1 Syfte

Att prediktera tillförlitligheten hos en produkt eller process[1] genom att för varje ingående komponent eller funktion identifiera möjliga felmod/felsätt[2], undersöka effekten av dessa samt _där kritikalitetsanalys utförs_ föreslå konstruktionsändringar[3] prioriterade efter allvarlighetsgrad.

2 Skede

Från produktdefinitionsfasen (system- / komponentdesign)[4] fram t o m systemets avveckling.

3 Ingångsmaterial

- Detaljerade designbeskrivningar över aktuellt analysobjekt (produkt/process)[5]
- Kända felmod och felfrekvenser för ingående, återanvända komponenter[6]

4 Resultat

- En rapport sammanställd för hela systemet med ifyllda FMEA-tabeller för varje analyserat objekt.
- Förteckning över kritiska systemelement (CIL, *Critical Item List*) kompletterade med nyidentifierade.
- Systemets riskkällelista uppdaterad med de riskkällor, som identifierats för kritiska analysobjekt.

Exempel på en FMECA-tabell:

Löp-nr	Analys-objekt	System-mod/fas	Felmod/ Felsätt	Feleffekt för närmaste objekt / delsystem / system			Orsak	Kritikalitet/ Allvarlighetsgrad	Felfrekvens/ Sannolikhet	Risk-källa	Åt-gärd
1	...	...	...	...	...	...	...	...	...	...	...

5 För- och nackdelar

\+ Noggrann, lättillämpad, verktygsstödd metod (givet kunskap i systemet samt i tillförlitlighet_systemsäkerhet)[7].
\+ Enstaka enheter, dess felyttringar o inträffandefrevens kan analyseras och värderas.
\+ Feedback av analysresultat till designprocessen genom tidigt bruk av den hierarkiska metodvarianten.
_ Svårt identifiera samtliga felsätt (i synnerhet för mjukvaruprodukter och andra komplexa system).
_ Samverkande felyttringar, gemensamma felorsaker, '*timing*'-problem, operatörsfel, missöden som ej beror av felyttringar i systemet eller som härrör från externa källor fångas ej.
_ Kompletterande systemsäkerhetsanalysmetoder nödvändiga.
_ Inkonsistenser kan lätt uppstå, dels mellan resultat från de olika säkerhetsanalysmetoder som tillämpats för systemet, dels mellan de FMEA-tabeller som tas fram på olika nivåer i systemet. Detta kan motverkas genom att länka designens olika abstraktionsnivåer med motsvarande FMEA-resultat/-tabeller.
_ Tidskrävande/omfattande: Även detaljer som inte direkt berör systemsäkerheten behöver penetreras.

---

[1] Predikteringen görs ofta i termer av MTBF/MTTF/MTTR (medeltid mellan felyttringar_till nästa felyttring_till reparation).

[2] **Felmod**: det sätt varpå en felyttring hos analysobjektet visar sig, det mod/tillstånd analysobjektet befinner sig i efter en felyttring. Mekaniska system har (till skillnad från programvarusystem) ett begränsat antal felmod o kan därför lättare konstrueras felsäkert. Ex på funktionella felmod hos programvara: Funktion uteblir/ ger felaktigt resultat/ inträffar vid fel tidpunkt (för tidigt/sent)/ i fel ordning. Systemuppstart ofullständig/felaktig. Exekvering stoppad/hänger/kraschad.

[3] T ex eliminering av enkelfel, införande av redundans/diversitet eller annan felsäker teknik, vilka minimerar sannolikheten för främst de mest riskfyllda felyttringarna.

[4] Olika analysvarianter finns (Jfr fotnot 8): **Traditionell FMEA** utförs från enstaka komponenter och upp. **Hierarkisk FMEA** utgår företrädesvis från systemnivå, [10], och efterföljs av mer detaljerade analyser ned på komponentnivå. Dessa detaljanalyser är tidskrävande, vilket talar för **FMECA** enbart på de kritiska komponenter, vilka identifierats vid den inledande systemsäkerhetsanalysen (t ex en övergripande, **funktionell FMEA** eller en HAZOP). Resultatet kan sedan utgöra underlag till olika FTAer.

[5] **Analysobjekt**: **produkt** (helt system, visst delsystem/komponent/funktion/variabel/händelse) eller **process** (produktion/underhåll/ drift). För **produk**t: strukturella o funktionella systembeskrivningar (flödesscheman, interaktionsdiagram etc där analysobjektet involverad). För **process**: dokumentation över utveckling, underhåll, användning, drift etc.

[6] Obs: Beteendet hos en mjukvarkomponent beror av dess kontext: Kan därför inte utan vidare återanvändas i ett nytt sammanhang!

[7] T ex för en händelsekedja: distinktionen mellan **fel**scenariet '*fault-error-failure*' (felkälla-feltillstånd-felyttring), vilket FMEA beaktar, resp **olycks**scenariet '*hazard-unsafe state-accident*' (riskkälla-risktillstånd-olycka), vilket FME**C**A är intresserad av.

6 Aktivitet/metod

- Initiera FME(C)A:
  - o Klargör analysförutsättningarna[8].
  - o Upprätta en arbets- o mötesplan för FME(C)A-analyserna[9].
  - o Sätt samman en analysgrupp.
  - o Samla in och distribuera ingångsmaterialet (se 3) för förberedande studier i analysgruppen.
- Håll analysmöte:
  - o Presentera analysunderlaget.
  - o Identifera de analysnivåer och analysobjekt[5], som är aktuella för mötet.
  - o För varje analysobjekt:
    - – Identifiera möjliga felmod/felsätt för varje operationell mod där analysobjektet aktivt.
    - – För varje felmod:
      - _ Utred effekten lokalt på aktuell nivå och uppåt (analysobjekt → övergripande system).
      - _ Länka felsätt/-effekter/-orsaker till övriga berörda systemdelar, [10].
      - _ Bedöm effektens allvarlighetsgrad, frekvens, orsak samt de riskkällor som kan resultera.
      - _ Identifiera möjlig teknik för feldetektering o felprevention (som underlag för nästa punkt).
      - _ Komplettera med förslag på säkerhetskrav/ designrestriktioner samt risklindrande åtgärder[10].
      - _ Fyll i aktuell FMECA-tabell.
      - _ Stäm av resultaten med systemdesignern.
  - o Dokumentera analysresultaten (se 4):
    - – För in identifierade, kritiska systemelement in en CIL (se 4).
    - – Sammanställ en rapport för hela systemet med FME(C)A-tabeller samt CIL.
    - – För in tidigare ej identifierade riskkällor i systemets riskkällelista (se t ex [2], [3]).
    - – Notera utestående frågor o oklarheter för vidare utredning av utpekad ansvarig efter mötet.
    - – Slutsignera FME(C)A-mötets resultat och notera gruppkonsensus.
- Följ upp vidtagna utredningar/åtgärder i efterföljande möte:
  - o Identifiera eventuella kvarstående/obesvarade åtgärder/frågor.
  - o Ompröva analysresultaten vid förändringar i system–omgivning–användning.

7 Referenser

Förutom de referenser som kan erhållas ur sökningar efter ‘FMEA’ / ’FMECA’ 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 108 ff.
[5] Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk, s 179.
[6] Hazard Analysis Techniques for System Safety, C.A. Ericsson, ISBN 0-471-72019-4, s 235 ff.
[7] System Safety Analysis Handbook, www.system-safety.org/ProductsSale.php, s 3-111 ff
[8] Safeware, System Safety and Computers, N G Leveson, ISBN 0-201-11972-2, s 341 ff.
[9] Safety-Critical Computer Systems, N Storey, ISBN 0-201-42787-7, s 34 ff.
[10] A Hierarchical FMEA Unified System Model for Comprehensive Hazard Analysis, Czerny et al, ISSC´06.
[11] MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, Nov 1980.

8 Dokumenthistorik

Version	Datum	Beskrivning
1.0	06-08-09	Faktablad enl [1].
1.1	06-08-18	Tillägg av ref.

[8] Systemets uppgifter/användning, omgivning/begränsningar. Analysens syfte (fokus tillförlitlighet/systemsäkerhet). Typ av analysobjekt (produkt/process: se fotnot 5). Analysvarianter (**funktionell**: baserad på systemets funktioner, **strukturell**: baserad på systemets delar, **hybrid**: både-och, jfr fotnot 4) etc.

[9] Arbetsprocess, startobjekt samt stoppkriteria för analysen (dvs högsta o lägsta analysnivå), tidplan, mallar, begreppsförklaringar. Analysordning: t ex en inledande **funktionell** FMEA på övergripande systemfunktioner, där involverade delar identifieras (se fotnot 4). **Strukturell** FMECA på de säkerhetskritiska delar som identifierats, där analysen fortsätter in på allt mindre komponenter.

[10] Designändringar, skyddsmekanismer, säkerhetsprocedurer (i fall där säkerhetsrisken bedöms leda till överskriden toleransnivå).