Systemsäkerhetsanalys

Aktuellt i fas:

Systemsäkerhetsarbete är aktuellt i samtliga faser av livscykeln, här fokuseras på det arbete som sker i Konceptfas, Utvecklingsfas och Produktionsfas.

Syftar till:

Systemsäkerhetsarbete syftar till att identifiera och analysera risker och konsekvenser för tekniska system eller operativa procedurer, samt att arbeta fram åtgärder för att minimera dessa risker och/eller konsekvenser. Systemsäkerhetsarbete i detta avseende adresserar risker som rör skada på människa, egendom och/eller yttre miljö (till skillnad mot exempelvis ekonomiska risker eller projektrisker).

Resultat:

Resultatet från en systemsäkerhetsanalys, oavsett i vilken av faserna systemet befinner sig, skall ligga till grund för i första hand fortsatt utveckling av systemet med avseende på systemsäkerhet, och slutligen ett Systemsäkerhetsgodkännande.

I de olika livscykelfaserna genomförs systemsäkerhetsarbete på olika sätt och det finns metoder som passar bättre eller sämre för de olika faserna. Generellt kan man dock säga att

- Systemsäkerhetsarbete i **Konceptfasen** innefattar:
  - Identifiering av Safety Critical Functions
  - Kritikalitetsklassning av Safety Critical Functions
  - Framtagande av förslag till utvecklingsaktiviteter (för isolerat system)

- Systemsäkerhetsarbete i **Utvecklingsfasen** innefattar:
  - Uppföljning av Safety Critical Functions (efter att utvecklingsaktiviteter genomförts)
  - Genomförande av System Hazard Analysis
  - Framtagande av förslag till utvecklingsaktiviteter (för system i samverkan med andra system)

- Systemsäkerhetsarbete i **Produktionsfasen** innefattar:
  - Uppföljning av System Hazards (efter att utvecklingsaktiviteter genomförts)
  - Genomförande av Operating and Support Hazard Analysis (System Safety Assessment)
  - Upprättande av Safety Case Report (Safety Assessment Report)

Metod:

Det finns en mängd olika metoder för genomförande av systemsäkerhetsanalyser. Metoderna är olika lämpade att använda beroende på i vilken fas systemet befinner sig, i kombination med systemets egenskaper. Ett första steg i systemsäkerhetsarbetet innebär ofta riskidentifiering; här kan exempelvis PHA (Preliminary Hazard Analysis) eller FHA (Functional Hazard Analysis) användas. Vid nästa steg, kritikalitetsklassning, kan exempelvis FTA (Fault Tree Analysis) eller FMECA (Failure Modes, Effects and Criticality Analysis) vara lämpliga. För att analysera systemsäkerheten i den kontext systemet ska användas, kan exempelvis HAZOP (Hazard and Operability Study) nyttjas.

Indata:

Indata vid systemsäkerhetsarbete för ett tekniskt system utgörs bl.a. av ritningar, tekniska specifikationer, beskrivningar av systemets användarmiljö och handhavandebeskrivningar.