STPA – systemteoretisk processanalys

Introduktion till systemteoretisk processanalys

Systemteoretisk processanalys STPA (Systems-Theoretic Process Analysis) är en riskanalysmetodik som jämfört med konventionell riskanalys har en mer omfattande riskmodell för både avsedda och oavsiktliga funktioner i ett system.
Riskanalysmetoder som felträdsanalys (FTA) eller feleffekts- och kritikalitetsanalys (FMECA) är inte avsedda för att hantera moderna systems komplexitet, som i tilltagande grad kan ha autonoma funktioner och ett okänt antal obekanta beroenden i en kontext som kan vara oöverskådlig.
Brister i systemarkitekturen och kravställning kan göra ett system farligt, trots att det uppfyller de tekniska krav som ställts på det och att dess komponenter är skadefria och fungerar som avsett. Med STPA kan även sådana brister identifieras som kan undgå mer konventionella metoder, för att den abstrakta kontrollmodellen i STPA omfattar säkerhetsrelevant kontrollstruktur med mer kontext utöver det aktuella systemet.

Några av fördelarna med STPA som är väl lämpad för system med sådan komplexitet är följande:

- Mycket komplexa system kan analyseras.
- STPA tillför kraftfull systemsäkerhetsmetodik för alla skeden av Försvarsmaktens livscykelmodell.

- Redan i konceptskedet kan STPA användas för att identifiera nödvändiga säkerhetskrav för utvecklingsskedet, så att kostsamma ändringar kan undvikas.
- Efter konceptskedet kan STPA även användas för att identifiera olycksrisker som behöver hanteras för att nå betryggande säkerhet eller tolerabel risknivå.
- Förutom att orsakas av att någonting går sönder eller slutar fungera som det ska, beaktas att olyckor även kan orsakas av farliga interaktioner mellan delsystem och komponenter som fungerar enligt givna specifikationer, eller att något är förbisett i en svåröverskådlig systemarkitektur.
- Det farliga som förut kunde hittas genom faktiska vådahändelser, kan med STPA identifieras tidigt i utvecklingsprocessen för att undanröjas eller reduceras.
- Metodiken är iterativ. I takt med att det tekniska utförandets detaljeringsgrad bestäms, förfinas även STPA-analysen för mer detaljerade nödvändiga säkerhetskrav.
- Fullständig spårbarhet från krav till alla systemegenskaper kan lätt underhållas, vilket förbättrar systemets underhållsbarhet och utveckling.

- Metodiken kan i samma modell inkludera mjukvara, människor, organisationer, säkerhetskultur etc. som orsaksfaktorer vid olyckor utan att behöva analysera dessa olika eller separat.
- STPA kan inkludera mjukvara, människor, organisationer, säkerhetskultur etc. som orsaksfaktorer vid olyckor och andra typer av förluster utan att behöva behandla dem olika eller separat.
- STPA ger underlag för nödvändig dokumentation om systems funktioner som ofta saknas eller är svår att hitta i stora, komplexa system.
- STPA kan enkelt integreras i din systemutvecklingsprocess och i modellbaserad systemutveckling.

Systemteori

Systemteori är en tvärvetenskaplig teori för att studera och förstå komplexa system. Teorin tar hänsyn till de olika delarna som utgör systemet, deras inbördes relationer och hur dessa interaktioner påverkar systemet som en helhet.

Systemteori är utvecklad för system som är:

- För komplexa för fullständig analys, t. ex. oöverskådliga system, ibland med obekanta inslag
- För organiserade för statistik analys. För mycket underliggande struktur som förvränger statistiken, dvs. inte så kaotiska att de inte lyder under några regler.

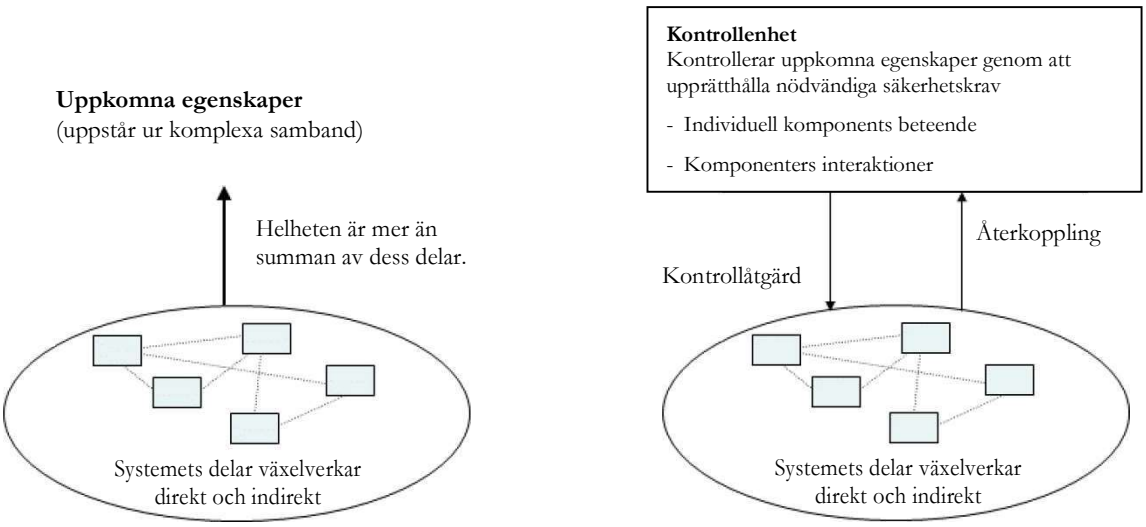
Inom systemteori finns det flera grundläggande principer, inklusive följande:

- **Systemet har delar med inbördes beroenden**: Detta innebär att varje del av systemet har en viktig funktion och påverkar andra delar av systemet.
- **Interaktioner mellan delarna skapar systemet**: Interaktionerna mellan systemets delar är vad som gör systemet till en helhet.
- **Systemet har en helhet som är större än delarna**: Systemet har egenskaper och funktioner som är större än de enskilda delarna som utgör det.
- **Systemet är dynamiskt och kan förändras över tid**: Systemet kan förändras över tid på grund av interna och externa faktorer.

Systemteori kan tillämpas på många olika områden, inklusive fysiska system som byggnader och maskiner, biologiska system som ekosystem och människokroppen, samt sociala system som organisationer och samhällen. Genom att tillämpa systemteori kan man få en bättre förståelse av hur system fungerar, och hur man kan förbättra dem genom att förändra eller optimera interaktionerna mellan dess delar.

Systemteori är väl lämpad för den ökade komplexiteten hos moderna tekniska system, där komponenters och delsystems beteenden kan ha inbördes beroenden som inte är uppenbara. Några unika aspekter av systemteorin är följande:

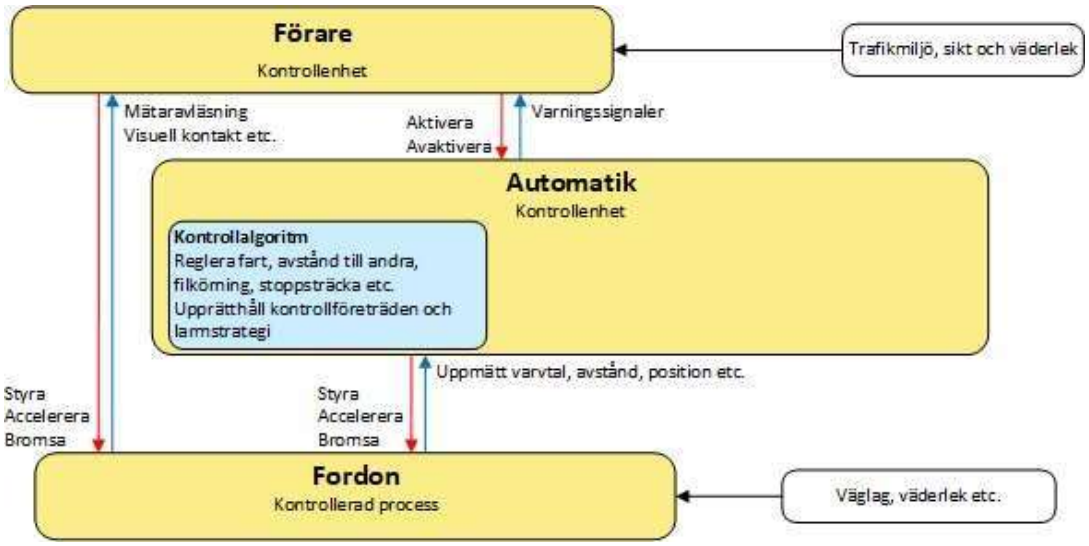
- Helheten är mer än summan av dess delar. Systemet måste därför behandlas som en helhet, inte som summan av delarna.
- Ett primärt bekymmer är de egenskaper som uppkommer ur systemet som en helhet. Dessa uppkomna emergenta egenskaper finns inte i summan av de enskilda komponenterna utan uppkommer när komponenterna växelverkar. Det kan ske både direkt och indirekt.
- Uppkomna egenskaper uppstår från relationer mellan delarna av systemet, genom hur de växelverkar och hur väl de passar ihop.
- Systemets uppkomna egenskaper kan endast behandlas adekvat genom att ta hänsyn till alla delars tekniska aspekter och kontext. Att dela upp ett system i moduler som analyseras var och en för sig kan därför inte ge en komplett analys av systemet som helhet. Det farliga är ett exempel på något emergent som uppstår ur systemet som en helhet i en given kontext.
- Om systemets uppkomna egenskaper är oönskade, exempelvis om systemet kan orsaka intressentförluster, är det rimligt att beteendet hos och interaktionerna mellan de individuella komponenterna måste begränsas och kontrolleras.



För att upprätthålla nödvändiga begränsningar och nödvändig kontroll på systemet behöver styrning eller reglering av individuella komponenter tillföras. Genom att skapa en abstrakt modell av kontroll-loopar där kontrollåtgärder och återkopplingar bildar en struktur med syftet att upprätthålla nödvändiga begränsningar för hur systemet kan uppnå sina mål.

Ett fordonssystem kan ha målet att köra från punkt A till punkt B. Att ingen ska skadas när det når sitt mål är ett exempel på en nödvändig begränsning ur systemsäkerhetssynpunkt.

Följande bild visar ett exempel på en kontrollstruktur för en bil med viss automatik. Observera att föraren inkluderas i den nödvändiga kontrollstrukturen i detta exempel. På en ytterligare högre hierarkisk nivå kan man utöka kontrollstrukturen med kontrollåtgärder från trafikövervakning, trafikregler etc.



Systemteoretisk olycksmodell och systemteoretiska processer

STAMP (System-Theoretic Accident Model and Processes) är en olycksriskmodell baserad på systemteori, som ger den teoretiska grunden för STPA. STAMP utökar den traditionella modellen för kausalitet bortom en kedja av direkt relaterade felhändelser eller komponentfel till att inkludera mer komplexa processer och farliga interaktioner mellan systemkomponenter, och den ligger till grund för bl. a. STPA.

Med STAMP behandlas säkerhet som ett kontrollproblem, föränderligt över tid och med ickelinjära inbördes beroenden, snarare än bara ett sätt att förebygga farliga komponentfel. Systemet kan ha brister trots att alla delar fungerar som de ska.

Genom att betrakta systemet som en helhet, inklusive dess struktur, processer och kontext uppnås ett synsätt för att upprätthålla nödvändiga krav på systemets beteende på ett sätt som lätt kan förbises med en linjära orsakssamband orsakade av komponentfel, dvs. att någonting går sönder eller slutar fungera som det ska och att det är farligt.

Några fördelar med att använda STAMP är följande:

- Den fungerar bra på mycket komplexa system eftersom analysen först ser systemet på övergripande nivå och sedan itereras för ökad detaljeringsgrad, dvs. uppifrån och ner snarare än nedifrån och upp som FMECA (feleffekts- och kritikalitetsanalys).
- Den inkluderar mjukvara, människor, organisationer, säkerhetskultur etc. som orsaksfaktorer och behandlar inte dessa olika eller separat.
- Den möjliggör kraftfulla verktyg, exempelvis STPA, olycksanalys CAST (Causal Analysis based on Systems Theory), identifieringshantering av ledande indikatorer på ökande risk, organisatorisk riskanalys, etc.

Genom att använda STAMP kan man förstå orsakerna till olyckor i komplexa system, och utveckla lämpliga strategier för att minimera risken för olyckor och förbättra systemets säkerhet.

Eftersom STAMP bygger på att ett system ska betraktas som en helhet kan STPA-metodiken användas för alla sådana uppkomna systemegenskaper.

STAMP har följande huvudelement:

- **Systemet**: Detta inkluderar alla delar av systemet, inklusive dess gränssnitt och interaktioner med andra system och användare.
- **Kontext**: Detta inkluderar de bredare faktorer som påverkar systemet, såsom organisationens struktur, policyer och processer, samt de sociala och tekniska miljöerna där systemet används.
- **Processer**: Dessa beskriver de underliggande processerna som driver systemet och dess funktioner, och hur de interagerar med varandra.
- **Händelser**: Dessa är de olyckor eller händelser som kan inträffa i systemet, och de konsekvenser som dessa händelser kan ha.

STAMP har följande grundläggande principer:

- **Gränssnittet mellan systemet och dess omgivning**: Detta fokuserar på att förstå gränssnittet mellan systemet och dess användare och omgivning, och hur interaktionen mellan dessa kan påverka säkerheten i systemet.
- **Hierarkiska kontrollstrukturer**: STAMP betonar vikten av hierarkiska kontrollstrukturer i systemet, och hur dessa kan påverka systemets säkerhet.
- **Information som styr resurser och beteenden**: Detta handlar om att förstå hur information påverkar resurser och beteenden i systemet, och hur detta kan leda till farliga situationer.
- **Diversifiering och redundans**: STAMP betonar vikten av diversifiering och redundans. Med diversifiering avses att använda olika teknologier eller tillvägagångssätt för att uppnå samma mål. Detta kan minska risken för att en gemensam händelse påverkar alla systemkomponenter på samma sätt. Redundans innebär att ha flera säkerhetsmekanismer på plats för att på så vis göra systemet mer robust mot komponentfel som kan leda till olyckor.
- **Mänskliga faktorer**: Detta fokuserar på mänskliga faktorer som kan påverka systemets säkerhet, inklusive människors beteenden, fel och misstag.
- **Systemets dynamik**: STAMP betonar vikten av att förstå systemets dynamik och hur det förändras över tid, och hur detta kan påverka systemets säkerhet.

Ledande indikatorer

Inom STAMP (Systems-Theoretic Accident Model and Processes) är ledande indikatorer viktiga för säkerhet. Ledande indikatorer är tidiga varningssignaler om missförhållanden. Att känna till systemets ledande indikatorer underlättar att kunna vidta förebyggande åtgärder för att minimera risken för olyckor eller incidenter. Det är en annan ansats än för släpande indikatorer, som indikerar händelser som redan inträffat och kan användas för att identifiera orsakerna till en olycka eller incident.

Exempel på ledande indikatorer kan vara antalet vådahändelser, säkerhetsavvikelser, observationer från inspektioner och revisioner, frekvensen av underhållsåtgärder eller prestandamätningar.

Systemteoretisk processanalys

STPA-metoden består av följande huvudsteg:

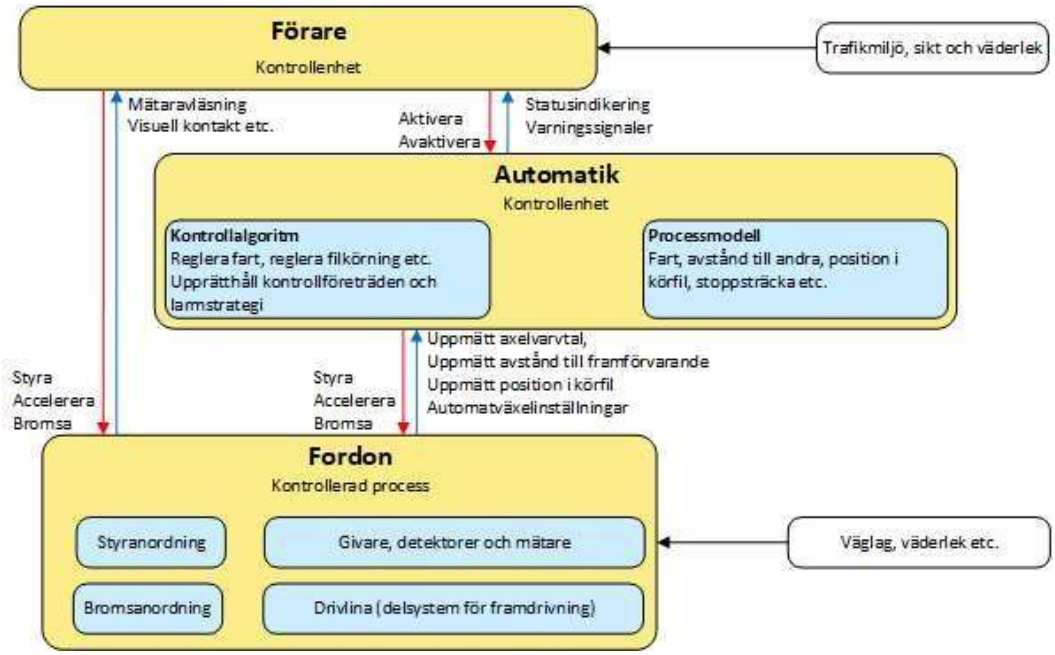
1. **Definiera syfte**: Översta hierarkiska nivån av krav måste finnas för att undvika oavsiktlig skada på person, egendom eller yttre miljö. Dessa tre krav kan detaljeras till cirka tio krav i första iterationen, men det är inte nödvändigt. Definiera i detta steg även systemets användningsområde, användningsmiljö, tekniska utförande och vilka tekniska gränsytor till angränsande system.
2. **Skapa modell av nödvändig kontrollstruktur**: Definiera systemförhållanden eller beteenden som systemet måste ha för att förhindra faror, som i sin förlängning förhindrar de förluster som ska undvikas. Bestäm nödvändiga begränsningar för hur systemet på ett säkert sätt ska nå sina mål och undvika de intressentförluster du har identifierat. Definiera en kontrollstruktur för att upprätthålla dessa begränsningar för systemet och systemets beteenden.
   Kontrollstrukturen ska i första iterationen vara så enkel och överskådlig som möjligt så att inget förbises, för att i kommande iterationer gradvis öka detaljeringsgrad efter hand som systemets tekniska utförande kan definieras utförligare.
3. **Identifiera farliga kontrollåtgärder**: Analysera om en kontrollåtgärd blir farlig om den uteblir, ges, ges för tidigt eller ges för sent eller uppgör för tidigt eller ges för länge. De av dessa som skulle kunna leda till de förluster som definierades i det första steget är farliga kontrollåtgärder. Utifrån dessa farliga kontrollåtgärder, identifiera nödvändiga begränsningar samt krav på systemet för att undvika farliga kontrollåtgärder.
4. **Identifiera förlustscenarion**: Det fjärde steget identifierar orsakerna till hur farlig kontroll kan uppstå i systemet. Olycksförlopp definieras för att förklara:
   a. Vad kan orsaka en farlig kontrollåtgärd, och kan den ha fler orsaker?
   b. Utöver farliga kontrollåtgärder, hur kan brister i kontrollslingan orsaka förlustscenarion, exempelvis felaktig återkoppling, otillräckliga tekniska krav, konstruktionsfel, komponentfel m.m.?
   c. I vilken kontext kan en till synes ofarlig kontrollåtgärd orsaka ett förlustscenario?

Integration av STPA i processerna för systemutveckling

När olycksförlopp väl har identifierats kan de användas för att skapa ytterligare krav på det tekniska utförandet, inklusive riskminskande åtgärder, beroende på när under livscykelprocessen STPA-metodiken tillämpas.

Exempel

Följande bild visar ett exempel på en övergripande kontrollstruktur för en bil med viss automatik, där kontrollåtgärder indikeras med röda nedåtgående pilar.



Varje kontrollåtgärd undersöks om det kan vara farligt om den ges på något av följande vis:

- inte ges när den borde,
- ges men i en kontext som gör den farlig,
- ges olägligt, dvs. för tidigt, för sent eller i fel ordning,
- ges för kort tid eller för länge.

För detta exempel visas hur automatikens bromsåtgärd kan identifieras som farlig i fyra avseenden. Flera farliga kontrollåtgärder av vardera slag kan vara möjliga.

Utebliven åtgärd	**Given åtgärd**	**Åtgärd ges för tidigt, ges för sent eller ges i fel ordning**	**Åtgärd avslutas för tidigt eller ges för länge**
UCA-1: Automatiken bromsar inte bilen alls inför hinder i körbanan.	UCA-2: automatiken bromsar bilen när den inte borde, så att bilen blir påkörd bakifrån av annat fordon. UCA-3: automatiken bromsar bilen till ett felsäkert tillstånd, stillastående med låsta bromsar, i en farlig kontext exempelvis på en järnvägsövergång	UCA-4: Automatiken bromsar bilen, men för sent för att undvika kollision med hinder i körbanan.	UCA-5: Automatiken bromsar bilen, men slutar bromsa för tidigt för att undvika kollision med hinder i körbanan.
[personskada, egendomsskada]	[personskada, egendomsskada]	[personskada, egendomsskada]	[personskada, egendomsskada]

Se UCA-1, undersök även vad som kan orsaka att automatikens bromsfunktion uteblir på ett farligt sätt, trots att systemet fungerar enligt givna specifikationer. Detta är det svåraste i hela processen men till stöd för det finns de farliga kontrollåtgärderna som har identifierats.

Se UCA-3, du behöver som STPA-användare även vara vaksam på om något utöver kontrollåtgärden i kontroll-loopen indirekt kan göra kontrollåtgärden farlig.

Att ge en bromssignal är ett sätt att föra systemet till ett felsäkert tillstånd, att stå stilla med låsta bromsar. Det skulle kunna bli farligt om bilen har stannat på en järnvägsövergång när det kommer ett tåg, dvs. farlig kontext kanske orsakat av en otillräcklig omvärldsuppfattning i kontrollenheten.

Formulera endast en av de farliga kontrollåtgärderna som har identifierats, i detta fall UCA-1, på ett format som innehåller följande uppgifter om kontrollåtgärdens ursprung, typ av farlig kontrollåtgärd, kontrollåtgärd, kontext och spårbarhet till förlust, enligt följande tabell.

Ursprung	**Typ**	**Kontrollåtgärd**	**Kontext**	**Förlust**
Automatik	ger inte	bromsåtgärd	vid hinder i körbanan	Personskada, Egendomsskada

Använd samma format för att identifiera hur intressentförluster ska undvikas, genom att ansätta motsatt typ, som i följande tabell.

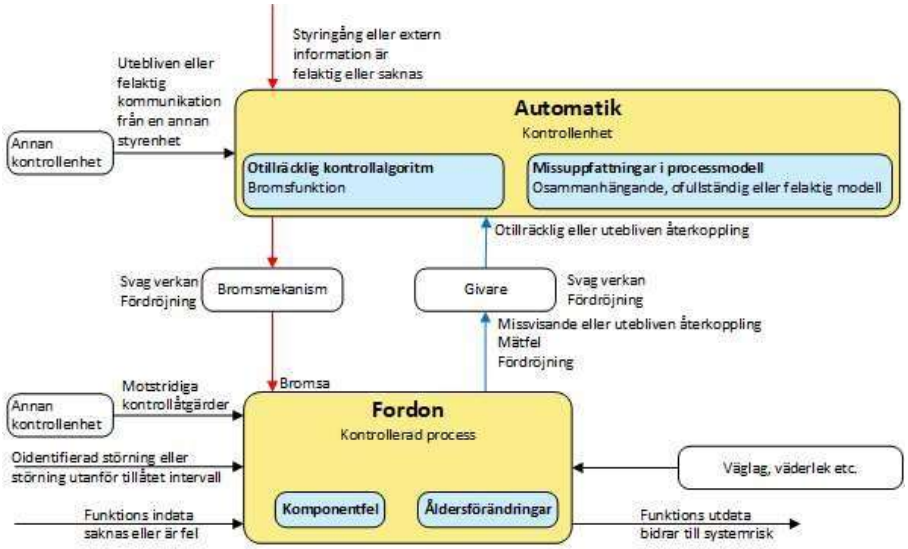
Ursprung	**Typ**	**Kontrollåtgärd**	**Kontext**	**Spårbarhet**
Automatik	måste ge	bromsåtgärd	vid hinder i körbanan	UCA-1

Detta övergripande krav behöver brytas ned till entydigt verifierbara tekniska krav. Det kan göras i kommande iterationer av kontrollstrukturen, i takt med att systemets tekniska utförande kan beskrivas med högre detaljeringsgrad.

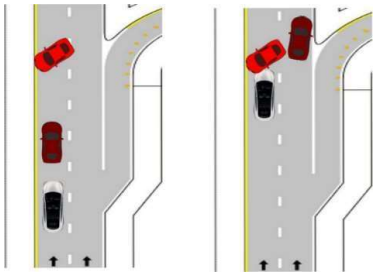
I detta exempel bedöms en utebliven kontrollåtgärd medföra risk för skada på person eller egendom. Det farliga tillståndet betecknas här farlig kontrollåtgärd UCA-1 (unsafe control action). För att identifiera vad som kan orsaka den krävs en fördjupad analys av den kontroll-loop där den farliga kontrollåtgärden förekommer.

Förlustscenarion kan även orsakas av andra brister i kontrollstrukturen än farliga kontrollåtgärder. Exempelvis kan en missvisande eller utebliven återkoppling från den kontrollerade processen skapa missuppfattningar i kontrollenhetens processmodell som ger systemet farliga beteenden.

Följande bild visar ett mer detaljerat exempel på kontroll-loop för automatikens bromsfunktion, och möjliga orsaker till att kontrollåtgärden kan utebli på ett farligt sätt.



Ett exempel på ett sådant olycksförlopp är att bil A automatiskt i hög fart följer tätt efter en annan bil B. Sikten till ett hinder C i körbanan är skymd av den framförvarande bilen B som väjer för hindret ganska sent, så att bil A inte hinner bromsa eller bromsar för sent.



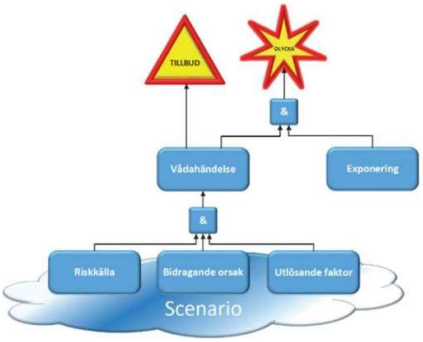
Risk identifierad 2016 med STPA av
Diogo Castilho och Megan France på MIT

Olycksförloppet inträffade i verkligheten 2018

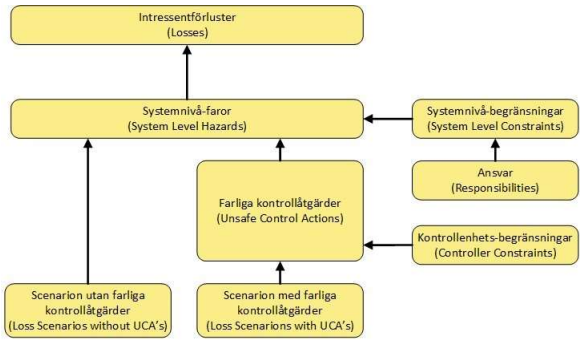
STPA och H SystSäk

Att genomföra STPA för att ett system ska undvika intressentförlusterna skada på person, egendom eller yttre miljö har samma syfte som systemsäkerhetsarbete enligt H SystSäk 2022. STPA kan vara en relevant metod vid genomförande av olika aktiviteter enligt MIL-STD 882 och H SystSäk 2022.

Inom STPA betraktas systemsäkerhet som ett dynamiskt kontrollproblem där olyckor orsakas av brister i en kontrollstruktur, och ger ett bra komplement till olycksriskmodellen i H SystSäk 2022.



Figur 1 Olycksriskmodell enligt H SystSäk 2022



Figur 2 Spårbarhet mellan STPA-utdata enligt STPA Handbook

Riskanalysen görs på den abstrakta kontrollmodellen, inte på det tekniska systemet som kan vara för komplicerat för en komplett analys. Kontrollmodellen kan inkludera mjukvara, människor, organisationer, säkerhetskultur etc. som orsaksfaktorer och behandlar inte dessa olika eller separat.

Systemteoretisk processanalys ska ses som ett komplement till gängse systemsäkerhetsarbete. Nyttan av STPA är störst för riskanalys av system som är för komplexa för en komplett analys, men följer vissa regler, så att statistiska analyser skulle vara missvisande.

STPA, liksom andra riskanalysmotoder, ger indata till säkerhetsrapporten (SAR) i form av risker, möjliga orsaker och nödvändiga begränsningar för att undvika eller mildra skadliga konsekvenser.

Det slutliga beslutsfattandet om hur, var och av vad vardera risk hanteras och beslut om stängning av systemsäkerhetsarbetet för vardera olycksrisk, hanteras inte med STPA. Som vilken riskanalysteknik som helst kan den bara ge indata till olycksriskvärderingar och klassificeringar av identifierade olycksrisker.