

reageren? computable.lezers@vnumedia.nl

ALS OPLOSSINGEN PROBLEMEN WORDEN

In de serie 'Als oplossingen problemen worden' belicht de redactie grootschalige ict-projecten die bedrijven en/of overheden in een lastig parket hebben gebracht.

Software aan het stuur



Autofabrikanten roepen jaarlijks miljoenen auto's terug, omdat de software op de chips en processoren in deze wagens onvoldoende betrouwbaar is. Een greep uit de problemen van het laatste jaar:

Wie en wat?

Vanaf februari 2007 riep Daimler-Chrysler 62.369 auto's terug, omdat de achterremmen van de wagen onder bepaalde remcondities geblokkeerd kunnen raken. De oorzaak: een softwarefout in de controlemodule van het ABS-systeem (Antilock Brake System). Het gevolg: de bestuurder kan mogelijk de controle over het voertuig verliezen.

In oktober 2006 kwam een probleem aan het licht met het drive-by-wire systeem van de Toyota Camry. Dit systeem onthoudt wat de rijstijl van de bestuurder is. Zodra de bestuurder handelingen verricht die de wagen niet van hem of haar gewend is, kan de software die de aansturing verzorgt voor de motor en de versnelling van slag raken, met bokkig gedrag tot gevolg. Wanneer een rustige rijder plotseling het gaspedaal indrukt om een andere auto te ontwijken, kan zoiets fataal zijn.

Door een softwarefout kan de airbag van de passagiersstoel van de Audi A8 gedeactiveerd raken als het voltage van de bijbehorende batterij te laag wordt. Vanaf december 2006 riep Audi deze wagens terug, zodat autodealers een update konden uitvoeren van de software voor de controlemodule van de airbag.

Wanneer?

Professor Chris Verhoef, hoogleraar Informatica aan de Vrije Universiteit in Amsterdam: "Je hoort of ziet er nauwelijks wat over, want fabrikanten proberen deze problemen zoveel mogelijk onder de pet te houden. Maar het ministerie van Transport van de V.S. heeft een databank online staan waarin wordt bijgehouden welke autotypen om welke reden worden

teruggeroepen door autofabrikanten. Ga naar <http://tinyurl.com/b7m2>, klik op Downloads, Recalls en FLAT_RCL.zip. Zoek binnen het gedownloade bestand op software en je vindt ontelbare voorbeelden van veiligheidsproblemen als gevolg van softwarefalen."

Wat ging er mis?

Dr. Gerard Holzmann, ontwikkelaar van SPIN (een veelgebruikte tool voor het testen van de betrouwbaarheid van software), in een interview in Computable 2 van dit jaar: "Ik zaai liever geen paniek, maar in elke auto zijn tegenwoordig verschillende processoren ingebed. In principe is de hele besturing van de auto geautomatiseerd. Dat geldt voor de remmen, maar ook voor bijvoorbeeld de besturing van de wielen. De software daarvoor wordt meestal in C geschreven. Die code wordt tegenwoordig nog onvoldoende gecontroleerd. Dat kan uiteindelijk tot consequenties leiden. Als die software faalt, kunnen er echt heel vervelende dingen gebeuren."

Prof. Dr. Ir. Boudewijn Haverkort, coördinator vanuit de Universiteit Twente van het 3TU.Centre for Dependable ICT Systems' (CeDICT): "De elektronica in auto's wordt steeds omvangrijker. De luxere auto's bevatten tegenwoordig vaak drie computernetwerken: eentje voor de multimedia, eentje voor kritische onderdelen zoals remmen en gas geven en eentje voor minder kritische onderdelen zoals de ruitwissers. Die netwerken mogen niet te duur zijn en niet te veel wegen. Liefst zou je het netwerk voor kritische onderdelen drievoudig uitvoeren, zodat er bij conflicten altijd een meerderheidsbeslissing mogelijk is, maar dat is helaas niet haalbaar. Dat gebeurt wel in de luchtvaartindustrie: diverse kritische besturingsonderdelen van de Space Shuttle zijn vijfvoudig uitgevoerd."

Blaren?

Afgezien van de financiële schade die autobedrijven lijden door dit soort softwarefouten, worden de levens van miljoenen automobilisten op het spel gezet.

Kan dat niet anders?

Verhoef: "Honderd jaar geleden vielen patiënten nog bij bosjes tegelijk neer omdat behandelmethoden niet werden onderzocht, geprotocolleerd of

gecontroleerd. Het maken van software is een zeer complexe aangelegenheid. Tegelijkertijd zijn we bijzonder afhankelijk van software in onze maatschappij. Toch mag iedereen software maken. Daar zijn geen opleidingseisen aan verbonden. Er is vrijwel geen regelgeving over softwareontwerp, -constructie en -gebruik. Natuurlijk werken er heel slimme mensen keihard aan ingebedde software voor auto's en doen ze er alles aan om dit soort fouten te voorkomen. Maar de medische en de voedselsector zijn duizendmaal beter gereguleerd dan dit soort kritische software."

Haverkort: "Het is enorm in opkomst om formeel gebaseerde methoden te gebruiken tijdens softwareontwikkeling, maar de tools daarvoor zijn simpelweg nog onvoldoende ontwikkeld om alle mogelijke situaties door te rekenen. De

complexiteit van ingebedde software is oneindig veel groter dan mensen zich realiseren. Het gaat vaak om miljoenen regels code, die alle mogelijke combinaties van omstandigheden moeten dekken. De droom is natuurlijk dat we de correctheid van nieuwe software mathematisch voor 100 procent kunnen bewijzen, maar zover zijn we helaas nog niet. We kunnen de software al wel zodanig testen dat de kans dat er problemen optreden aanvaardbaar klein is geworden, bijvoorbeeld één op de miljoen."

[JOLEIN DE ROOIJ]

TIPS?

Heb je tips voor deze serie? Mail ze naar computable@bp.vnu.com. Vermeldt in de titel: Als oplossingen problemen worden.



De airbag van de passagiersstoel van de Audi A8 kan gedeactiveerd raken.



Zodra de bestuurder van de Toyota Camry handelingen verricht die deze intelligente wagen niet van hem of haar gewend is, kan de software die de aansturing verzorgt voor de motor en de versnelling van slag raken, met bokkig gedrag tot gevolg.



Onder bepaalde remcondities kunnen de achterremmen van de Chrysler Sebring geblokkeerd raken.

**REDACTIONEEL****GEZOND VERSTAND**

Zo nu en dan steekt de discussie over ethiek op de werkvloer weer de kop op. Ethiek is zo belangrijk dat het zou moeten worden opgenomen in het lesprogramma van ict-opleidingen, zeggen de voorstanders. Nee, menen de tegenstanders, houd die onzin weg van de werkvloer. Gewone programmeurs hebben het al druk genoeg en bovendien zou de ethische verantwoording uiteindelijk toch liggen bij de manager of de directie.

Eigenlijk is voor beide standpunten wel iets te zeggen. Hoe je het ook wendt of keert, je hebt als ict'er nu eenmaal te maken met de kwetsbaarheid van de klant of eindgebruiker. Je loopt hoe dan ook aan tegen informatie die in potentie gevoelig is en bij verkeerd gebruik problemen kan opleveren. Ook belooft je dingen aan de klant en die kun je beter gewoon nakomen.

Maar als je gezond verstand volgt, ondervang je eigenlijk de meeste ethische kwesties wel. Dat zeggen veel ict'ers, en ik ben het wel met ze eens. Iedereen begrijpt wel dat de privémailtjes die de systeembeheerder kan lezen in mailboxen van anderen, niet voor zijn ogen bestemd zijn. Of dat de wijzigingen die een programmeur aanbrengt in een crm-toepassing grote ongewenste gevolgen kan hebben voor de eindgebruikers. Voor de ict'er is het volgens mij het belangrijkste dat hij/zij zich bewust is van de gevolgen van zijn/haar handelen. Of je daarvoor een apart vak ethiek moet opnemen bij de verschillende ict-opleidingen? Ik betwijfel het.

Voor de organisaties waar de ict'ers werken, is ethiek natuurlijk wel een belangrijk thema. Ze zijn vaak met handen en voeten gebonden aan afspraken over dienstverlening, privacy en accountability. De meeste aandacht voor ethiek op de werkplek zou dan ook vanuit de organisatie moeten komen. De directie die er in het beleid rekening mee houdt. Maar ook de managers die gebrand zijn op naleving van ethiek bij hun medewerkers. Of laten we het maar gezonde verstand noemen. Dat zou volgens mij genoeg moeten zijn.

Diederik Toet

advertentie

**Workshop
IT-contracten**
door praktijkspecialisten
**3, 6 en 12
december 2007**
Zie www.dirkzwager.nl
Dirkzwager
advocaten & notarissen

advertentie

Innoveren
met **ICT**

TNO.NL