

10 Reliability of safety systems

10.1 Introduction

I figur 10.1 visas en skiss av ett enkelt "safety instrumented system" (SIS).

10.2 Safety instrumented systems

I sista stycket på sida 425, skriver Rausand & Høyland: "... dangerous failure modes are hidden during normal operation and are therefore called *dangerously undetected* (DU) failure modes." Man exemplifierar med en ventil som ska stänga av ett gasflöde om något kritiskt inträffar och man vet inte om ventilen fungerar då den behövs. För att få reda på ventilens status och vid behov reparera den, så testas ventilen vid tidpunkterna $0, \tau, 2\tau, \dots$. Man kontrollerar då att ventilen stängs då kommandot ges och att den håller tätt.

10.3 Probability of failure on demand

Låt $X(t)$ vara en säkerhetskomponents tillstånd m.a.p ev icke-upptäckt farlig felfunktion. Då

$$X(t) = \begin{cases} 1 & \text{if no DU failure is present} \\ 0 & \text{otherwise} \end{cases}$$

Se figur 10.4.

Låt T beteckna tiden till DU-fel. Otillgängligheten m.a.p säkerhet, $\bar{A}(t)$, i det första tidsintervallet $(0, \tau]$ är

$$\bar{A}(t) = P(T \leq t) = F(t) \quad \text{för } 0 < t \leq \tau$$

Detta kallar man även för "probability of failure on demand" vid tidpunkten t . Man tänker sig nu att man vid kontrollerna vid tidpunkterna $\tau, 2\tau, \dots$ återställer enheten till "as good as new". Då kommer $\bar{A}(t)$ att bli periodisk och vad "long run average" överensstämmer med medelvärdet över en period. Detta medelvärde kallas för "probability of failure on demand" och är

$$\text{PFD} = \frac{1}{\tau} \int_0^{\tau} \bar{A}(t) dt = \frac{1}{\tau} \int_0^{\tau} F(t) dt = 1 - \frac{1}{\tau} \int_0^{\tau} R(t) dt$$

Exempel 10.3 Single item

Branddetektor med felbenägenheten λ_{DU} m.a.p DU-fel och som inspekteras med τ tidsenheter mellan inspektionerna. Överlevnadsfunktionen är $R(t) = \exp(-\lambda_{DU}t)$ och

$$\text{PFD} = 1 - \frac{1}{\tau} \int_0^\tau e^{-\lambda_{DU}t} dt = 1 - \frac{1}{\lambda_{DU}\tau} (1 - e^{-\lambda_{DU}\tau})$$

Då $\lambda_{DU}\tau$ är litet gäller

$$\text{PFD} \approx 1 - \frac{1}{\lambda_{DU}\tau} \left(\lambda_{DU}\tau - \frac{(\lambda_{DU}\tau)^2}{2!} \right) = \frac{\lambda_{DU}\tau}{2}$$

R&H exemplifierar med en viss branddetektor med felbenägenheten $\lambda_{DU} \approx 0.21 \cdot 10^{-6}$ fel/timma. Med $\tau = 3$ månader ≈ 2190 timmar, fås

$$\text{PFD} \approx \frac{\lambda_{DU}\tau}{2} = 0.00023$$

Så stor andel av tiden är alltså branddetektorn ur funktion. Antas den vara i kontinuerlig drift så svarar detta mot ca $0.00023 \cdot 8760 \approx 2$ timmar per år. □

Exempel 10.4 Parallell system

□

Exempel 10.5 2-out-of-3-System

□

Exempel 10.6 Series System

□

10.3.4 Staggered testing

”When we have two items in parallell, we may reduce the system PFD by testing the items at different times.”

Definieras på sida 425.

10.8 The Markov approach