1 Syfte

STAMP (*root cause analysis*): Att undersöka styr-, övervaknings o ledningsinteraktioner i ett system, dess produktionsprocesser samt för den organisation o de beslutsfattare, som ingår i dessa, med syfte att finna orsaker till säkerhetsbrister/olycksfall samt definiera kompletterande säkerhetsrestriktioner[1] nödvändiga för systemsäkerheten.

STPA (*hazard analysis*): Att under systemutvecklingen[2] identifiera systemets riskkällor samt m h a STAMP-metodiken studera ingående interaktionsslingor[3], för att ur dessa härleda kompletterande säkerhetsrestriktioner.

2 Skede

Från produktdefinitionsfasen (konceptuell resp preliminär design) fram t o m systemets avveckling.

3 Ingångsmaterial

- Dokumentation över aktuellt system[4] samt vid första analysfas (PHL): ingångsmaterial enl [2].
- CIL (*Critical Item List*), en förteckning över kritiska systemelement (upprättad vid tidigare analys/analysmetod).
- Tidigare framtagna riskkällelistor för systemet.

4 Resultat

- En analysrapport sammanställd för hela systemet, (jfr [5]), vilken bl a inkluderar
  - **(a) Grafer** över ingående systemdelar o komponenter, där grundläggande styrstrukturer kompletterats med säkerhetsmekanismer i form av styrkommandon o statusåtermatningar/bekräftelser.
  - **(b) Riskkällor** o bidragande faktorer samt motsvarande **säkerhetsrestriktioner** i form av kompletterande säkerhetskrav o designrestriktioner samt motiveringar av på vilket vis dessa bidrar till mildrad totalrisk.
- CIL-förteckningen uppdaterad med nyidentifierade kritiska systemelement.
- Systemets riskkällelista uppdaterad med nyidentifierade riskkällor.

5 För- och nackdelar

+ Systematisk, systembaserad[5] metod för analys o design m a p säkerhet (STPA) samt olycksutredningar (STAMP).
+ Fokus på systemsäkerhet som en **emergent**[6] egenskap i komplexa o dynamiska processer samt olycksförlopp som följd av bristande säkerhetsrestriktioner (snarare än inriktning mot linjära o diskreta händelsekedjor)[7].
+ Proaktivt systemsäkerhetsarbete: Identifiering av restriktioner samt tillsyn av efterlevnaden under design o drift.
+ Säkerhetsmodellering i tre varianter: **Statiska** (tidsstabila) resp **dynamiska** (tidsföränderliga) **styrstrukturer** samt **dynamiska förändringsprocesser** (säkerhetsdegenererande förändringar hos faktorer/procedurer i driftsatta system)[8].
+ Modellering av styr- o ledningsflöden i interaktionen mellan organisation-personal-tekniskt system.
+ Samverkande faktorer beaktas såväl för system-av-system som organisation i o m analys av ledning-styrning-återmatning hela vägen ned i systemhierarkin (*top-down approach*). Visar var djupare analys kan vara befogad.
+ Granskar **processerna** bakom ett olyckförlopp: Kompletterar de traditionella händelsebaserade systemsäkerhetsmetoderna, vilka genom fokusering på olyckskedjor o defekter i enskilt system o komponent[9] ofta blir *bottom-up*-orienterade och inriktade mot tillförlitlighet.
+_ Metodiken relativt ny i systemsäkerhetssammanhang: viss erfarenhet från större systemtillämpningar finns dock.

---

[1] Säkerhetsrestriktioner: Säkerhetskrav samt design- o handhavanderestriktioner.
[2] Riskkälleanalys (STPA) parallellt med systemutvecklingen för tidigast möjliga inverkan på designbeslut o utformning. Jfr [2],[3].
[3] En hierarki av styr-/regler-/kommando-ordrar med statusåtermatning/bekräftelser (*control actions with feed-back loops*), [6],[7],[10].
[4] (Infoflöde mellan) Subsystem/komponenter/funktioner/driftspersonal samt grundläggande styrstrukturer inom o mellan det tekniska systemet, involverad personal o organisation. Operationell användning vid olika systemmod och omgivningar.
[5] System ses som hierarkiska strukturer, där varje nivå lägger restriktioner på aktiviteterna inom den underliggande nivån.
[6] Emergens: Samverkanseffekt vid interaktion – ett utfall utöver summerade, enskilda bidrag från interagerande delar (synergieffekt).
[7] Olycksförlopp: Bristande säkerhetsrestriktioner (*safety control structures*) m a p systemets design o operation (interaktionsdelar).
[8] Ex: Odokumenterade/förändrade förutsättningar, praxis som med tiden kommit att avvika allt mer från skriftliga instruktioner.
[9] STPA kan ses som en generalisering av HAZOP, vilken analyserar avvikelser i informationsflöden o systemvariabler.

6 Aktivitet/metod

- Initiera STAMP/STPA-studien:
  - o Klargör analysförutsättningarna[10].
  - o Sätt samman en analysgrupp .
- Förbered arbetet:
  - o Samla in och studera ingångsmaterialet (se 3).
  - o Ta fram mallar (jfr [5]), skaffa stödverktyg och planera analysrapportens utformning.
  - o Upprätta en arbets- o mötesplan för analyserna.
- Håll analysmöte:
  - o Presentera studiematerialet.
  - o Identifiera de analysnivåer och analysobjekt, som är aktuella för mötet[11].
  - o Inled med en preliminär riskkälleanalys (PHA)[2] på **system**nivå:
    1. Identifiera toppsystemets generella krav samt ev. restriktioner på omgivningen.
    2. Rita/uppdatera grafen över hela systemet med ingående delar o grundläggande styrmekanismer[12].
    3. Identifiera/ompröva på översta/aktuell nivå systemets
       - a. **riskkällor** samt motsvarande
       - b. **bidragande faktorer/förutsättningar.** Härled ur dessa matchande
       - c. **säkerhetsrestriktioner** (dvs krav o designrestriktioner nödvändiga för motverka viss riskkälla)

       Eliminera – där möjligt – identifierade riskkällor från den konceptuella designen.
       Specificera i övriga fall styrmekanismer samt nya designrestriktioner som del av designarbetet.
       Utöka systemgrafen med dessa säkerhetsinriktade styrflöden[13] (dvs i princip återigen punkt 2).
    4. Undersök i den modifierade designen ytterligare möjligheter att förbigå säkerhetsrestriktionerna (säkerhetsmässigt bristfälliga styråtgärder, jfr punkt 6a, vilken avser komponentnivån).
       Avgör hur dessa kan föreligga (dvs identifiera ytterligare bidragande faktorer).
       Eliminera dessa riskkällor från systemdesignen.
       Reducera där möjligt resten till tolerabel risknivå.
       Gå till punkt 2.

  - o Övergå till detaljerad riskkälleanalys på **komponent**nivå, då ovanstående iteration på systemnivå klar:
    5. Övervaka återstående riskkällor genom att definiera motsvarande säkerhetskrav o -restriktioner. (en *top-down*förfining o iterativ (om)design ned till **komponent**nivå ledande till tolerabel risk på toppnivå):
       - a. Förfina systemgrafen med säkerhetsinriktade styrflöden[13] ned till komponentnivå
       - b. Detaljera komponentens åtaganden i form av nedbrutna säkerhetskrav
       - c. Ange säkerhetsrestriktioner *(safety constraints)*[13]
    6. Avgör för varje komponent om den fullföljer sina åtaganden (enl punkt 5b) eller om den är behäftad med bristfälliga styrmekanismer (enl punkt 6a).
       Identifiera – i detta senare fall – de scenarier (se punkt 6b1) där säkerhetsrestriktion kan förbigås:
       - a. Identifiera säkerhetsmässigt bristfälliga styrmekanismer *(hazardous control actions)*:
         - **a1.** Bristfälligt **designad** styrmekanism
           - i. Inkonsekvent/ofullständig/felaktig/ingen styrmekanism (felaktig/ingen feedback eller styråtgärd som motdrag till kvarvarande riskkälla, felaktig/ingen sensorinfo/operation, ingen hantering av komponentfel/externa störningar/förändring/möjliga kommunikationsavbrott)
           - ii. Osäker kommunikation mellan komponenter
           - iii. Styråtgärd utövad för sent, vid fel tidpunkt/situation eller för tidigt avslutad
           - iv. Bristfällig koordinering mellan övervakare/beslutsfattare
           - v. Designade styråtgärder som med tiden kommit att degradera
           - vi. Oklara föreskrifter om vilken prioritet att tillämpa vid motstridiga styrkommandon från olika beslutsfattare/ -stödsystem[14].

---

[10] Systemets omfattning, möjliga skador (ekonomiskt/personellt/materiellt/miljömässigt). Analysens syfte (t ex identifiera samtliga brister eller endast de säkerhetskritiska).

[11] **Analysnivå**: Vid 1:a mötet: Den översta nivån i ett system-av-system (vid **produkt**analys) resp i en organisationsstruktur (**process**analys). **Analysobjekt:** t ex för viss systemkonfiguration: styrflöden/interaktioner på toppnivån (1:a mötet), dito inom en viss grupp av delsystem/ komponenter/ organisationskomponenter (efterföljande möten).

[12] ***Basic control loop***: Styrkommando/-åtgärd (såväl tekniska som organisatoriska föreskrifter/regleringar) med statusåtermatning/ orderbekräftelse *(**basic control action with feedback path**)*.
Vid styrning av system krävs **(a)** en definierad målsättning för övervakande enhet (*controller*) (t ex visst, satt värde skall hållas), **(b-c)** systemets tillstånd kan påverkas samt avläsas av övervakaren, **(d)** övervakaren har en modell av systemet.

[13] ***Safety control loop:*** säkerhetsinriktade styrkommandon med återmatning ***(safety control action with feedback).***

a2. Bristfälligt **utförd** styråtgärd[15]
- **i.** Bristande efterlevnad hos operatör/driftspersonal av fastlagda styrprocedurer
- **ii.** Felaktig prioritering vid motstridiga styrkommandon från olika beslutsfattare/ -stödsystem[14].
- **iii.** Bristfällig kommunikation till verkställande organ/manöverdon *(actuator)*
- **iv.** Bristfällig/felaktig operation hos verkställande organ/manöverdon
- **v.** Tidsfördröjning (t ex mellan signalerad styråtgärd och dess verkställande)

b. Finn bidragande faktorer till bristfällig styrmekanism (dvs till identifierade fall under 6a):
- **b1.** Utöka styrstrukturen *(control structure)* med processmodeller för varje styrkomponent
- **b2.** Undersök varje ingående del till en bristfällig styrmekanism efter orsaker
- **b3.** Inför styr- samt risklindringsmekanismer/-åtgärder
- **b4.** Utred möjlig degradering över tiden av styrmekanismens design *(asynchronous evolution)*.

Beta av en riskkälla (bristfällig styrmekansim enl punkt 6a med matchande faktorer enl 6b) i taget.
Gå till nästa punkt, då samtliga kvarvarande riskkällor bedömts för alla komponenter:

7. Omdesigna systemet (eliminera/förhindra/övervaka ev. bristfällig styrning) och Uppdatera driftsanvisningar, utbildningsmaterial, träningsupplägg etc.
8. Upprepa från punkt 2 tills tolerabel risknivå uppnåtts.
9. Dokumentera motiveringar till valda konstruktionsalternativ samt länka designbeslut till motsvarande krav o restriktioner[16].

- Dokumentera analysresultaten (se avsnitt 4):
  - Sammanställ en STAMP/STPA-rapport för hela systemet
  - Komplettera med förslag på nya säkerhetskrav/designrestriktioner samt risklindrande åtgärder[17].
  - För in tidigare ej identifierade avvikelser/riskkällor i systemets riskkällelista (se t ex [2], [3]).
  - Notera utestående frågor o oklarheter för vidare utredning av utpekad ansvarig efter mötet.
  - Slutsignera analysmötets resultat och notera gruppkonsensus.

- Följ upp vidtagna utredningar/åtgärder i efterföljande möte:
  - Identifiera eventuella kvarstående/obesvarade åtgärder/frågor.
  - Ompröva analysresultaten vid förändringar i system–omgivning–användning (kolla bl a punkt 6b4).

7 Referenser

Förutom andra referenser som kan erhållas ur sökningar efter 'STAMP', 'STPA' på nätet:

[1] Uppdragsspecifkation SäkAnalysMetoder, FMVdokument 14910:88774/2005.
[2] PHL-analys, Faktablad för Preliminär riskkällelista, FMVdokument 14910:2662/2006.
[3] PHA, Faktablad för Preliminär riskkälleanalys, FMVdokument 14910:2795/2006.
[4] Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk.
[5] Mall för STAMP-baserad riskkälleanalys, FMVdokument 14910:44138/2007.
[6] A New Approach to System Safety Engineering, Leveseon, June 2002 (310 sid!).
[7] An Approach to Design for Safety in Complex Systems, Leveson et al.
[8] A Notation Supporting a Systems-Theoretic Hazard Analysis Technique, J.Howard, K.Kelley.
[9] STPA: A new Technique for Hazard Analysis Based on STAMP, Tutorial notes, N Leveson, G Lee.
[10] Fler referenser samt kursmaterial med tillämpningsexempel för prov av STAMP/STPA, SpecTRM etc: http://ocw.mit.edu/OcwWeb/Aeronautics-and-Astronautics/16-358JSpring-2005/CourseHome/index.htm

8 Dokumenthistorik

Mellanliggande versioner skrivs in som dold text.

Version	Datum	Beskrivning
1.0	07-10-10	Faktablad enl [1].
1.1	07-11-06	Förenklad beskrivning av de olika analysstegen. Tillägg av 6.a1.vi, 6.a2.ii , ref [10] samt fonot 14-15.
1.2	08-02-13	Korrigering under pkt 6b, ny ref.

[14] Komplettering m a a SESAM:s provanalys av STAMP på flygolyckan i Überlingen (ILBRA).
[15] *Timelines*, som beskriver aktörernas parallella handlingar strax före olycka, kan vara en bra utgångspunkt – speciellt vid haveriutredningar (jmf sista-minuten-förloppet i flygkabiner o ledningscentraler involverade i Überlingen-olyckan).
[16] Se avsn. 4.5.2.3 i [4].
[17] Designändringar, skyddsmekanismer, säkerhetsprocedurer (i fall där säkerhetsrisken bedöms leda till överskriden toleransnivå _ en bedömning utan detaljerade riskskattningar).