Hoe goed bent u in control over de robuustheid van uw ICT-keten?

Methodiek voor het bepalen van de mate van beheersing van robuustheid in ICT-ketens

(Gepubliceerd in: Informatie, maart 2011)

Harrie Bastiaansen, Rieks Joosten, Erik Meeuwissen, Frank Roijers
(TNO)

ICT-ketens worden enerzijds steeds complexer en anderzijds van steeds vitaler belang voor de maatschappij en voor organisaties. Daarmee neemt ook het belang van robuustheid van ICT-ketens en de beheersing daarvan toe. De auteurs beschrijven een nieuwe methodiek waarmee de mate van beheersing van de robuustheid van ICT-ketens kan worden vastgesteld.

Inleiding

De huidige maatschappij kan niet functioneren zonder haar ICT-diensten en -infrastructuren. Deze zijn in toenemende mate in ketens georganiseerd. Het falen van onderdelen in de keten kan leiden tot (grootschalige) verstoringen van de processen en diensten die hiervan afhankelijk zijn. Zo kan bijvoorbeeld communicatiestoring bij een vervoersbedrijf leiden tot een ontregelde dienstregeling die veel reizigers treft, het falen van het elektronisch betalingsverkeer in het weekend voor kerst groot maatschappelijk ongenoegen tot gevolg hebben en falend Internet voor consumenten in het nieuwe werken resulteren in gemiste arbeidsproductiviteit.

Door de steeds toenemende vitaalheid van deze diensten is er steeds meer aandacht voor de zogeheten “robuustheid” van hun ondersteunende processen en ICT-ketens. Vanwege het grote belang wordt hiernaar mondiaal onderzoek verricht, zie bijvoorbeeld initiatieven in de EU [ENISA, EU] en Nederland [TrustworthyICT].

In dit artikel beschrijven we een methodiek om enerzijds de mate van beheersing van de robuustheid in ICT-ketens vast te stellen en om anderzijds de bijbehorende risico’s ook ketenbreed te beheren. De methodiek richt zich op:

- ICT-ketens, dit in tegenstelling tot de huidige wijze van risico management (ook voor robuustheid) die veelal gebaseerd is op het beheren van risico’s binnen één ‘scope’ (d.w.z. de eigen organisatie).

- De mate van *beheersing van* (controle over) robuustheid, en niet op de robuustheid van een ICT-keten zelf. Je zou dus kunnen zeggen dat het gaat om de kwaliteit van de sturing op robuustheid en niet om de kwaliteit van de technische implementatie zelf.

In de volgende paragrafen van dit artikel zullen we achtereenvolgens stilstaan bij het toenemend belang van ICT-ketens, wat verstaan we onder robuustheid, het belang van de beheersing hiervan, de criteria en methodiek om de mate van beheersing van robuustheid van ICT-ketens vast te stellen en de bijbehorende risico’s te beheren.

Het toenemend belang van ICT ketens

In toenemende mate wordt het leveren van diensten ondersteund door ICT-ketens. Dit geldt niet alleen voor nieuwe diensten. Ook “ouderwetse” diensten worden vervangen door ICT ketens. Zo wordt het papieren geld vervangen door allerlei chipkaarten, waarmee de afhankelijk van ICT ketens toeneemt.

Behalve dat het aantal ketens sterk toeneemt, worden ze ook steeds complexer. Enerzijds omdat de ketens meer functionaliteiten ondersteunen. Met een chipkaart wordt bijvoorbeeld een betaling verricht, maar daarvoor wordt ook gecheckt of de kaart niet gestolen is en wordt contact gelegd met de bank om het saldo te controleren. Anderzijds zijn steeds meer partijen betrokken in ICT-ketens. Het uitvoeren van alle functionaliteit van een chipkaart ligt bijvoorbeeld niet bij één partij maar bij meerdere (externe) partijen: de dienstaanbieder, een communicatie provider, financiële instelling, chipkaart register, enzovoorts.

In het dagelijks leven zijn we op deze wijze in toenemende mate afhankelijk van de ICT-ketens. Het blijvend goed functioneren hiervan is daarmee van belang voor zowel de maatschappij als geheel als voor de individuele organisaties (of organisatieonderdelen) die afhankelijk zijn of onderdeel uitmaken van de ICT-ketens. De toename van het werken in ketens in combinatie met de groeiende complexiteit maakt de ICT-ketens ook in toenemende mate kwetsbaar. Daarmee neemt het belang de ‘robuustheid’ van de ketens sterk toe.

Wat verstaan we onder robuustheid?

In een omgeving waarin zowel het belang als de kwetsbaarheid van ICT-ketens steeds groter worden, is het de uitdaging voor organisaties (overheden en bedrijfsleven) om hun kritieke dienstverlening zeker te stellen. Indien de dienstverlening daarbij gebaseerd is op het intensief gebruik van ICT-technologie, dan betreden we het speelveld van robuuste ICT.

> *“De robuustheid van een ICT-keten is de mate waarin aan de verplichtingen van haar dienstverlening kan worden voldaan, onafhankelijk van de omstandigheden.”*

Met deze definitie omvat de scope van robuuste ICT-ketens zowel preventieve als het reactieve aspecten. Preventieve aspecten zijn gericht op het verhogen van de kwaliteit (bijvoorbeeld beschikbaarheid) van de kritieke dienstverlening, bijvoorbeeld door de kwaliteit van de individuele onderliggende systemen te verhogen. Reactieve aspecten omvatten de mate waarin een ICT-keten in staat is situaties te compenseren van verminderde kwaliteit van deelsystemen waar het van afhankelijk is. Globaal gezegd kun je dit samenvatten als: het systeem zelf moet robuust zijn (bijv. hoge beschikbaarheid), maar het moet ook het falen (of verminderd presteren) van haar deelsystemen of de systemen in haar omgeving kunnen opvangen.

Robuustheid heeft vaak betrekking op wat wordt aangeduid als de kwaliteitsaspecten of niet-functionele aspecten. Robuustheid van ICT is daarbij meer omvattend dan alleen de “klassieke” beschikbaarheid van individuele systemen. Figuur 1 geeft een overzicht van kwaliteitsaspecten waarop robuustheid van ICT-ketens van toepassing kan zijn. De figuur geeft de kwaliteitsaspecten weer volgens het Quint-model [Quint], welke is afgeleid van de ISO 9126 norm “Information technology - software product evaluation – quality characteristics and guidelines for their use”.

Functionality	Maintainability	Usability
suitability accuracy interoperability compliance security *traceability*	analysability changeability stability testability *manageability* *reusability*	understandability learnability operability *explicitness* *customisability* *attractivity* *clarity* *helpfulness* *user-friendliness*
Reliability	**Portability**	**Efficiency**
maturity fault tolerance recoverability *availability* *degradability*	adaptability installability conformance replaceability	time behaviour resource behaviour

Figuur 1: Kwaliteitsaspecten volgens het Quint-model.

Robuustheid kan betrekking hebben op elk van de kwaliteitsaspecten zoals benoemd in de figuur. Bij het beoordelen van robuustheid zal in een vroegtijdig stadium derhalve moeten worden vastgelegd welk kwaliteitsaspect het betreft, bijvoorbeeld fouttolerantie, veiligheid, verwerkingssnelheid, een beheeraspecten zoals onderhoudbaarheid of vervangbaarheid, of de “traditionele” beschikbaarheid.

Belang van beheersing van de robuustheid van ICT ketens

Het bepalen van de daadwerkelijke robuustheid van een ICT-keten is zeer complex. Hiervoor is geen algemene methode beschikbaar, in tegenstelling tot bijvoorbeeld communicatienetwerken waarvoor wel methodes bekend zijn [BellLabs] [Bhattacharyya]. Ten opzichte van communicatienetwerken hebben IT systemen extra aspecten die de robuustheid beïnvloeden, bijvoorbeeld het real-time of batch karakter van systemen, de load en capaciteit van systemen, het mechanisme van koppeling (bijvoorbeeld query-response) tussen systemen. Het kwantificeren van de robuustheid van ICT-ketens wordt daardoor een grote uitdaging [Littlewood].

In dit artikel focussen we daarom op de mate van *beheersing van* (in control zijn over) robuustheid van een ICT-keten i.p.v. op de robuustheid zelf. De ratio daarachter is dat de kwaliteit van de sturing op robuustheid een goede indicator zal zijn voor de mate van robuustheid zelf. Het geeft namelijk transparantie over de robuustheid gerelateerde risico’s die in een ICT-keten aanwezig zijn: welke risico’s zijn er, welke daarvan worden geaccepteerd en voor welke worden technische of bestuurlijke maatregelen ingevoerd.

In het vervolg van dit artikel beschouwen we daarom een methodiek om enerzijds de mate van beheersing van de robuustheid in ICT-ketens vast te stellen en om anderzijds de bijbehorende risico’s ketenbreed te beheren. De methodiek is gericht op ICT-ketens en richt zich op de mate van *beheersing van* robuustheid, en niet op de robuustheid van een ICT-keten zelf.

Wanneer bent u in controle over de robuustheid van een ICT-keten?

In een ICT-keten is een ketenverantwoordelijke (indien überhaupt benoemd) in steeds grotere mate afhankelijk van toeleverende partijen waar hij zelf geen volledige controle over heeft, maar desondanks wel van vitaal belang zijn voor het correct functioneren van "zijn" keten. Het is daarom voor de kwaliteit van de keten zeer belangrijk de keten zo goed mogelijk te organiseren, afspraken te maken over de (kwaliteit van) de dienstverlening van andere partijen en daarbij de kwaliteit over de gehele keten als leidraad te beschouwen.

Bijvoorbeeld voor betalingen met een chipkaart zal de ketenverantwoordelijke o.a. communicatie tussen chipkaart terminals en de achterliggende systemen moeten inkopen bij een derde partij. Zeer belangrijk is dat deze communicatie *"het altijd doet"*. In een Service Level Agreement (SLA) zal het beschikbaarheidniveau van de communicatie worden vastgelegd. Aangezien het een zeer essentieel onderdeel is van de chipkaart dienstverlening, zal de ketenverantwoordelijke zeer goed voor ogen moeten hebben of de derde partij zich aan gemaakte afspraken zal houden. Bij falen van de communicatie zal de ketenverantwoordelijke er namelijk op worden aangesproken dat zijn dienst niet goed georganiseerd is. Daarom zal de ketenverantwoordelijk behalve de SLA zelf, ook een beeld moeten vormen in hoeverre hij verwacht dat de derde partij eraan voldoet, hoe essentieel de ingekochte service is voor zijn dienst, en of hij eventueel compenserende maatregelen moet treffen voor het geval de derde partij de gemaakte afspraken niet nakomt. Het "blind" vertrouwen op de afspraken in de SLA is onvoldoende om in control te zijn over de robuustheid van een ICT-keten.

Voor het vaststellen van de mate van beheersing van de robuustheid van een ICT-keten zijn aanvullende criteria nodig. Deze criteria moeten ook nog eens (objectief) getoetst kunnen worden. We hebben daarom een nieuwe set van criteria voor het vaststellen van de mate van controle over de robuustheid van een ICT-keten geïdentificeerd. De criteria zijn geclassificeerd in vier categorieën, zoals weergegeven in Tabel 1.

Categorie	Beschrijving
Bestuurbaarheid	De mate waarin de ICT-keten is vormgegeven zodat het überhaupt mogelijk is om controle over de robuustheid uit te oefenen.
Regie	De wijze waarop de regie over (de robuustheid van) de ICT-keten wordt uitgeoefend. Daarbij maken we verder onderscheid in de subcategorie "***Ketenregie***" en inde subcategorie "***Ketenafspraken (SLA's)***"
Maatregelen	Dit omvat de maatregelen die zijn getroffen om de (controle over de) robuustheid van de ICT-keten te borgen, met een onderscheid in de subcategorie "***technische maatregelen***" en de subcategorie "***bestuurlijke maatregelen***".
Betrouwbaarheid	Dit betreft de betrouwbaarheid van de afspraken en maatregelen die genomen zijn, zowel binnen een organisatie als tussen de partijen in de keten

Tabel 1: Categorieën voor het vaststellen van de mate van beheersing over robuustheid van ICT-ketens.

Tabel 2 geeft een overzicht van criteria per categorie. Voor elk van de criteria is een set van toetsen opgesteld die kan worden gebruikt om het desbetreffende criterium te "scoren". Voor de overzichtelijkheid zijn deze toetsen niet in de tabel opgenomen. Wel is in de tabel middels de grijze arcering aangegeven welke criteria (ondanks de bijbehorende toetsen) niet volledig objectief zijn te scoren, maar waarvoor een meer subjectieve professionele beoordeling nodig is, gestoeld op ervarings- en vergelijkingsfeiten.

Regie		Bestuurbaarheid	
Ketenregie	***Verantwoordelijkheden toegewezen*** Rollen en verantwoordelijkheden voor het realiseren van robuustheid doelstellingen zijn gedefinieerd en toegewezen (RACI) ***Middelen beschikbaar gesteld*** De middelen en mogelijkheden om te sturen op robuustheid moeten aanwezig zijn. ***Uitvoering vormgegeven*** De eisen aan de robuustheid van het proces zijn op SMART en consistente wijze doorvertaald naar de eigen interne omgeving en naar de subprocessen (subscopes) ***Verantwoording afgelegd*** Door de verantwoordelijken wordt op reguliere basis over de realisatie van robuustheid verantwoording afgelegd.		***Doelstelling vastgelegd*** De doelstelling van robuustheid is eenduidig en op business niveau vastgelegd ***Afgebakend in omvang*** De (interne) scope is behapbaar in omvang ***Gemodulariseerd*** De robuustheid van de (interne) scope is onder controle
Ketenafspraken (SLA's)	***Robuustheideisen opgenomen*** In de (relevante) SLA's zijn zowel SMART kwantitatieve robuustheidseisen als de bijbehorende controlemaatregelen vastgelegd ***Verantwoordelijken benoemd*** Verantwoordelijkheden voor het realiseren van robuustheid doelstellingen bij toeleveranciers (subprocessen / subscopes) worden benoemd in de SLA's ***Verantwoording afgelegd*** Door de verantwoordelijken wordt op reguliere basis over de realisatie van robuustheid verantwoording afgelegd.	Maatregelen	
		Technisch	***Risicoprofielen opgesteld*** Het is bekend welke dreigingen er zijn m.b.t. de robuustheid van het proces. ***Maatregelen getroffen*** Voor de relevante robuustheiddreigingen is (op business niveau) over maatregelen besloten en deze zijn op toereikendheid getoetst.
		Bestuurlijk	***Ketenbreed risicoanalyse uitgevoerd*** Over de gehele keten van het proces dienen de grootste dreigingen, hun impact en maatregelen bekend te zijn en te worden afgestemd. ***Ketenbreed risicomanagementproces ingericht*** Over de gehele keten van het proces een adequaat proces voor het regulier managen van risico's te zijn ingericht.
		Betrouwbaarheid	
			Vertrouwen Er is vertrouwen dat de SMART gedefinieerde robuustheidafspraken door de toeleveranciers daadwerkelijk conform SLA worden gerealiseerd ***Toetsing*** De SMART gedefinieerde robuustheidafspraken door de toeleveranciers (subprocessen / subscopes) kunnen objectief gemonitored of getoetst worden

Tabel 2: Criteria per categorie.

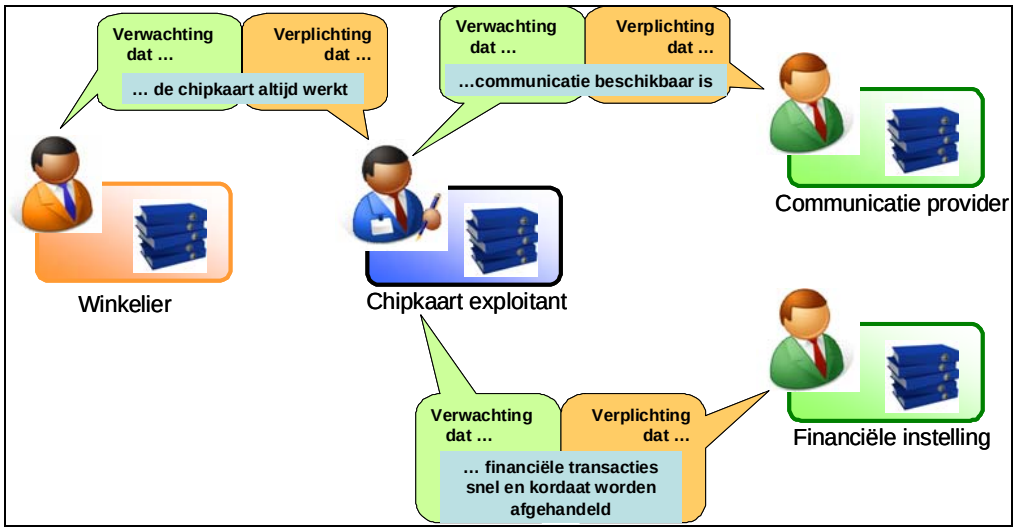
Voor het vaststellen van de mate van controle over de robuustheid in ICT-ketens is het nodig om de criteria uit de tabel op een herhaalbare, recursieve, wijze toe te kunnen passen. De criteria zijn immers zowel van toepassing voor de systemen onder intern beheer van de "eigen" schakel als voor de externe schakels in de ICT-keten. Deze externe schakels zullen bovendien weer hun eigen toeleveranciers hebben. In de volgende paragraaf zal daarom een methodiek worden beschreven om de criteria voor het vaststellen van de mate van beheersing van de robuustheid in ICT-ketens ketenbreed toe te passen. De methodiek kan enerzijds worden gebruikt voor het ketenbreed vaststellen van de mate van beheersing en anderzijds voor het operationeel beheren van de (risico's).

Methodiek voor controle over robuustheid van ICT-ketens

Voor het bepalen van de controle over de robuustheid gebruiken we de methode van gescoopt risico management [Joosten]. Het uitgangspunt is dat we inschatten hoeveel controle er over de robuustheid is vanuit de scope van de ketenverantwoordelijke.

Als voorbeeld beschouwen we de keten van een chipkaart exploitant, waarin winkeliers klant zijn en chipkaartfunctionaliteit van die exploitant afnemen. De winkeliers verwachten van de exploitant onder meer dat de chipkaart terminals, de achterliggende systemen en de communicatie daartussen altijd werkt. De exploitant heeft zich hiertoe (contractueel) verplicht en zal om aan die verplichtingen te voldoen, zelf weer verwachtingen koesteren ten aan zien van zijn toeleveranciers (voor bijvoorbeeld de communicatie, het gestolen chipkaart register en financiële functies).

Figuur 2 laat zien dat de verwachting van de ene partij (ten aanzien van een andere partij), verplichtingen voor die andere partij worden (ten aanzien van de ene partij). De chipkaart exploitant (ketenverantwoordelijke) is verantwoordelijk voor het maken van afspraken met toeleverende partijen (communicatie provider en financiële instelling) voor de benodigde functionaliteit en het regisseren van alle interne en externe afspraken die maken dat hij zijn eigen functionaliteiten kan leveren en zijn verplichtingen nakomen.



Figuur 2: Verwachtingen en verplichting voor een chipkaart exploitant.

Om in controle te blijven over de robuustheid van de keten, zal de chipkaart exploitant moeten bepalen:

- hoe belangrijk elk van de toegeleverde functionaliteiten is voor de gehele dienst; d.w.z. wat is de impact bij uitval, en
- in welke mate hij erop vertrouwt dat de toeleverende partij haar afspraken nakomt, i.e., wat de 'trustscore' is voor de toeleverende partij.

De gedachte hierachter is dat als een toeleverende partij in gebreke blijft, het gevolg hiervan zou kunnen zijn dat ook de ketenverantwoordelijke zelf niet langer in staat is zijn verplichtingen na te komen, terwijl zijn klanten geen genoegen zullen nemen met een verwijzing naar de subleverancier. Een winkelier die geen gebruik kan maken van de chipkaart, is immers niet geholpen als de chipkaart exploitant de verantwoordelijkheid voor een verstoring neerlegt bij de communicatie provider.

Indien de functionaliteit zeer belangrijk is of dat er onvoldoende vertrouwen is in de toeleverancier, dan zal de ketenverantwoordelijke zelf contingentiemaatregelen moeten nemen zoals het afnemen van communicatiediensten bij een tweede provider of het plaatsen van mobiele chipkaart terminals als backup.

Om inzicht te krijgen in de mate van controle over robuustheid kan de methode van 'gescoopt risicomanagement' [Joosten] worden gebruikt, waarbij we de criteria uit Tabel 2 zien als verwachtingen aan het robuustheidsgovernanceproces van de ketenverantwoordelijke. Als de ketenverantwoordelijke zijn eigen robuustheidsgovernanceproces beheert, zijn dit dus verwachtingen aan hemzelf (en daarmee dus ook verplichtingen voor hemzelf).

Praktisch betekent dit dat de ketenverantwoordelijke een risicomatrix (zie [Joosten]) invult, zoals weergegeven in Figuur 3. Deze matrix bevat een overzicht van de verplichtingen (kolom Verplichtingen[i]) en verwachtingen (rij Verwachtingen[j]), gegroepeerd volgens de partijen tegenover wie deze verplichtingen en verwachtingen gelden. Per verplichting O wordt de impact van het niet nakomen van deze verplichting weergegeven met scores 'L', 'M' en 'H' in de kolom Impact[i]. In een cel geeft de afhankelijkheidscoëfficiënt aan in welke mate de verwachting (kolom) van belang is voor het waarmaken van de verplichting (rij). Verder geeft de ketenverantwoordelijke per verwachting E aan in hoeverre hij erop vertrouwt dat de toeleverancier deze verwachting (die voor de toeleverancier een verplichting is), gaat nakomen. De figuur laat dat zien middels trustscores 'L', 'M' en 'H' onder elke verwachting

in de rij Trustscore[j]. Per verplichting wordt op basis van de afhankelijkheidscoëfficiënten en trustscores de kans op het niet nakomen van deze verplichting berekend in termen van de scores ‘L’, ‘M’ en ‘H’, zie kolom Kans[i]. Nu kan per verplichting het risico worden berekend op basis van kans en impact. De figuur toont dit middels scores ‘L’, ‘M’ en ‘H’ in de kolom Risico[i]. Indien een risico hoog uitkomt, heeft de ketenverantwoordelijke te weinig controle en zal hij contingentiemaatregelen moeten nemen, bijv. overgaan naar een betrouwbaardere toeleverancier.

Risicomatrix voor robuustheid					Jezelf		Een ander	
					E1	E2	E3	Verwachting[j]
Verplichting[i]	Impact[i]	Kans[i]	Risico[i]	Acceptabel risico?	H	M	L	Trustscore t[j]
O1	H	H	H	✗		+++	+++	
O2	M	L	L	✓	++	+		afh.coef.(i,j)
O3	L	H	M	✓		++	+++	

Trustscore: geeft voor elke verwachting (van jou) de mate van vertrouwen die jij hebt (= jouw besluit!) in het waargemaakt worden van die verwachting.

Afhankelijkheidscoëfficiënt: relatieve bijdrage van verwachting aan het waarmaken van eigen verplichting (‘+++’, ‘++’, ‘+’, ‘0’ of nvt/zwart)

Als jij Risico[i] (=risico inschatting horende bij verplichting [i]) acceptabel vindt, dan vink je dat bij die verplichting aan, en ben je klaar (voor die verplichting tenminste).

Figuur 3: Risicomatrix vanuit 1 scope.

Op deze manier kan dus niet alleen de mate waarin een ketenverantwoordelijke controle heeft over de robuustheid van die keten worden vastgesteld, maar heeft die ketenverantwoordelijke meteen een instrument in handen waarmee hij de (onacceptabel grote) risico’s die hieruit voortvloeien, kan mitigeren.

Conclusies

We hebben een methodiek voorgesteld om de kwaliteit van het besturingsproces op robuustheid van specifieke ICT-ketens te kunnen vaststellen. De sterkte van deze methodiek is dat hij in de ICT-keten, i.e. over de individuele schakels heen, gebruikt kan worden. De methodiek is schaalbaar en uitbreidbaar. Het geeft de aspecten weer waar kwaliteitsrisico’s gelopen worden, zowel intern binnen de individuele schakels als tussen de schakels (i.e. in de keten). Als zodanig kan de methodiek tevens als basis dienen voor keten-breed risico management proces. Een grote meerwaarde van de methodiek is daarbij het (near) real-time signaleren van het werk dat nog moet worden gedaan (en wie dat moet doen) om de grip op robuustheid van ICT-ketens te verhogen en het (near) real-time verstrekken van overzichten van deze werklast aan het management, zodat zij erop kunnen sturen dat dit werk (uiteindelijk) ook gebeurt.

Hoewel wij er van overtuigd zijn dat deze methodiek veel potentie heeft, moet dat nog wel in de praktijk worden beproefd. Daarom komen wij graag in contact met organisaties die samen met ons deze methodiek voor hun (bedrijfs-) of ketensituatie verder willen beproeven en ontwikkelen.

REFERENTIES

- [Bhattacharyya] S. Bhattacharyya, C. Diot, G. Iannaccone A. Markopoulou C.N. Chuah. Service Availability in IP Networks. SPRINT ATL RESEARCH REPORT RR03-ATL-071888.

- [BellLabs] Bell Labs Technical Journal, Volume 11, Number 3, 2006. Special Issue: Reliability.
- [ENISA]. ENISA. Network Resilience and Security: Challenges and Measures. December 2009. Available at: http://www.enisa.europa.eu/act/res/providers-measures/files/vwg-challenges-and-measures/
- [EU]. EU Dictorate_General. Information Society and Media. Availability and Robustness of Electronic Communications Infrastructures. DRAFT Final Report January 2007.
- [Joosten] R. Joosten, " 'Gescoopt' risico management", Informatiebeveiliging, Oktober 2010, blz 12 – 17.
  http://www.ict2030.nl/vitale_ict.html
- [TrustWorthyICT]. Towards Trustworthy ICT Service Chains (kruisbestuiving tussen IIP's SaaS + Vitale ICT). ICT-regie innovatieplatform. http://www.ict2030.nl/IIP-Cooperation-Challenge.html
- [Littlewood] B. Littlewood, L. Strigini. Software Reliability and Dependability: a Roadmap. The Future of Software Engineering, 177—188, 2000.
- [Quint] SERC, Kwaliteit van softwareprodukten - Praktijkervaringen met een kwaliteitsmodel, 1996

Dr. ir. Harrie J.M. Bastiaansen is consultant bij TNO op het gebied van Enterprise Architectuur en IT-besturing. E-mail: harrie.bastiaansen@tno.nl

Dhr. Rieks Joosten is onderzoeker bij TNO en doet onderzoek naar methoden voor governance, risico management en procesinrichting, met een bijzonder focus op de geautomatiseerde ondersteuning daarvoor. E-mail: rieks.joosten@tno.nl

Dr. ir. Erik Meeuwissen is consultant bij TNO op het gebied van het beheersen van de performance van ICT platformen en de kwaliteit van de diensten die hierover worden geleverd. E-mail: erik.meeuwissen@tno.nl

Dr. Frank Roijers is consultant bij TNO op het gebied van performance modellering en optimalisatie van ICT systemen. E-mail: frank.roijers@tno.nl