SESAM
Försvarssektors användargrupp
för
Sofware Engineering

PHA
Faktablad för systemsäkerhetsanalysfasen PHA

FMV dokumentbeteckning
14910:2795/2006

I-L Bratteby-Ribbing, FMV

Datum
2006-08-18

Ver 1.3

Preliminär riskkälleanalys (PHA, *Preliminary Hazard Analysis*)

1 Syfte

Att i ett tidigt skede minska systemsäkerhetsriskerna, genom att spåra tidigare oidentifierade riskkällor (*hazards*) och analysera dessa tillsammans med de tidigare identifierade, för att utreda bakomliggande faktorer och riskkällenivå (*hazard level*)[1] och p s s påverka systemutformningen under preliminär design.

2 Skede

Vid produktdefinitionsfasen (preliminär design) efter PHL-analys[2].

3 Ingångsmaterial

- Generella riskkällechecklistor[3],
- Riskkällelistor, olycksrapporter, säkerhetsanalyser samt erfarenheter från liknande applikationer,
- Preliminär riskkällelista[4], PHL, [6],
- Beskrivningar över aktuellt system[5].

4 Resultat

- Ett preliminärt dokument över systemets identifierade riskkällor[6], rimligheten[7] för viss riskkälla och den värsta typ av skada denna kan orsaka (s k riskkällenivå)[1], bidragande faktorer till riskkällans aktivering samt involverade systemdelar (dvs säkerhetskritiska funktioner/ komponenter/ moment)[9,10].
  ~De förutsättningar som gäller för analysen, ev. antaganden som gjorts under denna samt de rekommendationer, som går att ge i detta stadium (kompletterande systemsäkerhetskrav, designrestriktioner, designändringsförslag etc), anges (t ex i Risklindrings- och Kommentarfält).
  ~Riskkälla som efter identifiering befunnits vara irrelevant får kvarstå i listan och kommenteras med motiveringar till varför den ej längre är aktuell.

Exempel:

Riskkälla: Nr[6] / Olycksorsak[8]		**System-del[9]/mod[10]**		**Rimlighet[7]: Riskkälla / Olycka**		**Konsekvens(Effekt): Skadeart/-klass[11]**		**Bidragande faktorer**	**Risklindring[12]: Typ/ Riskutfall**		**Kommentar Åtgärder etc**	**Status[12]**
Haz-1	*Oavsiktlig avfyrning*	*Robot Syst*	*UH*	***A***	***B***	*Personförlust*	***I***	*SystemMod-Parameter*	*Parameter-Reset*	***IC***	*SW:DesignÄndr HW:UH-spärr*	*Öppen*

[1]Sannolikheten att en riskkälla föreligger samt dess konsekvens (skadeart/-klass[11]), [3]: s 107 fotnot 247.
[2]PHL & PHA är analystyper (snarare än -metoder): De anger i vilket skede analysen skall utföras. Se [3]: fig s 35, 174, 205.
[3]Checklista över allmänna riskkällor: Se t ex [2]:s 92, 96, [4]:s 62 + App. C, [7]: s 297, [8], [9].
[4]PHL anger riskkällor och motsvarande olyckscenarier (vådahändelser) identifierade under systemets konceptuella design. TLM, en lista över för systemet typiska olycksutfall, kan föreligga från PHL-analysen, [4].
[5]Preliminär systemdesign (subsystem/huvudkomponenter/–funktioner), användning/driftbild vid olika systemmod, omgivning.
[6]Identifierade riskkällor numreras. Beteckningen _används, där inga riskkällor identifierats för motsv. systemdel/-mod.
[7]Rimlighet (sannolikhet), t ex **A** (Mycket ofta), **B** (Ofta), **C** (Mindre ofta), **D** (Osannolik), **E** (Mycket osannolik), jfr [2]:s 61.
[8]Typ av riskkälla: kort beskrivning, t ex oavsiktlig robotavfyrning, friendly fire, orimliga flygdata, brott i syreförsörjningen.
[9]Systemkomponent/-funktion med beskriven riskkälla (dvs säkerhetskritisk del). Med en tabell per systemdel kan denna kolumn utgå: Motsvarande information ges då i fält ovanför tabellen (tillsammans med datum, analystyp, deltagare etc).
[10]Mod som kan rymma olika riskällemoment: Systemmod (uppstart/marktransport/stigning/lufttransport/landning), driftläge (normal/degraderad/underhåll), styrmod (manuell/automatisk), operativ mod (jakt/attack/spaning). Jfr [3]: fotnot 237.
[11]Skadeart: typ (Person/Egendom/Miljö) + grad av skada (Förlust/Allvarlig skada/Mindre allvarlig/Obetydlig), t ex Allvarlig miljöskada. Skadeklass (allvarlighetsgrad), t ex **I** (Katastrofal), **II** (Kritisk), **III** (Marginell), **IV** (Försumbar), se t ex [2]:s 35.
[12]Typ: Förslag till systemspecifika säkerhetskrav/designrestriktioner/-ändringar/skyddsåtgärder/–mekanismer etc (för att bemöta aktuell riskkälla och få ned den totala riskbilden till tolerabel nivå). Identitet för nytt krav kan ges i kommentarfältet. Riskutfall: Bedömd olycksrisk efter risklindring, t ex **II**B (se fotnot 7 o 11). Status: *Stängd* då risklindring verifierats.

5 Aktivitet/metod

- Klargör analysförutsättningarna[13].
- Sätt samman en analysgrupp[14] .
- Förbered arbetet:
  - Samla in och studera ingångsmaterialet (se 3).
  - Ta fram mallar.
  - Identifiera tillämpliga säkerhetskritera/-principer/-handledningar för systemdesignen.
- Håll analysmöte:
  - Utgå från PHL/TLM, riskkällechecklistor, olycksrapporter och erfarenheter från liknande system.
  - Avgör om den preliminära systemdesignen aktualiserat ytterligare någon riskkälla.
  - Ompröva tidigare identifierade riskkällor om system, användning, teknisk/social omgivning ändrats.
  - Använd en/flera säkerhetsanalysmetoder[15] för att detaljstudera identifierade riskkällor och utvidga/ förfina förteckningen över bidragande faktorer, säkerhetskritiska delar/aktiviteter[16] samt olycksutfall[11]. Undersök speciellt
    - gränssnittet Människa-System: interaktion mellan operatörer och mot automatiserade systemdelar
    - möjliga användningsfall[17] och omgivningar för systemets hela operativa tid
    - fasövergångar mellan olika systemfaser/-tillstånd/-mod[18] samt mellan olika operatörsprocedurer
  - Ge förslag på nya säkerhetskrav/designrestriktioner samt risklindrande åtgärder (designändringar/ skyddsmekanismer/-procedurer)[12] där bedömd risk ligger ovanför toleransnivån.
  - Skatta rimligheten att riskkälla leder till olycka –dels med, dels utan risklindrade åtgärder.
- Skriv analysrapport (se 4).
- Följ upp effekten av införda systemsäkerhetskrav och risklindringar. Kontrollera hur dessa verifierats.
- Underhåll spårbarheten mellan bidragande faktorer–riskkälla–olycksrisk (sannolikhet, konsekvens).
- Uppdatera utförda säkerhetsanalyser vid förändringar i system–omgivning–användning.

6 Referenser

[1] Uppdragsspecifkation SäkAnalysMetoder, FMVdokument 14910:88774/2005.
[2] Försvarsmaktens handbok för Systemsäkerhet, M7740-784851 H SystSäk, s 94 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 73 ff.
[5] System Safety Analysis Handbook, www.system-safety.org/ProductsSale.php, s 3-207 ff
[6] PHL-analys, Faktablad för Preliminär riskkällelista, FMVdokument 14910:2662/2006.
[7] Safeware, System Safety and Computers, N G Leveson, ISBN 0-201-11972-2, s 284, 295 ff.
[8] Generell riskkällechecklista, FMVdokument 14910:6057/2006.
[9] Checklista Programvarans riskkällor, FMVdokument 14910:12183/2006.

7 Dokumenthistorik

Version	Datum	Beskrivning
1.0	06-01-20	Faktablad enl [1]. För komplettering av SESAM-gruppens medlemmar.
1.1	06-01-31	Smärre uppdateringar (fotnot: 3, 11, 13, 16-18, ref: [7], [8], avsn: 5).
1.2	06-02-23	Tillägg ref [9].
1.3	06-08-18	Smärre uppdatering under avsn 5.

[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: HAZOP, STAMP.
[16] För checklista över säkerhetskritiska faktorer, se t ex [5]:s 78.
[17] Såväl 'normala'/rutinmässiga användningssituationer/procedurer som de mer speciella/udda/exceptionella.
[18] Ex: Operativa mod: uppstart, omstart, nedstängning, testning, prov ny metodik, nedmontering, underhåll/reparation, inspektion, problemsökning, modifieringar, omkopplingar, avvikande inmatningar, förändringar i närliggande system, stress/överbelastningar (m a p system, operatör, projekt:ekonomi/tid), negativa omständigheter.