Gespreksnotitie expertmeeting grote ICT-projecten bij de overheid

C. Verhoef

VU Amsterdam, Department of Computer Science,
De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands

x@cs.vu.nl

1 juni 2012

1 Achtergrond en aanleiding

De parlementaire werkgroep ICT-projecten bij de overheid heeft besloten expertmeetings te organiseren, ter voorbereiding op een onderzoek naar ICT-projecten bij de overheid. Onderwerpen van gesprek:

- privacy en security
- kostenbeheersing

Tijdens de expertmeeting willen de Kamerleden kennisnemen van mijn visie op bovenstaande onderwerpen. Hieronder behandel ik achtereenvolgens de onderwerpen van gesprek in bredere context (Hoofdstuk 2). Vervolgens de onderwerpen zelf (Hoofdstukken 3 en 4). Dan ga ik in op de vraag over welke projecten het onderzoek kan gaan (Hoofdstuk 5). Tenslotte geef ik sterk gestileerd aan hoe je dergelijk onderzoek uit kunt voeren in Hoofdstuk 6.

2 De onderwerpen in hun context

De Kamerleden stellen aspecteisen aan de orde. Men heeft zich door de berichtgeving gerealiseerd dat er aspecten zijn van niet functionele aard die er toe doen, zoals privacy en security. Maar ook de kostenbeheersing. Dit valt onder één noemer die in jargon RAMS SHEEP heet. Dit staat voor de belangrijke aspecten: Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economics en Politics.

Deze aspecten bijten elkaar: de best beveiligde computer staat uit. Kortom: optimaliseren naar security is minimaliseren naar availability. Het vinden van een optimum gegeven de randvoorwaarden die je stelt is een ontwerp slag die wel RAMS(SHEEP) analyse wordt genoemd.

Dit soort analyses blijft veelal achterwege zowel vanuit de opdrachtgever als de opdrachtnemer. Daarom wordt je keer op keer voor voldongen feiten gesteld bij IT-investeringen. De Kamerleden hebben nu dus twee van de negen aspecteisen te pakken: security (waar privacy onder valt) en economics. Je kunt die aspecten echter niet los zien van de andere belangrijke aspecten, omdat er ook een bepaalde beschikbaarheid

nodig is, om maar eens wat te noemen. Dus optimaliseren naar één van de aspecteisen leidt tot ondermaatse prestatie op andere aspecten.

Een groot probleem is de aanbestedingsproblematiek. Mijn ervaring is dat de mensen die het kunnen het niet worden en omgekeerd. De prijs is alom bepalend. Ergo: naar de E van Economics is geoptimaliseerd. Dat bijt met de andere aspecteisen. Normale gebruikers zien geen verschil tussen een website en een website die goed beveiligd is. Dat zit onder de motorkap, en daar merk je—als het goed is—niet of nauwelijks iets van in termen van functionaliteit. De prijs maakt echter wel uit. Als je geen security design maakt, geen privacy design maakt, geen Wbp compliant design maakt, je ontwerp niet laat toetsen door een onafhankelijke partij, bevindingen niet op hoeft te volgen, geen personeel met een gedegen opleiden hoeft te betalen, vlak voor en periodiek na indienststelling geen penetratietests hoeft uit te voeren, . . . , ja, dan wordt het een stuk goedkoper. De goedkoopste oplossing is meestal niet goed beveiligd.

De discussie is breder dan de huidige vraagstelling. De insteek is echter goed verklaarbaar omdat die aspecten zijn komen bovenborrelen. Maar de andere zijn er ook en zijn via een haat-liefde verhouding met elkaar verbonden. Je wilt namelijk *en* goed beveiligd zijn *en* de kosten beheersen *en* betrouwbaar *en* beschikbaar, etc.

3 Privacy & Security

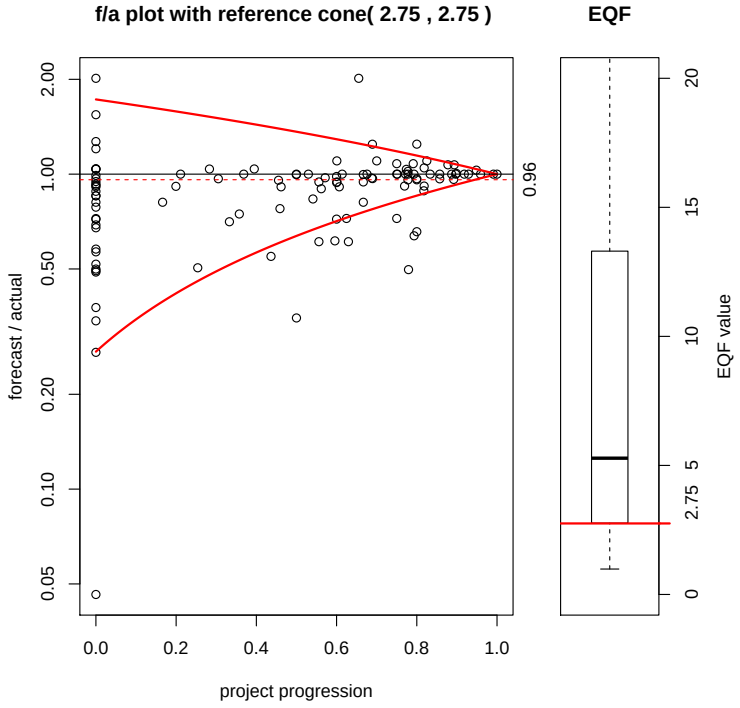
Aspecten moet je mee ontwerpen. Je kunt niet achteraf aspecteisen "toevoegen". Als aspecten niet goed zijn mee ontworpen dan komt dat nooit meer goed. Wat voorbeelden. Neem de E van Environment. Je kunt niet een auto ontwerpen en bouwen en bij de eerste start kijken of hij aan de emissierichtlijnen voldoet: dat moet je vanaf dag één meenemen in het ontwerp. Dat krijg je achteraf nooit meer goed. Of neem de S van Safety en de S van Security. Als een voertuig te water raakt wil je dat de elektrische ramen automatisch opengaan en niet door kortsluiting dicht blijven. Maar tegelijkertijd wil je ook niet dat door die voorziening de auto gevoeliger wordt voor inbraak. Dat door water in een deur te gieten het raampje vanzelf opengaat. Er is sprake van fatale ontwerpgebreken als aspecteisen niet van meet af aan gewogen zijn meegenomen. Aspecteisen ontwerpen is dus geen optie maar een must.

Dit geldt zeker voor een aspecteis zoals security. Zonder een integraal ontwerp waarin alle aspecteisen gewogen zijn meegenomen op basis van een vraagspecificatie waarin die aspecten aan de orde zijn gekomen, kun je nooit komen tot een systeem dat *en* functioneel naar behoren presteert *en* op de aspecten naar behoren presteert.

Mijn advies is dat de overheid onafhankelijk van een bepaald systeem overall eisen stelt aan deze aspecten. Je kunt eisen dat er geen persoonsgegevens onversleuteld mogen worden opgeslagen en/of verstuurd. Denk aan data minimalisatie eisen (need-to-know). Je kunt ook eisen dat de versleuteling aan bepaalde eisen voldoet. Zo eist de Amerikaanse overheid momenteel AES-256 (Advanced Encryption Standard, met een block size van 256 bits). Je kunt tevens eisen dat een dat als een nieuwe versleuteling noodzakelijk wordt, je de ene voor de andere kunt inwisselen zonder te hoge kosten (daarmee neem je ook de M van Maintainability mee). Je kunt eisen dat iedere partij die persoonsgegevens verwerkt een ISO 27001 certificering moet hebben en dat die periodiek verlengd moet worden. Je kunt allerlei toets- en controlemomenten afdwingen zoals penetratietesten, toetsen op het ontwerp op de aspecten privacy en security. Enzovoort. Kortom, de overheid kan hier sturend optreden. Dit doet de overheid al sinds jaar en dag bij civieltechnische constructies middels het bouwbesluit en de omgevingsvergunning. Onafhankelijk van welk gebouw dan ook worden eisen gesteld aan

aspecten zoals veiligheid. Dat kan hier ook.

4 Kostenbeheersing

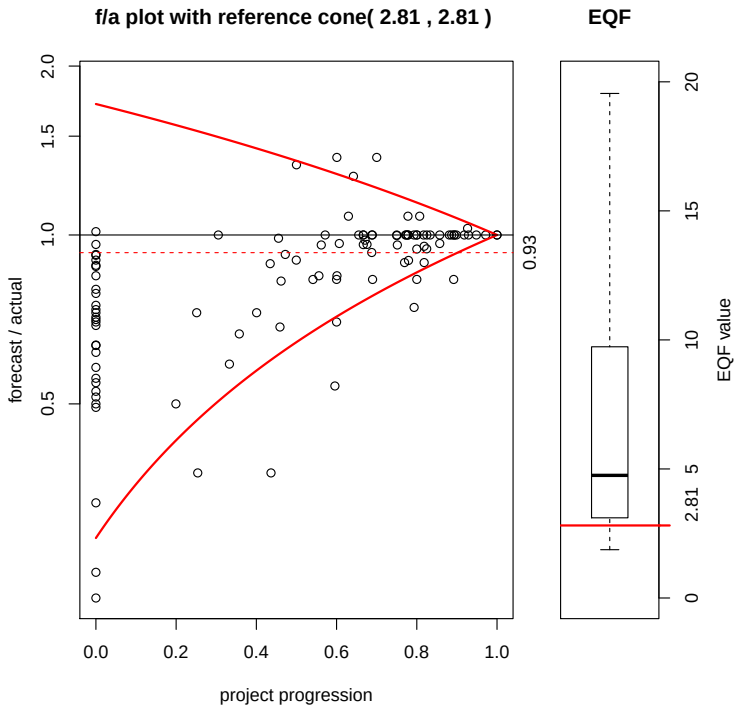


Figuur 1: Schattingskwaliteit van kosten door de overheid.

Een tot de verbeelding sprekend onderwerp is kostenoverschrijdingen. Initieel was het 10 miljoen, en uiteindelijk werd het 40 miljoen. Schande! Maar helaas ligt het niet zo simpel. Wat je hiermee namelijk vaststelt is wat de kwaliteit is van je slechtste schatting en die is bij de overheid inderdaad vaak niet best. Het bepalen van de kwaliteit van schattingen is wiskundig lastig maar wel mogelijk. Die kwaliteit is door mij bepaald vanuit de vorige jaarrapportage aan de Tweede Kamer[1]. Daar komt het volgende uit (zie ook Figuren 1 en 2).

- 50% van de schattingen voor kosten en doorlooptijd van de projecten zijn maximaal 20% te laag.
- Herijkingen vinden plaats pas na 20% van de einddatum van projecten.
- Initiële schattingen zijn allen veel te laag.
- Ook herijkingen zijn systematisch te laag.

[1]Zie: Schattingskwaliteit ICT-projecten van Rijksoverheid moet omhoog, http://www.cs.vu.nl/~x/knipselkrant/ag212011.pdf



Figuur 2: Schattingskwaliteit van doorlooptijden door de overheid.

- De mediane schattingskwaliteit zit boven het minimale industrie gemiddelde.

Uit een dergelijke exploratieve gegevensanalyse komen vragen naar voren. Zoals: waarom zijn alle initiële inschattingen van kosten en doorlooptijd te laag? Er zit een institutionele afwijking naar beneden in alle schattingen. Hoe komt dat? Het naar boven halen van de werkelijke oorzaken van deze systematische afwijking levert diep inzicht in het waarom en daarmee kan men ook bijsturen om deze ongewenste effecten weg te nemen. Een vermoeden is dat door het Europees aanbestedingsbeleid te lage bedragen worden geboden die nadien omhoog gemanaged moeten worden. Dat gaat stukje bij beetje (salamitactiek). Daarmee verhinder je als overheid dat een partij die het meteen voor dat geld had gedaan, en dan in één keer goed, het werk kan uitvoeren. Dit vermoeden kun je staven dan wel weerleggen op basis van feitenmateriaal.

5 Welke projecten

Dan de vraag van de Kamerleden welke projecten bekeken kunnen worden. Uit het voorafgaande is meteen duidelijk dat overzicht over kostenbeheersing zich beter in kaart laat brengen over zo veel mogelijk projecten dan een keus te maken uit vijf. Voor de kostenbeheersing is mijn advies dan ook als volgt.

Vraag bij alle ministeries, ZBOs, en andere instanties die meer dan een miljoen per jaar aan IT uitgeven dezelfde gegevens op zoals nu ook gebeurt bij de jaarrapportages. Uit die gegevens kunnen beelden worden geaggregeerd die laten zien hoe de huidige

stand van zaken is. Vanuit die feiten kunnen vervolgens verdere onderzoekingen uitgevoerd worden waarin oorzaken van aangetroffen ongewenste patronen een antwoord krijgen.

In het kader van privacy en security is het verstandig om projecten of organisaties door te lichten waar deze aspecten een prominente rol spelen. Ik noem met klem organisaties naast projecten. Diginotar is geen project maar een organisatie. Die had moeten worden doorgelicht. Daarnaast is het zo dat een project weliswaar een goed security design kan hebben maar als de organisatie daar verkeerd mee omgaat dan heb je nog niets.

In het blad PM heb ik gepleit voor onderzoeken aan *alle* kernsystemen van de overheid. Deze aanpak wordt steeds gebruikelijker binnen de private sector. Door het kennen van de boedel weet je waar de zwakke plekken zitten, kun je achterhalen waarom die er zijn en vervolgens kun je actie ondernemen. De vijf projecten die men kiest zie ik hooguit als de eerste vijf. Ik zou dan zelf kiezen voor zaken die nu lopen, dan kan op die projecten nog bijgestuurd worden. Dan zitten we hier over een paar jaar niet nog eens.

6 Hoe doe je dergelijk onderzoek?

De onderzoeksmethoden die hier gehanteerd dienen te worden moeten 100% op feitenmateriaal gebaseerd zijn, en niet op gesprekken en/of literatuur. Er zit over het algemeen een groot verschil tussen wat men zegt over projecten en wat men aantreft bij projecten. Een voorbeeld. Uit een gesprek kan volgen dat men aan versiebeheer van de broncode doet (best practice). Als je de versiebeheer administratie echter onderzoekt kan blijken dat stelselmatig de reden van een aanpassing niet vermeld wordt (bad practice). Dus uit het gesprek komt een heel ander antwoord dan uit een feitenonderzoek.

Dit soort (onbewuste) filterwerking moet worden uitgeschakeld omdat je anders niet tot de ware kern kunt doordringen. Op basis van het feitenmateriaal kun je feitelijke antwoorden op de onderzoeksvragen geven.

Hoe werkt dat dan? Ik breng in herinnering dat in de bijgeleverde stukken onder andere staat dat de Rekenkamer niet voor een Rijksbreed onderzoek pleit. Citaat:

> Geen Rijksbreed onderzoek. Een belangrijke voorwaarde voor zo'n onderzoek is dat er een minimale set betrouwbare informatie beschikbaar is over planning en realisatie op de onderwerpen tijd, omvang, beschikbare mensen en kosten van projecten. Hieraan is bij de projecten die wij onderzochten in het algemeen niet voldaan.

De veronderstelling dat er betrouwbare data moet zijn is een pertinente misvatting. Statistiek is juist het vak dat zich bezighoudt met betrouwbare uitspraken over *onbetrouwbare* data. Een voorbeeld over security en privacy. Stel je krijgt de complete project administratie van alle IT-projecten bij de overheid. Ja, dat is veel informatie. Per project kun je softwarematig alle woorden extraheren en daarvan de frequentie meten. Als de frequentie van woorden zoals beveiliging, security, privacy, en andere woorden die duiden op aandacht voor dit onderwerp niet tot nauwelijks voorkomen weet je dat er geen security en/of privacy by design heeft plaatsgevonden, althans niet expliciet traceerbaar. Je kunt dus op basis van heel veel project data *zonder een letter te lezen* toch vrij snel inkijkjes in die projecten krijgen. Dan kun je uitbijters onderzoeken zoals het project met de hoogste en/of de laagste score (niet-aselecte steekproef om de cost

of auditing sterk te drukken). Als je creatief bent, kun je met vrij simpele middelen al heel veel. Je moet dan wel precies weten waar je naar op zoek bent. Dat vergt iets van de commissie en van uitvoerenden. Mijn advies aan de commissie is dan ook om zich op dit punt solide te laten informeren. De Rekenkamer is er niet doorheen gekomen, dus simpel is dit geenszins.