Preliminär riskkällelista (PHL, *Preliminary Hazard List*)

1 Syfte

Att i tidigast möjliga skede minska systemsäkerhetsriskerna, genom att identifiera systemets potentiella riskkällor (*hazards*) och p s s påverka systemutformingen redan i dess konceptuella stadium.

2 Skede

Vid produktdefinitionsfasen (konceptuell design) före PHA (preliminär riskkälleanalys)[1].
PHL-analys är första fasen i den serie av säkerhetsanalyser[2] som tillämpas på ett system.

3 Ingångsmaterial

- Generella riskkällechecklistor[3],
- Riskkällelistor, olycks-/incidentrapporter (FRACAS), systemsäkerhetsanalyser samt erfarenheter från aktuellt applikationsområde,
- Beskrivningar över aktuellt system[4].

4 Resultat

- **PHL**, en förteckning över potentiella riskkällor[5], vilken – om möjligt – även inkluderar bidragande faktorer[6] för en riskkälla samt dess värsta konsekvens/effekt/olycksutfall[7].
  ~De förutsättningar som gäller för analysen, ev. antaganden som gjorts under denna samt de rekommendationer som går att ge i detta stadium anges (t ex i kommentarfält)[8].
  ~Riskkälla som efter identifiering befunnits vara irrelevant får kvarstå i listan och kommenteras med motiveringar till varför den ej längre är aktuell.
  ~PHL-innehållet är preliminärt – en del uppgifter kan eventuellt ej anges förrän efter mer ingående systemsäkerhetsanalyser under senare systemutvecklingsfaser, då systemets detaljer börjar ta form.

Exempel:

Riskkälla: Nr[5] / Olycksorsak[9]		**System-del[10] / mod[11]**		**Konsekvens[7]: Effekt/Olycksutfall**	**Bidragande faktorer[6]**	**Kommentar (Åtgärder)[8]**	**Status[12]**
Haz-1	*OavsiktlAvfyrning*	*RobotSystem*	*Underhåll*	*Personförlust*			*Öppen*
Ø	–						*Stängd*

- **TLM** (*Top-Level Mishap*), en sammanställning över typiska olycksutfall och involverade systemdelar[10,11]. Denna lista används i efterföljande analyser för identifiering av nya riskkällor, [4].

---

[1] Se [3]: fig s 35.
[2] Systemsäkerhetsanalysfas/-typ anger i vilket skede analysen skall utföras. Ex: PHA, SHA, SSHA, O&SHA. Se [2], [3]. Motsvarande systemsäkerhetsbedömningsprocess inom flyg är PFHA, FHA, PSSA, SSA, [8]. Notera distinktionen mot systemsäkerhetsanalysmetod, vilken beskriver hur analysen skall utföras, t ex HAZOP, FTA, FMECA. Se [3]: s 174, 205.
[3] Checklista över allmänna riskkällor: energi/ funktioner/ operationer/ komponenter/ material/ programvaruaspekter. Se t ex [2]:s 92, [4]:s 62 + App. C, [6]:s 297, [7] (ingen av dessa inkluderar dock programvaruaspekter). Jfr [9].
[4] Systemets övergripande design (huvudkomponenter och –funktioner), dess användning/driftbild och omgivning.
[5] Identifierade riskkällor numreras. Beteckningen Ø anger här, att inga riskkällor identifierats för motsv. systemdel/-mod.
[6] Bakomliggande omständigheter / utlösande händelser, t ex feltolkad information, kortslutning, elbortfall, installationsfel.
[7] Skadans art: **(**vad**,** grad**): (**Person/Egendom/Miljö**,** Förlust/Allvarlig skada/Mindre allvarlig/Obetydlig**)**, t ex Allvarlig systemskada.
[8] Ex: Nya systemspecifika säkerhetskrav/designrestriktioner som kan motverka effekten av identifierade riskkällor.
[9] Typ av riskkälla: kort beskrivning, t ex oavsiktlig robotavfyrning, friendly fire, orimliga flygdata, brott i syreförsörjningen.
[10] Systemkomponent/-funktion, som kan hysa en riskkälla (och därigenom är att betrakta som säkerhetskritisk).
[11] Mod som kan rymma riskällemoment: Systemmod (taxning/lättning/flygning/sättning/parkering), driftläge (normal/ degraderad/underhåll), styrmod (manuell/automatisk), operativ mod (jakt/attack/spaning). Jfr [3]: fotnot 237.
[12] Status *Öppen* ändras till *Stängd* efter verifiering att riskkällans riskbidrag reducerats till tolerabel nivå.

Exempel:

TLM nr	Olyckstyp[7]	Säkerhetskritisk del/aktivitet[10,11]
TLM-1	*Personförlust*	*Avfyrningssekvens vid transportmod, operativt mod & underhållsmod*

- Eventuella kompletteringar av de generella riskkälle checklistor[3] som använts.

5 Aktivitet/metod

- Klargör analysförutsättningarna[13].
- Sätt samman en analysgrupp[14] .
- Förbered arbetet:
  - Samla in och studera ingångsmaterialet (se 3).
  - Ta fram mallar.
- Håll analysmöte:
  - För varje systemdel resp systemmod: gå igenom de
    - generella riskkälle checklistorna,
    - riskkällelistor och olycksrapporter från liknande applikationer samt
    - deltagarnas erfarenhetsbank

    för att få fram potentiella riskkällor för det aktuella systemet.
    Undersök speciellt vilka
    - energikällor/ -flöden/-komponenter,
    - riskfyllda substanser[15],
    - potentiella interface-problem[16]

    som finns samt hur dessa hålls inom kontroll.
  - Utgå vid genomgången dels från riskkälla[9], dels från olycksutfall[7].
  - Använd ev. en '*light*'-variant av någon etablerad säkerhetsanalysmetod[17].
  - För varje identifierad riskkälla: utred (om möjligt)
    - Bidragande faktorer
    - Konsekvens
    - Åtgärder[8]
  - Sammanför likartade olycksutfall och identifiera de säkerhetskritiska delar/moment, som är involverade i varje olyckstyp.
- Skriv analysrapport (inkluderande PHL och TLM. Se 4).
- Uppdatera PHL vid förändringar i system–omgivning–användning.

6 Referenser

[1] Uppdragsspecifkation SäkAnalysMetoder, FMV dokument 14910:88774/2005.
[2] Försvarsmaktens handbok för Systemsäkerhet, M7740-784851 H SystSäk, s 90 ff.
[3] Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk
[4] Hazard Analysis Techniques for System Safety, C.A. Ericsson, ISBN 0-471-72019-4, s 55 ff.
[5] System Safety Analysis Handbook, www.system-safety.org/ProductsSale.php, s 3-209 ff.
[6] Safeware, System Safety and Computers, N G Leveson, ISBN 0-201-11972-2.
[7] Generell riskkällechecklista, FMV dokument 14910:6057/2006.
[8] Guidelines and Methods for Conducting the Safety Asessment Process on Civil Airborne Systems and Equipment, ARP4761.
[9] Checklista Programvaruriskkällor, FMV dokument 14910:12183/2006.

7 Dokumenthistorik

Version	Datum	Beskrivning
1.0	06-01-20	Faktablad enl [1].
1.1	06-01-31	Smärre uppdateringar (fotnot: 2,3,6,7,13,15, 16, ref: [6],[7], avsn: 5).
1.2	06-02-22	Putsningar efter SESAM gruppen Programvarusäkerhets 1:a PHL-analysmöte 06-02-14:fonot 2, ref [8], [9].

[13] Analysens syfte, systemets omfattning och gränser, möjliga ekonomiska/personella/materiella/miljömässiga skador.
[14] Fler än 2 personer: system- och applikationsexpert, systemsäkerhetsanalytiker, programvarutekniker etc.
[15] Ex: Bränsle, explosivämnen, giftämnen, radioaktiva ämnen, trycksystem, lasrar, vapen.
[16] Ex: Oförenliga material, kontamineringseffekter mellan material, miljöinverkan, möjligheter till oavsiktlig aktivering.
[17] Ex: HAZOP, STAMP.