DOCUMENT CONTROL SHEET

	ORIGINATOR'S REF.		SECURITY CLASS.
	TP 96019 U		Unclassified

ORIGINATOR
National Aerospace Laboratory NLR, Amsterdam, The Netherlands

TITLE
Het ontwikkelen van bedrijfszekere avionica

PRESENTED AT
de themadag "Kwaliteit in de tijd, het ontwikkelen van bedrijfszekere elektronica", georganiseerd door het Centrum voor Micro-Elektronica, Ede, 30 november 1995.

AUTHORS	DATE	pp	ref
L.J. Aartman	960109	20	10

DESCRIPTORS

Avionics
Computer aided design
Electronic equipment tests
Environmental tests
Product development
Quality control
Software reliability
Software engineering

ABSTRACT
Elektronica is niet weg te denken uit de moderne lucht- en ruimtevaart. Er worden zeer hoge eisen getseld aan avionica systemen met betrekking tot functionaliteit, veiligheid, bedrijfszekerheid, testbaarheid en onderhoudsaspekten.
Tijdens het gefaseerde ontwikkeltraject worden methoden, technieken en procedures toegepast om aantoonbaar te kunnen voldoen aan de gestelde eisen. Dit is van belang voor de kwalificatie en eventuele certificatie van systemen.

NLR TECHNISCHE PUBLIKATIE

TP 96019 U

HET ONTWIKKELEN VAN BEDRIJFSZEKERE AVIONICA

door

L.J. Aartman

Dit rapport is een bijdrage aan de themadag "Kwaliteit in de tijd, het ontwikkelen van bedrijfszekere elektronica", georganiseerd door het Centrum voor Micro-Elektronica, Ede, 30 november 1995.

(H)afdeling : Elektronica en Informatie
Opgesteld : LJA/ 10/1/96
Goedgekeurd : HS/ 11/1/96

Afgesloten : 960109
Ordernummer : 082.022
Typ. : LJA/MM

Samenvatting

Elektronica is niet weg te denken uit de moderne lucht- en ruimtevaart. Er worden zeer hoge eisen gesteld aan avionica systemen met betrekking tot functionaliteit, veiligheid, bedrijfszekerheid, testbaarheid en onderhoudsaspekten.
Tijdens het gefaseerde ontwikkeltraject worden methoden, technieken en procedures toegepast om aantoonbaar te kunnen voldoen aan de gestelde eisen. Dit is van belang voor de kwalificatie en eventuele certificatie van systemen.

Inhoudsopgave

(20 pagina's totaal)

Lijst van afkortingen en acroniemen

CAE	Computer Aided Engineering
CASE	Computer Aided Software Engineering
CDR	Critical Design Review
DRL	Data Requirements List
ESS	Environmental Stress Screening
FMECA	Failure Mode Effect and Criticality Analysis
FMEA	Failure Mode Effect Analysis
HDBK	Handbook
ILS	Integrated Logistics Support
M/T	Maintainability/Testability
MTBF	Mean Time Between Failures
PDR	Preliminary Design Review
QR	Qualification review
R/M	Reliability/Maintainability
ROM	Read Only Memory
RTCA	Radio Technical Commission for Aeronautics

Deze pagina is opzettelijk blanco.

1 Inleiding

Ieder modern vliegtuig of ruimtevaartuig bevat veel elektronica. Het betreft niet alleen communicatie- en navigatiesystemen nodig voor de besturing (avionica), maar ook systemen voor observatie van de aarde of van de sterren.
Het succes van een missie kan daarmee in hoge mate afhangen van het succesvol functioneren van deze elektronica.
In de ruimtevaart gaan meestal jaren van ontwikkeling en test vooraf aan de werkelijke missie, die in het geval van bemande missies naar verhouding vaak van korte duur is (soms slechts enkele dagen). Voor satellieten die jaren in hun baan blijven is behalve de bedrijfszekerheid, ook de zelf-repareerbaarheid van belang.
In de luchtvaart worden dagelijks vele duizenden passagiers vervoerd met 'Fly-by-wire' toestellen als de Airbus A320, die voor de besturing direct afhankelijk is van computers en elektronica.
Omdat de bedrijfszekerheid van deze elektronische systemen van groot belang is, dient hieraan al tijdens het ontwikkeltraject aandacht besteed te worden.
In de volgende paragrafen wordt in het bijzonder ingegaan op de wijze waarop de bedrijfszekerheid van een produkt tijdens het gefaseerde ontwikkelproces bepaald wordt, en welke methoden en technieken hierbij gehanteerd worden. Een belangrijke leidraad hierbij uit de militaire sector zijn de handboeken MIL-HDBK-217 'Reliability Prediction of Electronic Equipment' (Ref. 1) en MIL-HDBK-338 'Electronic Reliability Design Handbook' (Ref. 2).
Door het hanteren van MIL-HDBK-217 is het mogelijk een getalswaarde toe te kennen aan de bedrijfszekerheid van elektronica. Hoewel niet altijd de absolute waarde betrouwbaar is, kan met deze methode wel worden nagegaan wat het effect is van bepaalde ontwerpmaatregelen. Ook wordt deze methode voorgeschreven en gehanteerd om in het voortraject de bedrijfszekerheid van elektronica van verschillende leveranciers met elkaar te kunnen vergelijken.

Daar avionica veelal uit hardware, software en firmware componenten bestaat, zal ook ingegaan worden op de bedrijfszekerheid van deze firmware en software. Tenslotte wordt het belang van computerondersteuning bij het ontwikkelen van bedrijfszekere avionica in relatie tot 'concurrent engineering' geschetst.

2 Het opstellen van eisen

Behalve over de functionaliteit wordt vooraf ook nagedacht over de bedrijfszekerheid- en beschikbaarheidseisen die aan een systeem gesteld worden.
Het opstellen van specificaties voor kritische elektronische systemen is op zich al een complex proces dat niet mag worden onderschat. De opdrachtgever wil vaak het 'onderste uit de kan' en heeft niet zelden met elkaar in strijd zijnde eisen en wensen. Naast functionele eisen zijn er de zogenaamde prestatie-eisen: bedrijfszekerheid ('reliability'), onderhoudbaarheid ('maintainability'), testbaarheid ('testability') en veiligheid ('safety'). Verder kunnen er beperkingen zijn aan de kostprijs van het produkt, het volume, de massa en het te consumeren en te dissiperen elektrisch vermogen. In de lucht- en ruimtevaart spelen daarnaast de vaak extreme omgevingscondities waaraan de systemen blootgesteld worden een prominente rol, zoals extreme temperaturen, trillingen en schokken, lage druk, luchtvochtigheid, maar ook kosmische straling en elektromagnetische straling zijn van belang. Al deze 'stressors' kunnen het functioneren in negatieve zin beïnvloeden, waardoor er tijdens de ontwikkeling beschermende maatregelen in het ontwerp moeten worden opgenomen. Een gedetailleerde specificatie van de omgeving waarbinnen het systeem moet kunnen functioneren vormt een essentieel onderdeel van de totale systeemspecificatie.

In bijvoorbeeld een militair operationele omgeving zijn de 'life-cycle' kosten van groot belang. De operationele kosten overstijgen niet zelden de initiële aanschafkosten. Veel produkteigenschappen zijn een parameter bij de bepaling van de life-cycle kosten, maar de bedrijfszekerheid, de repareerbaarheid (aspect van onderhoudbaarheid) en de produktprijs zijn hierbij maatgevend.

Onderstaand voorbeeld illustreert de specificatie van de bedrijfszekerheid:
de opdrachtgever eist dat de te ontwikkelen functie niet vaker dan 1 op 10.000 missies mag mislukken, waardoor de bedrijfszekerheid op 0.9999 gesteld wordt. Als de duur van de missie 8 uur is, dan wordt een Mean Time Between Failure (MTBF) vereist van 80.000 uur.
Dit betekent dat de MTBF van de afzonderlijke componenten waaruit het systeem is opgebouwd, hiervan een veelvoud zal moeten zijn.

Om te voorkomen dat ontwikkelende instanties al te makkelijk de kritische eisen zullen accepteren, worden er soms boetes opgelegd door de opdrachtgevers, wanneer de uiteindelijke produktspecificaties significant van de eisen afwijken. Bekende voorbeelden hiervan uit de luchtvaart zijn de massa en de bedrijfszekerheid. Deze boete clausules worden contractueel vastgelegd.

3 De levenscyclus van een produkt

Een ontwikkeling vormt slechts een onderdeel van de levenscyclus van een avionica-produkt of een systeem. Veel bedrijven maken gebruik van een produkt- of systeemlevenscyclusmodel (Ref. 2, 3, 4), met een aantal helder gedefinieerde fasen en goed omschreven overgangen tussen de opvolgende fasen. Globaal kunnen de volgende fasen met daarbij de belangrijkste activiteiten worden onderscheiden:

Fase	Activiteiten
Vooronderzoek Acquisitie	Definitie systeem/missie eisen Haalbaarheidsonderzoek Voorontwerp
Ontwikkeling	Opstellen en analyseren van de eisen Ontwerp prototype fabricage en test integratie en test kwalificatie certificatie
Operationele fase	Serieproduktie Installatie Onderhoud

Voordat de overgang naar een volgende fase kan plaatsvinden worden er reviews gehouden. Het doel van een review is om formele instemming van de opdrachtgever te verkrijgen inzake eerder gemaakte ontwerpbeslissingen. Daartoe is het van belang dat de resultaten van de uitgevoerde activiteiten (zoals specificatie, ontwerp en test) in documenten worden vastgelegd.
Op de operationele fase zal hier niet nader worden ingegaan.

3.1 Het vooronderzoek

Voordat een ontwikkelingsproject kan starten, zal er tijdens de acquisitie sprake moeten zijn van het zorgvuldig beoordelen van de eisen, waardoor een goed beeld ontstaat van de gevraagde eigenschappen en van de kosten die gemoeid zijn om deze eigenschappen van het produkt te realiseren.
Daarom wordt vaak een voorontwerp gemaakt, waarmee de vinger op de zere wonde gelegd wordt, door de maatgevende en kritische eisen vast te stellen. Kritische vragen als 'kan dit complexe produkt dat onder deze omstandigheden feilloos moet werken wel voor dit bedrag worden gebouwd?' moeten in deze fase worden gesteld en beantwoord.

Wanneer de bedrijfszekerheidseisen van belang zijn wordt in dit stadium meestal een eenvoudige

analyse van de bedrijfszekerheid uitgevoerd volgens de zogenaamde 'Parts Count Analysis' methode volgens MIL-HDBK-217, waarbij een globale waarde voor de bedrijfszekerheid van het produkt wordt geschat onder gegeven omstandigheden.
Reeds in dit stadium zullen er oplossingen bedacht worden waarmee de eisen van de klant gehaald kunnen worden.

Door het opstellen van een voorontwerp moet zowel de ontwerper als de opdrachtgever het gevoel krijgen dat de bedrijfszekerheidseisen haalbaar zijn. Dit kan bereikt worden door bijvoorbeeld:

- vereenvoudiging van het ontwerp;
- toepassing van (vaak dure) standaard gekwalificeerde componenten;
- adequate maatregelen te nemen om de stress in en op systeemcomponenten te beperken, door bijvoorbeeld de dissipatie te beperken of door een effectief thermisch ontwerp;
- redundantie toe te passen.

Technieken als redundantie en zelfrepareerbaarheid worden bijvoorbeeld toegepast voor satellieten waaraan zeer hoge MTBF waarden worden toegekend, omdat ze jaren dienst moeten doen en moeilijk of niet te repareren zijn.

Wanneer na een zorgvuldig uitgevoerd voorontwerp één en ander nog steeds niet haalbaar lijkt, zal een alternatief aan de opdrachtgever worden aangeboden: 'een lagere bedrijfszekerheid' of 'een hogere prijs'. Een opdrachtgever zal eerder geneigd zijn hierin mee te gaan wanneer de problematiek helder en degelijke onderbouwd wordt, met een reproduceerbare analyse als basis. Daarom wordt een voorontwerp vaak in een document vastgelegd en aan de opdrachtgever als onderdeel van het projectvoorstel overhandigd.

Vervolgens moet een beeld van de ontwikkelkosten worden verkregen. Hiervoor is het noodzakelijk dat de te nemen stappen geïdentificeerd worden, en dat een beeld gevormd wordt van de inspanning die met de ontwikkeling gemoeid is. De kwaliteit van het ontwikkelproces is vooral van belang wanneer er sprake is van software of firmware componenten in de avionica.

In een ontwikkeltraject als dat van avionica zal vooral aandacht besteed moeten worden aan het bewijs dat het produkt aan alle eisen die eraan gesteld worden, voldoet. De formele kwalificatie, vaak nodig voor de certificatie is een kostbare en tijdrovende activiteit. Iedere eigenschap zal geverifieerd moeten worden tegen de gestelde eis, door middel van inspectie, test, analyse, demonstratie of op basis van gelijkheid met reeds eerder ontwikkelde systemen. Voor het bepalen van de ontwikkelkosten, zal reeds in het offerte stadium bekend moeten zijn welke eisen op welke manier geverifieerd gaan worden.

Opdrachtgevers van avionica zijn vaak 'lastige klanten': ze willen niet alleen vooraf al van alles weten, maar ook blijven ze vaak nauw bij de ontwikkeling betrokken, om het ontwikkelproces te kunnen beoordelen en om het desgewenst te kunnen bijsturen. Daartoe is een vertegenwoordiger van de opdrachtgever vooral bij reviews en voortgangsbesprekingen aanwezig.

Vooraf wordt vastgesteld in welke documenten ('data') de resultaten worden vastgelegd. In een 'Data Requirements List (DRL)' worden de documenten en inlever criteria (meestal in relatie tot een fase overgang) door de opdrachtgever aangegeven.
Een voorbeeld van een DRL is hieronder gegeven:

Equipment :
Purchase company :
Supplier :

No Item	Item	CRIT	PDR	CDR	QR	COMMENTS
7 RELIABILITY						
7.1	reliability plan	A	-	-	-	1 month after EDC
7.2	component part list	R	-	X	X	3 months before CDR
7.4	reliability prediction report	R	X	X	X	2 months before PDR/CDR, update at QR
7.5	reliability critical item list	R	X	X	X	2 months before PDR, update at CDR/QR, info upon request
7.6	FMECA (including signal/function list)	R	X	X	X	3 months before PDR/CDR, update at QR
7.8	Reliability status report	I	-	-	-	included in quarterly program progress report after PDR

PDR = Preliminary Design Review
CDR = Critical Design Review
QR = Qualification Review

Het ontwikkeltraject dat zal worden doorlopen wordt vooraf zorgvuldig beschreven in plannen, zoals project of program management plannen en (systeem, hardware en software) ontwikkelplannen. Ook voor de andere disciplines (niet 'management' en 'engineering') worden plannen opgesteld, waardoor binnen een complex project ook aparte plannen bestaan voor kwalificatie (en eventueel certificatie), bedrijfszekerheid, testbaarheid, onderhoudbaarheid, veiligheid en Integrated Logistic Support (ILS).

Een bedrijfszekerheidsplan, ook wel 'reliability program plan' of 'Reliability/Maintainability (R/M) Program Plan' genoemd, wordt evenals het voorontwerp aan de opdrachtgever als onderdeel van het projectvoorstel overhandigd [2]. Dit document bevat een beschrijving van de organisatie, de uit te voeren taken en de wijze waarop de documenten op het gebied van bedrijfszekerheid tot stand zullen komen.

Een voorbeeld van een inhoudsopgave van een (engelstalig) plan (Ref. 2) is hierna gegeven.

Reliability program plan	
1	GENERAL
1.1	Introduction
1.1.1	Scope
1.1.2	Purpose
1.2	Reference documents
1.2.1	Military standards
1.2.2	Other standards
1.3	List of documents to be delivered by the supplier
2	MANAGEMENT
2.1	Company/consortium organisation
2.2	Reliability Organisation
2.3	Tools and Resources
2.4	Lines of Communication
3	RELIABILITY PROGRAMME
3.1	Reliability Programme Control Tasks
3.1.1	Updating of the Reliability plan
3.1.2	Production of a Component Partlist
3.1.3	Production of a FMECA
3.1.4	Production of a Reliability Prediction Report
3.1.5	Maintenance of the Reliability Critical Item list
3.1.6	Informal reliability monitoring
3.2	Reliability Assessment and Analysis
3.3	Verification Tests
3.4	Reliability programme timeline
4	RELIABILITY METHODOLOGY COMPLIANCE MATRIX

3.2 De ontwikkeling

Na soms uitgebreide en langdurige contractonderhandelingen kan de feitelijke ontwikkeling starten. Binnen de lucht- en ruimtevaart zijn harde tijdschema's aan de orde van de dag, de passage van de komeet Halley kan niet worden uitgesteld en de vervanging van operationele systemen (vliegtuigen of helikopters) kan dringend zijn in verband met aflopend onderhoud.

Om de ontwikkelkosten en -tijd te beperken is het onvermijdelijk dat veel van de ontwikkelactiviteiten niet na elkaar, maar parallel worden uitgevoerd door een ontwikkelteam. Dit proces wordt ook wel 'concurrent engineering' genoemd, waarbij na een zorgvuldig uitgevoerd vooronderzoek, goed bekend is wat er gelijktijdig kan worden uitgevoerd. Uitwisseling van gegevens tussen de verschillende disciplines (systeem, software, hardware, mechanica etc) is alleen mogelijk wanneer de plannen en de interfaces tussen de componenten zorgvuldig op elkaar zijn afgestemd en wanneer het ontwikkelteam ervaren is en goed geleid wordt. Om het overzicht te behouden en om het ontwikkelproces te kunnen sturen wordt de ontwikkeling zelf ook weer gefaseerd uitgevoerd.

3.2.1 'Preliminary design'

De formele ontwerpactiviteiten starten met het voorlopig ontwerp ('preliminary design'), waarin het conceptontwerp zijn vorm krijgt. De systeemarchitectuur wordt vastgelegd, verschillende oplossingen worden naast elkaar gezet en de meest geschikte oplossing wordt gekozen. Dit is de fase waarin de belangrijke en maatgevende ontwerpbeslissingen genomen worden, voordat het detail ontwerp wordt uitgevoerd.

In het algemeen wordt de bedrijfszekerheid tijdens de preliminary design fase bepaald met de Parts Count Analyse (PCA), waarin voor een gegeven omgevingsconditie met een gemiddelde stress gerekend wordt. Verder wordt aandacht besteed aan bescherming tegen de omgevingscondities zoals temperatuur, druk etc. die het functioneren van de avionica nadelig kunnen beïnvloeden.
Om de veiligheidseisen, die aan het ontwerp gesteld worden, te kunnen aantonen, wordt een Fault Tree Analyse (FTA) en Failure Mode Effect Analyse (FMEA) uitgevoerd. Met FTA wordt van een hiërarchisch systeemontwerp bepaald, welke kritische fouten op een hoger niveau, veroorzaakt kunnen worden als gevolg van falende delen op een lager niveau. FTA werkt 'top-down' waarbij het effect van het falen van het systeem binnen zijn omgeving als uitgangspunt genomen wordt. FMEA is een soortgelijke analyse, die vanaf het laagste niveau ('bottom-up') met het ontwerp als basis wordt uitgevoerd.
In beide gevallen is het van belang om het systeem vroegtijdig in functionele blokken op te delen met duidelijke interfaces (signalen). Een éénduidige naamgeving van de functies en signalen in het systeem draagt bij aan verbeteren van de communicatie met de opdrachtgever en binnen het ontwerpteam.

De preliminary design fase wordt formeel afgesloten met een 'Preliminary Design Review (PDR)', waarin ook de bedrijfszekerheid aan de orde komt.
De reviewer ontvangt tijdig de documenten waarin de resultaten van de voorlopige bedrijfszekerheidsanalyse zijn opgenomen. De reviewer heeft de volgende taken:

Nr.	Taakomschrijving
1	vergelijk de voorlopige voorspellingen met de eisen
2	controleer de gehanteerde methode
3	beoordeel de maatregelen die in het ontwerp zijn genomen om aan de bedrijfszekerheidseisen te voldoen
4	beoordeel de toepassing van redundantie
5	beoordeel kritische signaalpaden en stel vast of het 'fail-safe/fail-soft' ontwerpprincipe gehanteerd wordt
6	stel vast of de ontwerpregels ten aanzien van de bedrijfszekerheid bekend zijn. Denk aan elektrische en thermische derating.
7	stel vast of de activiteiten conform het plan zijn uitgevoerd.

3.2.2 'Critical design'

De ontwerpactiviteiten worden afgerond in de 'critical design' of detailontwerp-fase, waarna een prototype van het systeem wordt gebouwd en getest. Nu het volledige functionele en technische ontwerp bekend is, kan in detail de bedrijfszekerheid worden bepaald, waarbij met de stress van de afzonderlijke componenten rekening gehouden wordt. Hierdoor kan ook een definitieve FMEA worden uitgevoerd: de kans dat een gegeven 'failure effect' zich voordoet, als gevolg van een falend component, kan worden bepaald.
In het algemeen wordt de bedrijfszekerheid tijdens de critical design fase bepaald met de Parts Stress Analyse (PSA) (Ref. 2).

Deze fase wordt afgesloten met een Critical Design Review (CDR).
Tijdens deze review worden ook aspecten van bedrijfszekerheid van het produkt getoetst. Dit kan plaatsvinden aan de hand van een checklist.

Nr.	Design review checklist
1	Is het ontwerp eenvoudig? Is het aantal onderdelen geminimaliseerd, zonder dat de funktionele eigenschappen zijn aangetast?
2	Op welke wijze is er bij het ontwerp rekening gehouden met de omstandigheden waaronder het systeem moet functioneren? (Voorkom resonanties door goede trillingsisolatie en bescherm de apparatuur tegen schokken, vocht, corrosie etc.
3	Zijn er voldoende mogelijkheden om kritische functies te verifiëren?
4	Worden de bedrijfszekerheidseisen gehaald?
5	Worden er hi-rel onderdelen toegepast? Wat zijn de selectie criteria geweest voor de onderdelen? Zijn er onderdelen waarvan de bedrijfszekerheid (kritisch) laag is? Zijn er standaard onderdelen toegepast of onderdelen waarvan de technologie nog in de kinderschoenen staat?
6	Is er een thermische analyse uitgevoerd? Welke thermische ontwerp maatregelen zijn er genomen? (Houdt de component temperatuur laag d.m.v. warmte-afvoer door 'heat-sinks', speciale plaatsing van de onderdelen en indien noodzakelijk geforceerde koeling). Is er een stress analyse uitgevoerd? Zijn er derating factoren op de afzonderlijke onderdelen toegepast, waardoor de 'failure rate' verlaagd wordt en de levensduur verlengd?
7	Is er een worst-case analyse uitgevoerd? (Denk hierbij ook aan timing in digitale schakelingen).
8	Zijn er waar mogelijk solid-state onderdelen toegepast? (Mechanisch schakelende onderdelen zijn immers onderhevig aan slijtage).
9	Zijn er onderdelen toegepast die uit een 'batch' geselecteerd moeten worden?
10	Is er redundantie toegepast om de bedrijfszekerheid te verhogen?
11	Zijn de resultaten van de FME(C)A teruggekoppeld naar het ontwerp?

Uitgebreidere checklijsten zijn te vinden in MIL-HDBK-338 (Ref. 2).

3.2.3 Test en kwalificatie

In de testfase wordt vastgesteld in hoeverre het gerealiseerde produkt aan de ontwerpeisen voldoet, hoewel het reeds tijdens het ontwerp nuttig kan zijn om op het prototype of op delen daarvan, verificaties door middel van test uit te voeren.

De avionica die firmware of software bevat dient zorgvuldig getest te worden. Het aantal gevonden fouten en de mate waarin dit aantal tijdens het verloop van het testen afneemt, is in

het algemeen een maat voor de kwaliteit van de ontwikkelde software. Een groot aantal fouten kan duiden op een slechte implementatie, maar ook op een onduidelijke of onvolledige specificatie.

Fouten in de assemblage of zwakke onderdelen komen tijdens een burn-in vaak aan het licht. In kritische toepassingen gaat men vaak nog verder en wordt er een Environmental Stress Screening (ESS) uitgevoerd, waarbij het systeem zowel aan thermische, mechanische als elektrische stress wordt blootgesteld.

Voor de luchtvaart zijn diverse omgevingstestcondities en procedures vastgelegd in RTCA DO-160. Uiteraard worden alleen die testen uitgevoerd waarvoor eisen zijn geformuleerd.
Het testen kan onderdeel uitmaken van het kwalificatieproces, waarmee het gerealiseerde systeem getoetst wordt aan de oorspronkelijk gestelde eisen. Niet altijd behoeft een test te worden uitgevoerd. Kwalificatie door ontwerp, analyse of inspectie of op basis van eerder gekwalificeerde systemen behoort tot de mogelijkheden.

Indien het systeem gecertificeerd moet worden, worden de kwalificatieplannen, -procedures en rapporten door de certificerende instantie beoordeeld.

4 Bedrijfszekerheid van software

Naast hardware componenten bevat avionica veelal ook software of firmware componenten. Firmware is een categorie software die in hardware (Read Only Memory ROM) is vastgelegd en daardoor niet kan worden gewijzigd. Voor het ontwerpen van firmware wordt de software-ontwerpmethodiek toegepast (Ref. 3).

Het testen van software kost in het algemeen meer tijd dan het testen van hardware. Door de complexiteit van software is ook de dekkingsgraad van de uitgevoerde testen lager dan bij hardware. Niet alle 'paden' worden getest. Verder is een kwantitatieve bedrijfszekerheidsanalyse van software, op basis van bijvoorbeeld correctheidsbewijzen, voor de gemiddelde programmeur nog steeds moeilijk uitvoerbaar (Ref. 6).

In verband hiermee wordt bij het ontwerpen van bedrijfszekere software de nadruk gelegd op het beheersen van de complexiteit en het vermijden van ontwerpfouten.
Software waarin geen fouten zitten zal nooit falen. Het is echter bijna onmogelijk om foutvrije software te ontwikkelen, waardoor deze software eens kan falen.

Vandaar dat er in de praktijk gewerkt wordt naar een geringe waarschijnlijkheid dat er fouten in een software ontwerp zitten. Dit wordt bereikt door:

- het software ontwikkeltraject zorgvuldig (bv. volgens DO-2167A) te doorlopen, waarbij reviews op de overgang van de fasen en er formele 'code-walk throughs' gehouden worden (Ref. 7);
- gevalideerde (ADA) compilers te gebruiken;
- de software zorgvuldig en voldoende lang met voldoende mensen te testen.

De ontwikkeling van bedrijfszekere software kan derhalve een kostbaar proces zijn. Kritische systeemcomponenten, waarvan de bedrijfszekerheid ook kwantitatief moet worden vastgesteld, worden bij voorkeur in hardware uitgevoerd.

RTCA DO-178 (Ref. 8) beschrijft de technieken en methodes die tijdens het ontwikkelproces gehanteerd moeten worden om te komen tot gecertificeerde software. Het accent ligt hierbij op het tot stand komen van documentatie waarmee het verloop van het proces zichtbaar gemaakt wordt.

5 Het toepassen van CAE-hulpmiddelen in het ontwikkeltraject

Een steeds groter deel van de ontwerpactiviteiten wordt met de computer ondersteund. De voordelen van 'Computer Aided Engineering' (CAE) zijn inmiddels alom bekend en zijn zowel van invloed op de kwaliteit van het te ontwikkelen systeem als op de kosten van de ontwikkeling. Eigenschappen van CAE zijn onder meer:

- ondersteuning bij rekenintensieve toepassingen (simulatie);
- beheersing van de complexiteit van een ontwerp;
- verbeterde toegankelijkheid van ontwerpinformatie binnen het ontwikkelteam;
- versnelling van de ontwikkeling.

Een geïntegreerde CAE infrastructuur kan de drager vormen van de CAE ontwikkelhulpmiddelen (Ref. 9) en is een belangrijke factor voor het bereiken van concurrent engineering (Ref. 10).

Het voorkomen van fouten is één van de belangrijkste mogelijkheden die CAE biedt: de uitvoer van het ene ontwerpproces wordt als invoer voor het andere gebruikt, zonder tussenkomst van de mens. Het voorkomen van fouten is tevens één van de belangrijkste factoren die in het proces van het ontwikkelen van complexe systemen en van bedrijfszekere avionica in het bijzonder een rol speelt.

Daar een belangrijke foutenbron het gevolg is van onjuiste of onvolledige ontwerpspecificaties, is het zaak om de eisen zorgvuldig vast te leggen en te reviewen. Met moderne 'Computer Aided Software Engineering (CASE)' hulpmiddelen kan de overgang naar een gestructureerd systeemontwerp plaatsvinden.

Rekenintensieve en complexe bedrijfszekerheidsanalyses zoals MTBF bepaling, FMEA's en FMECA's laten zich uitstekend met CAE ondersteunen. Als invoer hiervoor dienen van schema's afgeleide lijsten en modellen met parameters uit componentenbibliotheken. Gegarandeerde reproduceerbaarheid en uniforme rapportage zijn hierbij belangrijke voordelen.

6 Conclusies en slotopmerkingen

Moderne avionica systemen bevatten zowel hardware als software componenten, waaraan bedrijfszekerheidseisen gesteld worden.

De bedrijfszekerheid van een systeem wordt niet alleen bepaald door de eigenschappen van de bouwstenen (MIL-SPEC, Hi-Rel, Rad-Hard) en de aard van het ontwerp (zoals het introduceren van redundantie), maar ook door de wijze waarop het ontwikkelproces wordt doorlopen.

De eisen die aan het ontwikkelproces gesteld worden zijn zwaarder naarmate de toepassing waarbinnen de avionica zijn functie moet vervullen kritischer is. Het beschikken over een adequaat kwaliteitssysteem is voor het ontwikkelen van zowel de hardware als de software componenten van avionica onontbeerlijk, zeker wanneer certificering een rol speelt.

Het voorkomen van fouten is één van de belangrijkste factoren bij het ontwikkelen van complexe systemen en van bedrijfszekere avionica in het bijzonder. Het gebruik van CAE en CASE hulpmiddelen biedt hierbij belangrijke voordelen.

7 Referenties

1. MIL-HDBK-217, Reliability Prediction of Electronic Equipment, Department of Defense.
2. MIL-HDBK-338, Electronic Reliability Design Handbook, Department of Defense.
3. van Mourik, C.; van der Ouderaa, E.M.; Hage, C.G., Management van Research en Development, Deventer: Kluwer, ISBN 90-267-1605-2, 1991.
4. Kasser, Joe, Applying total quality management to systems engineering, Artech House, ISBN 0-89006-767-8, 1995.
5. Environmental Conditions and Test Procedures for Airborne Equipment, RTCA DO-160.
6. van Vliet, J.C., Software engineering, Leiden: Stenfert Kroese, ISBN 90-207-1646-8, 1988.
7. Military Standard: Defense System Software Development, DOD-STD-2167A, February 1988.
8. Software Considerations in Airborne Systems and Equipment Certification, RTCA DO-178 / EUROCAE ED-12.
9. Mathijssen, R.; Aartman, L.J.; Manders, P.J.M.; Slot, H., Het Informaticabeleid ten aanzien van Elektronische Technologie; De NLR Infrastructuur voor CAE van Elektronica (NICE), NLR TP 91001.
10. Medhat, Sa'ad, Engineering Data Management - from Electronic Design Automation to Concurrent Engineering, Proceedings of the International Conference on Concurrent Engineering and Electronic Design Automation (CEEDA '94), Bournemouth, United Kingdom, April 1994, pp. 519-532.