiviteterna för att minska felriskerna, speciellt för de riskhändelser som kan medföra de allvarligaste konsekvenserna, blir en form av optimeringsproblem.

När vi konstruerar ett felträd, indelas topphändelsen i delhändelser som i sin tur bryts ned in delhändelser o.s.v. tills vi når den lägsta nivån. Då går vi upp genom trädet igen och beskriver för varje händelse vad som skall göras för att nedbringa omfattningen av eller sannolikheten för dess inträffande. När vi når topphändelsen igen har vi en bild av vad vi skall göra för att nedbringa risknivån, och en uppskattning om storleken på den totala risknivån. (se ITOP-metoden kap.7).

6.4 Hur kan riskanalysen ligga till grund för inriktning av V&V-aktiviteterna?

En riskanalys bör vara en god bas för inriktning av V&V-aktiviteterna. De riskhändelser som identifierats genom riskanalysen värderas och rangordnas med avseende på hur omfattande konsekvenser dessa händelser kan leda till. För varje riskhändelse bestäms största acceptabla risktal vi är villiga att acceptera. Detta sker i form av ett antal klasser (t. ex. låg, medium, hög) och är beroende av modellens syfte. Därefter upprättas en åtgärdslista, varvid vi avgör möjliga orsaker till respektive riskhändelse, och rangordnar dessa efter svårighet att åtgärda (undvika). Kombinationen konsekvenser, max risktal och åtgärdslista kan sedan ligga till grund för inriktning av V&V-insatserna.

7. ITOP-metoden: En struktur för inriktning av V&V-aktiviteter

VV&A of M&S WGE 7.2 inom ITOP (International Test Operations Procedures) är ett pågående internationellt samarbete mellan Frankrike, Tyskland, Storbritannien och USA, där Sverige medverkar som observatör. Med syftet att stödja utbyte av V&V-information bland de deltagande nationerna utvecklas i första hand ett dokument för att tillhandahålla en standard (ITOP 1-1-002, "VV&A of M&S") för framtagande och dokumentation av den information som ligger till grund för ett ackrediteringsbeslut.

ITOP-processen baseras på ett koncept uppbyggt som ett rättsfall av påståenden (claims), argument och evidenser, som tillhandahåller en logisk struktur för att presentera multipla V&V-resultat. Man skiljer här på V&V av modell, data och modell användning, men samma koncept används för alla tre.

Det övergripande påståendet, att simuleringsmodellen är lämplig för dess avsedda syfte, kan brytas ned i underpåståenden (sub-claims), som stöds av en kedja av argument som bestyrks av evidenser. Hur nedbrytningen i underpåståenden går till måste tydligt framgå och vara spårbart genom argument och/eller evidenser. Ett argument är en resonerande förklaring, medan evidenser är resultat av V&V-insatser som stöder påståenden och argument. På samma sätt kan underpåståenden brytas ned ytterligare, tills en hierarki av påståenden och argument har konstruerats. Den lägsta nivån av påståenden skall kunna styrkas av evidenser från V&V-insatserna. På detta sätt kommer tillfredsställande argument och evidenser för påståenden på lägre nivå i sin tur att bidra till tillfredsställande argument och evidenser för påståenden på högre nivå, tills man nått den högsta nivån. Med en välutvecklad hierarkisk struktur av påståenden, argument och evidenser kommer trovärdigheten i påståendet på den högsta nivån att kunna beläggas.

Bild 6 nedan ger ett exempel på en hierarki av påståenden, argument och evidenser.

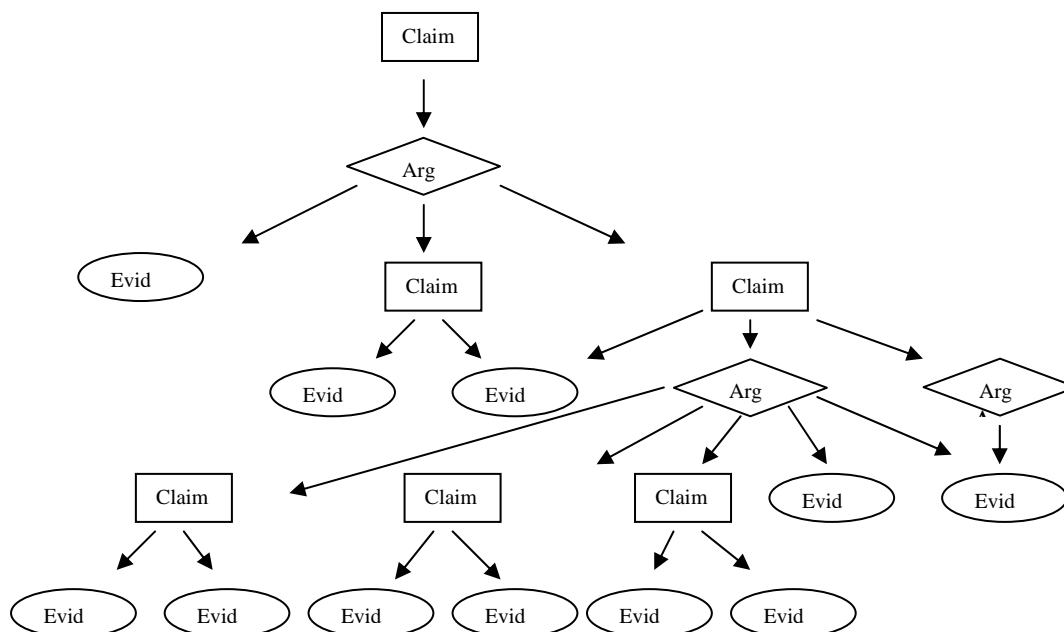


Bild 6 [ITOP 2002]

Nedbrytningen baseras på att styrkan i argumentationen och bevisningen för varje påstående styrs av betydelsen av att veta/känna till dess eventuella negativa inverkan på beslut baserade på (eller annat nyttjande av) resultatet från M&S.

Denna struktur kan med fördel användas som ett led i en riskanalys.

8. Exempel: Riskanalys av en modell för ett autonomt samverkande robotsystem

8.1 Bakgrund

För att studera riskaspekter utifrån ett V&V-perspektiv genomfördes under våren och sommaren 2002, inom ramen för projektet, ett examensarbete med titeln "A Risk Perspective on Verification and Validation efforts in Simulation Models – Specifically on an Autonomous Co-operating Missile System Model" [Eliasson 2002].

Syftet med arbetet var att genom en praktisk tillämpning undersöka värdet av en riskanalys, för att bestämma nivån på och inriktning av V&V-insatserna samt vilka frågeställningar och svårigheter som uppkommer under ett sådant arbete.

8.2 Val av modell

Resultatet av ett sådant arbete är naturligtvis mycket beroende av vilken typ av modell man väljer att studera. I detta fall valdes en forskningsmodell för samverkande missiler. Anledningarna till detta val var flera:

- Ett examensarbete genomförs under en mycket begränsad tidsperiod av ca fem månader, där även en hel del kunskapsuppbyggnad inom området ingår. Detta innebär att modellens komplexitet måste stå i relation till tidsramen. Vidare får modellen inte vara för enkel om den ska kunna ge ett meningsfullt bidrag.
- Tät kontakt med de personer som har kunskap om modellen måste kunna förekomma, varför en forskningsmodell "i huset" ansågs lämplig.
- Ett uttalat intresse från projektledaren för att genomföra detta arbete ansågs viktigt, för att kunna erhålla det stöd från projektet som krävs för att genomföra arbetet.
- Modellutvecklingen måste befina sig i ett sådant skede att en riskanalys är meningsfull.
- En modell som är under utveckling och lever vidare kan också få de största vinsterna av att en riskanalys genomförs, dvs större synnergieffekter.

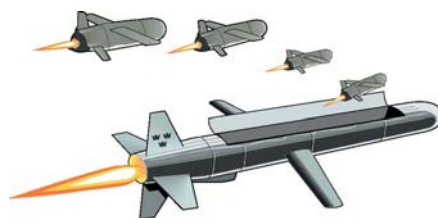
8.3 Beskrivning av modellen

Nedan följer en sammanfattning av den beskrivning som ges i [Eliasson 2002] av bakgrund, teknisk beskrivning och scenarieval.

Bakgrund

Ett autonomt missilsystem är ett missilsystem som, utan mänsklig inblandning, söker ut mål och beslutar vilket mål som skall attackeras. Fördelarna med ett sådant system är bl.a. att man kan angripa mål som tidigare betraktats för riskfyllda för attackflygplan att angripa. Nackdelarna med ett sådant system är dock att vid anfall med multipla missiler är sannolikheten för att de angriper samma mål relativt hög. Varje missil gör sin egen optimering av situationen vilket betraktat utifrån det övergripande systemet är suboptimeringar som ofta ej leder till en optimering av hela systemet.

1995 initierades på FOA (numera FOI) ett forskningsprojekt [Alvå 2002] för att studera hur man kan uppnå ett autonomt robotsystem där missilerna kan kommunicera med varandra och därigenom samarbeta i form av en koordinerad attack. Syftet var också att undersöka för- och nackdelar med ett sådant system. Projektet innefattar forskning rörande optimal målsökning, målfördelningsalgoritmer och störningsalgoritmer. För detta ändamål utvecklas en simuleringsmodell för att kunna testa olika teorier rörande ett sådant system. Simuleringar skall genomföras på såväl taktisk som teknisk nivå och syftet är också att belysa frågan hur mycket bättre effekt ett system av samverkande missiler skulle ha, jämfört med det system vi har idag med missiler som inte kan kommunicera med varandra.



Källa: [Ulriksson2001]

Teknisk beskrivning av modellen

Vapensystemet i modellen består av en transportmissil utrustad med åtta submissiler. Vid en förbestämd punkt frigörs submissilerna. Fram till dess fungerar systemet som en enhet. Submissilerna aktiveras nu och blir samarbetande individer. De fortsätter mot målområdet och börjar söka efter mål. Kommunikationen sker med hjälp av en laserlänk som är svår för fienden att upptäcka. Missilerna använder sensorer för att finna och identifiera mål. En målmultisensor består av en videokamera, en infraröd sensor och laserradar. När en submissil upptäcker mål sänds informationen till de övriga submissilerna och attacken samordnas automatiskt med optimeringsalgoritmer.

Scenario

Det scenario som används för riskstudien bygger på ett scenario som skapats för att demonstrera systemet. Detta består av en invasion av Sverige, där fiendestyrkor har landsatts vid Kapellskär norr om Stockholm (se bild 7 nedan). Invasionsstyrkan rör

sig mot Stockholm och Arlanda flygplats med stridsvagnar, stridsfordon, artilleripjäser och luftvärnsbatterier. Situationen har lett till att ÖB beslutat använda samverkande robotsystem för att bekämpa dessa. Inom målområdet följer submissilerna förhandsberäknade optimala flygbanor för att söka fiendestyrkor. När fiendestyrkan upptäcks genomförs en optimerad attack. För närvarande modelleras fienden mycket okomplex, t.ex. använder han inte motmedel för att försvara sig.

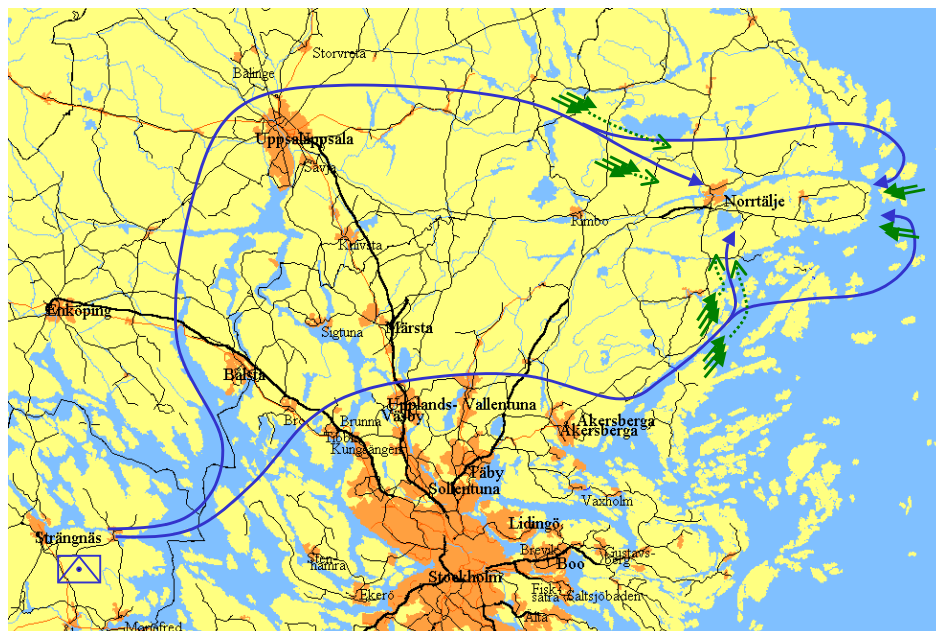


Bild 7: Exempel på ett scenario. [Jerberyd 2002]

8.4 Genomförande av riskstudien

8.4.1 Metodik för riskanalysen

Nedan följer en sammanfattning av den metodik som valdes för examensarbetet, vilken presenteras i sin helhet i [Eliasson 2002]. Resten av kap. 8.4 illustrerar sedan hur resultatet från detta arbete kan ligga till grund för det koncept för en riskanalys som beskrivits under kap.6.

Den metodik som valdes för examensarbetet vilar på fyra ben:

- Historiskt materiel
- Ämnesområdesexperter
- Felinsättningsanalys
- Känslighetsanalys

Genomgång av historiskt materiel

Idén med denna tillbakablick är att dra nytta av historiska erfarenheter och kunskap. Här görs en jämförelse mellan vad som gjorts tidigare och vad som är helt nytt i simuleringsstudien. Nya områden är svårare eftersom jämförelsemateriel saknas och det kan vara svårt att avgöra om resultaten är rimliga.

En amerikansk statistik över misstag gjorda under ett antal modellutvecklingsprojekt lär finnas, men inom ramen för examensarbetet har denna inte lyckats identifieras och utnyttjas. En sådan databas baserad på svenska erfarenheter, rörande felfrekvenser och felkällor, skulle kunna vara en intressant del i en riskanalys.

Ämnesområdesexperter

Ämnesområdesexperter bör anlitas för ett flertal ändamål under en modellutvecklingsprocess. Detta är personer som besitter expertkunskap inom områden av stor vikt för modellutvecklingen. För riskanalysen behövs personer som är kunniga på det verkliga systemet för att bedöma felriskerna med den konceptuella modellen, personer som är insatta i modellutvecklingsarbetet för att bedöma felriskerna i utvecklingsarbetet, personer som kommer att använda den färdiga modellen för att få värdefulla användaraspekter o.s.v.

För robotmodellen valdes att göra en enkät- och intervjuundersökning med ett antal personer från projektgruppen för att få modellutvecklarnas egen uppfattning om tillförlitligheten i olika delar av modellen. I modellutvecklingsgruppen finns såväl systemkunskap inom robotområdet som kunskap om modellutvecklingen. Vidare är det modellutvecklarna som i det här fallet är de primära användarna av modellen.

Projektledaren tillfrågades om lämpliga kandidater (med tillräcklig insikt i modelleringsproblemet och simuleringsprojektet) för enkätundersökningen. Missilprojektet omfattar 14 forskare på FOI. Av dessa betraktade projektledaren åtta som lämpliga för undersökningen, av vilka en inte fanns tillgänglig vid denna tidpunkt. Dvs endast sju personer ingick i undersökningen. Från en undersökning baserad på så få personer går inte att dra några säkerställda statistiska slutsatser, utan dessa expertutlåtanden skall enbart behandlas som sju personers individuella uppfattningar, men det kan ändå ge en värdefull vägledande information. Det är dock viktigt att man har detta i minnet.

Enkätundersökningens frågor var baserade på felträdet i bild 5. Ämnesområdesexperterna fick ge sin uppfattning om var det är troligast att det gått fel på varje nivå, genom att fördela procenttal som summeras till 100% bland de olika alternativa orsakerna. Vidare fick de besvara frågor om hur mycket V&V som behövs i förhållande till andra studier och om deras egen expertkunskap inom området för frågan. För varje fråga fanns möjlighet till egna kommentarer. Enkäten följdes upp med intervjuer.

Felinsättningsanalys

Felinsättningsanalys (fault insertion analysis) innebär att fel eller svagheter avsiktligt implementeras i modellen för att sedan studera var och när det förväntat felaktiga beteendet inträffar. Härigenom kan komponenter som är kritiska för modellen identifieras.

Bild 8 nedan ger en schematisk överblick över modellen för samverkande missiler. Modellen består av fem parallella loop-processer som varje missil genomgår från starten: uppdatering av flygbanan, sändande av existensmeddelande, kontroll av att

det finns en ledare, målsökning och attack. Processerna fortsätter tills attackloopen förstör missilen eller tiden runnit ut.

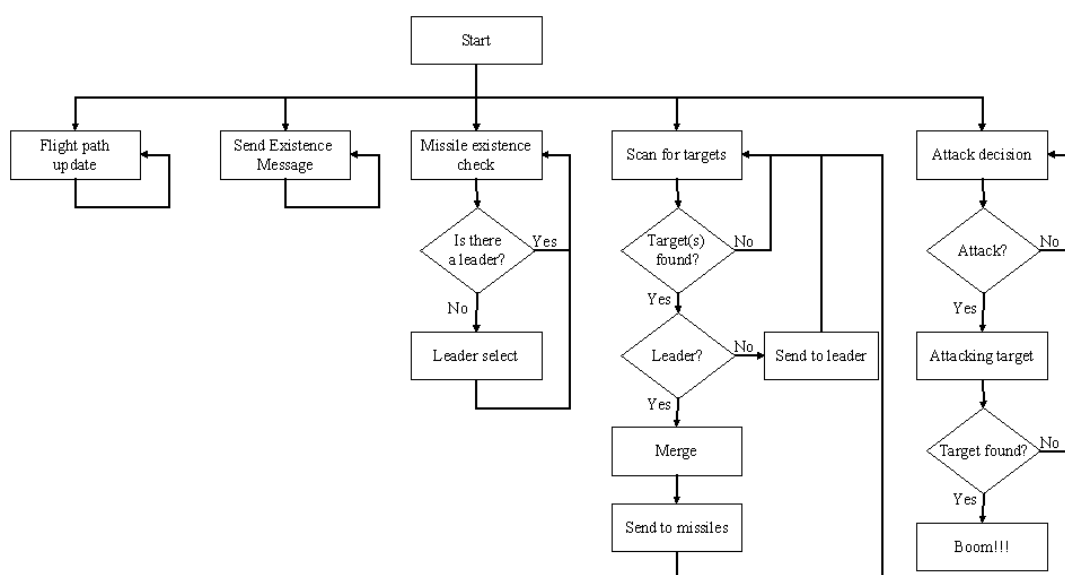


Bild 8: Modell representation [Jerberyd2002]

De för studien mest kritiska funktionerna ansågs vara kommunikation och sensorer.

Tre olika typer av fel studerades.

1. Kommunikationen fullständigt ur funktion för en eller flera missiler.
2. Konsekvenser av sändarfel. Missilen kan motta andra missilers meddelanden, men inte sända egen information.
3. Sensorfel, sensorn kan inte finna målet.

För att minska sannolikheten att resultaten av slump blev förvrängda av ett scenario, kördes alla felinsättningar på tre olika scenarier. Alla scenarier baserades på fiendelandsättningen vid Kapellskär (se kap. 8.3). Scenarierna består av totalt sex autonoma samverkande missiler, som rör sig mot målområdet Kapellskär. Fienden består av sex primära mål (stridsvagnar) och sex sekundära mål (stridsfordon och lastbilar). Uppdraget för de autonoma samverkande missilerna är att finna och slå ut de sex primära målen så snabbt som möjligt. Scenarierna skiljer sig åt i sättet missilerna söker av målområdet och i hur fienden avancerar.

Felen placerades in i antingen en eller två missiler och i olika missiler.

Känslighetsanalys

Känslighetsanalys (sensitivity analysis) går ut på att identifiera variabler och parametrar för vilka modellen är särskilt känslig, genom att systematiskt ändra modellens indatavariabler och -parametrar över något intressant område och

kontrollera effekten av detta på modellens uppträdande. Detta visar även osäkerheten i modellen. En modell som är mycket känslig för även små störningar i data ger större felsannolikheter, varför de identifierade variablerna/parametrarna bör hanteras med extra stor noggrannhet.

För att genomföra en känslighetsanalys måste man först finna lämpliga utvärderingsfaktorer. Olika val av faktorer kan ge helt olika resultat. Därefter måste man bestämma vilka variabler och parametrar som skall analyseras. I ett tidigt skede av modellutvecklingen kanske inte alla indatavariabler och -parametrar finns tillgängliga. För att begränsa omfattningen av analysen är det också önskvärt att ha maxvärde, minvärde och mest sannolikt värde för variablerna och parametrarna. Utanför detta område fanns i det aktuella fallet ingen anledning att testa modellen.

Med avseende på studiens syfte valdes som indatavariabler och -parametrar för analysen de som teoretiskt kunde påverka prestationsförmågan för missilernas samarbete och som var tillgängliga för analysen.

Följande variabler/parametrar valdes

- kommunikationsräckvidd
- sensorräckvidd
- avsökningsperiod
- avsökningsvinkel
- öppningsvinkel
- processorns överföringshastighet
- missilernas hastighet
- fiendeobjektens hastighet

För varje variabel/parameter erhöles max, min och mest sannolikt värde från projektledaren. Varje utvald variabel/parameter varierades inom sitt värdeområde, medan de övriga variablerna/parametrarna hölls konstanta och utdata från simuleringen analyserades. Om resultatet inte visade någon skillnad mellan max, min och mest sannolikt värde för alla tre scenarierna avskrevs variabeln/parametern som icke-känslig. Ett test genomfördes också där fler än en variabel eller parameter varierades.

Analysen genomfördes för samma scenarier som användes i felinsättningsanalysen.

8.4.2 Vilka riskhändelser kan uppstå?

Första steget vid genomförandet av en riskanalys är enligt tidigare att besvara frågan: Vilka riskhändelser kan inträffa och vilka konsekvenser kan dessa få? För att kunna göra detta måste vi noga klargöra vilken typ av modell det är frågan om och till vad denna skall användas.

Den modell vi här betraktar är en militär forskningsmodell, vilket innebär att det verkliga systemet inte existerar. Detta i sin tur medför att vi inte kan erhålla verkliga data samt att konceptet för det tänkta framtida systemet är diffust formulerat.

Det bör kanske påpekas att den aktuella riskanalysen inte avser att granska risker med ett autonomt samverkande robotsystem, utan endast risker med att använda modellen för dess avsedda syfte.

Syftet med modellen är att studera hur man kan uppnå ett autonomt robotsystem där missilerna kan kommunicera med varandra, samt att analysera för- och nackdelar med ett sådant system. Detta skall utmynna i rekommendationer till FM om man skall satsa på ett sådant system eller ej.

Vilka typer av riskhändelser kan vi urskilja? Topphändelsen i detta fall är att vi ger felaktiga rekommendationer till FM. Denna kan brytas ned i de två delhändelserna:

1. Simuleringsresultaten visar felaktigt att vi inte bör satsa på samverkande autonoma missilsystem.
2. Simuleringsresultaten visar felaktigt att vi bör satsa på samverkande autonoma missilsystem.

Dessa båda händelser kan sedan brytas ned i mer detaljerade delhändelser som kan leda fram till dessa felaktiga resultat. Innan vi gör detta analyserar vi vilka konsekvenser de två fallen ovan kan få.

8.4.3 Vilka följder kan riskhändelserna få?

Första fallet, där vi avråder från en satsning på samverkande autonoma robotsystem, kan medföra att fortsatta studier av detta område tills vidare läggs ned. Detta innebär att vi längre lever kvar med ett sämre system än vad som skulle vara fallet annars. De negativa konsekvenserna av detta och omfattningen av dessa måste bedömas av fackområdesexperter.

Beträffande det andra fallet, där vi förordar en satsning på samverkande autonoma robotsystem, måste vi först klargöra hur stor påverkan rekommendationen baserad på simuleringsstudien har på det slutliga beslutet. En trolig följd kan vara att en större studie initieras för att ytterligare studera denna fråga. Om denna studie visar att den tidigare rekommendationen var fel har detta mest haft konsekvensen att tidsmässiga och ekonomiska resurser satsats på fel område.

Inför alternativet att studien istället felaktigt kan komma att styrka rekommendationen, är för oss frågan, vilken påverkan den i projektet utvecklade simuleringsmodellen kan komma att ha på den senare studiens resultat. Kan det tänkas att man kommer att använda den i projektet utvecklade modellen och eventuellt modifiera eller vidareutveckla densamma? Kan fel i simuleringsmodellen leva vidare och ge fel även i den kommande studien?

Då vi kommit så långt fram i händelsekedjan är fakta väldigt oklara och en fortsatt analys känns inte meningsfull, varför vi nöjer oss med att betrakta konsekvensen att en ny studie initieras. Riskerna med felaktiga resultat från denna studie får senare behandlas för sig, när mer fakta om omständigheterna existerar.

Vi nöjer oss därför med att konstatera att riskerna med fel rekommendationer kan i första fallet fördröja utvecklingen av ett användbart system och i andra fallet medföra

att pengar och tid satsas på en meningslös studie. Ingen av dessa konsekvenser bedömer vi som katastrofala eller kritiska.

Vilka är då nyttoeffekterna av att utveckla simuleringsmodellen? Modellen utvecklas för att vinna kunskap om ett framtida autonomt samverkande robotsystem. Modellanvändningen kan med stor sannolikhet förväntas ge insikter i svårigheter och möjligheter samt för- och nackdelar med ett sådant system.

Då följderna av en felaktig rekommendation bedöms som mycket små i förhållande till nyttan med simuleringsmodellen kan även en hög risknivå accepteras, och utvecklingen av simuleringsmodellen kan anses klart motiverad.

Fortsättningen av analysen går ut på att identifiera de felkällor som får de allvarligaste följderna samt de med störst risktal, för att försöka förhindra att dessa inträffar bl.a. genom att inrikta V&V-aktiviteterna mot dessa felkällor.

8.4.4 Vad kan orsaka riskhändelserna?

För att identifiera vilka orsaker som kan leda fram till att simuleringsstudien lämnar fel beslutsunderlag kan vi följa den nedbrytning i delhändelser som redovisades i kap. 6.3.3.

Eftersom den modell vi betraktar ligger i framkanten på dagens forskning är det historiska materialet begränsat. Dock finns delområden i modellen som studerats i tidigare projekt som t.ex. robotens dynamiska uppträdande. De nya områdena gäller i första hand missilernas samarbete och inkluderar funktioner som optimal målsökning, målfördelning mellan missilerna och störningsalgoritmer.

Resultaten från felinsättningsanalysen visade som väntat att dessa vitala områden har stor påverkan på resultaten. Det värsta av de tre feltyperna som studerades genom felinsättningsanalysen var sensorfel. Missilerna blir oförmögna att finna nya mål, och de mål de tilldelats av ledaren kommer inte heller att bli funna och således inte attackerade. De övriga missilerna antar att målet blir attackerat och ignorerar det för tillfället. I detta fall leder samarbete till sämre resultat än utan.

Det bör dock påpekas att resultaten endast är giltiga för de undersökta scenarierna.

Felet att stänga av kommunikationen leder till att missilen agerar på eget bevåg och resulterar i ett sub-optimalt agerande hos systemet. Både missilen med kommunikationsfel och ledarmissilen för de övriga kommer att besluta att anfälla samma mål, omedvetna om vad den andra företar sig, varför fiendemål kommer att attackerats av två missiler.

Sändningsfel leder till något bättre resultat jämfört med kommunikationsfel. Missilen med felet kommer fortfarande att höra de övriga missilerna, men får ingen order eftersom ledaren är oinformerad om dess närvaro. Så småningom kommer den felande missilen att bli sin egen ledare och sedan utföra en attack med den information den tidigare fått av de övriga missilerna.

8.4.5 Hur troligt är det att riskhändelserna inträffar?

Från ett historiskt perspektiv är det mycket troligt att den modell vi betraktar producerar felaktiga simuleringsresultat, eftersom en forskningsmodell i viktiga stycken saknar jämförelsedata och kunskap baserad på erfarenhet. Dock är det mer troligt att resultaten underskattar än överskattar möjligheterna. Orsaken till detta är att det är svårt att skatta utvecklingsmöjligheterna för algoritmerna, när systemet evalueras används befintliga algoritmer.

Beträffande felaktig användning av modellen kan vi här konstatera att det är modellutvecklarna själva som använder modellen som ett forskningsverktyg, varför de kan förväntas känna till antaganden och begränsningar som ligger till grund för modellen. Däremot kan man inte bortse från risken för olämpliga scenariorval eller feltolkning av resultaten.

Enkätundersökningen visade också att projektmedlemmarna själva bedömde sannolikheten för felaktiga resultat som högre jämfört med andra modeller i allmänhet.

Vad det gäller fel i själva simuleringsmodellen skiljer vi på

- Fel i den konceptuella modellen
- Fel i den programmerade modellen
- Fel i parameterdata

Den historiska analysen och enkätundersökningen låg till grund för bedömning av de två första punkterna, medan den tredje punkten baserades på resultat från känslighetsanalysen.

Resultat av enkätundersökningen

Det mest konsistenta svaret från undersökningen var att denna modell behöver mer V&V jämfört med andra modeller. Experterna trodde att på de flesta nivåer skulle modellen producera fler felaktigheter än andra modeller. Det är inte så förvånande beträffande en forskningsmodell. Den orsak som pekades ut som den troligaste var fel i den konceptuella modellen. F.ö. var svaren så mångtydiga, man rangordnade alternativen så olika, att de inte gav någon ytterligare vägledning.

Resultat från känslighetsanalysen

Resultaten från känslighetsanalysen visade att simuleringen var ganska stabil för alla undersökta scenarier, variabler och parametrar. Mest känsliga var de variabler och parametrar som var involverade med "kommunikationsräckvidd" och "avsökningsperiod". "Kommunikationsräckvidd" testades för ytterligare värden. Även då denna variabel sattes till minimum, var resultaten inte i närheten av då man stängde av kommunikationen helt. "Avsökningsperiod" kunde p.g.a. begränsningar i simuleringsmodellen bara sättas till positiva heltal, vilket inte lämnade stort rum för analysen.

Baserat på det som framkommit genom riskanalysen, bedöms sannolikheten för felaktiga resultat från modellen som hög. Däremot bedöms konsekvenserna av

riskhändelserna som relativt små och nyttan med modellen som stor, varför ett högt risktal är helt acceptabelt.

8.4.6 Hur bör V&V-aktiviteterna inriktas på basis av riskanalysen?

Genom enkätundersökningen framkom att relativt stora resurser behöver satsas på V&V-aktiviteter av modellen för att få ned risktalet. Det faktum att modellutvecklarnas egna åsikter gick mycket isär om var de största svagheterna i modellen finns, indikerar att osäkerheter finns i många delar av modellen. V&V-insatserna bör därför inriktas mot de delar av modellen som bedöms mest intressanta för resultatet.

Med tanke på studiens syfte får kommunikations- och sensormodulerna anses som de mest kritiska delarna av modellen, och V&V-aktiviteterna bör fokusera på dessa. Vidare pekade enkätundersökningen ut att stor tonvikt i V&V-aktiviteterna bör läggas på den konceptuella modellen, då denna av många ansågs som den svaga länken. Detta stärks även av den historiska analysen.

Känslighetsanalysen visade att de parametrar och variabler som modellen var känsligast för var de som var involverade med ”kommunikationsräckvidd” och ”avsökningsperiod”, men inte heller för dessa var modellen speciellt känslig. Dock bör dessa röna en viss grad av uppmärksamhet under V&V-arbetet.

8.5 Vad kom ut av riskstudien?

I kap.6.2 redovisades fyra skäl för att genomföra en riskanalys. Vi kan nu ställa oss frågan om riskanalysen har uppfyllt dessa förväntningar. Man bör dock hålla i minnet att examensarbetet genomfördes under en begränsad tid, där mycket av tiden åtgick till kunskapsinhämtning inom ett flertal områden, varför en alltför omfattande analys inte kunde genomföras.

- Riskerna är så pass väl specificerade att kraven på trovärdighet är möjliga att formulera. Nyttan med denna simuleringsmodell är att vinna insikter om för- och nackdelar med ett framtida robotsystem. Omfattningen av riskhändelserna bedömdes så pass liten i förhållande till nyttan, att studien ansågs klart motiverad.
- Riskanalysen har till viss del belyst känsliga sidor hos modellen och osäkerheter i densamma, samt identifierat riskhändelser. Genom att senare beskriva V&V-insatserna och dess resultat, kan kunden ges en bild av trovärdigheten för modellen. Ett tillvägagångssätt här är att tillämpa konceptet från ITOP-arbetet (kap. 7).
- V&V-resursernas omfattning beror på risknivån. Här bedömdes faktorn ”omfattningen av riskhändelserna” som ganska liten, medan risktalsfaktorn bedömdes som hög, varför den resulterande risknivån får betraktas som medium.

Amerikanska studier av ett antal modellutvecklingsprojekt har visat att kostnaderna för oberoende V&V ofta ligger runt 15% av modellutvecklingskostnaderna. Robotmodellen är en forskningsmodell och för dess syfte behövs ingen oberoende V&V, men en ordentlig V&V-insats från modellutvecklingsgruppen får anses motiverad, för att trovärdigheten för modellen ska kunna beläggas.

- Beträffande den sista punkten, att en riskanalys också bör kunna vara en god grund för inriktningen av V&V-åtgärderna, kan vi konstatera att riskanalysen i detta fall pekade ut kommunikations- och sensormodulerna som de mest kritiska delarna av modellen, och att V&V-aktiviteterna bör fokuseras på dessa.

Vidare indikerade analysen att stor tonvikt i V&V-aktiviteterna bör läggas på den konceptuella modellen. För övrigt gick modellutvecklarnas åsikter isär ifråga om var det är troligast att det gått fel under modellutvecklingsarbetet.

Känslighetsanalysen visade att modellen var ganska stabil för de undersökta parametrarna.

Sammantaget kan man säga att vad riskanalysen i detta fall indikerat, var precis det man kunde vänta sig. Inga andra insikter nåddes i detta fall rörande inriktning av V&V-insatserna.

Det finns flera faktorer som medför osäkerheter i riskanalysen, t. ex. det faktum att vi idag inte vet hur algoritmerna i systemet kommer att utvecklas och att jämförelsedata saknas beträffande viktiga delar av modellen. Däremot är de bedömningar som gjorts inom ramen för riskanalysen så pass grova, inga slutsatser har dragits på mer detaljerad nivå, att osäkerheten i analysen ändå får bedömas som acceptabel.

9. Generella slutsatser

Riskanalysen för robotmodellen genomfördes som ett första steg för att öka vår insikt inom området riskanalys av simuleringsmodeller. Nyttiga erfarenheter har erhållits genom detta arbete.

Riskhändelser samt deras orsaker och konsekvenser gick att beskriva i för tillämpningen tillräcklig omfattning. Som man kunnat förutse var däremot felsannolikheterna svåra att kvantifiera, men i termer som låg, medium och hög kunde en viss insikt uppnås. Beträffande inriktningen av V&V-aktiviteterna framkom i detta fall inga oväntade resultat, men riskanalysen ger ändå en stabilare grund för V&V-arbetet.

Omfattningen av en riskanalys måste anpassas efter tillämpningens art och syfte för att en rätt balans mellan resurser till riskstudien, till V&V-arbetet och till det övriga modellutvecklingsarbetet skall uppnås. I detta fall har riskstudien i sig varit en V&V-

insats genom att fel i modellen påträffats och rättats till vid genomförandet av felinsättnings- och känslighetsanalyserna. Det finns alltså en stark koppling mellan riskanalysprocessen och V&V-processen. En riskanalysprocess bör på samma sätt som en V&V-process starta innan modellutvecklingen börjar och pågå under modellens hela livscykel. En fråga vi kommer att studera framöver är om det skulle vara lämpligt att låta riskanalysen vara en del av V&V-processen.

En riskprocess stärker, bara genom sin existens, riskmedvetandet hos såväl beställare som modellutvecklare, vilket i sig är en positiv faktor. Även en som i detta fallet ganska enkel riskanalys ger en förhållandevis god känsla för trovärdigheten för modellen och bedöms vara ett framgångsrikt sätt att ge kunden/användaren insikt i modellens trovärdighet.

Mycket arbete återstår innan en gedigen struktur för området riskanalys av simuleringsmodeller skapats och införlivats i M&S-utvecklingsprocessen, och vi bedömer detta som ett viktigt område inom modellering och simulering.

10. Fortsatt arbete

Som ett fortsatt led i vårt arbete kommer vi att följa ett antal ytterligare projekt med utveckling av andra typer av modeller. Syftet är att utarbeta en mer detaljerad och förbättrad struktur för hur en riskanalys skall genomföras, och för hur metoder att basera denna på skall väljas. Vi kommer vidare att titta på hur en riskanalysprocess och en VV&A-process bör samordnas för att ge synergieffekter.

11. Referenser

- [Alvå2002] Alvå Peter, et al., *Studie av Samverkande Robotsystem*, Avdelningen för Systemteknik, FOI Stockholm, 2002
- [Beford och Cooke2001] Bedford T. och Cooke R., *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press, 2001.
- [Eliasson 2002] Eliasson F, *A Risk Perspective on Directing Verification and Validation Efforts in Simulation Models –Specifically on an Autonomous Co-operating Missile System*, Royal Institute of Technology, Stockholm 2002.
- [Grimvall 1998] Grimvall G., Jacobsson P., Thedéen T., *Risker i tekniska system*, Utbildningsradions förlag, Stockholm 1998.
- [Hofmann 2001] Hofmann M., *Validation – Possibilities and Limits in High Resolution Combat Simulation Systems*, European Simulation Interoperability workshop 2001.
- [ITOP 2002] Under utarbetning
- [Jerberyd2002] Jerberyd M.L., *Development of a Simulation Model for Moving Targets Handling in an Autonomous Co-Operating Missile System*, Systems Technology, FOI Stockholm, 2002.
- [MIL-STD-882C 1993] Department of Defense, *System Safety program requirements, Appendix A: Guidance for Implementation of System Safety Program requirements, 1993*
- [MIL-STD-882D 2000] Department of Defense, *Standard Practice for System Safety, MIL-STD-882D, 2000.*
<http://131.82.253.19/docimages/0001/95/78/STD882D.PD8>
- [Muessig1997] Muessig Paul R. et al., *Optimizing the Selection of VV&A Activities: A Risk/Benefit Approach*, Proceedings of the 1997 Summer Computer Simulation Conference, 1997.
- [Rasmussenrapporten 1974] U.S. Atomic Energy Commission, *Reactor safety Study*, Report WASH-1400, 1974.
- [Rausand1991] Rausand R., *Risikoanalyse*, Tapir Forlag, 1991.
- [RPG2000] VV&A Recommended Practices Guide, *Verification, Validation and Accreditation (VV&A)*, Department of Defense, Defense Modeling and Simulation Office, Virginia, USA, 2000. <http://msiac.dmsomil/VV&A/>
- [Thedéen1981] Thedéen T., Wallin U, Öhrvik J., *Statistisk analys av säkerhetsrelaterade incidenter för kärnkraftverk: Rapport över en pilotstudie*, 1981.
- [Ulriksson2001] Ulriksson J., *An Investigation and Prototype Development of a Simulation Model of an autonomous Co-operating Missile System*, FOI-D-0017-SE, Systems Technology, FOI, Stockholm, 2001.