Fault-tolerant satellite computing with modern semiconductors

Fuchs, C.M.

Nederlandse Samenvatting

Moderne semiconductortechnologie maakt het mogelijk om geminiaturiseerde satellieten te bouwen, die goedkoop zijn om te lanceren en een betaalbaar platform bieden voor vele verschillende wetenschappelijke en commerciële instrumenten. Vooral de kleinste en lichtste satellieten maken ruimtemissies mogelijk die voorheen technisch niet haalbaar, onpraktisch of simpelweg oneconomisch te duur waren. Vooral zogenaamde CubeSats kunnen snel tegen lage kosten gebouwd worden, met beperkte hulpmiddelen in een academische omgeving. Dit soort satellieten heeft echter te maken met een lage betrouwbaarheid. Daarom zijn ze tot op heden voornamelijk gebruikt voor minder kritieke missies en missies met een laag budget, waar risico's genomen kunnen worden.

Vele geavanceerde wetenschappelijke en commerciële toepassingen passen tegenwoordig in een geminiaturiseerde satelliet, waarvoor een lange missieduur wenselijk is. Theoretisch kunnen zulke ruimtevaartuigen gebruikt worden voor verscheidene kritieke en complexe missies, waaronder wetenschappelijke hoge-prioriteitsmissies binnen het Zonnestelsel of voor astronomische toepassingen. Echter, door hun lage betrouwbaarheid zijn dit soort ruimtevaartuigen tot nu toe alleen gebruikt op ruimtemissies voor secundaire taken.

Miniatuursatellieten bestaan voor een groot gedeelte uit elektronica welke zijn verantwoordelijk voor een groot gedeelte van de kritieke subsystemen. Gezien het lage gewicht van de satelliet, moet deze elektronica lichter, kleiner en energiezuiniger zijn dan traditionele ruimtevaartcomponenten. Daarom gebruiken alle geavanceerde CubeSats tegenwoordig hoogwaardige computerontwerpen die gebaseerd zijn op commerciëel verkrijgbare ontwerpen voor de ingebed systemen en de mobiele markt. Tegen minimale kosten geeft dit soort elektronica hoge prestaties, verbruikt het minder energie en is het makkelijker om mee te werken dan hun tegenhangers die historisch voor ruimtemissies zijn ontwikkeld.

Conventionele computers die gebaseerd zijn op het System-on-chip-principe, missen echter de fouttolerantie van computerontwerpen op grotere ruimtevaartuigen. Subsystemen die draaien op dit soort componenten zijn verantwoordelijk voor de meeste storingen nadat miniatuur satellieten gelanceerd zijn en ingezet zijn in de ruimte. Door budget-, energie-, massa- en volumebeperkingen van miniatuursatellieten kunnen fouttolerantiesystemen van bestaande grotere ruimtevaartuigen niet toegepast worden.

Op het moment van schrijven bestaat er geen fouttolerante computerarchitectuur, bestaand uit halfgeleiders uit de mobiele markt, die aan boord van miniatuursatellieten gebruikt kan worden zonder te breken met het fundamentele concept van goedkope, simpele, energiezuinige en lichtgewicht satellieten die op grote schaal geproduceerd en tegen lage kosten gelanceerd kunnen worden. Ontwerpers van miniatuursatellieten

hebben daarom de volgende opties:

Vergroten: Gebruik maken van traditionele ruimtevaartcomponenten. Dit gaat meestal samen met het vergroten van het ontwerp van het ruimtevaartuig, aangezien zulke componenten meer energie gebruiken en minder functionaliteit, flexibiliteit en rekenkracht bieden. In de praktijk verhoogt dit de kosten, benodigde mankracht en ontwikkelingstijd drastisch. Daarom is deze aanpak niet praktisch voor de meeste nieuwe ruimtemissieconcepten, die juist gebruik willen maken van ruimtevaartuigen die snel ontwikkeld kunnen worden of die klein of goedkoop moeten zijn.

SpareSats: Het risico van vroege uitval verminderen door één of meerdere SpareSats te bouwen die een CubeSat vervangen zodra deze een storing heeft. In de praktijk verhoogt dit niet alleen de kosten, maar worden storingen ook waarschijnlijker aangezien het aantal componenten dat wordt gelanceerd nam drastisch toe. Daarom wordt deze aanpak alleen rendabel zodra systemen robuust genoeg zijn. Op dit moment heeft deze aanpak alleen nut voor satellietnetwerken, waarbij satellieten in hoog tempo en continue vervangen worden (bijv. Planet Lab) en individuele satellieten die werken met een uitzonderlijk groot budget (bijv. MarCo).

Accepteren: Het gebrek aan betrouwbaarheid accepteren. De ruimtemissie is bewust van korte duur, in de hoop dat alle missiedoelen gehaald worden voordat de satelliet uitvalt. Voor toekomstige langdurige missies met miniatuursatellieten, kan geluk geen factor zijn waarop het systeem is gebaseerd.

Op het moment van schrijven van deze thesis, zijn de meeste ontwikkelaars van miniatuursatellieten gedwongen om de derde optie te volgen. Voor simpele en korte CubeSatmissies resulteert deze aanpak meestal in succes, maar ook in vele vroege storingen. Gokken tegen tijd en hopen dat een satelliet niet beïnvloed zal worden door processen in de ruimte is echter onacceptabel en wordt steeds minder getolereerd door overheden, ruimtevaartorganisaties en investeerders. Om success te garanderen voor geavanceerde en langdurige CubeSat missies, zijn betere en betrouwbaardere systeemontwerpen nodig. Daarom zijn fouttolerante concepten nodig die geschikt zijn voor computers, gebaseerd op moderne commerciële halfgeleiders, in CubeSats.

De resultaten van deze thesis

Om de technologische tekortkomingen van kleine satellieten te overwinnen wordt in deze thesis een nieuw fouttolerante computer architectuur gepresenteerd. Deze architectuur is geschikt om in lichte wetenschappelijke CubeSats ingebouwd te worden, die gebruik maken van moderne commerciële halfgeleiders.

Om de architectuur die gepresenteerd wordt in deze thesis te ontwikkelen, worden resultaten en concepten uit verschillende wetenschappelijke vakgebieden en het ingenieurswezen gebruikt, waarbij de ontwikkeling van deze architectuur beide vakgebieden overstijgt. Daarom combineren wij het beste van twee werelden: we integreren

wetenschappelijke vooruitgang, conceptuele en theoretische kennis met een praktische implementatie en de grondige tests die standaard zijn in het vakgebied van ruimte- en elektronische bouwkunde.

Om de resultaten van dit onderzoek toegankelijk te maken voor zowel wetenschappers en ingenieurs, zijn Hoofdstukken 2 en 3 bedoeld als informele introductie en definitie van het foutmodel dat gepresenteerd wordt in deze thesis. Hoofdstuk 2 bevat een kort overzicht van essentiële aspecten van hedendaagse ruimtevaart, voor lezers die onbekend zijn met dit onderwerp. Dit hoofdstuk fungeert als motivatie voor deze thesis, en introduceert ook concepten die gerelateerd zijn aan fouttolerante computerontwerpen. Om een effectief en efficient fouttolerant computersysteem te ontwerpen en ontwikkelen, is het essentieel om het effect van de ruimte op een computer te begrijpen. Hoofdstuk 3 behandelt deze effecten in detail, beperkingen voor ruimteelektronica en overwegingen gedurende de ruimtemissie, zoals communicatietijd en hemelmechanica.

Gebaseerd op de voorgaande hoofdstukken, presenteren we in Hoofdstuk 4 een fouttolerante computer architectuur, die softwarematige fouttolerantieconcepten combineert met FPGA[1] herconfiguratie en mixed criticality. Dit wordt verder aangevuld met verscheidene conventionele fouttolerantietechnieken en correctiemaatregelen. Fouttolerantie in deze architectuur wordt geïmplementeerd in verschillende, onderling gelinkte, stappen, die een lange levensduur van computers aan boord van kleine satellieten garanderen.

Voor deze functionaliteit gebruiken we een softwarematige coarse grain lockstep, die in detail wordt beschreven in Hoofdstuk 4. Deze functionaliteit alleen biedt uitstekende fouttolerantie, maar niet genoeg voor langdurige ruimtemissies. Daarom beschrijven we in Hoofdstuk 5 hoe herconfigureerbare logica gebruikt kan worden om vele verschillende systeemfouten te herstellen. Wij gebruiken FPGA herconfiguratie om de integriteit van een system-on-chipontwerp te garanderen, zodat de bruikbare levensduur van de computer verlengd kan worden. Op den duur zullen tijdens een langdurige ruimtemissie defecte onderdelen van een FPGA niet meer te herstellen zijn. Daarom zal de hoeveelheid intacte programmeerbare logica die beschikbaar is in een computer met de tijd afnemen. In Hoofdstuk 6 tonen we hoe mixed criticality een computer kan helpen zich aan te passen aan systeemfouten, in plaats van spontaan uit te vallen zoals traditionele systemen doen. Wij kunnen deze functionaliteit gebruiken om autonoom systeemprestatie in te ruilen voor energiezuinigheid en robuustheid tijdens de runtime. Dit zorgt er voor dat de kernfunctionaliteit van de computer bewaard blijft en het maximaliseert de overlevingskansen van de satelliet.

Al deze functionaliteit bestaat als software die draait op een multiprocessor system-on-chip die geïmplementeerd is in FPGA. Software, ladinginformatie en logica geprogrammeerd in een FPGA zijn data waarvan de integriteit bewaard moet blijven gedurende de gehele ruimtemissie. In Hoofdstuk 7 worden beschermende concepten voor verschillende soorten geheugentechnologiën aan boord van moderne satellieten beschreven.

De voorgaande, op software gebaseerde, fouttolerantieconcepten die toegepast kunnen worden op moderne halfgeleiders klinken vaak goed in theorie, maar blijken in realiteit onpraktisch te zijn. Op het moment van schrijven is er nog geen fouttolerante architectuur geïmplementeerd en getest, terwijl dit wel een kritieke stap is. In Hoofdstuk 8 tot 10 van deze thesis nemen wij deze kritieke stap.

De lockstepfunctionaliteit die gebruikt wordt in onze architectuur wordt getest

[1] field-programmable gate array

door middel van foutinjectie in Hoofdstuk 8. In Hoofdstuk 9 beschrijven wij een praktisch multiprocessor system-on-chipontwerp dat geïmplementeerd kan worden in een FPGA, wat een ideaal platform is voor deze architectuur. Hoofdstuk 10 is gewijd aan de praktische implementatie van de concepten en ontwerpen die beschreven worden in voorgaande hoofdstukken. Hierdoor kunnen we laten zien hoe een computer met deze architectuur aan boord van een miniatuursatelliet er in het echt uitziet, door een test opstelling te bouwen met ontwikkelingskit. Dit werdt gedaan met de volgende zes Xilinx FPGAs:

- Kintex UltraScale KU60,
- Kintex UltraScale+ KU11p, KU3p, de KU5p van een Xilinx KCU116 ontwikkelingskit en het
- Virtex UltraScale+ VU9P of a Xilinx VCU118 ontwikkelingskit.

Voor drie van deze FPGAs, de KU60, KU11p en KU3p, geven we gedetailleerde gebruiks- en stroomverbruikdata.

Conclusies

Aan het begin van deze thesis begonnen we met de volgende vraag:

Kan een fouttolerante computerarchitectuur gemaakt worden met moderne, mobiele-markttechnologie, zonder over de massa-, ruimte-, complexiteit- en budgetbeperkingen van miniatuursatellieten te gaan?

En PhD, vele gepubliceerde onderzoeksartikelen en verschillende ongelukken later, is het nu mogelijk om deze vraag op de volgende manier te beantwoorden:

Ja. *Een fouttolerante computerarchitectuur voor miniatuursatellieten is technisch mogelijk met bestaande commerciële en industriële technologie. Zodra alle componenten samengevoegd zijn tot een prototype, kan deze architectuur gebruikt worden om de levensduur van moderne CubeSats drastisch te verlengen, waardoor ze bruikbaar worden voor kritieke en langetermijn ruimtemissies.*

De softwarecomponenten van de architectuur die gepresenteerd wordt in deze thesis kunnen zonder grote ingrepen geïmplementeerd worden. Ze bieden bescherming voor bestaande toepassingen, zonder dat deze programma's herschreven moeten worden. Met bestaande software tonen wij aan dat deze mechanismes fouten snel kunnen detecteren en met hoge zekerheid en nauwkeurigheid en dat succesvol van fouten hersteld kan worden, tegen in de meeste gevallen lage computationele kosten. We demonstreren dat de prestaties van deze architectuur economisch zijn en effectief blijven, zelfs wanneer ze gebruikt worden in gebieden van de ruimte met uitzonderlijk hoge hoeveelheden straling.

Met bestaande commerciële componenten kan een system-on-chipontwerp, dat geldt als ideaal platform voor deze architectuur, zelfs geïmplementeerd worden in de kleinste Ultrascale+ FPGA die slechts 1.94W aan energie verbruikt. Daarom kan deze computerarchitectuur toegepast worden op satellieten ter grootte van 2U CubeSats.

Aangezien de grootte van een systeem bepaald wordt door technologie, zal vooruitgang in halfgeleiderproductie in de volgende generatie FPGAs deze aanpak nog aantrekkelijker maken en bruikbaar voor nog kleinere ruimtevaartuigen. Ook kan het de efficiëntie en schaalbaarheid aan boord van zwaardere ruimtevaartuigen verbeteren. Hopelijk kunnen we op deze manier in de toekomst de gebieden ver buiten de grenzen van het zonnestelsel onderzoeken.