1 Syfte

Att identifiera ett systems riskkällor, genom att söka efter avvikelser från dess avsedda konstruktion och drift samt föreslå motåtgärder i form av systemförändringar.

2 Skede

Från produktdefinitionsfasen (konceptuell resp preliminär design) fram t o m systemets avveckling[1].

3 Ingångsmaterial

- Detaljerade, designgranskade beskrivningar över aktuellt system[2]
- Tidigare framtagna riskkällelistor.
- Nyckelordstabeller[11] och guidelines för HAZOP

4 Resultat

- En rapport sammanställd för hela systemet med ifyllda HAZOP-tabeller för varje studerad parameter [11].
- Förteckningen över kritiska systemelement (CIL, *Critical Item List*) kompletterad med nyidentifierade.
- Systemets riskkällelista uppdaterad med de avvikelser som bedömts innebära en systemsäkerhetsrisk.

Exempel på en HAZOP-tabell för hela systemet:

Löp-nr[3]	Studienod	Studienodens syfte/funktion	Parameter	Nyckel-Ord	Avvikelse[3] (riskkälla)	Orsak	Konsekvens	Åtgärd	Kommentar
1	*MissilSystem*	*Övervakning, Styrning*	*Avfyrnings-kommando*	*Delvis*	*Ofullständigt kommando*	*Opera-törsMiss*	*Oavsiktlig avfyrn (UH)*	…	…

5 För- och nackdelar

\+ Systematisk, kreativ, verktygsstödd metod, speciellt värdefull vid ny design där PHL ej finns att tillgå
\+ Ingående systemdelar samt interaktion mellan olika systemdelar belyses
_ Enstaka avvikelser (snarare än samverkande) i fokus
_ Ofullständiga nyckelordslistor kan innebära att vissa riskkällor/driftstörningar ej identifieras
_ Tidskrävande/kostsam: En HAZOP-analys innebär många HAZOP-möten[4], deltagare[6], samt studieparametrar.
+_ Hög detaljeringsgrad av ingående systemdelar samt noggrann metodikledning/-styrning en förutsättning

6 Aktivitet/metod

- Initiera HAZOP-studien:
  - Klargör analysförutsättningarna[5].
  - Sätt samman en analysgrupp[6] .
- Förbered arbetet:
  - Samla in och studera ingångsmaterialet (se 3).
  - Ta fram mallar och planera HAZOP-rapportens utformning.
  - Upprätta en arbets- o mötesplan för HAZOP-analyserna[7].
- Håll analysmöte:
  - Presentera studiematerialet.
  - Dela in systemet i studienoder[8] på system-, delsystem-, komponent- och subprogramnivå.

---

[1]Ex: HAZOP som del av PHL eller PHA (för systemdel av högre kritikalitet även som del av SHA eller SSHA). Se [2],[3].
[2](Infoflöde mellan) Subsystem/komponenter/funktioner. Operationell användning vid olika systemmod och omgivningar.
[3]Unik identifikation för varje tabellelement/avvikelse. **Avvikelse**: avsteg från planerat/förväntat/avsett beteende eller resultat.
[4] En HAZOP-studie kan bestå av ett flertal möten, typiskt i form av två 3-timmarspass/dag under 3 dgr/vecka i 3-4 veckor.
[5] Systemets omfattning, möjliga skador (ekonomiskt/personellt/materiellt/miljömässigt). Analysens syfte (t ex identifiera samtliga avvikelser eller endast säkerhetskritiska).
[6]Optimalt 4-7 personer: Protokollförare, System- resp applikationsexpert (konstruktör, användare), Systemsäkerhetsanalytiker, Metodikkunnig o projektoberoende HAZOP-ledare (vilken inte behöver vara den, som initierat HAZOP-studien).
[7] 1:a mötet: en grov HAZOP (kommentarinsamling), som förfinas under HAZOP-studiens inplanerade, efterföljande möten.

- Undersök varje studienod samt dess kopplingar till och interaktioner med omvärlden[9]:
  - Identifiera för varje studienod/gränssnitt dess flödeselement o elementens parametrar[10].
  - Upprätta en nyckelordstabell för varje parametertyp[11].
  - Komplettera standardnyckelorden med nyckelord specifika för varje enskild parameter.
  - Leta efter möjliga felorsaker/avvikelser/driftstörningar orsakad av viss parameter:
    - Genomför en *'brainstorming'* styrd av frågor baserade på framtagna nyckelord.
    - Undersök ev. avvikelser från avsedd design hos aktuell parameter och
    - Fyll i motsvarande nyckelordstabell.
  - Då denna procedur tillämpats för parameterns samtliga nyckelord o tolkningar, för elementets samtliga parametrar samt för samtliga element, upprepas den för resterande studienoder.
- Dokumentera analysresultaten (se 4):
  - Sammanställ en HAZOP-rapport för hela systemet (möjliga avvikelser-orsaker-konsekvenser).
  - Komplettera med förslag på nya säkerhetskrav/designrestriktioner samt risklindrande åtgärder[12].
  - 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 HAZOP-mötets resultat (HAZOP-ledare/-initiator) 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.

7 Referenser

Förutom de referenser som kan erhållas ur sökningar efter 'HAZOP' 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 Systemsäkerhet, M7740-784851 H SystSäk, s 119 ff.
[5] Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk, s 174.
[6] Hazard Analysis Techniques for System Safety, C.A. Ericsson, ISBN 0-471-72019-4, s 365 ff.
[7] System Safety Analysis Handbook, www.system-safety.org/ProductsSale.php, s 3-137 ff
[8] Safeware, System Safety and Computers, N G Leveson, ISBN 0-201-11972-2, s 335 ff.
[9] Safety-Critical Computer Systems, N Storey, ISBN 0-201-42787-7, s 39 ff.
[10] HAZOP Studies on Systems Containing Programmable Electronics, DS 00-58.
[11] System Safety: HAZOP and Software HAZOP, F Redmill et al, ISBN 0-471-98280-6.
[12] Ledord/nyckelord vid HAZOP-analys, FMVdokument 14910:17122/2006.

8 Dokumenthistorik

Mellanliggande versioner ligger som dold text.

Version	Datum	Beskrivning
1.0	06-02-03	Faktablad enl [1].
1.4	06-08-09	Sakinnehållet oförändrat: formuleringarna ensade mot ett senare framtaget FME(C)A-faktablad.

[8] Ex på **studienoder för programvara**: System, komponent, process, kommunikationskanaler, datalager, subprogram.

[9] **Interaktioner:** realiserade t ex via direkta anrop eller via gemensamma datalager. **Flödet** in/ur studerad komponent ses som element/entiteter med vissa parametrar/attribut/egenskaper. Ex på flöde: Elström, tryck, gas, vätska, materiel, data, signal.

[10] Ex: **Studienod:** komponent, kommunikationskanal, **Element:** datapost, **Parameter/attribut:** överfört värde, överföringshastighet.

[11] Den allmänna nyckelordstabellen anpassas för varje typ av studerad parameter,[11]-[12]. (Jfr [4]: s 120, [5]: fotnot 348, [6]:s 373, [8]:s 336, [9]:s 40, [10]:s 11). Ex på nyckelord aktuella för några parametertyper inom en studienod av typ **subprogram**:

Typ av Parameter/Attribut	Nyckelord/Ledord	Avvikelse (Tolkning/Definition)
Kommando	Ingen, Fel (oavslutat, avbrutet), Extra	Inget kommando, Fel kommando, Extra kommando
Enkelt datavärde	Inget, Noll, För lågt, För högt	Inget värde, värdet noll, för lågt/högt värde
Timing vid datakommunikation	Inte alls, För tidigt/sent, Före/efter avsedd ordningsföljd	…etc
Information/signal/dataflöde	Ingen, Felaktig, Inkonsistent, Fel ordningsföljd, Extra	…etc
Lagring	Instabil, Förstörd, Oåtkomlig, Skräp	…etc

[12] Designändringar, skyddsmekanismer, säkerhetsprocedurer (i fall där säkerhetsrisken bedöms leda till överskriden toleransnivå _ en bedömning utan detaljerade riskskattningar).