MISSIE: FOUTVRIJE SOFTWARE IN DE RUIMTE

Het Esa-project Compass beoogt een geïntegreerde, coherente aanpak te ontwikkelen voor het ontwerp en de analyse van ruimtevaartsoftware. In dit artikel bespreken de betrokken onderzoekers van de RWTH Aachen University enkele praktijkstudies die zij in dit kader hebben uitgevoerd.

Harold Bruintjes
Joost-Pieter Katoen

Ruimtemissies zijn nog steeds erg risicovol. De mislukte landing van de Exomars Schiaparelli van 19 oktober 2016 staat menigeen nog op het netvlies. Doordat de berekende hoogte negatief was, werden de remmen bij de landing te vroeg uitgeschakeld, met een noodlottige landing op Mars tot gevolg. De Schiaparelli heeft geen enkel bruikbaar beeldmateriaal opgeleverd van de planeet. Vijf weken na de lancering verloor de Japanse ruimtevaartorganisatie Jaxa in maart 2016 het contact met de Hitomi-röntgentelescoop nadat problemen waren ontstaan met de besturing van de hoogte en oriëntatie van het instrument. Het geplande onderzoek naar het ontstaan van het heelal en zwarte gaten is tot na 2020 uitgesteld.

Een belangrijke oorzaak van het falen van ruimtemissies ligt in software. De hoeveelheid code in satellieten, raketten en robots groeit exponentieel. Het zijn in feite vliegende computerprogramma's. Deze trend zet zich verder door, aangezien ruimtemissies steeds geavanceerder worden: de voor 2018 geplande Proba-3-missie van Esa behelst het met millimeterprecisie sturen van satellieten die op honderdvijftig meter van elkaar in formatie vliegen.

Door de almaar groeiende complexiteit wordt de software steeds lastiger te beheersen. Behalve allerlei berekeningen uitvoeren, moeten de systemen de temperatuur regelen en ervoor zorgen dat er altijd genoeg energie is en dat de aansturing van de gyroscopen de missie op de juiste positie houdt. Dan moeten ze vaak ook nog gegevens uitwisselen met de aarde. Dit moet echter allemaal gebeuren met hardware die wij allang niet meer in onze huis-tuin-en-keukenlaptops aantreffen.

De ruimtevaartindustrie is enorm terughoudend met de inzet van nieuwe technologie. Zo zijn quadcore processoren nog niet te vinden in de huidige missies en is parallelle verwerking nog ver weg. Als er al dualcore wordt toegepast, is het om de betrouwbaarheid te verhogen, niet om berekeningen sneller uit te voeren. De hoeveelheid geheugen is eerder te meten in mega- dan in gigabytes, en als de datapaden 32 bits breed zijn, dan is het al heel wat.

Honderd miljard

Sinds een jaar of tien zijn wij binnen het Compass-project (zie kader) bezig om modelgebaseerd systeemontwerp – zowel hardware als software – in te bedden in het gestandaardiseerde ontwerpproces. Hierbij maken we in hoge mate gebruik van krachtige softwaretools en de laagdrempelige modelleertaal AADL (Architecture Analysis & Design Language). De tools ondersteunen het ontwerpproces vanaf het opstellen van de requirements tot het doorlichten van de modellen op fouten en het bepalen van kwantitatieve maten zoals de faalkans binnen tien jaar.

Een van de praktijkstudies hebben we uitgevoerd naar aanleiding van een succesvolle vergelijkbaar onderzoek in 2011, waarbij parallel aan het initiële ontwikkeltraject van een satelliet (de Preliminary Design Review, fase B) is gewerkt. Die studie duurde zes maanden, inclusief leercurve en ontwikkeling. Het vervolgonderzoek richtte zich op de volgende fase in het ontwikkeltraject (de Critical Design Review, fase C), met een looptijd van een jaar. Het hierbij ontwikkelde model had een omvang van circa 250

Compass

Het Compass-project (Correctness, Modeling and Performance of Aerospace Systems) heeft het Europese ruimtevaartagentschap Esa in 2008 uitgeschreven aan de RWTH Aachen University, Fondazione Bruno Kessler en Thales Alenia Space. Het doel is een coherente en integrale aanpak op te stellen voor het ontwerp, de verificatie en de validatie van ruimtevaartsystemen, in het bijzonder van hun besturingssoftware. Op basis van de industriële standaard AADL hebben de partners een toolset ontwikkeld die de modernste formele methoden uit de academische wereld integreert. Deze gereedschapskist hebben ze uitgebreid toegepast op industriele casestudies. Het r&d-project is onderdeel van Esa's Technology Research-programma, dat zich ten doel stelt technieken te ontwikkelen ter realisatie van de toekomstige generatie ruimtevaartsystemen.
www.compass-toolset.org

componenten met meer dan vijftienhonderd verbindingen.

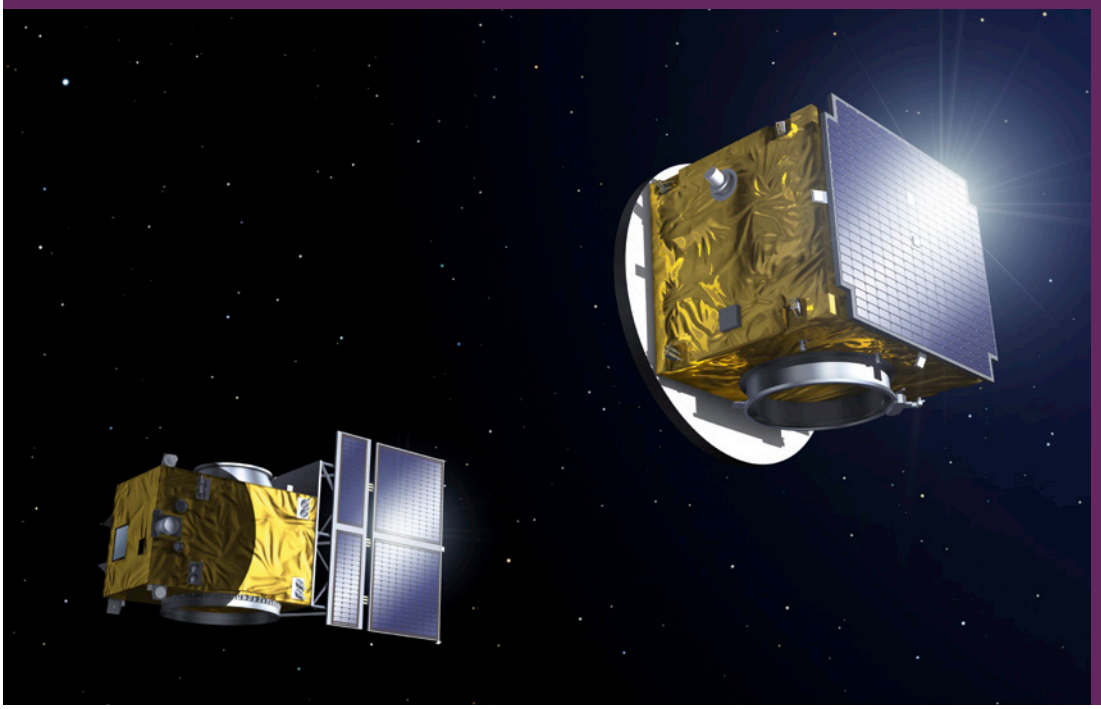
De focus van de studie lag op het bepalen van modelleringsstrategieën voor modellen van een dergelijke omvang en op het doorlichten van de sensorconfiguratie bestemd voor foutdetectie. Slim modelleren is belangrijk; het ontwikkelde model omvat al een half miljard toestanden als we enkel permanente fouten in ogenschouw nemen, en meer dan honderd miljard onder medeneming van kortstondige (tijdelijke) fouten.

Op het model hebben we verschillende analyses uitgevoerd, waaronder foutboomanalyse (zowel statisch als dynamisch), fdir-analyse (*fault detection, isolation, recovery*), fmea (*failure mode and effect analysis*), betrouwbaarheidsanalyse en *diagnosability*. Betrouwbaarheidsanalyse richt zich op de berekening van de foutkans over een bepaalde tijdsduur. Diagnosability kijkt of gebeurtenissen overeenkomend met een systeemfout correct terug te leiden zijn tot sensormeetwaarden. Deze analyses verlopen volledig geautomatiseerd.

Veelbelovend

Voor een recentere praktijkstudie in 2014 was de aanleiding een project samen met Airbus DS (toen nog Astrium geheten), waarbij de focus lag op verbetering van de ondersteuning voor de analyse van systemen met tijdsafhankelijk gedrag. Zulke systemen komen veelvuldig voor in lanceerplatformen (raketten), waarbij ze razendsnel beslissingen moeten nemen in het geval er een fout optreedt. Nieuwe ontwikkelingen laten toe om subsystemen die tijdelijk door een fout zijn uitgevallen weer in te schakelen, om zo de kans op een algeheel systeemfalen te verkleinen.

Om analyses van zulke systemen mogelijk te maken, en daarbij de kans van falen of succes te berekenen, hebben we in het project gekozen voor een aanpak waarbij we duizenden tot miljoenen simulaties draaien volgens de Monte Carlo-methode tot we een vooraf bepaalde statistische zekerheid over de uitkomst hebben behaald. Dit is een bijzonder schaalbare aanpak, aangezien



Ruimtemissies worden steeds geavanceerder: de Proba-3-missie behelst het met millimeterprecisie sturen van satellieten die op honderdvijftig meter van elkaar in formatie vliegen.

Illustratie:
Esa - P. Carril, 2013

we de simulaties in parallel kunnen uitvoeren. Bij de analyse dienen we wel enkele aannames te maken over niet-deterministisch gedrag in het model (waarbij het resultaat van een beslissing niet vooraf is bepaald), die invloed hebben op de uitkomst. Dit is echter configureerbaar.

Na afronding van het project hebben we in de praktijkstudie een model gemaakt van de aansturing van een lanceerplatform, bestaande uit 37 componenten. Binnen dit model hebben we systemen met twee- of drievoudige redundantie uitgerust, waarbij fouten tot tijdelijke of permanente uitval kunnen leiden en hun optreden is geassocieerd met een kansverdeling.

De resultaten zijn veelbelovend. Hoewel bij kleine modellen simulatie meer tijd nodig heeft, blijft deze tijdsduur constant naarmate de modellen groeien. Het geheugengebruik blijft in alle gevallen beperkt (enkele tientallen megabytes), waar andere analyses snel het beschikbare geheugen kunnen uitputten. Hierbij dienen we wel aan te tekenen dat deze analyses met hogere precisie kunnen werken (de tijdsduur van simulatie neemt kwadratisch toe met hogere precisie).

Catalogus

In een nog recenter Compass-project hebben we ons gestort op verbetering van het proces rondom de specificatie van eisen. Dit gebeurt vaak in natuurlijke taal, waardoor het niet mogelijk is om te controleren of ze wel compleet en consistent zijn. In het project hebben we een catalogus gemaakt van typen eisen die zich richten op systeemgedrag en die te koppelen zijn aan eigenschappen van het systeem, bijvoorbeeld reactietijd. Deze koppeling maakt het mogelijk eisen direct terug te leiden naar het (formele) systeemmodel, wat weer toelaat om ze te koppelen aan analyseresultaten.

Verder hebben we contractgebaseerde analyse toegevoegd. Hierbij leggen we het systeemgedrag vast in een contract. Wanneer we het systeem tijdens de ontwikkeling verfijnen in subsystemen, kunnen we het geheel verifiëren door de losse onderdelen onder de loep te namen. Dit vereenvoudigt de analyse significant en maakt het makkelijker om te itereren door het ontwerpproces.

Deze studies geven een beeld van wat we hebben bewerkstelligd. Dit is onderzoek dat Esa en het bedrijfsleven de komende tien jaar wellicht adopteren. De verwachting is dat ruimtemissies op zijn vroegst na 2030 op deze technieken zijn gestoeld.

Joost-Pieter Katoen is hoogleraar softwaremodellering en -verificatie aan de RWTH Aachen University. Harold Bruintjes is als wetenschappelijk medewerker verbonden aan die leerstoel.

Redactie Nieke Roos