



MINISTERIE VAN BZK
INGEKOMEN
0 2 NOV 2009
Onderdeel: <i>BPR 2009-58026</i>
Agenda:
RAPPEL NA:



SECRETARIAAT KIESRAAD

Aan de Staatssecretaris van Binnenlandse Zaken en
Koninkrijksrelaties
Postbus 20011
2500 EA Den Haag

Datum
28 oktober 2009

Ons kenmerk
2009-0000606396

Inlichtingen
mw. mr. R. Hoorweg
T 070 - 426 6266
F 070 426 64 89

Uw kenmerk
-

Blad
1 van 1

Aantal bijlagen
1

Bezoekadres
Herengracht 21
2511 EG Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Internetadres
www.kiesraad.nl

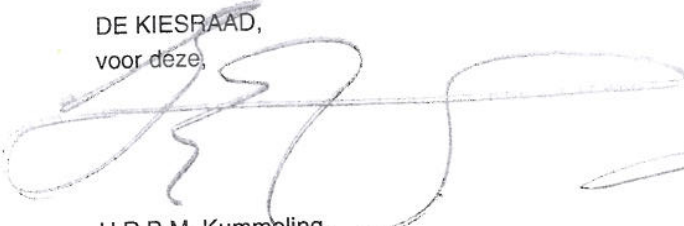
Emailadres
kiesraad@kiesraad.nl


Onderwerp
Aanbieding laatste deelrapport onafhankelijke
instantie toets (OSV)

Eerder dit jaar ontving u van ons de eerste twee deelrapporten inzake de toets van de Ondersteunende Software Verkiezingen (OSV) aan de eisen voor programmatuur die gebruikt wordt door centrale stembureaus bij het berekenen van de uitslag en de zetelverdeling.¹ Deze twee deelrapporten hadden betrekking op de software zoals deze wordt gebruikt voor Europese Parlementsverkiezingen. Conform een van deze eisen is de toets uitgevoerd door een onafhankelijke instantie.

Hierbij bieden wij u het laatste deelrapport aan. Hierin staan de resultaten van het onderzoek van de software voor de overige verkiezingen: Tweede Kamer, gemeenteraden, deelraden, provinciale staten en referenda. Ook nu luidt de conclusie van het onderzoek dat de software voldoet aan de gestelde eisen.

DE KIESRAAD,
voor deze,


H.R.B.M. Kummeling,
voorzitter


R. Hoorweg,
plv. secretaris-directeur

¹ Kamerstukken II 2007/2008, 31 200 VII, nr. 55.



01650

0221020001620



Software Improvement Group

© 2014 SIG

Toetsing eisen OSV 4 en 5 voor verkiezingen voor de Tweede Kamer, gemeenteraden, deelraden, Provinciale Staten en referenda Rapport t.b.v. de Kiesraad

19 oktober 2009
Dr. Sieuwert van Otterloo
+31 20 314 0950
s.vanotterloo@sig.nl



Software Improvement Group

Arent Janszoon Ernststraat 595-H
NL-1082 LD Amsterdam
t +31 (0)20 314 09 50
f +31 (0)20 314 09 55
info@sig.nl
www.sig.nl

Managementsamenvatting

De Kiesraad heeft programmatuur laten ontwikkelen ter ondersteuning van het verkiezingsproces en stelt deze programmatuur beschikbaar aan de stembureaus voor gebruik bij verkiezingen. De eerste versie van deze software is gebruikt voor de Europese verkiezingen op 4 juni 2009.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties heeft eisen gesteld waaraan deze programmatuur moet voldoen. Eén van deze eisen is dat er door een onafhankelijke instantie een toets gedaan wordt. Het gaat hierbij om toetsing van deel 4 en 5 van de programmatuur *Ondersteunende Software Verkiezingen* (OSV), omdat deze delen gebruikt zullen worden voor de verwerking van verkiezingsresultaten. De Software Improvement Group is door de Kiesraad gevraagd om deze toetsing uit te voeren. Dit rapport geeft de resultaten voor OSV 4 en OSV 5 voor gebruik bij verkiezingen voor de Tweede Kamer, gemeenteraden, deelraden, Provinciale Staten en referenda. In twee eerdere rapporten is de toetsing beschreven van OSV 4 en OSV 5 voor gebruik bij de Europese verkiezingen.

In de vorige rapporten is reeds vastgesteld dat de programmatuur bovengemiddeld scoort op belangrijke kwaliteitsaspecten waaronder ontwerp en modulariteit. Uit de toetsing aan gestelde eisen is naar voren gekomen dat de programmatuur OSV 4 en OSV 5 op de volgende kanttekeningen na voldoet aan gestelde eisen:

- Er is tot nu toe slechts gedeeltelijk aan eis 4c (open source) voldaan. Als positief punt valt op te merken dat de broncode beschikbaar is ter inzage. Om vast te stellen dat de programmatuur conform eis 4c 'open source' ontwikkeld is, moet de broncode onder een goedgekeurde open source-licentie worden gepubliceerd. Dit is niet gebeurd.
- Gerelateerd aan eis 7 (authenticiteit programmatuur) geldt dat zolang de programmatuur in een afgeschermd omgeving gebruikt wordt, er aan eis 7 voldaan is.
- In eis 9 (formele methodes) wordt gesproken over wiskundig aangetoonde correctheid. Dit is een zeer zware eis die alleen voor zeer kritieke en lastig wijzigbare programmatuur gebruikelijk is. Er is vastgesteld dat de broncode waarop deze eis van toepassing is ruim gedocumenteerd en getest is. De geleverde wiskundige definitie is echter niet voldoende volledig om deze eis als voldaan te beschouwen.

Tevens is vastgesteld dat de programmatuur voldoende onderhoudbaar en daarmee toekomstvast is.



Inhoudsopgave

1	INLEIDING.....	7
1.1	Context.....	7
1.2	Aanleiding.....	7
1.3	Scope.....	7
1.4	Onderzoeksvragen.....	8
1.5	Structuur van dit rapport.....	8
2	ONDERZOEKSPROCES.....	9
2.1	Uitgangspunten.....	9
2.2	Bronnen.....	9
2.3	Betrokken personen.....	10
3	ANTWOORDEN TOETSING AAN EISEN.....	12
3.1	Eis 1: functionaliteit.....	12
3.2	Eis 2: documentatie.....	12
3.3	Eis 3: ontwerp.....	13
3.4	Eis 4: open standaarden en open source.....	14
3.5	Eis 5: verschillende besturingssystemen.....	15
3.6	Eis 6: diakritische tekens.....	16
3.7	Eis 7: authenticiteit programmatuur.....	16
3.8	Eis 8: authenticiteit gegevens.....	16
3.9	Eis 9: formele methodes.....	17
3.10	Eis 10: onafhankelijke toetsing.....	19
3.11	Eis 11: elektronisch stemmen.....	19
4	TECHNISCHE KWALITEIT VAN OSV 4 EN 5.....	21
4.1	Conclusie voor de technische kwaliteit.....	21
4.2	Onderbouwing.....	21
5	CONCLUSIES EN AANBEVELINGEN.....	22
5.1	Conclusies.....	22
5.2	Aanbevelingen.....	22
A.	AANVULLENDE INFORMATIE VOOR TOETSING EISEN.....	24
A.1	Algemene informatie: omvang en technologieën.....	24
A.2	Eis 1: functionaliteit.....	24
A.3	Eis 2: documentatie.....	25
A.4	Eis 3: ontwerp.....	28
A.5	Eis 5: verschillende besturingssystemen.....	29

1 Inleiding

1.1 Context

De Kiesraad heeft programmatuur laten ontwikkelen ter ondersteuning van het verkiezingsproces en wil deze programmatuur beschikbaar stellen aan de stembureaus voor gebruik bij verkiezingen. Het gaat om een verzameling programma's genaamd 'Ondersteunende Software Verkiezingen (OSV)'. Deze programmatuur stelt stembureaus in staat om getelde stemmen in te voeren, op te slaan, samen te voegen en tenslotte de gekozen kandidaten te bepalen.

De programma's OSV 4 en OSV 5 zijn de programma's uit OSV die door de verschillende stembureaus gebruikt worden na de verkiezingen voor verwerking van uitslagen. De overige programma's zijn voor het aanmaken van de benodigde informatie (verkiezingsdefinities en kandidatenlijsten) ter voorbereiding van verkiezingen.

1.2 Aanleiding

Door middel van een brief aan de Tweede Kamer op 9 april 2008 heeft de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties eisen gesteld waaraan OSV 4 en 5 moeten voldoen, voordat zij gebruikt kunnen worden in het verkiezingsproces. Eén van deze eisen is dat er door een onafhankelijke instantie een toets gedaan wordt in opdracht van de Kiesraad of de programmatuur aan deze eisen voldoet. Daarnaast heeft de Kiesraad er belang bij om de onderhoudbaarheid van de programmatuur vast te laten stellen. Dit onderzoek heeft als doel om deze toetsing uit te voeren en secundair de onderhoudbaarheid vast te stellen.

1.3 Scope

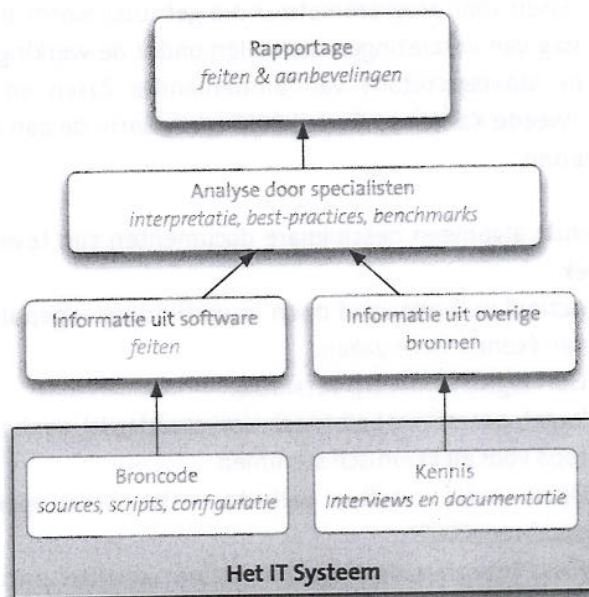
Het gehele onderzoek heeft betrekking op programma 4 en programma 5 van de OSV programmatuur. Aangezien de resultaten van dit onderzoek beschikbaar moeten zijn voor acceptatie van de verschillende delen van de programmatuur, zijn in totaal drie rapporten door de SIG geschreven, waarvan de eerste twee een beperkte scope hebben. Dit laatste rapport bevat alle resultaten van het onderzoek.

Titel rapport	Scope	Status
Toetsing eisen OSV 4 voor Europese verkiezingen	Toetsing eisen voor OSV 4 voor Europese verkiezingen	Verschenen op 18 mei 2009
Toetsing eisen OSV 5 voor Europese verkiezingen	Toetsing eisen voor OSV 5 voor Europese verkiezingen	Verschenen op 5 juni 2009
Toetsing eisen OSV 4 en 5 voor verkiezingen voor de Tweede Kamer, gemeenteraden, deelraden, Provinciale Staten en referenda	Toetsing eisen voor OSV 4 en 5 voor de overige verkiezingen: Tweede Kamer, gemeenteraden, deelraden, Provinciale Staten en referenda	Beschikbaar (is dit rapport)

2 Onderzoeksproces

2.1 Uitgangspunten

De SIG is gespecialiseerd in het uitvoeren van onderzoek naar kwaliteit van onderhoudbaarheid van programmatuur op basis van broncode-onderzoek. De basis van het onderzoek wordt daarom gevormd door de feiten verzameld door onderzoek van de aangeleverde broncode. Daarnaast is er aanvullende documentatie als bron gebruikt en zijn gesprekken gevoerd met medewerkers van de leverancier IVU ter verduidelijking. Op basis van de hieruit vastgestelde feiten is er een interpretatie gedaan door SIG medewerkers om te komen tot antwoorden op de onderzoeksvragen. Deze antwoorden zijn gemotiveerd vanuit de vastgestelde feiten. Deze werkwijze is schematisch weergegeven in Figuur 1.



Figuur 1: Opzet van een onderzoek naar software op basis van broncode. De SIG hanteert een werkwijze waarin eindconclusies gebaseerd zijn op vastgestelde feiten.

2.2 Bronnen

De volgende broncode is door de SIG ontvangen en gebruikt als basis voor dit onderzoek:

- Source code OSV 4 en 5, versie van 17 april 2009
- Test source code, versie van 17 april 2009
- Source code OSV 4 en 5, versie van 25 september 2009

Naast deze broncode heeft de SIG de volgende ondersteunende documentatie ontvangen ten behoeve van dit onderzoek:

- Gedetailleerde specificatie OSV 1.3.3, ontvangen op 17 april 2009
- Handleiding programma P4 v0.2, ontvangen op 17 april 2009
- Handleiding programma P5 v0.1, ontvangen op 17 april 2009
- Handleiding programma P4 v1.2, ontvangen op 23 september 2009

Tijdens het onderzoek zijn de volgende meetings gepland als vaste contact momenten als onderdeel van de onderzoeks aanpak. Naast deze sessies is er informeel contact geweest tussen de medewerkers van de SIG en IVU en met Mr. Koëter.

Datum	Meeting	Aanwezig
9 april 2009	Bespreking assessment - aanpak	E. Denert, R. Mulder, S. Eulitz, S. van Otterloo, Y. Kanellopoulos
16 april 2009	Technische sessie - uitleg OSV door IVU experts	S. Eulitz, D. Cosic, S. van Otterloo, Y. Kanellopoulos, J. Heijmans
28 april 2009	Bespreking formele methoden (telefonisch)	J. Nottebaum, S. van Otterloo, Y. Kanellopoulos, J. Heijmans
29 april 2009	Validatie sessie (telefonisch) - validatie van door de SIG vastgestelde technische feiten door IVU	S. Eulitz, D. Cosic, J. Nottebaum, S. van Otterloo, Y. Kanellopoulos, J. Heijmans
8 mei 2009	Eindpresentatie OSV 4 voor Europese verkiezingen	J. Schipper-Spanninga, R. Hoorweg, S. van Otterloo, M. Hissink Muller, J.H. van der Linden
2 juni 2009	Eindpresentatie OSV 5 voor Europese verkiezingen	J. Schipper-Spanninga, R. Hoorweg, T. Kuipers
7 oktober 2009	Bespreking resultaten toetsing OSV 4 en 5	J. Schipper-Spanninga, R. Hoorweg, S. van Otterloo

3.3 Eis 3: ontwerp

3.3.1 Eis en conclusie

Gestelde eis:

Het ontwerp van de programmatuur voldoet aan geaccepteerde kwaliteitseisen c.q. best practices voor de ontwikkeling van programmatuur. Daartoe:

- a. Is de programmatuur gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn.*
- b. Zijn kritische functies in de programmatuur gescheiden.*
- c. Zijn gegevens die aan verandering onderhevig zijn (configuratieparameters) zonder aanpassingen van programmatuur te wijzigen.*
- d. Wordt toevallig of opzettelijk foutief gebruik van de programmatuur, voor zover als redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen.*

Conclusie:

- Ja, er is voldaan aan de eis als geheel en de vier genoemde deel-eisen.

3.3.2 Motivatie 3a en 3b

Er is een duidelijke module-structuur, die zorgt voor een scheiding van bijvoorbeeld berekening uitslag, data-opslag en in- en uitvoer. Deze modulestructuur is weergegeven in de appendix. Hiermee wordt voldaan aan 3a en 3b.

3.3.3 Motivatie 3c

Door middel van een 'election definition file' kan het programma zonder aanpassingen voor een volgende verkiezing gebruikt worden. Door herinstallatie kan het programma in een andere rol of voor een andere regio gebruikt worden zonder aanpassingen aan de code. Hiermee is voldaan aan eis 3c.

3.3.4 Motivatie 3d

Er worden geen nieuwe risico's geïntroduceerd door gebruik van de programmatuur, omdat het programma niet van buiten toegankelijk is. De programmatuur zal gebruikt worden op een afgezonderde netwerkomgeving die geen verbinding met de buitenwereld heeft. Hiermee wordt misbruik van buitenaf uitgesloten. Programma P5 bevat geen invoerschermen die controles behoeven die onopzettelijk foutief gebruik tegengaan. Opzettelijk foutieve invoer door een stembureaumedewerker is ook zonder programmatuur mogelijk en kan redelijkerwijs technisch niet voorkomen worden.

3.3.5 Motivatie eis 3 als geheel

De hoofdtekst van eis 3 gaat verder dan de genoemde deel-eisen, omdat er ook in het algemeen gesproken wordt over geaccepteerde eisen. De SIG doet daarom een toetsing aan door de SIG gehanteerde kwaliteitseisen voor technische kwaliteit van programmatuur. De resultaten van deze toetsing staan in hoofdstuk 4. Het resultaat van deze toetsing is dat de programmatuur voldoende tot goed scoort op alle kwaliteitseisen en daarmee voldoet aan best practices.

- XSLT is een open standaard, waarvoor Xalan een open source interpreter is. Hiervoor is een actieve gemeenschap die te bereiken is via <http://xml.apache.org/xalan-j/>.

3.4.4 Motivatie 4c

- Het actieplan Nederland Open In Verbinding stelt op pagina 28: “Open source software is software die een door het open source initiative goedgekeurde licentie heeft en daarmee voldoet aan twee kenmerken: de broncode is vrij beschikbaar; in het licentiemodel is het intellectueel eigendom van de software en de bijbehorende broncode dusdanig geregeld dat de licentienemer de broncode mag inzien, gebruiken, verbeteren, aanvullen en distribueren.”
- De broncode is niet gepubliceerd onder een licentie die voldoet aan de geciteerde definitie van open source.
- De kern van de programma’s OSV 4 en OSV 5 is gebaseerd op een eerder voor een derde partij ontwikkeld programma, namelijk een programma ontwikkeld voor het Duitse overheidsorgaan Destatis. Destatis heeft het intellectueel eigendomsrecht op deze kern.
- Er zijn wel afspraken gemaakt met Destatis die de Kiesraad in staat stellen de programmatuur ter inzage te publiceren, te gebruiken en aan te passen. De Kiesraad heeft de broncode van de programmatuur op 5 juni gepubliceerd op zijn website ter inzage. Hiermee wordt aan het tweede deel van eis 4c voldaan.
- De kern van OSV 4 en 5 is niet specifiek voor de kiesraad ontwikkeld, en dus is het derde deel van eis 4c niet van toepassing.

3.5 Eis 5: verschillende besturingssystemen

3.5.1 Eis en conclusie

Gestelde eis:

De programmatuur is beschikbaar op verschillende systeemarchitecturen en verschillende besturingssystemen, waaronder in ieder geval gangbare open source besturingssystemen.

Conclusie:

- Ja, er is aan deze eis voldaan.

3.5.2 Motivatie

- Het programma is gebaseerd op het JBoss platform. JBoss is zelf gebaseerd op het Java-platform.
- De leverancier van JBoss geeft aan dat JBoss geschikt is voor alle besturingssystemen die een juiste versie van het Java-platform bieden en een standaard database-omgeving. Hieraan is voldaan voor onder andere Linux, Windows en Mac OS X.
 - Voor zowel Linux, Windows en Mac OS X is er een juiste versie van het Java-platform
 - Voor zowel Linux, Windows en Mac OS X is er een geschikte database

Conclusie:

- Ja, er is aan deze eis voldaan.

3.8.2 Motivatie

- Bij elke uitvoer van gegevens wordt een 'hashcode' berekend en weergegeven in een afdrukbaar document. Door dit afgedrukte document kan de authenticiteit bij inladen van gegevens worden gecontroleerd.
- Er wordt gebruik gemaakt van een cryptografisch sterk hash algoritme (SHA-1) dat voor 2009 voldoende veiligheid biedt. Als het in de toekomst nodig mocht blijken om dit algoritme te wijzigen kan dit door wijziging van één regel in de broncode.

In de appendix is een overzicht opgenomen van de opzet van de report generator module, waarin is weergegeven hoe een hashcode berekend wordt.

3.9 Eis 9: formele methodes

3.9.1 Eis en conclusie

Gestelde eis:

Met behulp van formele methoden is wiskundig aangetoond dat berekeningen in de programmatuur precies datgene doen wat door de wet- en regelgeving is voorgeschreven.

Conclusie:

- Nee, er is niet voldaan aan deze eis omdat het wiskundig document waarin de correctheid aangetoond wordt niet voldoende volledig is.

3.9.2 Motivatie

- Deze eis is van toepassing op het gedeelte van de broncode waarin de zetelverdeling bepaald wordt aan de hand van de getelde stemmen. De relevante regelgeving hiervoor is beschreven in hoofdstuk P van de Kieswet.
- Het wiskundig correct bewijzen van programmatuur is een zeer zware eis die alleen voor zeer kritieke en lastig wijzbare programmatuur gebruikelijk is, zoals bijvoorbeeld besturingsprogrammatuur van voertuigen. Voor overige toepassingen wordt door de meeste organisaties het documenteren en testen van programmatuur als afdoende beschouwd.
- Bij de invulling van deze eis heeft de leverancier niet gekozen voor een uit de literatuur bekende techniek, maar voor het valideren van de ontwikkelde broncode door middel van een wiskundige definitie in het document 'Determination of the Election Result'. Deze definitie is door de SIG beoordeeld.
- Bij deze controle is vastgesteld dat de definitie in bepaalde secties, aangegeven in de appendix, niet voldoende volledig is. Hierdoor is niet aan deze eis voldaan.
- De programmatuur is ruim gedocumenteerd door middel van het document 'Determination of the Election Result' en getest door de leverancier.

3.9.3.4 Opmerkingen en bevindingen deelvraag a

In de appendix is per subsectie aangegeven of er aan de deelvraag voldaan is en wat de opmerkingen zijn.

3.9.3.5 Opmerkingen en bevindingen deelvraag b

Van alle bestanden in het package 'de.ivu.wahl.result' is nagegaan of deze berekeningen bevatten. Voor de bestanden waarvoor dat geldt is nagegaan of deze bestanden genoemd zijn in de wiskundige omschrijving, en dat bleek het geval te zijn, met drie eenvoudig te maken aanvullingen. Hierdoor is gevalideerd dat de broncode geen berekeningen uitvoert die niet wiskundig zijn omschreven, en is aan deelvraag b voldaan.

3.9.3.6 Opmerkingen en bevindingen deelvraag c

In een aantal secties is er geen duidelijke relatie te leggen tussen de door de Kieswet gedefinieerde procedure en de wiskundige omschrijving. Bij verschillende secties is er namelijk geen linkerzijde, of zijn aan de linkerzijde teksten opgenomen die niet afkomstig zijn uit de Kieswet. Ook heeft de specificatie op een aantal punten meer het karakter van een informele omschrijving dan een formele specificatie. Hierdoor is deelvraag c niet positief te beantwoorden, en is niet aan de eis voldaan. In de tabel in de appendix zijn de per sectie de opmerkingen en bevindingen voor deelvraag c weergegeven.

3.10 Eis 10: onafhankelijke toetsing

3.10.1 Eis en conclusie

Gestelde eis:

De programmatuur wordt in opdracht van de centrale stembureaus door een of meer onafhankelijke instanties getoetst voordat de centrale stembureaus de programmatuur accepteren en gebruiken. De uitkomst(en) van de toets(en) zijn openbaar.

Conclusie:

- Ja er wordt aan deze eis voldaan door publicatie van de SIG rapporten, waaronder dit rapport.

3.10.2 Motivatie

- De SIG heeft deze toetsing onafhankelijk uitgevoerd.
- De eerste twee rapporten van de SIG zijn door de Kiesraad openbaar gemaakt via de Kiesraad website.
- Dit eindrapport mag door de Kiesraad openbaar gemaakt worden als resultaat van toetsing van OSV 4 en 5 voor alle soorten verkiezingen.

3.11 Eis 11: elektronisch stemmen

3.11.1 Eis en conclusie

Gestelde eis:

Voor zover nog verder van toepassing dient de programmatuur te voldoen aan de aanbevelingen van de Raad van Europa voor elektronisch stemmen.

4 Technische kwaliteit van OSV 4 en 5

In dit hoofdstuk wordt het eindoordeel ten aanzien van de technische kwaliteit van OSV 4 en 5 uiteengezet. Deze technische kwaliteit is van belang voor de onderhoudbaarheid van het systeem in de komende jaren.

4.1 Conclusie voor de technische kwaliteit

Op basis van verschillende relevante technische aspecten concludeert de SIG dat de onderhoudbaarheid van OSV 4 en 5 drie sterren is, op een vijf-niveau schaal van één ster tot vijf sterren, waarbij één ster staat voor zeer slecht en vijf sterren voor zeer goed.

De technische kwaliteit (onderhoudbaarheid) van OSV 4 en 5 is drie sterren.

Een score van drie sterren of hoger geeft aan dat het systeem de komende jaren onderhouden kan worden en daardoor toekomstvast is. Een score van drie sterren geeft aan dat dit kan gebeuren tegen marktgemiddelde inspanning.

4.2 Onderbouwing

Deze conclusie is gebaseerd op het model in Appendix B, dat de relatie toont tussen de verschillende ISO 9126 eigenschappen voor onderhoudbaarheid (*maintainability*) en de technische aspecten die SIG tijdens een Software Risk Assessment in beschouwing neemt.

	High-level architecture	Separation of concerns Modularisation	Complexity	Unit length	Duplication	Exception handling Volume	Unit-test quality	Assessment Process	
Rating	+	o	+	o	o	o	++	o	o
Analysability		X	X		X	X	X		X
Changeability	X		X	X		X		X	
Stability							X	X	X
Testability			X	X	X			X	

Figuur 2: Relatie tussen technische aspecten en ISO 9126 kwaliteitsattributen.

De beoordeling voor de vier eigenschappen van onderhoudbaarheid wordt afgeleid door de beoordeling voor de verschillende technische aspecten die van invloed zijn (zoals blijkt uit de kruisjes in de tabel) te middelen, waarbij de waarderingen vertaald zijn in scores van 1 (--) tot 5 (++)

Het eindoordeel voor de technische kwaliteit (onderhoudbaarheid) is het gemiddelde van de beoordelingen van de vier kwaliteitseigenschappen voor onderhoudbaarheid. De analyseerbaarheid van het systeem wordt net als 'goed' beoordeeld, de andere aspecten als Neutraal (drie sterren). Het totaaloordeel wordt hierdoor drie sterren.



Java ontwikkelde 'Jar signing'. Het gebruik van deze of een soortgelijke methode verhoogt het beveiligingsniveau.

Beveiligingsniveau van Java

Beveiligingsniveau	Beveiligingsniveau
1	1
2	2
3	3
4	4
5	5

De Java runtime wordt geïnstalleerd op de computer van de gebruiker. Het is belangrijk dat de gebruiker weet dat het softwarepakket van de aanbieder is en niet van een andere partij. Het is ook belangrijk dat de gebruiker weet dat het softwarepakket van de aanbieder is en niet van een andere partij.

Beveiligingsniveau van Java

Beveiligingsniveau	Beveiligingsniveau
1	1
2	2
3	3
4	4
5	5

Module/package	Functionaliteit	Locatie
Wahl.Eingang	Manual input of voting data in EML 150 format. Manual input of voting data. This part contains validity and plausibility checks.	P4, P5 specific code
Wahl.l18n	Functionality to show program in different languages.	Business layer
Wahl.mbean	Extension to JBoss for creating data base structure, and for making exported files available via the web browser.	mbean
Wahl.Modell	Persistence Functionality to store election data elements in the database.	Persistence
Wahl.result	Functionality of P5 to assign seats based on the voting data.	P4, P5 specific code
Wahl.runtime	Caching mechanism to store computed results to improve performance. It is not clear whether this is currently used, but may be needed in future.	Business layer
Wahl.util	Not used.	Business layer
Reportgenerator	Functionality to create EML files and PDF/RTF output.	Report generator
xmlsecurity	Code to determine how EML files are validated, including the choice for the SHA-1 hash function.	Business layer

A.3 Eis 2: documentatie

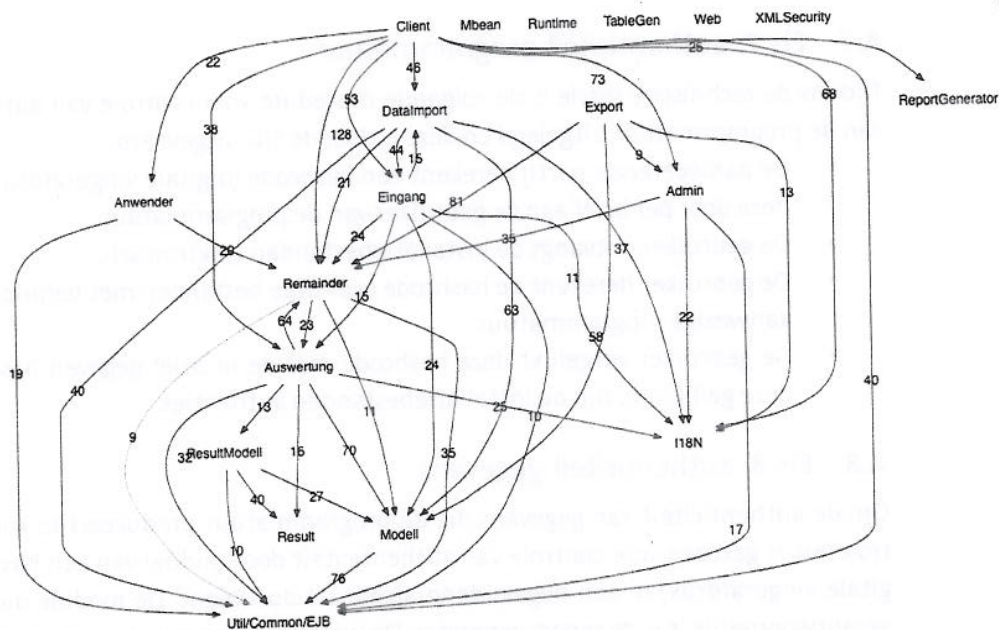
In de onderstaande tabellen is het resultaat weergegeven van de review van de gedetailleerde specificatie. De eerste tabel bevat eisen specifiek voor de functionaliteit van P4, de tweede tabel bevat specifieke eisen specifiek voor de functionaliteit van P5, de derde tabel bevat eisen over algemene functionaliteit die voor beide programma's gelden.

Eisen specifiek voor OSV 5

Section (page)	Summary	OK?	Remarks SIG
2.7 (61)	P5 determines the distribution of seats based on the votes.	Yes	Tested.
2.7.1 (61)	An administrator must prepare the application for use.	Yes	Tested.
2.7.2.1 (61)	Access restriction by ID/password. There are three kinds of use(r)s: administration, data entry and finalization of data.	Yes	All three uses were demonstrated and tested, but all with an administration user.
2.7.2.2 (62)	Description of what user interface looks like, the available menu items.	Yes	Demonstrated and tested, not verified if each button is present in the right situation.
2.7.2.3 (64)	The file with voting lists and candidates (including address data) can be uploaded by an administrator.	Yes	Tested.
2.7.2.4 (65)	Process description of input of election results by EML file. Validity of input file is verified by hash code. The user has to enter (part of) a hash code provided together with the EML file.	Yes	Tested.
2.7.2.5 (66)	The seat distribution is calculated in the manner described by the formal specification.	Yes	Tested.
2.7.2.6 (67)	In some situations, manual drawing of lots is required for the seat distribution.	Yes	Tested.
2.7.3 (67)	Relevant steps during seat distribution are logged.	Not observable	This cannot be verified in demonstration or user testing.
2.7.4. (67)	A <i>proces verbaal</i> can be generated after calculation of the seat distribution (in EML, PDF and/or RTF).	Yes	Tested, but not verified if the documents are of the specified subtypes and contain all described fields.
2.7.5 (68)	Voting results can be exported to a predefined location on disk.	Yes	Tested.
2.7.6 (69)	Inline help functionality is present.	Yes	Tested

A.4.2 Afhankelijkheden tussen modules

Door middel van broncode-analyse is vastgesteld wat de afhankelijkheden tussen deze modules zijn. Hiervoor is bepaald hoe vaak de code in een bepaalde module een aanroep doet van een code-eenheid in een andere module. Dit is weergegeven in Figuur 4.



Figuur 4: De module-structuur van OSV 4 en 5. De pijlen geven aanroepen vanuit de ene module naar de andere aan, met daarbij het aantal aanroepen. Pijlen met minder dan 8 aanroepen zijn weggelaten. Uit deze figuur blijkt dat er twee cyclische afhankelijkheden zijn: Dataimport en Eingang en Auswertung en Remainder.

Het valt op dat er op twee plaatsen wederzijdse afhankelijkheden zijn tussen modules: tussen Dataimport en Eingang en tussen Auswertung en Remainder. In een toelichting heeft de leverancier aangegeven dat Eingang en Data-import inderdaad verwant zijn, en dat deze modules samengevoegd worden of er naar een andere oplossing zal worden gekeken. De wederzijdse afhankelijkheid tussen Auswertung en Remainder kan worden opgelost door het verplaatsen van de class Gebietsinfo van Auswertung naar Remainder. Aanbevolen wordt om op deze punten de moduleverdeling te verbeteren. Na deze aanpassingen is het aantal afhankelijkheden dat tegen de architectuur in gaat relatief laag. Op basis hiervan kan gezegd worden dat de broncode bovengemiddeld scoort op het gebied van modulestructuur.

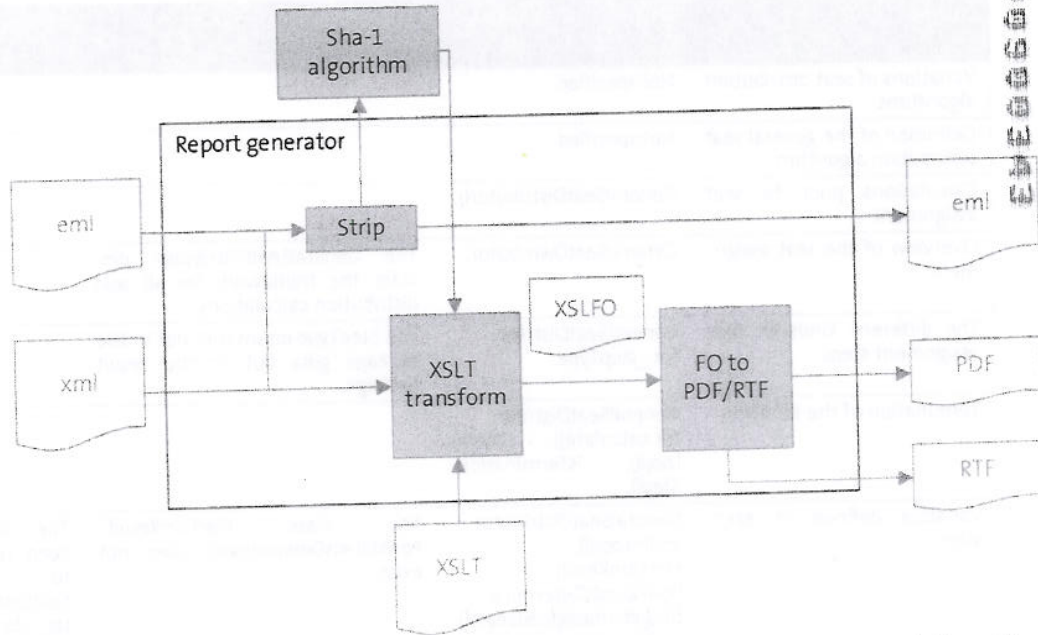
A.5 Eis 5: verschillende besturingssystemen

In de in Figuur 3 weergegeven architectuur is te zien dat de programmatuur gebaseerd is op het JBoss-platform dat weer gebaseerd is op het Java-platform.

A.6 Eis 6: diakritische tekens

In het logisch ontwerp versie 3.6 van het GBA wordt ook gesproken over het mogelijke gebruik van Unicode voor het weergeven van de voor het GBA gebruikte diakritische tekens.

Bij de uitwisseling van gegevens gebruikt de LRD Unicode en niet de manier van coderen die is beschreven in Bijlage II Teletex. Unicode wordt gebruikt omdat de



Figuur 5: Werking van de report generator. Aan de linkerkant komt uit te voeren informatie vanuit de programmatuur binnen. Verkiezingsdata is hierbij weergegeven in EML. Deze wordt rechts uitgevoerd in gestripte vorm. Tegelijkertijd wordt een begeleidend afdrukbaar document (PDF of RTF) gemaakt dat de hashcode van dit bestand bevat.

A.9 Eis 9: formele methodes

Voor eis 9 zijn voor dit rapport de volgende deelvragen beantwoord:

- Komen voor iedere subsectie de stappen in de aangegeven broncode overeen met de wiskundige omschrijving?
- Is elk bestand uit de broncode dat berekeningen bevat benoemd in het definitiedocument?
- Biedt voor elke subsectie de rechterhelft een goede wiskundige weergave van de Kieswettekst aan de linkerhelft?

A.9.1 Bevindingen deelvraag a: overeenkomst specificatie en broncode

In de volgende tabel is per subsectie aangegeven of er aan deelvraag a voldaan is. Op 5 punten is de leverancier gevraagd een toelichting te geven of het document te verbeteren. Na deze toelichting en correcties is er voor alle secties aan deze deelvraag voldaan.

	<code>cialBarrierNumerator() Elec- tion.getPreferencialBarri- erDenominator().</code>			
Characteristics of the elections to the house of representatives	Not specified.	There is an unclear note: "The number of electoral districts is not reflected in the source code."	The note was added to express that the number of district is not hardcoded. It will be re-phrased	Ok
Characteristics of the elections for the European Parliament	Not specified.	Same remarks as for section 3.1.1.	Same response as for section 3.1.1	Ok
Determination of total number of votes and calculation of the electoral quota	<code>VotesCounter.</code>			Ok
Determination of the number of candidates	<code>CandidatesCounter.</code>			Ok
Determination of the valid combined lists and their total number of votes	<code>CombinedListValidator.</code>			Ok
Assignment of seats to P4.2-lists	<code>ElectionResultDeterminator.assignSeatsToP42Lists()</code> .			Ok
Assignment of seats to P3-lists (within a P4.2-list)	<code>ElectionResultForP3ListsDeterminator.calculate() ElectionResultDeterminator.assignSeatsWithinP42Lists()</code> .	The implementation note for step 2 refers to <code>ElectionResultForP3ListsDeterminator.calculate()</code> – this method is really in its super class. The note for step 5 refers to <code>assignSeatsWithinP42Lists()</code> , yet <code>assignSeatsWithinP42List()</code> actually implements the mentioned behaviour, but is called from the former method.		Ok
Assignment of seats to P2-lists (within P3-lists)	<code>AbstractElectionResultDeterminator.assignSeatsToP2Lists() ElectionResultForP2ListsDeterminator.calculate()</code> .	The method mentioned in the 1a note (<code>assignSeatsToP2Lists()</code>) does not exist in the mentioned class. The <code>calculate()</code> method appears to implement the intended behaviour. The note for step 5 refers to <code>assignSeatsWithinP3Lists()</code> (with s), where <code>assignSeatsWithinP3List()</code> actually implements the mentioned behaviour.		Ok if correction is made
Preface on order relations	<code>OrderUtil.sortAndGroup()</code> .	According to API specification, Comparators should impose a total ordering, the section suggests non-total orderings can also be used with <code>OrderUtil</code> .		Ok
Nomination of candidates elected by preferential votes	<code>ElectionResultForCandidatesDeterminator()</code> .	Actual sorting occurs in step 7 and is not found in the implementation notes (it is found in <code>SortCandidatesUtil</code>). The method mentioned for step 10 does not exist, neither do the methods in <code>SeatDistributionInP3List</code> mentioned in the notes for step 15.	On remark one, the note will be corrected. On remark 2, a clarification will be added that this happens in the maps that are defined in the code	Ok
Nomination of all remaining candidates	<code>P2ListForRemainingSeatsDeterminator.calculate() handleLateListExhaustion()</code> .	Class name of mentioned method is omitted. <code>handleLateListExhaustion()</code> handles a case that "can never happen." This issue is discussed in 7.5.7, but there is no reference to that section.		Ok

File	Contains calculations	Result of deelvraag b	Remarks SIG
de.ivu.wahl.result.determination.Abstr actElectionResultDeterminator	Yes	Yes	
de.ivu.wahl.result.determination.Assig nmentTracer	Yes	Yes	
de.ivu.wahl.result.determination.Candi dateForSorting	Yes	Yes	
de.ivu.wahl.result.determination.Candi datesCounter	Yes	Yes	
de.ivu.wahl.result.determination.Comb inedListValidator	Yes	Yes	
de.ivu.wahl.result.determination.Electi onResultDeterminator	Yes	Yes	
de.ivu.wahl.result.determination.Electi onResultForCandidatesDeterminator	Yes	Yes	
de.ivu.wahl.result.determination.Multi pleElectedCandidate	Yes	Yes if corrections from deelvraag a are made	Not mentioned in docu- ment. Only MultipleElect- edCandidateHandler is mentioned.
de.ivu.wahl.result.determination.Multi pleElectedCandidateHandler	Yes	Yes	
de.ivu.wahl.result.determination.P2List ForPrioritySeatsDeterminator	Yes	Yes	
de.ivu.wahl.result.determination.P2List ForRemainingSeatsDeterminator	Yes	Yes	
de.ivu.wahl.result.determination.SortC andidatesUtil	Yes	Yes, if correction to document is made	Not mentioned in table 7.4.2, but in implementa- tion notes.
de.ivu.wahl.result.determination.Votes Counter	Yes	Yes	
de.ivu.wahl.result.gsda.GeneralSeatDist ributor	Yes	Yes	
de.ivu.wahl.result.gsda.PartlyRamdomIt erator	Yes	Yes, if correction to document is made	Not mentioned in table 7.4.2, but in implementa- tion notes.

Tabel 2: Resultaat van validatie van deelvraag b voor eis 9. Alle broncode bestanden die bere- keningen bevatten zijn weergegeven. Per bestand is nagegaan of deze omschreven in het document met de wiskundige specificatie.

A.9.3 Bevindingen deelvraag c: juistheid vertaling Kieswet in specificatie

In een aantal secties is er geen duidelijke relatie te leggen tussen de door de Kieswet gedefinieerde procedure en de wiskundige omschrijving. Bij verschillende secties is er namelijk geen linkerzijde, of zijn aan de linkerzijde teksten opgenomen die niet afkomstig zijn uit de Kieswet. In de eerste onderstaande tabel zijn de secties weergegeven waarvoor nog verduidelijking van de brontekst (de linkerzijde) nodig is. De overige sec- ties voldoen wel aan deelvraag c.

Proces	Het team gebruikt een ge-automatiseerd proces voor het bouwen van de programmatuur. Er wordt gebruik gemaakt van standaard tools and Eclipse en ANT. Het ontwikkelproces is als <i>Neutraal</i> beoordeeld.
--------	---

Tabel 3: Overzicht van kwaliteitsaspecten.

B.1.4 Complexity

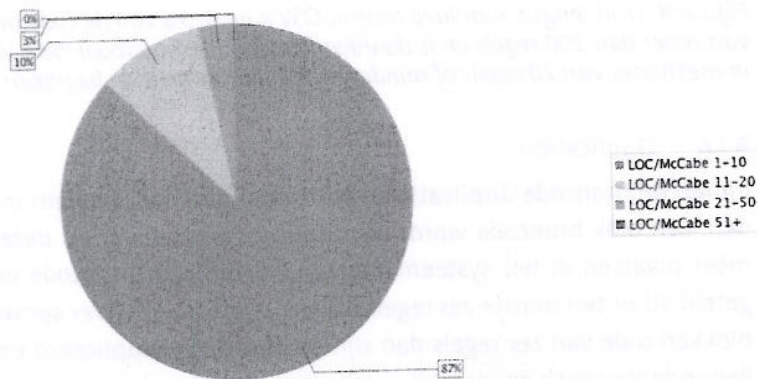
Om de complexiteit van broncode van een systeem te bepalen gebruikt SIG de Cyclomatische Complexiteit van McCabe, een technologieonafhankelijke metriek die in 1976 gedefinieerd is door T. McCabe.

De McCabe-waarde telt het kleinste aantal individuele executiepaden door de kleinste eenheid van broncode. Voor Java is dit een methode. Hoe hoger de McCabe-waarde, des te lastiger de code is te begrijpen.

Om complexiteitsniveaus te benoemen en geassocieerd risico te bepalen wordt gebruik gemaakt van de volgende classificatie van het Software Engineering Institute (SEI) van Carnegie Mellon University.

McCabe-waarde	Risico
1-10	Makkelijk te begrijpen, laag risico
11-20	Complex, medium risico
21-50	Zeer complex, hoog risico
>> 50	Ontestbare code, zeer hoog risico

Tabel 4: Classificatie van McCabe-waarden en bijbehorende risico's.

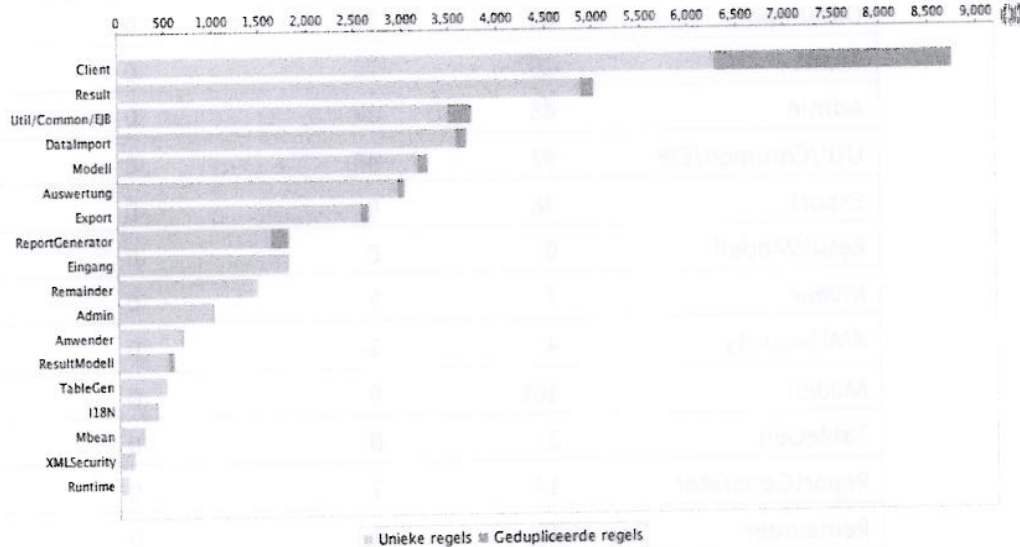


Figuur 7: Complexiteit van de Java code in OSV 4 en 5. Het merendeel, 87%, van de code bevindt zich in de laagste risicocategorie en daardoor goed begrijpelijk en testbaar. Er is geen code aangetroffen die praktisch ontestbaar is.

B.1.5 Unit lengte

De lengte van eenheden van code is een maat voor de begrijpbaarheid. Hoe langer een eenheid, des te moeilijker deze is te begrijpen. Om de lengte van eenheden te classificeren wordt gebruik gemaakt van de volgende tabel.

In Tabel 6 is de duplicatie per technologie aangegeven. De duplicatie van Java, de technologie met het meeste volume, is in lijn met wat men van een neutraal onderhoudbaar systeem kan verwachten. De duplicatie voor Javascript, JSP en XSLT is erg hoog waardoor deze technologieën moeilijker onderhoudbaar zijn.



Figuur 9: Duplicatie per module in Java. De meeste geduplicateerde code komt voor in de client module, waar op sommige plaatsen gekozen is voor duplicatie in plaats van ontwikkeling van generieke methodes. De andere modules hebben zeer weinig duplicatie wat goed is voor de onderhoudbaarheid.

B.1.7 Exception handling

Ieder softwaresysteem kan tijdens de operatie onverwachte situaties tegenkomen, bijv. tijdens het niet kunnen toewijzen van geheugen of bij een falende poging om een tekst file van het filesysteem in te lezen. Om dergelijke situaties op correcte wijze af te handelen kent software 'foutafhandelingsconstructies' zodat er een fout aan de eindgebruiker getoond kan worden en er bijv. een omschrijving van de foutsituatie in een error-log geschreven kan worden.

Het juiste gebruik van foutafhandelingsconstructies is een indicatie van de professionaliteit van het ontwikkelteam. Het mechanisme stelt het beheerteam in staat om te analyseren welke uitzonderlijke situatie opgetreden is, zodat de fout in de toekomst mogelijk voorkomen kan worden. Een juist gebruik van foutafhandelingsconstructies verhoogt de betrouwbaarheid van het systeem.

In het systeem zijn geen 'empty exceptions' aangetroffen. Dit betekent dat opgetreden fouten nergens genegeerd worden. Wel zijn er 205 'too general exceptions' aangetroffen. Op deze plaatsen wordt niet aangegeven wat voor exceptie afgehandeld wordt en wordt daarom mogelijk een te generieke actie gedaan. Aanbevolen wordt om als code met een 'too general exception' aangepast wordt, deze foutafhandeling te verbeteren. De hoeveelheid aangetroffen constructies van foutafhandeling is weergegeven in Tabel 7.



C. Disclaimer

Alle conclusies in dit rapport zijn gebaseerd op een *best effort* analyse. De analyse is in een beperkte tijd uitgevoerd. De Software Improvement Group kan niet garanderen dat de interpretatie van de bevindingen in dit rapport foutloos is. Het is mogelijk dat verdere gesprekken met de onderhoudsmedewerkers van de systemen alsmede een verdere analyse van de broncode, tot een andere interpretatie van de bevindingen dan die in dit rapport is beschreven kunnen leiden.