A certain risk: quantitative risk management for high-tech systems

INAUGURELE REDE DOOR PROF. DR. MARIELLE STOELINGA

change perspective

Radboud Universiteit

INAUGURELE REDE
PROF. DR. MARIELLE STOELINGA

Bijna dagelijks worden we geconfronteerd met ongelukken van high-tech systemen. Denk bijvoorbeeld aan het dramatische ongeluk met de stint in Oss, de stroomstoring waardoor Schiphol dicht moest, of de zelfrijdende auto van Uber die in maart een voetganger dood reed. Innovatieve systemen komen inherent met risico's. De leerstoel kwantitatieve risicoanalyse richt zich op het in kaart brengen van deze risico's om effectieve maatregelen te treffen ter voorkoming van ongelukken en storingen. Doel is het ontwikkelen van bruikbare risicomodellen die inzicht geven in aard, grondoorzaken en gevolgen van ongelukken en storingen, en waarmee ook het effect van maatregelen te evalueren is.

Marielle Stoelinga is hoogleraar Risicomanagement van high-tech systemen aan de Radboud Universiteit en aan de Universiteit Twente. Eerder was zij als post-doc verbonden aan de University of California at Santa Cruz. Zij is een erkend expert op het gebied van methoden voor kwantitatieve risicoanalyse. Stoelinga werkt nauw samen met industriële en maatschappelijke partners.

Radboud Universiteit

A CERTAIN RISK: QUANTITATIVE RISK MANAGEMENT FOR HIGH-TECH SYSTEMS

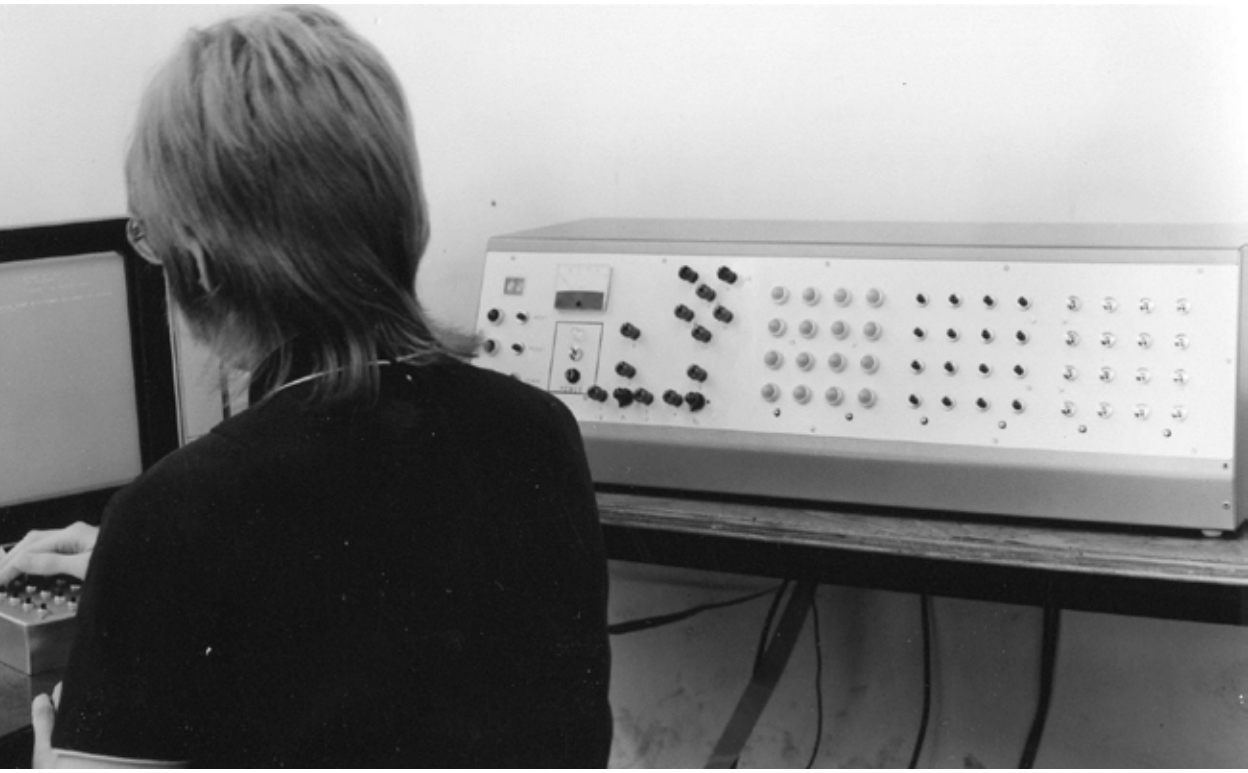
Opmaak en productie: Radboud Universiteit, Facilitair Bedrijf, Post & Print
Fotografie omslag: Bert Beelen

A certain risk:
quantitative risk management for high-tech systems

Rede uitgesproken bij de aanvaarding van het ambt van hoogleraar Quantitative Risk Assessment of Software Systems aan de Faculteit der Natuurwetenschappen, Wiskunde en Informatica van de Radboud Universiteit op donderdag 22 november 2018

door prof. dr. Marielle Stoelinga

INHOUDSOPGAVE



1. IN DEN BEGINNE

Dames en heren,

Ik wil jullie meenemen naar het jaar 1967. Toen er nog geen high-tech systemen waren. Hoogstens wat computers, geprogrammeerd door een handjevol programmeurs, zoals de vrouw op de foto. Sommige mensen in de zaal herkennen haar misschien. Dit is namelijk mijn moeder. Zij werkte als één van Nederlands eerste wetenschappelijk programmeurs op de Technische Hogeschool Eindhoven, tegenwoordig de Technische Universiteit Eindhoven.

Hier ontmoette mijn moeder mijn vader en ze trouwden in 1969. *And the rest is history* zou je kunnen zeggen. Maar zo snel zijn jullie niet van mij af.

Mijn moeder volgde hier college bij de bekendste informaticus uit de Nederlandse geschiedenis, namelijk Edsger Dijkstra. In 1972, mijn geboortejaar, ontving hij, als enige Nederlander ooit, de prestigieuze ACM Turing Award.

Mijn vader had, als elektrotechnicus, voor ons een set met schakelingen en lampjes in elkaar gezet. Hierdoor maakten mijn broer en ik als eerste kennis met seriële en parallelle poorten --- mijn zus was een jaar of twee dus te klein om mee te doen. Tegenwoordig kun je dit soort dozen in de speelgoedwinkel kopen, maar die zijn allemaal van een dusdanig belabberde kwaliteit dat ik blij ben dat mijn vader ook mijn kinderen op deze manier het licht laat zien. Later introduceerde hij ook *relais*, maar omdat ik als negenjarige niet fundamenteel kon begrijpen hoe die werken, weigerde ik daarmee aan de gang te gaan. Mijn broer had hier beduidend minder moeite mee; hij is ingenieur geworden en ik wetenschapper. Met mijn zus is het, ondanks het gebrek aan elektronica, toch nog goed gekomen, zij is werktuigbouwkundige geworden. Het is jammer dat wij vandaag niet in gebouw Meander van de Universiteit Twente zitten, want daar heeft zij de sprinklerinstallatie van ontworpen.

Het lijkt vanzelfsprekend om Informatica te gaan studeren, als je uit zo'n familie komt. Maar dat is niet zo. Ik heb ook hard overwogen om Frans, of Culturele Antropologie te gaan doen. Informatica was voor mij een uitgestelde keuze. Informatica is overal, dacht ik, dus als ik dat nou ga doen, kan ik altijd nog kijken welk toepassingsdomein mij het meeste aanspreekt. Daarom ging ik aan de Radboud Universiteit studeren, een brede universiteit. En dat ik daarbij op kamers moest, was een bijkomend voordeel. Later in mijn studie maakte ik de keuze voor Wiskunde & Informatica, weer omdat ik vond dat ik informatica niet fundamenteel kon begrijpen zonder wiskunde.

2. NO RISK, NO FUN

Maar nu naar risicomanagement.

Regelmatig worden we geconfronteerd met ongelukken van high-tech systemen. Denk bijvoorbeeld aan het dramatische ongeluk met de stint in Oss begin september. Vorige maand moest de Sojoez-raket een noodlanding maken omdat één van de motoren niet meer functioneerde. In maart reed een zelfrijdende auto van Uber een voetganger dood, waarop Uber besloot daarop zijn testprogramma voor zelfrijdende auto's te stoppen. Deze zomer was er stroomstoring op Schiphol doordat de noodstroomvoorziening niet werkte. Schiphol moest er zelfs tijdelijk door sluiten; het was een enorme chaos.

Hier geldt echter: *no risk, no fun.* Nieuwe technologie, zoals stints, zelfrijdende auto's, robots, 3D printers, komt inherent met risico's. Sterker nog, voor bedrijven is het vaak riskanter om niet te innoveren, omdat zij dan door de concurrentie weggeïnnoveerd worden - denk aan V&D.

Maar hoe moet dat dan wel, het managen van de risico's van high-tech systemen? Dat is de leeropdracht die ik met mijn ambt als hoogleraar aanvaard. De kern van het antwoord ligt in het gecalculeerd nemen van risico's. Ik zeg bewust *gecalculeerd,* want ik wil vandaag een pleidooi houden om risico's zo systematisch, transparant en kwantitatief mogelijk te benaderen.

Figuur 3a: Wereldwijde risico's naar kans en impact

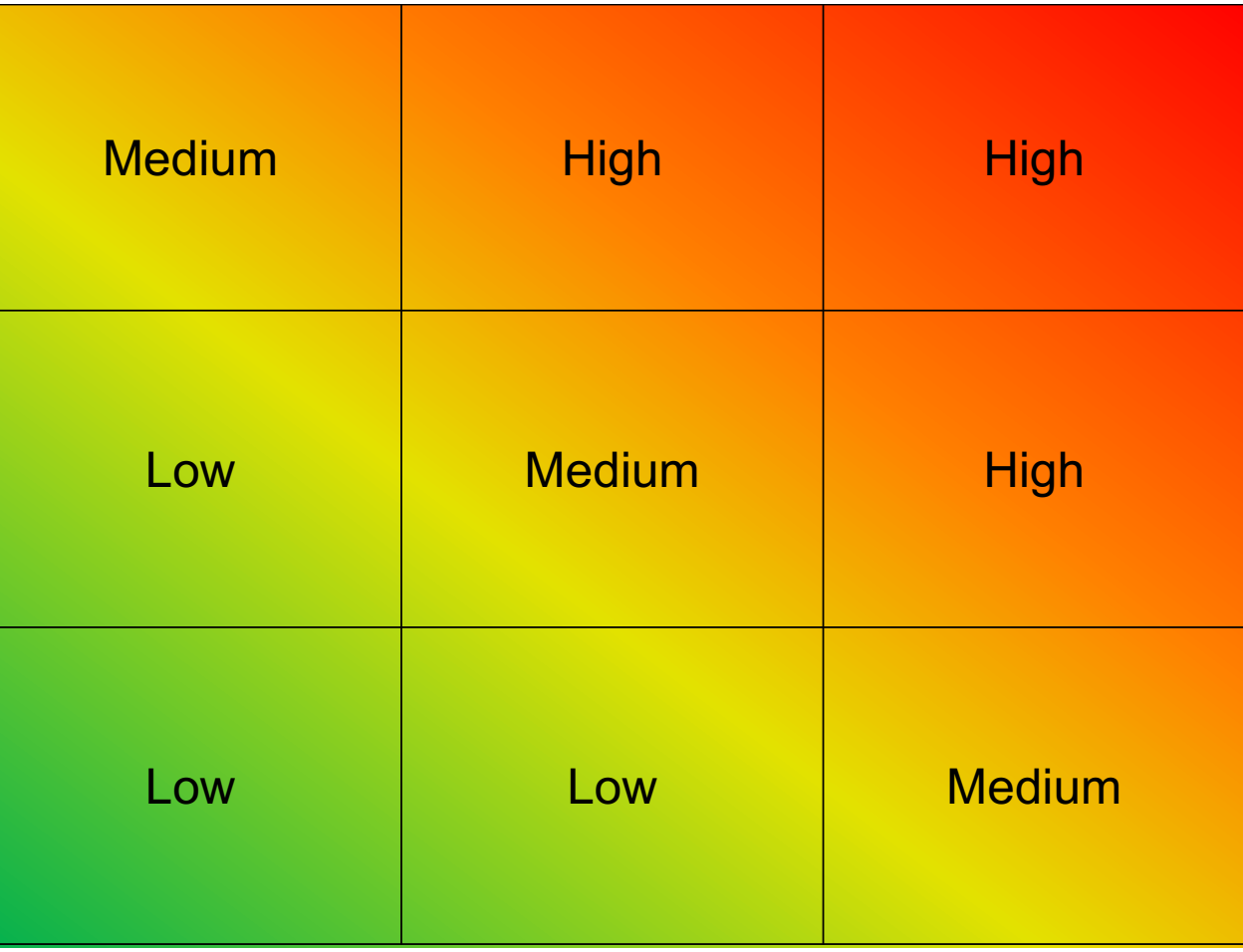
3. RISK HAPPENS

Je zou, door de aanhoudende nieuwsberichten over rampen en ongelukken, de indruk kunnen krijgen dat we in onveilige tijden leven. Dat is echter niet zo; sterker nog, we leven in veiliger tijden dan ooit. Dit is duidelijk terug te zien in de statistieken: we leven langer en er zijn aantoonbaar minder ongelukken. Het leuke is dat u veel van dit soort gegevens zelf kunt opzoeken, onder andere bij het Centraal Bureau voor de Statistiek[1] en via de Risicoatlas[2].

Maar waar moeten we dan wel bang voor zijn? Dat is uitgezocht door het World Economic Forum, in zijn jaarlijkse *Global Risk Report*[3]. Hierin worden wereldwijd de belangrijkste risico's geïdentificeerd en uitgezet naar waarschijnlijkheid en impact. Dit zien we in Figuur 3a. Hoewel de gevolgen van klimaatveranderingen (groene punten) het hoogst scoren, zien we ook dat technologische risico's (paars) een prominente plaats innemen. Opvallend genoeg wordt *Failure of Critical Infrastructure* gezien als economisch risico, terwijl ik dat als technologisch zou classificeren. Daarnaast laat het *Global Risk Report* zien dat technologische risico's sterk verweven zijn met andere risico's zoals werkloosheid, terroristische aanslagen en natuurrampen. De uitdaging voor het beheersen van technologische risico's ligt volgens het World Economic Forum in het omgaan met de afhankelijkheden tussen systemen:

> *Humanity has become remarkably adept at understanding how to mitigate countless conventional risks that can be relatively easily isolated and managed with standard risk management approaches. But we are much less competent when it comes to dealing with complex risks in systems characterized by feedback loops, tipping points and opaque cause-and-effect relationships that can make intervention problematic.*

Het goed in kaart brengen van afhankelijkheden tussen risico's, zoals feedbackloops, is typisch iets waarmee mijn leerstoel zich bezighoudt: het ontwikkelen van geschikte risicomodellen die oorzaak-gevolgrelaties zo goed mogelijk in kaart brengen en zo inzicht geven in zaken als *tipping points*.


Medium
High
High
Low
Medium
High
Low
Low
Medium

4. WAT IS RISICO?

Er bestaan vele definities van het begrip risico[4]. Hun gemeenschappelijke deler is dat risico twee belangrijke ingrediënten heeft:

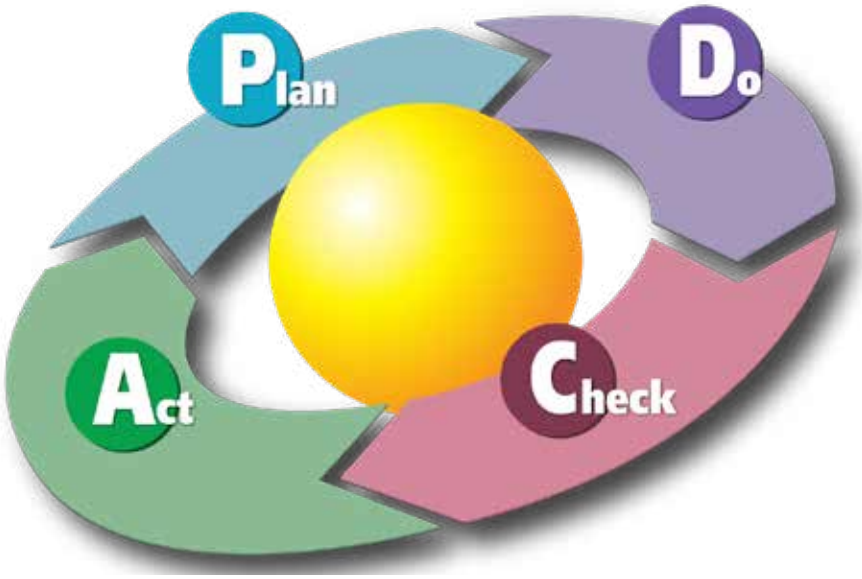
- negatieve impact
- onzekerheid

Positieve gebeurtenissen noem je geen risico. Je loopt niet het risico om de loterij te winnen. Economen zullen zeggen dat je *opportunities* juist wel moet meenemen als onderdeel van risico, maar dat ligt voor high-tech systemen minder voor de hand. Daarnaast gaat risico inherent gepaard met onzekerheid. Als je zeker weet dat iets gaat gebeuren (we gaan bijvoorbeeld allemaal dood), dan is het ook geen risico.
Een eenvoudig hulpmiddel om risico's te visualiseren is de zogenaamde *risico-hittekaart* [5]. Hierin wordt de kans op een negatieve gebeurtenis afgezet tegen de impact daarvan, zoals weergegeven in de figuur links. Risicomanagement[7] draait om het nemen van effectieve maatregelen om risico's zo veel mogelijk te beheersen. Globaal gezien zijn er vier risicostrategieën:

Vermijden. Allereerst kun je het risico mijden: je besluit om de Mount Everest niet te beklimmen, of stopt de ontwikkeling van zelfrijdende auto's. Je mist dan natuurlijk ook de *fun*, maar soms is dit een goede beslissing. Ook het besluit van minister Van Nieuwenhuizen om stints te verbieden op de openbare weg is risicomijding. Mijn vraag hierbij is vooral of geschikte risicomaatregelen zouden kunnen leiden tot een heroverweging van dit besluit[6].
Accepteren. Een tweede manier is om risico's te accepteren en budget vrij te maken om de negatieve gevolgen te dragen. Bij contactloos pinnen wordt er geen pincode vereist. Het maximale bedrag is echter maar 25 euro per dag.
Overdragen. Ten derde kun je risico's overdragen aan derden. Verzekeraars nemen de financiële schade over bij diefstal of brand.
Reduceren. Tenslotte kun je risico's reduceren. Dat kan op twee manieren, die eigenlijk neerkomen op voorkomen of genezen. We kunnen de kans verlagen dat een gebeurtenis optreedt. Daarom zijn rijbewijzen verplicht en is appen in het verkeer verboden. We kunnen ook de impact van een event verkleinen. Autogordels en airbags verlagen niet de kans op een ongeluk, maar wel de gevolgen daarvan.

De onzekere factor van het begrip risico maakt het kiezen van de juiste risicostrategie en bijbehorende maatregelen tot een ingewikkelde kwestie. Vandaag wil ik een pleidooi houden om risicomanagement meer *accountable* te maken, dat wil zeggen:

- *systematisch,* zodat we geen relevante zaken over het hoofd zien.
- *transparant,* zodat aannamen en keuzes de risicobeslissingen expliciet zijn.
- *kwantitatief,* onderbouwd met cijfers.


Plan
Do
Act
Check

5. RISICOMANAGEMENT: OMDAT HET KAN, NIET OMDAT HET MOET

Goed risicomanagement begint bij de risicomanagementcyclus[5]. Deze cyclus is in de jaren '50 bedacht door de Amerikaanse statisticus William Demming, en wordt ook wel de *Plan-Do-Check-Act* cyclus genoemd, naar de stappen waaruit deze cyclus bestaat:

- *Plan:* Stel de doelstellingen vast, en maak een actieplan.
- *Do:* Voer de geplande acties uit.
- *Check:* Evalueer de resultaten ten opzichte van de geformuleerde doelstellingen.
- *Act:* Stel het proces bij aan de hand van de gevonden resultaten.

Deze stappen worden iteratief doorlopen totdat de check fase aangeeft dat de doelstellingen bereikt zijn. De cyclus is terechtgekomen in diverse internationale risicostandaarden, zoals de 31000 standaard[8] van het Internationale Standaardisatiecommittee ISO. Mijn onderzoek gaat vooral over *Check* en *Act*: Voldoet een systeemontwerp aan de gewenste betrouwbaarheidseisen, en zo nee, welke verbeteringen kunnen we in het ontwerp aanbrengen?

Goed risicomanagement betekent dat de Demming-cyclus diep geïntegreerd is binnen de levenscyclus van een product, ook wel de *system's engineering life cycle* genoemd. De levenscyclus beschrijft de verschillende fasen in de ontwikkeling van een product: In de Vereistenfase wordt het de gewenste functionaliteit vastgesteld; in de Ontwerpfase wordt een ontwerp gemaakt om deze functionaliteit te realiseren; binnen de Implementatiefase wordt het product geproduceerd; en in de Testfase wordt het getest. Tenslotte wordt het in gebruik genomen.

Het woord product moet hier ruim worden opgevat. Of je een product, dienst, proces, of een missie ontwikkelt, de risicomanagement principes zijn dezelfde. Binnen iedere stap in de levenscyclus moet de PDCA-cyclus doorlopen worden. In de vereistenfase komen bijvoorbeeld financiële en marktrisico's aan bod; in de implementatiefase fabricagefouten, of het niet halen van planningen.

Veel organisaties worstelen met risicomanagement: risicoprocessen zijn niet goed verankerd, of taken en verantwoordelijkheden niet goed belegd. Te vaak worden risicoanalyses gedaan omdat het moet, ofwel van de wetgever, ofwel om een bepaalde certificering te krijgen. Dit vind ik een bijzonder slecht idee: risicoanalyse wordt daarmee een doel, in plaats van een middel. Ik pleit voor risicoanalyses *omdat het kan:* omdat je ongelukken kunt voorkomen, omdat de productiviteit omhoog kan, omdat klanten tevreden zijn als producten voldoen aan hun wensen.


IK51070.51

6. RISICOMAATREGELEN

Ook in het dagelijks leven nemen we veel risicomaatregelen. Hoe zorg je er bijvoorbeeld voor dat je vakantie veilig en aangenaam verloopt? Een belangrijk principe hierbij is om systemen weerbaarder te maken tegen storingen. Problemen of storingen op onderdelen zijn vaak niet te voorkomen. Het is dan zaak te voorkomen dat zulke problemen zich doorvertalen naar storingen op systeemniveau. Merk op dat deze maatregelen de *impact* verlagen van een storing op componentniveau, maar de *kans* verlagen op een storing op systeemniveau. De risicohittemap uit Paragraaf 4 is da nook niet zo handig is voor het visualiseren van samengestelde risico's. Enfin, ik loop een aantal maatregelen met u door.

Redundantie wil zeggen dat sommige onderdelen dubbel en soms nog vaker, worden uitgevoerd. Op vakantie nemen wij altijd twee telefoons mee. Is er één kapot is, of is de batterij leeg, hebben we de andere nog. Een speciale vorm van redundantie zijn *reserveonderdelen,* zoals het reservewiel in je auto. Redundantie is echter niet bestand tegen zogenaamde *common cause failures,* storingen door gemeenschappelijke oorzaken. Als er geen netwerkverbinding is, dan helpt dat extra mobieltje niet. In dat geval is *diversificatie* handiger, een echt andere implementatie van je onderdeel. In dit kader is het verstandig om je bankpas en creditcard op een andere plek te bewaren; dan zijn ze beter bestand tegen de *common cause* diefstal. *Fail-safe mechanismen* zorgen ervoor dat als een systeem faalt, deze in een veilige toestand terecht komt. Zo maken vluchtstroken langs de snelweg het mogelijk om je auto veilig te parkeren als er zich een probleem voordoet. Daarnaast is *onderhoud* essentieel om je auto in goede conditie te houden. *Noodprocedures* zijn belangrijk om in te grijpen als er toch onverwacht iets misgaat. Als je onverwacht strandt, helpt de ANWB pechhulp je weer op weg. Veel van deze maatregelen vragen om *detectie* van een storing. Als je reservewiel het ongemerkt begeven heeft, dan helpt deze noodmaatregel niet als je met een lekke band zit. Daarom zijn auto's uitgerust met allerlei waarschuwingslampjes, maar ook *periodiek testen* helpt.

Dit zijn weliswaar huis-tuin-en-keukenvoorbeelden, maar 'in het echt' gaat het precies zo. In datacentra zijn bijvoorbeeld de servers, netwerkkabels en airconditioning dubbel of tripel redundant. Redundante servers worden niet in hetzelfde *rack* geïnstalleerd en soms zelfs op een andere locatie, een vorm van diversificatie. Ook hebben datacenters een noodstroomvoeding, zodat ze bij een stroomstoring blijven functioneren. Noodprocedures kunnen inhouden dat er bij calamiteiten extra servers 'in de cloud' worden ingehuurd, bijvoorbeeld bij Amazon.

7. RISICOPERCEPTIE

Risicomanagement draait om het nemen van beslissingen: welke van de vele mogelijke maatregelen gaan we implementeren om bijvoorbeeld zelfrijdende auto's veilig te krijgen? Moeten we stints toelaten op de openbare weg? Kiezen we wel of niet voor kernenergie? Wat is de juiste onderhoudsstrategie voor infrastructuur zoals tunnels en bruggen? Hoe kunnen we de gevolgen van klimaatveranderingen beperken?

De onzekere factor van het begrip risico maakt nemen van goede beslissingen lastig. Wellicht daarom worden veel risicobeslissingen *ad hoc* genomen, op basis van intuïtie. Dit vind ik onverstandig, want mensen zijn notoir slecht in het inschatten van risico's. Ze zijn bijvoorbeeld bang om te vliegen, maar appen rustig op de fiets.

Risicoperceptie is goed onderzocht, onder anderen door Nobelprijswinnaar Daniel Kahneman[13]. Uit zijn talloze experimenten blijkt keer op keer hoe slecht mensen kansen en risico's kunnen inschatten. Volgens Kahneman zijn er twee systemen in onze hersenen aan het werk: Systeem I dat snel, en automatisch beslissingen neemt en Systeem II dat langzaam, systematisch en rationeel is. Systeem I is handig als we objecten moeten lokaliseren, of gezichtsuitdrukkingen moeten interpreteren, maar is niet geschikt voor het inschatten van kansen. Dat kunnen we beter aan Systeem II overlaten.


OVER HERE
NO, THIS WAY

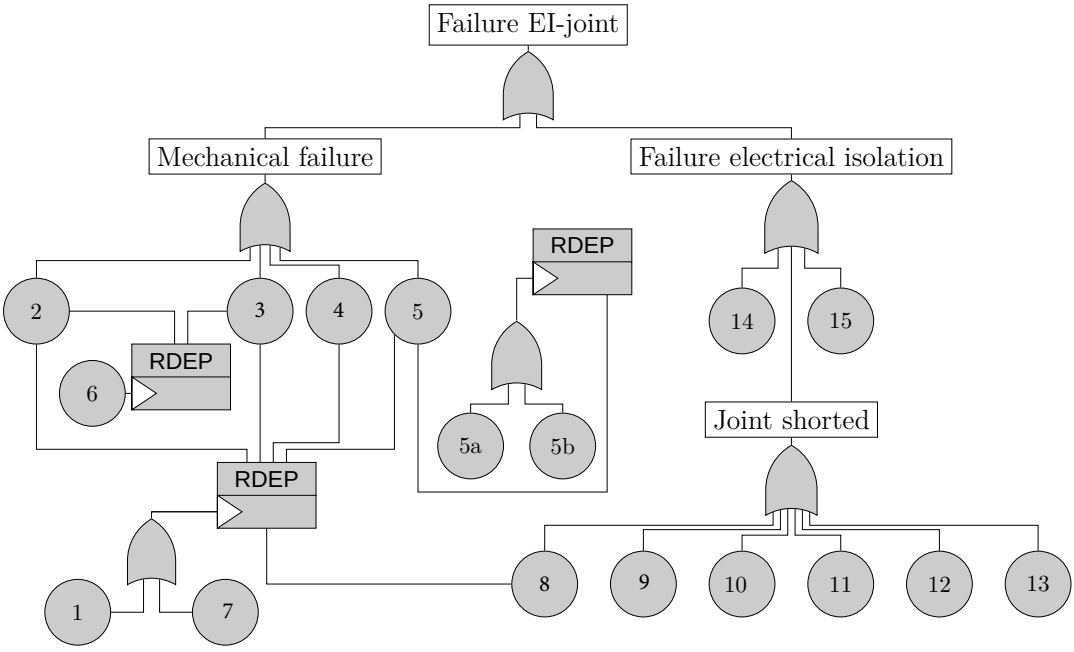
8. RISICOBESLISSINGEN

Kahnemans's bevindingen zijn een pleidooi voor het gebruik van risicomodellen. Deze modellen verleiden ons om Systeem II in te zetten, door complexe risico's systematisch uiteen te rafelen in deelrisico's, en achterhalen zo de grondoorzaken en factoren die het risico beïnvloeden. Ook kunnen zij afhankelijkheden tussen risico's in kaart brengen.

Mijn onderzoek richt zich op het ontwikkelen van bruikbare risicomodellen om beslissingen ondersteunen: modellen waarmee risicoanalisten goed uit de voeten kunnen, die inzichten geven in hoe risico's ontstaan, welke factoren eraan bijdragen, en hoe risico's samenhangen. Vervolgens kunnen we uitrekenen welke risicomaatregelen het beste scoren ten opzichte van relevante criteria.

Ik noem een aantal voorbeelden van eerder onderzoek waarin ik, samen met collega's, risicomodellen vruchtbaar heb toegepast.

- Een consultancybureau wilde weten of het verstandig was om, gezien hun verwachte groei, met hun webservice in de cloud te gaan. Met onder andere Anne Remke heb ik berekend dat dit niet nodig was, aangezien de bottleneck lag in de netwerkverbinding.
- De Nuclear Research Group wilde weten wat de optimale strategie was voor het in voorraad houden van reserveonderdelen[24]. Conclusie: de huidige strategie voor realiseert de veiligheidsvereisten van het systeem.
- Met collega's van Psychologie heb ik de risico's van digitale communicatie voor slachtoffer-daderbemiddeling onderzocht, en vervolgens het meest geschikte communicatiemiddel geselecteerd.
- Met NS en ProRail heb ik gerekend aan onderhoudsstrategieën voor het spoor- en treinenonderdelen, en een kosten-batenanalyse gemaakt[20,23].



Figuur 9. Foutenboom van de elektrische scheidingslas

9. FOUTENBOMEN

Laten we naar een voorbeeld kijken. De linker pagina toont een risicomodel, een zogenaamde foutenboom,[17,18], dat ik samen met mijn promovendi en experts van ProRail heb ontwikkeld[20] voor de elektrische scheidingslas. Deze lassen worden gebruikt voor treindetectie: zij sturen een elektrisch signaal via de rails. Als er een trein op een baanvak staat, dan ontstaat er via de wielen van de trein een gesloten circuit, waardoor dit signaal gedetecteerd kan worden. Scheidingslassen zijn belangrijk om te voorkomen dat er twee treinen hetzelfde baanvak bezetten.

Ons risicomodel pelt systematisch de risico's van de scheidingslas af: we zien dat deze scheidingslassen op twee manieren kunnen falen, namelijk ofwel door een mechanische storing, ofwel door een storing in de elektrische geleiding. Beide manieren worden verder uiteengerafeld in verdere oorzaken: Mechanische oorzaken, met nummer 1 tot 7, zijn bijvoorbeeld gebroken bouten, platen of lijm. Electrische faaloorzaken, genummerd 8 tot 13 zijn onder andere splinters op de rails.

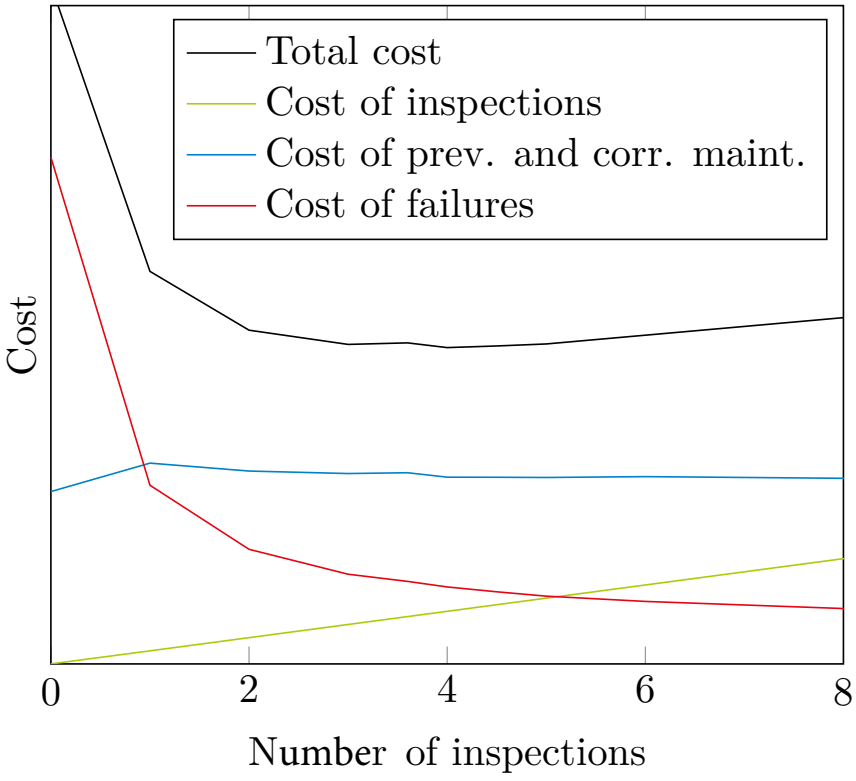
Een belangrijk fenomeen dat onze modelering expliciteert is dat bepaalde storingen andere storingen versnellen. Dit is in de foutenboom weergegeven met RDEP-blokken: ingaande lijnen (bij de witte driehoek) zijn versnellende factoren voor de uitgaande lijnen (bij het grijze gedeelte). Slijtage aan de spoorkop (faaloorzaak 4 in de figuur links) versnelt het afbreken van bouten en de spoorkop (oorzaken 2 en 6 in de figuur).

10. MODELLEN EN DATA

Foutenbomen zijn in de jaren zestig van de vorige eeuw ontwikkeld door Boeing[29]. Tegenwoordig worden ze veelvuldig toegepast in de high-tech industrie, door bedrijven als Shell, Siemens, Airbus, Tesla, NS, Rijkswaterstaat, ESA en NASA. Huidig onderzoek richt zich vooral op het analyseren van krachtigere versies van foutenbomen, die onder andere het dynamisch gedrag beter in kaart brengen.

Een andere belangrijke ontwikkeling is het automatisch leren van modellen uit data, door middel van technieken uit de artificiële intelligentie. Risicomodellen worden nu veelal met de hand gemaakt. Van de ene kant is dat een kracht: het maken van een model levert belangrijke inzichten in systeemrisico's. *The journey is the destination,* kun je zeggen. Van de andere kant is het maken van modellen ook erg tijdrovend.

Om dit proces te vergemakkelijken wordt er veel onderzoek gedaan naar het automatisch genereren van modellen met behulp van technieken uit de artificiële intelligentie: als we heel veel gegevens hebben over systeemstoringen, kunnen we dan automatisch een model afleiden dat dit storingsgedrag beschrijft? In een mooie samenwerking met RU en UT collega's[22] hebben we automatisch foutenbomen geleerd op basis van (synthetische) storingsgegevens. De eerste resultaten zijn veelbelovend: we kunnen accurate foutenbomen leren, die goed matchen met de data. Waar ik naar toe wil is een goede combinatie tussen handmatig gecreëerde modellen, en geleerde modellen. De risicoanalist kan een schematisch model opstellen met de belangrijkste faalmechanismen, en algoritmen kunnen dit verder verfijnen, bijvoorbeeld door faalfactoren te achterhalen. Het zou bijvoorbeeld heel mooi zijn als de versnellende factoren die wij met RDEPs hebben gemodelleerd automatisch uit data zouden kunnen worden afgeleid.



Figuur 11: Onderhoudskosten als functie van het aantal inspecties

11. REKENEN AAN RISICO'S

Heb je eenmaal een risicomodel, dan kun je diverse vragen beantwoorden, zowel kwalitatief als kwantitatief. Kwalitatieve analyses richten zich op het achterhalen van kritische componenten en kwetsbare plekken in een systeem.

Kwantitatieve analyses richten zich op het berekenen van betrouwbaarheidsmetrieken [25]. Deze *key performance indicatoren* aangeven hoe goed een systeem scoort op diverse betrouwbaarheidscriteria. Inzicht in zulke metrieken is bijzonder nuttig bij het nemen van beslissingen: door verschillende maatregelen of ontwerpalternatieven te scoren op relevante metrieken, kunnen we achterhalen welke het meest (kosten-)effectief zijn.

Bekende betrouwbaarheidsmetrieken zijn:

- De *betrouwbaarheid,* ook *bedrijfszekerheid* genoemd, is de kans dat een systeem faalt tijdens zijn missietijd. De kans dat een kerncentrale faalt mag bijvoorbeeld maar 10^{-12} zijn.
- De *beschikbaarheid*, of *uptime,* is het gemiddelde percentage van de tijd dat het systeem functioneert. Datacentra kunnen hun klanten bijvoorbeeld een uptime van 99 procent garanderen.
- De *mean-time-to-failure* is de gemiddelde tijd tussen twee storingen.

Voor ProRail heb ik gekeken naar het effect van het aantal inspecties op de betrouwbaarheid van de elektrische scheidingslas: Tijdens inspecties controleert onderhoudspersoneel het spoor op gebreken, zoals gebroken bouten ---precies die gebreken die in de foutenboom staan. Als er gebreken worden geconstateerd, worden deze gerepareerd. Inspecties zijn nuttig, maar ook duur. Een belangrijke afweging is daarom hoeveel inspecties nodig zijn. Dit hebben wij voor ProRail uitgerekend, middels de eerder getoonde foutenboom, waaraan we inspectiemodellen en hun kosten hebben toegevoegd. Het resultaat van deze analyse ziet u op de linker pagina. Deze grafiek laat de verwachte onderhoudskosten zien als functie van het aantal inspecties. We onderscheiden hier kosten van inspecties zelf (groen), kosten van onderhoudsacties (blauw) en kosten van storingen (rood) en totale kosten (zwart). Als we geen inspecties doen, dan zijn de inspectiekosten laag, maar de storingskosten hoog. Doen we meer inspecties, dan nemen de storingskosten af en de inspectiekosten toe. Het optimum ligt rond de drie inspecties.

Met vergelijkbare methoden gerekend aan het onderhoudsmodel voor treincompressoren[23] en aan reserveonderdelen[24].

12. HET WISKUNDIG HART VAN RISICOANALYSES

Om te rekenen aan risico's moet je gebruik maken van kanstheorie. De definitie van risico zelf is gestoeld op kansen en ook de eerdergenoemde metrieken zijn kanstheoretische begrippen: de betrouwbaarheid is gedefinieerd als de *kans* dat een systeem faalt binnen zijn missietijd; en de beschikbaarheid is het is het gemiddelde, dus de *verwachtingswaarde* van de tijdsduur dat een systeem operationeel is; de mean-time-to-failure is de verwachtingswaarde van de tijdsduur tussen twee storingen.

Een van de meest prominente historische beschrijvingen van het begrip risico, het boek *Against the Gods, the remarkable story of risk*[26] van de bekende financieel econoom Peter Bernstein zegt hierover:

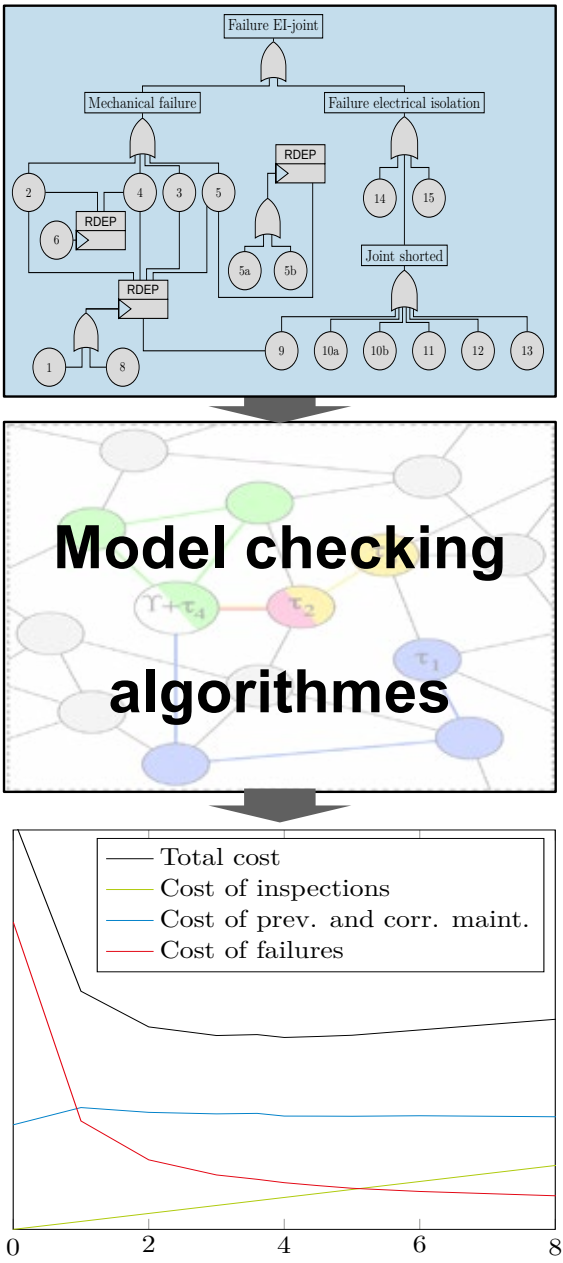
> *Probability theory is an instrument for organizing, interpreting and applying information. As one genius idea was piled on top of another, quantitative techniques of risk management have helped trigger the ideas of modern times.*

Kanstheorie is daarmee het wiskundig hart van de risicoanalyse; het is het instrument waarmee we de storingskansen van de elektrische scheidingslas kunnen uitrekenen.

Kanstheorie is niet bij iedereen populair. Uitgebreide risicoberekeningen hebben de financiële crisis van 2008 niet kunnen voorkomen, en het kernongeval bij Fukushima ook niet. Echter, het feit dat risicoberekeningen niet alle problemen heeft kunnen voorkomen, wil niet zeggen dat daarmee een waardeloos instrument is. Zoals Bernstein zegt:

> *Without the command of probability theory and other instruments of risk management, engineers could never have designed the great bridges that span our rivers, [..] polio would still be maiming children, no airplanes would fly, and space travel would just be a dream.*

Wel moeten we beter omgaan met kanstheorie: overzichtelijkere modellen maken, meer inzicht geven in hoe berekeningen tot stand komen, en vooral objectieve data verzamelen waar dat kan, en werken met subjectieve inschattingen waar dat moet.


Failure EI-joint
Mechanical failure
Failure electrical isolation
RDEP
RDEP
RDEP
Joint shorted
1
2
3
4
5
5a
5b
6
8
9
10a
10b
11
12
13
14
15
Model checking
algorithmes
Total cost
Cost of inspections
Cost of prev. and corr. maint.
Cost of failures
0
2
4
6
8

13. STOCHASTISCH MODELCHECKEN

Een van de problemen die zich voordoet als je een systeem met veel afhankelijkheden wil doorrekenen is dat de kanstheoretische analyse ingewikkelder wordt. Moderne, dynamische foutenbomen hebben extra modeleringskracht om deze afhankelijkheden te modeleren, maar worden door sommingen gezien als computationeel onmogelijk. Twee recente artikelen[30,31] uit prominente tijdschriften zeggen hierover:

> *Although DFTs are powerful in modeling systems with dynamic failure behaviors, their quantitative analyses are pretty much troublesome, especially for large scale and complex DFTs.*

> *Although many extensions of fault trees have been proposed, they suffer from a variety of shortcomings. In particular, even where software tool support exists, these analyses require a lot of manual effort.*

Ik wil deze beweringen hier graag ontkrachten. Recent onderzoek, van mijzelf maar ook van Joost-Pieter Katoen, heeft laten zien dat we wel degelijk industriële dynamische foutenbomen kunnen doorrekenen die risico's modeleren van bijvoorbeeld zelfrijdende auto's, spoorwegen, en ruimtevaartmissies[27,28].
Dit is mogelijk door gemaakt de inzet van moderne kanstheorie, te weten stochastisch model checken. Deze techniek is een vruchtbare combinatie van twee andere krachtige technieken, te weten modelchecken en kansrekening, ofwel stochastiek.
Veel systemen bestaan uit toestanden en overgangen tussen deze toestanden, ook wel *transities* genoemd; we noemen deze systemen dan ook *transitiesystemen*. Een component kan bijvoorbeeld in twee toestanden zijn: operationeel, of kapot. Tijdens de levensduur kan een component van toestand veranderen: eerst is hij operationeel en vervolgens is hij kapot. Wordt dit component gerepareerd, dan kan hij weer operationeel worden. Modelchecken analyseert zulk soort systemen en wordt veel toegepast door hardware-fabrikanten om nieuwe chips door te rekenen op fouten. De kracht van deze techniek is dat zij snel en krachtig is en wiskundig heel goed onderbouwd, met wortels in de wiskundige logica en modeltheorie. Daarom hebben ook de uitvinders van deze techniek de prestigieuze ACM Turing award ontvangen in 2013.
Bij stochastisch modelchecken kennen we kansen toe aan toestandsovergangen. Stel een component heeft een storingskans van 1/10 per week. Repareren kost ook 1 week. We kunnen dan de beschikbaarheid van het systeem, dus de gemiddelde tijd dat het systeem in de operationele toestand uitrekenen. In dit geval is dat 10/11: gemiddeld gaat het systeem eens per 10 weken kapot. Het duurt 1 week om het te repareren. Het is dus 10 van de 11 weken beschikbaar. Als er twee van zulke componenten zijn en er maar één reparateur is, dan wordt het al ingewikkelder. Stochastisch modelchecken heeft krachtige methoden ontwikkeld om dit soort systemen te analyseren.

14. BOUWBLOKKEN VOOR RISICOMODELLEN

Behalve met lampjes heb ik als kind natuurlijk ook veel met LEGO gespeeld. De reden dat LEGO zo'n geweldig speelgoed is, heeft te maken met een eigenschap die wij informatici vangen in de term: *compositionaliteit*. Compositie betekent samenstellen, met andere woorden je kunt uit kleine basisblokken heel grote modellen bouwen.
Het leuke van stochastisch modelchecken is dat je grote kansmodellen kunt opbouwen uit kleine kansmodellen. Dat is erg prettig. Als ik van een risicomodel een kansmodel moet opstellen, dan hoef ik dat niet in één keer te doen, maar ik maak voor elk onderdeel uit mijn risicomodel een klein kansmodel. Vervolgens stel ik deze samen tot een groot kansmodel voor mijn risicomodel. Als ik twee componenten heb en één reparateur maak ik dus drie modellen. Als ik een foutenboom heb, dan maak ik voor alle cirkels en blokken een eigen kansmodel.
Het bouwen van grote modellen uit kleine onderdelen heeft meerdere voordelen:

- *Begrijpelijkheid:* het snappen van één groot model is veel lastiger dan het snappen van kleinere componentenmodellen.
- *Flexibiliteit:* als er één onderdeel van je model verandert, dan hoeft alleen dat onderdeel aangepast te worden. Om in LEGO-termen te blijven: een ander dak op een LEGO-huis is geen probleem, op een huis van klei is dat veel moeilijker.
- *Rekenkracht:* op kleine componenten zijn berekeningen sneller, en soms kun je deze resultaten direct doorvertalen naar het hele systeem.

Daarnaast heeft stochastisch modelchecken een arsenaal aan technieken ontwikkeld om snel stochastische systemen door te rekenen.

- *Snelle algoritmen.* De basis van snelle rekenkracht zijn slimme algoritmen om allerlei kansen uit te rekenen over kansmodellen gegeven als transitiesystemen met kansen.
- *Reductie.* Kansmodellen van realistische systemen zijn enorm groot; vaak zijn er meer toestanden dan elementaire deeltjes in het heelal. Reductietechnieken vereenvoudigen grote modellen tot kleine modellen die dezelfde resultaten opleveren. Vergelijk dit met het vereenvoudigen van expressies: $3x-5y+y+6x = 9x-4y$.
- *Uitdrukkingskracht.* Omdat het opstellen van kansmodellen lastig kan zijn, zijn er diverse talen ontwikkeld om deze modellen op te schrijven, zeg maar programmeertalen voor kansmodellen. Datzelfde geldt voor de metrieken die je wil uitrekenen, ook daar zijn handige talen voor om die op te schrijven, waardoor je ook je eigen metrieken kunt definiëren.

Al met al kun je stochastisch model checken zien als een handige toolbox met vele gereedschappen om berekeningen te kunnen doen. Om de industriële foutenbomen door te rekenen, heb je ze allemaal nodig.


My BFF Rocks
Love is Selfless. Always have loving hearted and Reflectful
Accept all the things that life gives you be adorable towards your life. If you can't argue with the stealth don't do it with life.
- (ARZOO)
Live Young!
Life is So awesome Just change the way you see it.
Aditya
KISS
Keep It Simple
Set Fire to the world with your brokenness.
Please Spread the message of gender neutrality all over the world
I Love my Mother
Believing favorites the brave Go, Be Brave!
Ranjhan (RD) (KAJU)
CA Piyush
9531134219

15. SLOTOPMERKINGEN

Modelmatig werken maakt dat we Systeem II gaan inzetten en niet Systeem I. Enkele opmerkingen zijn wel op zijn plaats.

Ten eerste zijn modellen een versimpelde weergave van de werkelijkheid, en bevatten daarom onherroepelijk omissies en onjuistheden. Risicomodelering is geen Newtoniaanse mechanica dat precies voorspelt wat er gaat gebeuren, maar een hulpmiddel om beslissingen te nemen. Dit wordt mooi samengevat door de Amerikaanse statisticus G.E.P. Box:

All models are wrong, and some are useful.

Model-gebaseerde risicoanalyses zijn uiteraard geen wondermiddel. In het bijzonder zijn ze geen antwoord op de zogenaamde Zwarte Zwanen: onvoorspelbare gebeurtenissen met een enorme impact[35]. Zwarte zwanen kunnen niet voorspeld worden, dus ook niet door modellen. Daarom is een goede risicoanalyse altijd een combinatie van systematisch nadenken en out-of-the-box analyses.

Tenslotte is er de paradox rond risicokwantificatie. Van de ene kant is het kwantificeren van risico's bijzonder lastig en haast onmogelijk; van de andere kant zijn alle risicobeslissingen kwantitatief *by nature*. Er moet beslist worden welk budget er besteed gaat worden, en aan welke maatregelen. Daarom is kwantificatie onvermijdelijk. We moeten er niet voor vluchten omdat het moeilijk is. Als er geen objectieve gegevens beschikbaar zijn, dan moeten we met subjectieve inschattingen werken. Hiervoor zijn goede methoden ontwikkeld, zoals Bayesiaanse statistiek. Waar het om gaat is, dat er op basis van de beschikbare informatie de beste beslissing genomen wordt. Ik vind dat dat het beste lukt door systematisch, transparant, en kwantitatief te werk te gaan.

16. WHAT'S NEXT?

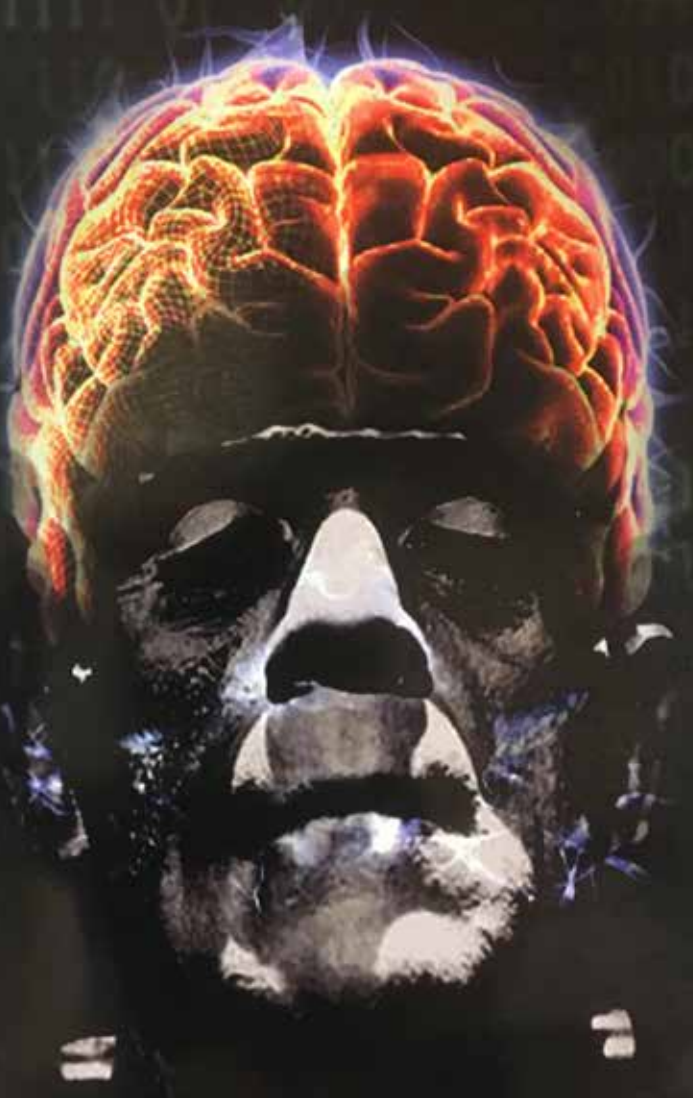
Welke richting gaat het onderzoek in risicomanagement op? Ik noem een aantal ontwikkelingen.

Van risico naar resilience. Eigenlijk is risicomanagement alweer uit; het nieuwe buzzword is *resilience,* veerkracht. Resilience richt zich vooral op risicoreductie door de impact van ongewenste gebeurtenissen te verlagen, ongeacht hun (on)waarschijnlijk. Stel dat er een jaar geen regen valt, of geen wind is, wat betekent dat dan? Uiteraard zie ik goede mogelijkheden voor de inzet van risicomodellen hier. Juist omdat onze risicoanalyses modulair manier zijn opgebouwd, is het heel goed mogelijk om resilience-scenario's als extra component toe te voegen aan onze modellen, of deze te combineren met agent-models.
Predictive maintenance: Een ander cruciaal thema is *predictive maintenance*, voorspellend onderhoud. Sensoren kunnen allerlei metingen doen aan de conditie van het systeem, zoals de vorming van haarscheuren door trillingen. Met big data analyse kunnen we storingen beter voorspellen, en onderhoud doen precies wanneer het nodig is; idealitair net voordat een component kapot dreigt te gaan. McKenzie ziet predictive maintenance als een van de meest veelbelovende toepassingen van het Internet-of-Things, met een totale economische waarde van meer dan 63 biljoen op jaarbasis. Om dit potentieel te benutten, zijn nog wel wat hobbels te nemen, onder andere rond de schaalbaarheid van algoritmen, maar ook rond het goed integreren van de veschillende optimalisatiestappen in de maintenanceketen.
Integratie van safety en security. Ik heb vandaag vooral gesproken over veiligheid, *safety.* Security, moedwillige aanvallen door hackers, is echter net zo belangrijk. Het probleem is dat safety en security elkaar vaak in de weg zitten: maatregelen die de safety verhogen, verlagen vaak de security. Het Internet-of-Things biedt goede mogelijkheden om de veiligheid van systemen te monitoren. Echter, met zijn vele accesspoints biedt het Internet-of-Things ook veel kansen aan hackers om binnen te dringen. Een integrale aanpak van safety en security is daarom een belangrijk onderwerp voor toekomstig onderzoek.
Van praktijk naar theorie. Ik heb met ontzettend veel plezier gewerkt aan industriële cases. Dit kon, omdat ik in de jaren daarvoor geïnvesteerd had in theorie. Dit onderzoek is mooi, nuttig, relevant, en vruchtbaar en we moeten dit vooral blijven doen. Sommige technieken die in de praktijk blijken te werken, vergen echt een betere theoretische onderbouwing. Wil Nederland ook op de lange termijn innovatief blijven, dan is investeren in theoretisch onderzoek net zo belangrijk als praktische onderzoek: het zijn kanten van dezelfde medaille. Ik hoop dat de Nederlandse overheid dit ook gaat inzien, en naast het belangrijke impact gedreven onderzoek, ook fondsen reserveert om de fundamenten hiervan te onderzoeken.

Have Fun & Play! end exhibition_

Futureflash 200
_from Frankenstein to Hyperbrain

03/07/2018



10:00 walk_in
10:30 official_opening*
10:45 student_pitches
11:00 exploring_installations

*by Thom Palstra

Creative Technology
GOG BOT UNIVERSITY OF TWENTE.

17. HAVE FUN & PLAY!

Naast het doen van onderzoek, geef ik natuurlijk ook onderwijs. Het opleiden van studenten en professionals is natuurlijk een kerntaak van de universiteit, maar het is ook gewoon heel erg leuk. Daarbij refereer ik graag aan een uitpraak van Nelson Mandela: *Education is the most powerful weapon which you can use to change the world.*

Een bijzonder vak geef ik aan eerstejaars studenten Creative Technology aan mijn andere werkgever, de Universiteit Twente. Dit is een Bacheloropleiding op de grens van techniek, kunst en design.

In mijn vak, met controversiële naam *Have Fun & Play!,* ontwerpen en bouwen eerstejaarsstudenten interactieve installaties. Ik werk hierin samen met het multimedia art festival GOGBOT, één van Nederlands meest toonaangevende festivals op het gebied van kunst en techniek. De beste installaties worden geselecteerd en deze mogen studenten dan tentoonstellen op GOGBOT. Om inspiratie op te doen, organiseer ik samen met het Rijksmuseum Twenthe een aantal museumbezoeken en gastlezingen door toonaangevende interactie-kunstenaars en ontwerpers; een gaaf vak dat ik graag zelf een keer zou willen volgen.

Ik probeer de beleidsmakers aan deze universiteit zo ver te krijgen om ook zo'n vak op te zetten. Dat lijkt mij een cool plan.

Ik krijg regelmatig de vraag of zo'n vak niet haaks staat op mijn onderzoek over risicomanagement. Zelf zie ik dat niet zo; juist Creative Technology helpt out-of-the-box denken; en juist moderne technologie helpt het vakgebied vooruit. Denk aan drones die inspecties uitvoeren, aan trainingen voor piloten via VR en *serious games* om mensen risicobewuster te maken. Samen met mijn afstudeerders Mitch de Vries[36] en Jorien Kip[37] heb ik met veel plezier gewerkt aan risicovisualisaties voor foutenbomen. Zulke visualisaties bieden veel inzicht in de werking van risicomodellen. Ik laat jullie een korte animatie zien.

18. NERD DES VADERLANDS

Op deze plaats wil ik ook graag wat zeggen over *outreach*. Veel mensen hebben naar mijn smaak een verkeerd beeld van het vakgebied Informatica. Men denkt dat het vooral over programmeren gaat. Ik hoop dat ik vandaag heb laten zien dat dat niet zo is; het gaat juist over modellen, over algoritmen, over elegantie.

Informatica speelt een centrale rol bij vele innovaties: robots, het Internet-of-things, 3D printing, artificiële intelligentie, big data. Deze innovaties zijn bepalend voor hoe onze toekomstige maatschappij eruit gaat zien.

Daarbij vind ik dat informatici zich niet genoeg roeren in belangrijke debatten over ons vakgebied. Natuurlijk, mijn collega's Bart Jacobs en Vanessa Evers zijn boegbeelden als het gaat over cybersecurity en robotica, maar veel discussies rond zelfrijdende auto's, artificiële intelligentie, blockchains worden gevoerd door filosofen, economen en anderen. Uiteraard hebben zij een belangrijke visie, maar wij informatici moeten ook een stevige rol in het debat opeisen. Wij zijn veel beter op de hoogte van de technologische ontwikkelingen, hun risico's, mogelijkheden en onmogelijkheden.

Daarom is het wat mij betreft tijd voor het aanstellen voor een *Nerd des Vaderlands*. We hebben een Denker des Vaderlands, een Dichter des Vaderlands en in dat rijtje pas heel goed een *Nerd des Vaderlands*. Hij, en bij voorkeur zij, kan dan heel goed uitleggen wat de essentie is van de nieuwe technologieën die ik hierboven noemde en natuurlijk ook de schoonheid daarvan.


thank
you

19. DANKWOORD

Iedere dag weer voel ik hoe goed ik het heb: drie gezonde kinderen, een lieve man en twee gave banen. En daar hebben heel veel mensen aan bijgedragen, meer dan ik hier kan noemen.

Allereerst wil ik alle ondersteuners bedanken, die het Bedrijf Wetenschap tot een geoliede machine maken: accountants, onderwijsondersteuners, schoonmakers. Uit mijn ervaringen in het buitenland weet ik dat dit ook heel anders kan. Hiertoe horen zeker ook drie fantastische secretaresses: Ida den Hamer, Ingrid Berenbroek, en eerder Joke Lammerink.

Ik heb het geluk gehad met heel goede en inspirerende mensen te mogen werken: mijn afstudeerbegeleiders Erik Barendsen en Henk Barendregt; mijn promotor Frits Vaandrager; in mijn postdoc-tijd Luca de Alfaro, Tom Henzinger, en Rupak Majumdar. Daarnaast hebben Ed Brinksma, Holger Hermanns, Christel Baier, Jaco van de Pol en Marieke Huisman een cruciale invloed op mijn carrière gehad. Speciale dank gaat naar Joost-Pieter Katoen, voor de jarenlange samenwerking, de vele 'strakke bakkies' en voor het wedstrijdje wie het meeste Starbucksfilialen bezoekt.

Obviously, the results mentioned today were not possible without the vital contributions of my PhD students and postdocs: Enno Ruijters, Marcus Gerhold, Rajesh Kumar, Stefano Schivo, Carlos Budde, Jeroen Meijer, Arnaud van Harmelen, Waheed Ahmad, Dennis Guck, Florian Arnold, Mark Timmer, Hichem Boudali, Taolue Chen, Laura Bradan Briones. Ook wil ik mijn industriële partners bedanken voor de goede samenwerking en het delen van kennis: Bob Huisman en zijn team, Martijn van Noort, Jaap van Ekris, Judi Romijn, Gea Kolk, Wietske Postma. Verder ben ik veel dank verschuldigd aan mijn vele collega's. Iedere dag weer merk ik hoe collegiaal de samenwerking is, hoe leuk het is om samen onderwijs te geven en onderzoek te doen, zowel op de Universiteit Twente, als op de Radboud Universiteit.


thank
you

20. THE THINGS THAT REALLY MATTER

Maar nu, de dingen die er echt toe doen. Als drukke wetenschapper neem ik vaak *short-cuts* in mijn sociale bestaan. Met name mijn vrienden, buren en familieleden lijden daaronder.

Mijn schoonouders, Ans en Ben van Rossum, hebben ons altijd met raad en daad bijgestaan. Als we op vakantie gingen, was opeens ons huis geschilderd en de tuin gedaan. Tegenwoordig zijn zij het vaste oppasadres tijdens schoolvakanties. Mijn ouders hebben mij de liefde voor wetenschap bijgebracht: altijd vragen stellen, dingen echt proberen te doorgronden. Mijn broer en zus hebben mij op deze weg vergezeld. We hebben heel wat legobouwwerken opgebouwd, kapot gemaakt, opnieuw gebouwd.

Mijn allergrootste dank bewaar ik voor mijn gezin. Lieve Peter, het moeilijkste aan het schrijven van deze oratie was het vinden van woorden om jou te bedanken. Hoe meer de deadline naderde, hoe moeilijker het werd. Daarom ga ik het niet proberen. Anderen kunnen dat beter uitdrukken. Daarom laat ik liever een muziekstuk horen waar we allebei van houden.

Quinten, Milena, Florian. Iedere dag geniet ik van jullie aanwezigheid, van verrassende opmerkingen, van jullie vrolijkheid, gekkigheid, van alle dingen die we samen doen. Zonder jullie zou mijn leven heel erg leeg zijn. Jullie klagen wel eens: 'Mam, moet je nu alweer werken, het is weekend', of: 'Als wij niet mogen gamen, dan mag jij ook niet achter je computer zitten.' Daar hebben jullie natuurlijk gelijk in. Ik geloof ook niet in de vervanging van quantity time door quality time. Hoewel ik te vaak schort-cuts neem als het gaat om vrienden en andere familie, probeer ik dat bij jullie juist niet te doen. Ik hoop, ik denk, dat dat meestal lukt.

Ik wil mijn oratie eindigen met een uitspraak van de basketbalspeler Michael Jordan:

Just Play. Have Fun. Enjoy the game.

Ik heb gezegd.

VERANTWOORDING VAN FOTO'S EN FIGUREN

1. Familiearchief Otto Stoelinga.
2. Stint press kit.
3. Created based on Global Risks Report, World Economic Forum, 2018.
4. Marielle Stoelinga.
5. Karn G. Bulsuk (http://www.bulsuk.com). Eerder gepubliseerd in http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html - Eigen werk. Originally developed for Taking the First Step with PDCA, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=5236801.
6. https://pixabay.com/nl/datacenter-bigdata-computer-2803200/
7. https://www.stockvault.net/photo/239532/having-doubts---drawing-of-a-man-on-blackboard.
8. https://pixabay.com/en/direction-directory-away-decision-1033278/
9. E. Ruijters, D. Guck, M. van Noort en M. I. A. Stoelinga. *Reliability-centered maintenance of the Electrically Insulated Railway Joint via Fault Tree Analysis: A practical experience report*. Proceedings of DSN, pp. 662–669, 2016.
10. https://pixabay.com/nl/bal-http-www-crash-beheerder-63527/
11. E. Ruijters, D. Guck, M. van Noort en M. I. A. Stoelinga. *Reliability-centered maintenance of the Electrically Insulated Railway Joint via Fault Tree Analysis: A practical experience report*. Proceedings of DSN, pp. 662–669, 2016.
12. Marielle Stoelinga.
13. Marielle Stoelinga.
14. https://pixabay.com/en/lego-pieces-toy-brick-build-3129352/
15. https://pixabay.com/nl/post-it-notities-kleverige-nota--s-1284667/
16. https://pixabay.com/en/binoculars-dusk-sunset-birding-1269458
17. Floor Stolk.
18. ttps://pixabay.com/en/artificial-intelligence-robot-ai-ki-2167835/
19. https://pixabay.com/en/calligraphy-pen-thanks-thank-you-2658504/
20. https://pixabay.com/en/calligraphy-pen-thanks-thank-you-2658504/

REFERENTIES

1 Centraal bureau voor de Statistiek. *StatLine:* https://opendata.cbs.nl/

2 GBO Provincies. *Risicokaart:* https://www.risicokaart.nl/home

3 World Economic Forum, The Global Risks Report, 13th Edition, 2018.

4 A. Šotić en R. Rajić. *The Review of the Definition of Risk*. Online Journal of Applied Knowledge Management, vol. 3(3) pp. 17–26, 2015.

5 P. Hopkin. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management,* Kogan Page, 2107.

6 M.I.A. Stoelinga. UT-professor geeft 5 lessen uit Stint-drama. Tubantia, 5 November 2018.

7 C. L. Pritchard. Risk Management: Concepts and Guidance, CRC Press, 2014.

8 International Standardization Organization. *ISO 31000: Risk Management,* 2018.

9 N. R. Tague. *Quality Toolbox,* ASQ Press, 2005.

10 C. Carlson, *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes using Failure Mode and Effects Analysis,* Wiley, 2012.

11 ISO/IEC. ISO/IEC 64443. Software engineering – Product quality. ISO/IEC, 2001.

12 K. K. Aggerwal. *Reliability Engineering*. Springer, 1993.

13 D. Kahneman. *A perspective on judgment and choice: Mapping bounded rationality*. American Psychologist, vol. 58(9) pp. 697–720, 2003.

14 D. Kahneman. *Thinking Fast and Slow,* Farrar, Straus & Giroux, 2013.

15 U.S. Department of Defense. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis.* MIL-P-1629, 1949.

16 Society of Automotive Engineers. *SAE Architecture Analysis and Design Language (AADL) Annex Volume 1: Annex E: Error Model.* AS5506/1A, 2015.

17 W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, *Fault Tree Handbook,* Office of Nuclear Regulatory Reasearch, U.S. Nuclear Regulatory Commision, 1981.

18 E. Ruijters and M. I. A. Stoelinga, "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools", *Computer Science Review*, vol. 15–16, pp. 29–62, Elsevier, 2015.

19 M. Stamatelatos, W. Vesely, J. Bechta Dugan, J. Fragola, J. Minarick, and J. Railsback, *Fault Tree Handbook with Aerospace Applications,* Office of safety and mission assurance, NASA headquarters, 2002.

20 E. Ruijters, D. Guck, M. van Noort en M. I. A. Stoelinga. *Reliability-centered maintenance of the Electrically Insulated Railway Joint via Fault Tree Analysis: A practical experience report.* In Proceedings of DSN, pp. 662–669, 2016.

21 F. W. Vaandrager: *Model learning.* Communications of the ACM 60(2): 86-95, 2017.

22 M. Nauta, D. Bucur, M.I.A. Stoelinga: *LIFT: Learning Fault Trees from Observational Data.* QEST 2018: 306-322.

23 E. Ruijters, D. Guck, P. Drolenga, M. Peters, M, and M.I.A. Stoelinga. *Maintenance Analysis and Optimization via Statistical Model Checking: Evaluating a Train Pneumatic Compressor*. In Proceedings of QEST, pp. 331–347.

24 R. Heijblom, W. Postma, V. Natarajan, M.I.A. Stoelinga, DFT Analysis Incorporating Spare Parts in Fault Trees. Annual Reliability and Maintainability Symposium (RAMS), 2018.

25 M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications,* John Wiley & Sons, 2004.

26 P.L. Bernstein, *Against the Gods,* Wiley and Sons, 1996.

27 J.-P. Katoen, M. Stoelinga: *Boosting Fault Tree Analysis by Formal Methods.* ModelEd, TestEd, TrustEd 2017: 368-389.

28 M. Bozzano, A. Cimatti, J.-P. Katoen, P. Katsaros, K. Mokos, V. Y. Nguyen, T. Noll, B. Postma, M. Roveri: *Spacecraft early design validation using formal methods.* Rel. Eng. & Sys. Safety 132: 20-35 (2014).

29 A. F. Hixenbaugh. *Fault Tree for Safety.* The Boeing Company, 1968.

30 D. Ge, M. Lin, Y. Yang, R. Zhang, and Q. Chou. *Quantitative analysis of dynamic fault trees using improved sequential binary decision diagrams.* Reliab. Eng. Syst. Safety, 142:289 - 299, 2015.

31 S. Kabir. *An overview of fault tree analysis and its application in model based dependability analysis.* Expert Syst. Appl., 77:114 - 135, 2017.

32 C. Baier and J.-P. Katoen, *Principles of model checking,* MIT Press, 2008.

33 M. Z. Kwiatkowska, G. Norman, and D. Parker, "Stochastic model checking", in 7th *International Conference on Formal Methods for Performance Evaluation (SFM), LNCS* vol. 4486, pp. 220–270, Springer, 2007.

34 A.K.I. Remke and M. I. A. Stoelinga (eds.), *Stochastic Model Checking, LNCS* vol. 8453, Springer, 2014.

35 N. N. Taleb. *The Black Swan: The Impact of the Highly Improbable.* Penguin Books, 2008.

36 M. de Vries. *Fault Tree Visualization using visualization techniques and interaction design.* BSc thesis, University of Twente, 2016.

37 J. Kip. *Developing a Data Visualization Tool for Minimal Cut Sets.* BSc thesis, University of Twente, 2017.