



memo

DOC-0055 Continue systemen en de faalkans van software

Bijlage(n)

nvt

1.1 Inleiding

Deze memo is opgesteld om de faalkans per vraag, die uit het TOPAAS-model komt, om te rekenen naar een faalkans per uur. Deze omrekening is een voorstel van de TOPAAS-expertgroep en dient nog gevalideerd te worden.

1.2 Overgang van TOPAAS-score naar faalkans

Een expliciete doelstelling van TOPAAS 1.0 was het gebruik voor laag-frequent aangesproken veiligheidssystemen, zoals de waterkeringen. Deze systemen kennen een aanspreekfrequentie van eens per jaar, waar TOPAAS ook op ontworpen en gekalibreerd is.

De aanname dat het systeem eens per jaar zou worden aangesproken bleek in praktijk onhoudbaar omdat in de praktijktoepassingen (Tunnels, Sluizen) TUBs veel frequenter werden aangesproken (soms wel tientallen keren per dag). Ook kent elke veiligheidscomponent twee taakuitvoeringen: "*Ingrijpen als het moet*" maar ook "*Niet ingrijpen als het niet moet*". Voor veel tunnels speelt de discussie over onterecht sluiten van de tunnel ten gevolge van fouten in de besturing. Het omrekenen van de faalkans op basis van faalkans * aanspreekfrequentie resulteerde vaak in zeer onrealistische faalkansen waarbij objecten meer dan maandelijks in storing zouden staan.

Omrekening met behulp van aanspreek frequentie

De experts binnen en buiten de expertgroep geven ook aan dat dit niet overeenstemt met de realiteit: een object dat meer dan dagelijks aangesproken wordt, heeft vanuit de expert (en praktijk) vaak een lagere faalkans per vraag omdat fouten in gedrag veel sneller worden opgemerkt. Daarom is ervoor gekozen om in de omrekening ook de aanspreekfrequentie mee te nemen.

Als een systeem meer dan één keer per jaar wordt aangesproken wordt de TOPAAS-score op een andere wijze afgebeeld op faalkansen.

TOPAAS score	< 1x/jaar	< 1x/maand	<2x/ dag	Overig: Continu (λ)
>-2	Deze score levert geen kwantificatie op			
-2	10^{-2}	10^{-3}	10^{-5}	$10^{-6}/\text{uur}$
-3	10^{-3}	10^{-4}	10^{-6}	$10^{-7}/\text{uur}$
-4	10^{-4}	10^{-5}	10^{-7}	$10^{-8}/\text{uur}$

TOPAAS score	< 1x/jaar	< 1x/maand	<2x/ dag	Overig: Continu (λ)
-5	10^{-5}	10^{-6}	10^{-8}	10^{-9} /uur

Tabel 1: Relatie TOPAAS-scores en faalkans

De bovenstaande tabel die de TOPAAS-score en aanspreekfrequentie koppelt aan een faalkans is besproken met de TOPAAS-expertgroep. De "uitersten" van deze schaal zijn deels gebaseerd op de IEC 61508, waarin gereflecteerd wordt dat de industrieconsensus is dat de inspanning voor specifieke Q's en λ 's identiek is (uitgedrukt in een gelijk SIL-niveau), wat zeer bewuste gelijkschakeling suggereert. Op basis van de uitersten zijn de tussenliggende waarden via interpolatie bepaald.

Hier wordt wel een expliciete kanttekening bij geplaatst. De huidige referentieset bevat alleen expertinschattingen voor veiligheidssystemen. Om de overige kolommen te valideren dient de referentieset uitgebreid te worden, hetgeen in TOPAAS 2.0 nog niet gedaan is. Daarnaast zou onderzocht moeten worden of interpolatie van tussenliggende aanspreekfrequenties gerechtvaardigd is.

1.3

Van TOPAAS-score naar faalkans voorbeeld

De TOPAAS-score wordt bepaald door de scoring van elke vraag op te tellen en het totaal naar boven af te ronden. De TOPAAS-score is daarmee altijd een geheel getal boven de -5.

Om tot de faalkans te komen moet van de TUB ook de aanspreekfrequentie vastgesteld worden. Dit kan in de volgende staffels van (minder dan) één keer per jaar, één keer per maand, twee keer per dag of continu-(de rest).

Bijvoorbeeld uit de optelling komt het resultaat -3,6. Naar boven afgerond is dit -3. Met een aanspreekfrequentie van één keer per jaar is de faalkans van de TUB dan 10^{-3} .

TOPAAS

Nummer:	1319
Versienummer standaard:	2.0
Versienummer document:	
Status:	In beheer
Type:	Kader
Inhoudelijk beheerder:	Jeroen Horstman
Verantwoordelijke afdeling:	Afd. IB Systeemtechniek
Netwerken:	Hoofdvaarwegennet, Hoofdwatersysteem, Hoofdwegennet
Rollen:	Technisch Manager
Fase:	Realisatie
Proceseigenaar:	Proceseigenaar Aanleg en Onderhoud
Link om te reageren:	Link