Moet het **interval** van een functietest worden gebaseerd op de **betrouwbaarheid** van de beveiligings-loops?

Door slimmer te ontwerpen is het falen van grote delen van beveiligings-loops waarneembaar geworden. Traditioneel gezien wordt het interval van een functietest bepaald op basis van de betrouwbaarheid van de gehele beveiligings-loops[1,2]. In dit artikel betoogd de auteur aan de hand van de RCM-theorie dat deze benadering leidt tot vaker testen dan nodig.

Op elke productielocatie bevinden zich misschien wel tienduizenden beveiligingen; ze beschermen ons tegen gevolgschade en verlagen het risico op veiligheids- en milieu-incidenten. Ze vormen onze last-line-of-defense. Functietesten is vaak de enige strategie voor het beheren van deze beveiligingsmiddelen. De uitvoer van een complete end-to-end test vergt vaak een productiestop, dure manuren en verhoogt regelmatig de kans op de storing die het nu juist wil voorkomen. De functietesten verdienen het dan ook om met de grootste zorgvuldigheid en zo vaak als vereist te worden uitgevoerd, maar ook niet (veel) vaker dan nodig.

Beveiligingen zijn bedoeld om de kans op een meervoudige storing te verlagen. Een meervoudige storing is dan bijvoorbeeld de explosie die volgt op het falen van de temperatuurregeling van een exotherme reactie (de beveiligde functie) terwijl de maximale temperatuurbeveiliging (beveiligingsmiddel) niet in staat is om het proces te *trippen*.

Tijdens een functietest wordt vastgesteld of de beveiligings-loops werkt. Door regelmatig een functietest uit te voeren en het beveiligingsmiddel zo nodig te repareren, wordt de beschikbaarheid van heimelijk falende beveiligingen verhoogd en wordt de kans op de meervoudige storing verlaagd. Een functietest heeft geen toegevoegde waarde als de storing zichzelf al zou melden (waarneembaar is).

Nu zijn er allerlei slimmigheden bedacht om het falen van beveiligingen waarneembaar te maken. PLC's worden dubbel uitgevoerd en bewaken elkaars stuurwaarden en commando's. Signalen van sensoren worden bewaakt op afwijkingen. Actuatoren van beveiligingscircuits worden opgenomen in de dagelijkse besturing. In sommige gevallen is uitsluitend een verkeerd setpoint of die ene schakeling op de PLC die actief wordt boven dat *setpoint* nog heimelijk.

Indien een waarneembare storing voldoende snel wordt gerepareerd en in de tussentijd het proces "handmatig" wordt bewaakt, dan kan de beschikbaarheid van de waarneembaar falende delen als 100% worden beschouwd.

Dat betekent dat het functietest-interval kan worden berekend op basis van de betrouwbaarheid van het heimelijk falende gedeelte. Deze betrouwbaarheid kan tientallen malen groter zijn, waardoor volstaan kan worden met een tientallen malen groter functietest-interval.

Het interval van een functietest moet dus worden gebaseerd op de betrouwbaarheid van het heimelijke gedeelte van de beveiligings-loops.

1) Benadering MTBF van het beveiligingscircuit: $1/M_{tot} = 1/M_{sensor} + 1/M_{bedrading} + 1/M_{AD} + 1/M_{PLC} + 1/M_{actuator}$

2) Functietest-interval (enkelvoudig beveiligingsmiddel): $SDI = 2 * M_{ging} * M_{ligd} / M_{ms}$.

Auteur: *Pieter Jan Hische van Operational Excellence Transfer – www.rcm2.nl*