Het wachten is op de toestandsexplosie

Regelsysteem kan niet alles overzien

Door de toenemende complexiteit van sturende computersystemen is hun betrouwbaarheid steeds moeilijker in te schatten. Grote computerrampen komen op ons af.

Door onze redacteur
Michiel van Nieuwstadt

NIJMEGEN, 11 OKT. Computerprogramma's besturen treinen, vliegtuigen en in toenemende mate ook onze auto's. Maar zijn die regelsystemen ook veilig? Daarvoor valt geen garantie te geven. Sterker, het is vooralsnog *onmogelijk* om de betrouwbaarheid van dit soort systemen te kwantificeren.

Dat wordt duidelijk uit onderzoek van Goran Frehse, gisteren gepromoveerd aan de Radboud Universiteit Nijmegen. Frehse heeft een softwarepakket ontwikkeld dat inzicht kan geven in boordcomputers en andere systemen waarin een computer (digitale) commando's geeft op grond van (continue) informatie die vanuit zijn omgeving wordt aangeleverd. Maar dergelijke systemen zijn zo complex en kennen zo veel variabelen dat het bij voorbaat onmogelijk is om alle eventualiteiten te overzien. Dat fenomeen heet een toestandsexplosie. „Het aantal mogelijke combinaties waarmee je rekening moet houden groeit enorm", zegt Frehse. „Dat is het grote probleem waar we tegenop lopen." Frehse's dissertatie, bijna 200 bladzijden vol wiskundige formules, is een soort trukendoos om enige grip op dat probleem te krijgen. Een belangrijke vernieuwing is het opdelen van het proces in deelsystemen die soms wél wiskundig onder controle zijn te brengen.

„Het is absoluut een stap in de goede richting", zegt promotor Frits Vaandrager, hoogleraar Informatica van Technische toepassingen aan de Radboud Universiteit Nijmegen. „Aan het probleem van de toestandsexplosie zullen we de komende twintig jaar onze handen vol hebben, ook al omdat de systemen waarmee we te maken hebben steeds krachtiger worden."

Hoe ingewikkeld de analyse van hybride systemen is, valt te illustreren met een eenvoudig voorbeeld. Met een andere promovendus heeft Vaandrager al eens een lego-autootje met rupsbanden ontwikkeld dat moest rijden over een stuk zwarte tape. Het autootje was aan de onderkant voorzien van twee kleine sensoren die het voertuig op de weg moesten houden. De algoritmen voor de software in de kleine boordcomputer waren eenvoudig: als de linker sensor vaststelde dat het karretje van de 'weg' (de tape) afraakte moest de rupsband aan de rechterkant dat herstellen. Vaandrager: „De dynamica van zo'n autootje is eenvoudig te begrijpen en de logica van het ingebouwde computerprogramma is ook simpel. De combinatie van beide systemen is echter uiterst complex."

Cockpitinterieur van een Boeing 777 verkeersvliegtuig. (Foto Bloomberg)

Het autootje slaagde er moeiteloos in om de tape te volgen, alleen als het te veel dwars op de tape kwam te staan raakte het soms het spoor totaal bijster. Vaandrager en zijn collega's slaagden er uiteindelijk in om precies uit te rekenen onder welke omstandigheden dit gedrag optreedt, maar de kwestie illustreert de problemen die ontstaan als een computer met een simpel commando ingrijpt in een fysisch of dynamisch proces dat op zichzelf met wiskundige vergelijkingen goed te beschrijven valt. Vaandrager: „Het aantal mogelijke scenario's dat je moet doorrekenen neemt explosief toe en daarmee ook de complexiteit. Dan kun je je voorstellen wat er gebeurt in de cockpit van een vliegtuig, met zeg, honderd knopjes die allemaal aan of uit kunnen staan."

De mens kan ingrijpen in het handelen van de computer, maar dat hoeft niet altijd tot een veiliger situatie te leiden. Frehse leidt zijn dissertatie in met het voorbeeld van de Russische Toepolev die op 1 juli 2002 boven het Bodenmeer in botsing kwam met een Boeing 757. Het Traffic Alert and Collision Avoidance System (TCAS), aan boord van beide toestellen verordonneerde de piloot van de Toepolev om hoger te gaan vliegen, maar een vliegverkeersleider ging daar tegenin en eiste dat het toestel juist lager ging vliegen. De botsing die volgde kostte 71 passagiers en bemanningsleden het leven. Intussen heeft de internationale luchtvaartorganisatie ICAO afgesproken dat piloten TCAS moeten gehoorzamen, ongeacht wat de luchtverkeersleider zegt. Vaandrager spreekt van het uitsluiten van 'de menselijke loop', maar hij betwijfelt of het vliegverkeer daardoor veiliger wordt. Op de lange termijn is de veiligheid van computersystemen meer gebaat bij een structurele aanpak zoals die van Frehse. Op dit moment wordt de betrouwbaarheid van computersystemen, als die al wordt getest, vaak in kaart gebracht met een simulatie. Een riskante aanpak, omdat onmogelijk met alle denkbare omstandigheden rekening kan worden gehouden, zodat een simulatie die wekenlang probleemloos draait aanleiding kan geven tot onterecht vertrouwen.

In modellen zoals die van Frehse kunnen ook niet alle variabelen worden meegenomen, maar er wordt wel geprobeerd om de complexiteit op een slimme manier te reduceren. Vaandrager: „Een vliegtuigingenieur kan een boekwerk schrijven over de werking van een vliegtuig. De kunst is om van een groot deel daarvan te abstraheren en in je model de paar cruciale vergelijkingen te gebruiken die er werkelijk toe doen." Een complex systeem is op te breken in deelsystemen waarvan wiskundig is te bewijzen dat ze onder bepaalde randvoorwaarden feilloos werken. Deze aanpak in compartimenten is volgens Vaandrager het meest vernieuwende element in de methode van Frehse.

Vaandrager voorspelt dat er de komende jaren nog grote computerrampen op ons af zullen komen. Dat komt doordat de hoeveelheid software in apparatuur nog altijd toeneemt. „Het is bekend dat bij het schrijven van elke paar honderd regels software tenminste één fout worden gemaakt. Een bepaald percentage van deze fouten resulteert in een probleem voor de gebruiker. Op grond van zo'n sommetje kun je vaststellen dat de zaak af en toe zal uitvallen. Dit soort problemen zijn te ondervangen door de zaak goed te modelleren, analyseren en testen, maar daar is vaak geen geld voor."