



Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

RWS ONGECLASSIFICEERD

TOPAAS Audit framework – Deel 6 (Informatief)

Een structurele aanpak voor faalkansanalyse van software intensieve systemen

Datum	17 juli 2018
Status	Definitief

Colofon

Uitgegeven door	RWS Grote Projecten en Onderhoud
Informatie	J. Horstman
Telefoon	06 – 46172132
Uitgevoerd door	J.A. van Gelder
Datum	17 juli 2018
Status	Definitief
Versienummer	1.0

Inhoud

Inleiding—6

1 Achtergrond—7

- 1.1 Achtergrond—7
- 1.2 Uitgangspunten—7
- 1.3 Doel—7

2 Audit framework—8

- 2.1 Opzet—8
- 2.2 Framework—8

3 Toepassing—9

- 3.1 Gebruik—9
- 3.2 Invul parameters—9
- 3.3 Fase—10

4 Score en berekening—11

- 4.1 Score—11
- 4.2 Oordeel en advies—11
- 4.3 Berekening—11

5 Referenties—12

- A.1 Audit framework—13
- A.2 Voorbeelden van bewijzen—14
- A.3 Voorbeelden rapportage—16

Inleiding

Rijkswaterstaat is bezig om de kwaliteit van haar systemen met behulp van RAMS eigenschappen te specificeren en te beheren, waarbij RAMS staat voor betrouwbaarheid (Reliability), beschikbaarheid (Availability), onderhoudbaarheid (Maintainability) en veiligheid (Safety). Centraal in deze aanpak van risicogestuurd bouwen en beheren is de kwantitatieve risicoanalyse.

In toenemende mate is (complexe) software onderdeel van de systemen die Rijkswaterstaat laat bouwen en beheert. Software moet daarom ook worden meegenomen in de kwantitatieve risicoanalyse.

In opdracht van Rijkswaterstaat heeft een consortium van bedrijven en wetenschappers uit het ICT-domein een methode ontwikkeld die zowel richtlijnen geeft voor het modelleren van software falen in foutenbomen als voor het schatten van de faalkans van een taakuitvoering door een softwaremodule. Deze methode wordt TOPAAS genoemd en wordt beschreven in een theoretische uiteenzetting [1] en bijbehorende handleiding [2].

De basis aanname van TOPAAS is dat software in modulen wordt opgedeeld en dat het (mogelijk) falen van deze modulen in een foutenboom als basisgebeurtenis kan worden opgenomen.

Het schatten van de faalkans van een softwaremodule gebeurt op basis van expert opinion. Deze schatting wordt vervolgens gebruikt in een parametermodel. Dit model genereert dan een schatting van de faalkans van de softwaremodule per aanspraak.

Dit document geeft een audit framework als aanvulling op de handleiding [2] voor het toepassen van TOPAAS. Het framework wordt toegepast in (IT-)audits¹ om een oordeel te geven over de kwaliteit van de software. Zoals beschreven in [1] en [2] wordt in TOPAAS gekeken naar inhoudelijke aspecten als ook organisatorische aspecten. In de ontwerpfase worden, ten aanzien van deze aspecten, aannames gedaan (ontwerpkeuzen). Aan de hand van het framework kan tijdens en na de bouw worden vastgesteld of de aannames ook zijn ingevuld.

¹ Voorheen ook wel EDP-audit genoemd

1 Achtergrond

1.1 Achtergrond

In 2009 is voor het eerst in een tunnelproject de TOPAAS methode gebruikt om de betrouwbaarheid van de besturingssoftware vast te stellen. Opdrachtnemer heeft hiervoor samen met Rijkswaterstaat een praktische invulling gegeven aan het theoretische kader van TOPAAS [1]. De projectorganisatie heeft samen met een IT-auditor een Audit framework opgesteld. Met behulp van dit framework is gecontroleerd of de software leverancier hier daadwerkelijk invulling aan heeft gegeven.

In dit document is het in het project uitgewerkte audit framework omgezet naar een meer generiek audit framework. Dit framework in generieke vorm is als richtlijn beschikbaar voor projecten. Het framework maakt onderdeel uit van de totale set aan TOPAAS documenten².

1.2 Uitgangspunten

Het initiële framework, zoals ontwikkeld in het tunnelproject, bevatte nog veel items die niet zuiver voortvloeiden uit TOPAAS maar behoorden bij contract en projectmanagement en in projecten over het algemeen binnen de contractafspraken worden afgedekt. Het voorliggende audit framework bevat alleen onderdelen die zijn gebaseerd op de TOPAAS theorie [1].

Belangrijk is te beseffen dat het framework vooral een richtlijn is, het belang van de betrokkenheid van een expert moet worden onderstreept. De audit dient daarom te worden uitgevoerd door een IT-auditor. Dit is van belang om de kwaliteit van de software goed te kunnen schatten en een betrouwbaarheidsgetal vast te stellen dat betrouwbaar is. Het audit framework is daarin ondersteunend voor de auditor en dient voor het onderbouwen van zijn beoordeling ten aanzien van TOPAAS.

Het is de verantwoordelijkheid van de auditor om het controle kader te toetsen op bruikbaarheid en volledigheid voor toepassing in de door hem uit te voeren audit.

1.3 Doel

Het doel van het audit framework is de IT-auditor een kader te geven waartegen kan worden getoetst. Tevens voorziet het door de gelaagde opzet in een onderbouwing per controledoelstelling.

² De TOPAAS documenten bestaan uit de TOPAAS theorie [1], TOPAAS handboek [2], het audit framework en eventueel later aanvullende documenten.

2 Audit framework

2.1 Opzet

Het audit framework is gebaseerd op de theorie [1] en het handboek [2] TOPAAS en geeft een verdere uitwerking van de 15 vragen uit de TOPAAS vragenlijst.

De opbouw volgt de uitsplitsing naar de in [1] beschreven dimensies, waar de foutenboom als dimensie 1 is toegevoegd:

1. Opzetten foutenboom
2. Totstandkomingproces
3. Product
4. Requirements traceability/verifieerbaarheid
5. Testen
6. Executieomgeving/gebruik

De genoemde dimensies zoals binnen TOPAAS worden gedefinieerd moeten worden ingevuld voor de belangrijke of kritische functies van het systeem³. Het is van belang voor die functies waarvoor het stellen van een betrouwbaarheidsgetal van belang is.

Het audit framework bestaat uit een aantal lagen waardoor er een duidelijke herleidbaarheid behouden blijft naar de hierboven genoemde dimensies. Per dimensie zijn een of meer controledoelstellingen opgenomen. De controledoelstelling zijn zo opgesteld dat ze één op één overeenkomen met de 15 vragen uit de TOPAAS vragenlijst. Vervolgens zijn de controledoelstelling verder uitgewerkt naar maatregelen en vervolgens naar testen.

De testen maken onderdeel uit van de uit te voeren audit en beogen een beeld te geven van de situatie zodanig dat voor een maatregel kan worden bepaald of deze geïmplementeerd en / of werkend is gedurende de auditperiode. Per test wordt een type aangegeven, hierin wordt duidelijk of de test de opzet, het bestaan of de werking van een maatregel controleert.

Het beeld van de maatregelen moet een beeld geven van de situatie voor een controledoelstelling. Het behalen van de maatregel heeft geen één op één relatie met het behalen van de controledoelstelling.

De audit moet op verschillende momenten worden uitgevoerd (0-meting, tussenliggende fase en/of de eindmeting), per controledoelstelling is aangegeven of de doelstelling in de betreffende meting moet worden gecontroleerd.

2.2 Framework

Het audit framework bestaat uit een Excel document met daarin de volgende tabbladen:

- Theoretische dimensies
- Controledoelstellingen
- Maatregelen
- Testen
- Ontvangen documenten

³ voor de toepassing bij tunnels gaat het om de totstandkoming van de software voor de veiligheidskritische functies (VKF's).

3 Toepassing

3.1 Gebruik

De testen geven een redelijke mate van zekerheid over de opzet, het bestaan en de werking van de maatregelen, maar het is aan de IT-auditor om te bepalen of de testen voldoende zijn.

De afweging van de auditor over een maatregel aan de hand van de testresultaten en over de score voor de controle doelstellingen aan de hand van de status van de maatregelen blijft altijd een zaak van Professional Judgement.

De audit wordt ten minste tweemaal uitgevoerd. Aan de start van de bouw van de software kan een 0-meting worden uitgevoerd, hiervoor dient ten minste een samenhangende set/module gereed te zijn. Aan het eind of bij voorkeur na oplevering kan een eindmeting worden uitgevoerd, in deze meting kan dan bijvoorbeeld de velddata worden meegenomen. Eventueel kan een tussenmeting worden uitgevoerd. De planning van de metingen is afhankelijk van het softwareontwikkelp proces.

3.2 Invul parameters

De tabbladen theoretische dimensies, controledoelstellingen en maatregelen dienen ter achtergrondinformatie en overzicht.

De tabbladen testen en ontvangen documenten kunnen worden ingevuld.

Tabblad testen bevat daarvoor de volgende kolommen:

- Testresultaat
Hier wordt het testresultaat vermeld in een samenvatting
- Testkwalificatie
Hier wordt de kwalificatie gegeven en kan bestaan uit; gehaald, niet gehaald, niet uitvoerbaar, gehaald met opmerkingen, maatregel gecompenseerd
- Gebruikt bewijs
Hier een korte beschrijving van het bewijs dat is gebruikt (zie bijlage A.2 voor voorbeelden)
- Teststatus
Hier wordt de status van de test aangegeven en kan bestaan uit; in uitvoering, test uitgevoerd, gecontroleerd
- Testdatum
- Tester
- Bewijs ID
Hier de verwijzing naar het nummer van het document uit het tabblad 'Ontvangen documenten' opnemen
- Opmerkingen
Vrij veld voor het plaatsen van aanvullende opmerkingen

Toelichting testkwalificatie

Gehaald

Het resultaat van de test wordt als voldoende beoordeeld en is daarmee gehaald.

Gehaald met opmerkingen

Het resultaat van de test wordt als voldoende beoordeeld en is daarmee gehaald, maar de auditor heeft daar wel een aanvullende opmerking bij geplaatst.

Maatregel gecompenseerd

De maatregel waartegen te test wordt uitgevoerd is niet ingevoerd, in plaats daarvan is een alternatieve maatregel ingevoerd die dezelfde doelstelling beoogd. De resultaat van de test wordt als voldoende beoordeeld tegen de achtergrond van de alternatieve maatregel en is daarmee gehaald.

Niet gehaald

Indien de test wel wordt uitgevoerd maar niet het gewenste resultaat levert dan is de test 'niet gehaald'. Het niet halen van een of meerdere testen leidt tot het niet behalen van de maatregel. De mate waarin het niet behalen van een test bijdraagt aan het oordeel dat de maatregel 'niet behaald' is, wordt bepaald door de auditor. Er is geen rekenkundige onderbouwing voor het niet behalen van de maatregel.

Niet uitvoerbaar

Indien een maatregel (nog) niet getest kan worden omdat het proces, waarvoor deze maatregel geldig is, nog niet voltooid is of niet optreedt. Dan wordt de maatregel gekwalificeerd als 'niet uitvoerbaar'.

Indien 'niet uitvoerbaar' dan heeft de maatregel geen invloed op het behalen van de controledoelstelling omdat de effectiviteit van de maatregel niet beoordeeld kan worden.

Tabblad ontvangen documenten bevat de volgende kolommen:

- #
Hier staat een volgnummer waar naar, vanuit het tabblad Testen, kan worden verwezen
- Ontvangen document
Vermeld hier titel, subtitel van het document
- Organisatie
- Auteur
- Versie
- Status
- Datum
- Referentie
Eventueel vermelde referentie

3.3

Fase

Per controle doelstelling is aangegeven of deze wordt meegenomen in de 0-meting, tussenmeting of eindmeting. Vanzelfsprekend geldt dit dan ook voor onderliggende maatregelen en testen. Desgewenst kunnen ten behoeve van deze fasen kolommen worden toegevoegd op het tabblad Testen.

4 Score en berekening

4.1 Score

In een audit wordt bepaald wat de bevinding en daarmee de perceptie is van de kwaliteit ten aanzien van de controledoelstellingen. De perceptie is daarbij gebaseerd op de mate waarin de maatregelen zijn behaald. Het is aan de auditor om te bepalen wat de gevolgen zijn voor de controledoelstelling.

Niet gehaald

Er is er geen rekenkundige onderbouwing voor het behalen van de controledoelstelling. De auditor bepaald of alle maatregelen zijn geïmplementeerd en of ze effectief werken en in welke mate het niet effectief werken van een maatregel leidt tot het niet behalen van de controledoelstelling.

Niet uitvoerbaar

Indien de maatregel (nog) niet getest kan worden omdat het proces, waarvoor deze maatregel geldig is, niet voltooid was of niet optreedt.

4.2 Oordeel en advies

Uit de audit volgt een beoordeling per controledoelstelling (zoals hierboven gemeld) en een advies ten aanzien van de niet behaalde maatregelen. Op basis van het beeld van de controledoelstelling kan de score van de TOPAAS vraag worden bepaald.

In het oordeel en uiteindelijke advies worden de volgende formuleringen gebruikt om aan te geven welk beeld uit de audit is ontstaan.

Absolute zekerheid

Het geven van “absolute zekerheid” kan alleen indien alles gecontroleerd wordt en voor iedere test een wiskundige zekerheid van de juistheid van het resultaat van deze test kan worden gegeven. Dit is voor een deel niet mogelijk waardoor soms gesteund moet worden op de expert opinie van de auditor. Een expert opinie geeft geen absolute zekerheid. Daarnaast kan bij absolute zekerheid geen gebruikt gemaakt worden van selecties en steekproeven.

Beperkte mate van zekerheid

Een “beperkte mate van zekerheid” wordt afgegeven indien de auditor om moverende redenen slechts een beperkte controle heeft uitgevoerd. De auditor heeft “geen redenen gevonden” om een afkeurende verklaring af te geven.

4.3 Berekening

Aan de hand van het behalen van de controledoelstellingen kan worden berekend wat de faalkans voor de software moet zijn zoals beschreven in [1] en [2]. Indien een controledoelstelling niet wordt behaald dan moet dit worden vertaald als onbekend voor de score op de TOPAAS vraag.

5 Referenties

- [1] S.E. van Manen e.a., TOPAAS Een structurele aanpak voor faalkansanalyse van software intensieve systemen, versie 2.0, RWS DI 1-4-2011, digitaal doc: TOPAAS - de theorie v2
- [2] S.E. van Manen e.a., Handleiding TOPAAS Een structurele aanpak voor faalkansanalyse van software intensieve systemen, versie 0.7, RWS DI 10-1-2013, digitaal doc: TOPAAS – de handleiding v0.7

Dit zijn de laatste vigerende versies van de documenten op moment van uitbrengen van dit document. Mocht in de toekomst een nieuwe versie beschikbaar komen dan kan deze worden gebruikt.

A.1 Audit framework

A.2 Voorbeelden van bewijzen

Onderstaande lijst bevat voorbeelden van bewijsdocumenten die door de auditor kunnen worden opgevraagd. Deze lijst is niet compleet of volledig en is geen checklist of voorschrift.

Foutenboom beschrijving	Afstemming kwaliteitsmodel tussen alle betrokken partijen
Goedkeuring van de foutenboom	Beschrijving ingerichte kwaliteitstooling
Bouwtekeningen	Vastgelegde software metrieken voor complexiteit (Mc Cabe index ⁴)
Beschrijving failure mode	Complexiteitsberekeningen voor de modules
Beschrijving effectanalyse	Software objectbeschrijvingen (inclusief compiler id)
Functionele beschrijving systeem	Compiler-beschrijving
Overzicht van alle softwaremodules	Compiler-certificaat
Beschrijving van de betrokken softwaremodules	Beoordelingsrapport t.a.v. ervaring met de compiler
Beschrijving van de mogelijke acties van software modules	Producteisen van op te leveren systeem
Beschrijving van de relaties tussen acties van softwaremodules	Functioneel ontwerp systeem
Beschrijving alternatieve scenario's om de missie te bereiken	Technisch ontwerp systeem
Documentatie softwaremodules	Bewijsrapport correcte traceerbaarheid
Broncode selectie	Testplan
Projectplan	Testplan goedkeuring
Use cases	Documentatie t.a.v. betreffende testtechniek
Testscenario's	(Infrastructuur)architectuur documentatie
Testresultaten	Operationeel Beheerplan
Software architectuur beschrijving	Beschrijving aanwezige velddata
SIL certificeringsrapport	Beschrijving taakuitvoering van systeemcomponent
Beschrijving ontwikkelproces	Beschrijving monitoring inrichting van systeemcomponent
Software ontwikkelplan (afgestemd)	Beschrijving ingerichte Lifecycle Model Management systeem
Inspectiebeleid software ontwikkeling	Trainingsmateriaal
Inspectieplan software ontwikkeling	Trainingscertificaten
Inspectierapport softwareontwikkeling	Systematisch programma voor aanname van gekwalificeerd personeel om te voldoen aan de behoeften van het project
Inspectie softwareontwikkeling resultaten	Objectieve criteria voor het evalueren van de prestaties van projectmedewerkers
Actieplan management n.a.v. inspectierapport softwareontwikkeling	Evaluaties van de prestaties van projectmedewerkers
Toewijzing en acceptatie van management van acties n.a.v. inspectierapport softwareontwikkeling	Beschrijving test-tooling
Functiebeschrijving en CV's van inspecteurs	Beschrijving geïmplementeerde test-tooling
Inspectiedossier met geïnspecteerde documenten	Systeem testplan
Configuratiemanagement-database	Software Requirements Specification
Ontwerpdokumentatie	Beschrijving Software Requirements Specification Tooling
Requirements documentatie	Beschrijving Configuratiemanagement-systeem
Configuratiemanagementplan	Configuratie-items (selectie)
Beoordelingsrapport cultuur en samenwerking	Beschrijving Configuratiemanagement-systeem tooling
Organisatie classificatierapport	Criteria t.a.v. software installatie die

⁴ http://en.wikipedia.org/wiki/Cyclomatic_complexity

	compliance met de software installatie-eisen demonstreren
CV's van de ontwikkelaars	Criteria t.a.v. de doelomgeving voor installatie
Functie-eisen t.a.v. ontwikkelopdracht voor ontwikkelaars	Bewijs van Back-up van last working system version
Ontwikkelprojectplan	Software Detail ontwerp
Resultaten selectieprocedure voor ontwikkelopdracht	Software Detail ontwerp tooling
CV's projectmedewerkers	Coding standards
Functie-eisen t.a.v. ontwikkelopdracht voor projectmedewerkers	Overzicht (opsomming) van te produceren en geproduceerde documenten
Beschrijving ingerichte informatie en communicatiekanaal	Opgeleverde systeemonderdelen (selectie)
Beschrijving kwaliteitsmodel voor de opdracht	Unit tests

A.3 Voorbeelden rapportage

De rapportage van de audit bevat de conclusie en onderbouwing van de betreffende audit, eventueel voorzien van aanvullende adviezen.

De rapportage bevat ten minste de volgende onderdelen:

1. Beschrijving van de audit zoals het doel, de fasering, aanpak, gebruik van het framework, aanvullende randvoorwaarden.
2. Management samenvatting
3. Conclusie van de audit (eventueel alleen in de eindrapportage)
4. Overzicht van de gebruikte aannames (op basis van de TOPAAS vragenlijst) en toetsing in hoeverre hiervoor onderbouwing is (aantoonbaarheid van de aanname)
5. Bevindingen samengevat per theoretische dimensie (zie ook tabel 1). Eventueel voorzien van aanvullende toelichting of onderbouwing
6. Bevindingen samengevat per controledoelstelling (zie ook tabel 2). Eventueel voorzien van aanvullende toelichting of onderbouwing
7. Aanbevelingen per maatregel (beschrijf de maatregel, de test, het resultaat, de oorzaak, het risico en de aanbeveling).
8. Bijlage met de resultaten van de audit (ingevuld audit framework zoals weergegeven in bijlage A.2).
9. Eventueel aanvullende informatie zoals een overzicht van de geïnterviewde personen.

Maak bij elke meting (0-meting, eventuele tussenmetingen, eindmeting) een update van het rapport.

Dimensie	Aantal controle doelstellingen	Aantal maatregelen	Aantal testen	Niet gehaald	Niet uitvoerbaar
1 Opzetten Foutenboom	5	25	38	#	#
2 Totstandkomingsproces	6	25	63	#	#
3 Vaststellen producteigenschappen	4	7	18	#	#
4 Verificatie van de eisen	1	4	14	#	#
5 Testen van de (deel) producten	1	5	19	#	#
6 Gebruiken van de producten	3	8	24	#	#
TOTAAL	20	74	176	#	#

Tabel 1: Voorbeeld bevindingen samengevat per theoretische dimensie

Controle doelstelling	Kwalificatie controle doelstelling	Gehaald	Maatregelen Niet gehaald	Niet uitvoerbaar
1.1 De Foutenboom is beschreven	Gehaald/ niet gehaald	#	#	#
2.1 Het ontwikkelproces voldoet aan een van de	Gehaald/ niet gehaald	#	#	#

SIL's (Safety and Integrity Levels) van de IEC					
3.1	De complexiteit van de beslislogica is vastgesteld	Gehaald/ niet gehaald	#	#	#
5.1	Formele testtechnieken zijn aantoonbaar gebruikt tot een vastgestelde dekkinggraad	Gehaald/ niet gehaald	#	#	#
TOTAAL			#	#	#

Tabel 2: Voorbeeld bevindingen samengevat per controledoelstelling

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