Movares
adviseurs & ingenieurs

Het venijn van redundantie

Over de kosten en baten van redundante netwerken in tunnels

8 oktober 2019

wij verbinden

Movares
adviseurs & ingenieurs

Peter Overduin
Werkt als senior-adviseur VTTI bij Movares en heeft ervaring opgedaan in ontwerp, aanleg en onderhoud van in totaal meer dan 17 tunnels (landtunnels, zinktunnels, boortunnels, wegtunnels en spoortunnels, RWS-tunnels, gemeentelijke tunnels en provinciale tunnels, nieuwbouwprojecten en renovatieprojecten). Hij is lid expertpool KPT (Kennisplatform Tunnelveiligheid) van het Ministerie van Infrastructuur en Waterstaat.

Movares
adviseurs & ingenieurs

Samenvatting

In de praktijk blijkt sprake te zijn van een te vanzelfsprekend toepassen van redundantie in het tunnel-besturingsnetwerk (in de breedste zin) en in subsystemen van tunnels. Het gebruik van redundantie is 'common practice', maar gezien de kosten/baten niet noodzakelijkerwijs 'best practice'. Dit artikel roept op tot een zorgvuldige afweging van het gebruik van redundantie, omdat het middel in veel tunnels erger is gebleken dan de kwaal.
Er is een methode aangegeven waarmee het risico van 'instabiliteit' van het netwerk ten gevolge van redundantie in rekening gebracht kan worden bij de betrouwbaarheids-berekeningen.

Abstract

Redundant control networks are found in most tunnels in the Netherlands. The use of redundancy in these tunnel control networks is, although common practice, not necessarily best practice. This article argues that the use of redundant networks in tunnels must be carefully considered because the use of redundancy can even worsen the reliability of a tunnel, rather than improving it. A recommendation for calculation of the effects of network instability because of redundancy is provided. This can be used in the reliability analysis of redundant networks in tunnels.

Met speciale dank aan de volgende personen, die mij met veel geduld en vriendelijkheid hulp en advies hebben geboden over dit onderwerp en bij het maken van dit artikel:

Adriaan Eigenraam
Consultant RAM- en Safety Management
Movares, Utrecht

Jaap van Ekris
Senior Consultant in IT Risk, Maintainability and Reliability
Delta Pi, Vught

Michiel Blaauboer
Manager SysteemIntegratie, Systems Engineering en Industriële Automatisering
Movares, Utrecht

Gea Kolk
Senior adviseur en manager RAMS- en Risicomanagement
Movares, Utrecht

Arno Willems
Senior Consultant Risk & Reliability Engineering
IV-Infra, Papendrecht

Petra Heijnsbroek
Psychotherapeut / GZ-psycholoog (getrouwd met de auteur)
Auteur van de paragraaf: Frustratie en illusie van controle, een psychologische invalshoek.

Leeswijzer

Er bestaat veel spraakverwarring als gesproken wordt over het onderwerp van dit artikel. Dit begint bij de termen 'netwerk', gevolgd door 'redundant' en gaat verder naar zaken als 'betrouwbaarheid' en 'veiligheid'.

In deze leeswijzer worden enkele, in dit artikel gebruikte, definities gegeven. Het is mogelijk dat de definities in een andere context dan dit artikel variëren.
Er volgt een korte inleiding met het algemene idee.

- Hoofdstuk 1 geeft aan wat de aanleiding was voor het artikel en de context waarin het geschreven is.
- Hoofdstuk 2 geeft aan op welke wijze in het algemeen een hoge betrouwbaarheid kan worden bereikt.
- Hoofdstuk 3 behandelt zaken die mis kunnen gaan met het aantrekkelijke idee van 'redundantie'.
- Hoofdstuk 4 werkt een (praktijk-)voorbeeld uit waarin toepassing van redundantie een verslechtering van de betrouwbaarheid oplevert, in plaats van een verbetering.
- Hoofdstuk 5 geeft enkele praktijkvoorbeelden en illustraties.
- Hoofdstuk 6 geeft een eindconclusie en aanbevelingen.

Definities, zoals gehanteerd in dit artikel.

Netwerk
'Netwerk' wordt gebruikt in brede zin. Het omvat in dit artikel het (glasvezel-)transmissienetwerk met switches, de PLC's van de besturing en de servers voor het SCADA-systeem, met alles wat daar op en aan zit, zoals de voedingen. Het is geen objectenboom-onderdeel van een project.

Redundantie
Het woord betekent letterlijk *'overtollig'* of *'overbodig'*.
De volgende beschrijving is bijzonder passend in het kader van dit artikel:
'Redundancy is a system design in which a component is duplicated so if it fails there will be a backup.' Interessant is de toevoeging: 'Redundancy has a negative connotation when the duplication is unnecessary or is simply the result of poor planning.'

Betrouwbaarheid:
Betrouwbaarheid is een algemene term voor de mate van zekerheid waarmee een gewenste actie wordt uitgevoerd als dat nodig is, of gevraagd wordt. Soms wordt dit 'bedrijfszekerheid' genoemd. In dit artikel is hier niet voor gekozen.
'Beschikbaarheid' is een vorm van betrouwbaarheid, waarbij specifiek gekeken wordt naar het aantal uren per jaar dat de functie vervuld wordt (verkeer door de tunnel).
In dit artikel wordt de volgende definitie van 'betrouwbaarheid' gebruikt:
'De waarschijnlijkheid dat een systeem gedurende een bepaald tijdsinterval zonder falen zijn functie vervult.'

RAMS (Reliability, Availability, Maintainability, Safety) splitst 'betrouwbaarheid' op in vier verschillende aspecten. Verwarrend is, dat het eerste woord 'reliability' ook de algemene term is die de andere drie aspecten in zich draagt. In dit artikel komen enkele aspecten van RAMS aan de orde. Verder wordt niet op RAMS ingegaan.

In dit artikel wordt van het volgende uitgegaan:
- het gebruik van robuuste componenten;
- goed onderhoud;
- tijdige vervanging van alle componenten aan het einde van hun 'levensduur'.

Een zuivere discussie over het nut van redundantie wordt bemoeilijkt, omdat een combinatie van bovenstaande uitgangspunten in de praktijk bij tunnels niet vaak voorkomt.

Voor praktijkvoorbeelden wordt verwezen naar hoofdstuk 5.

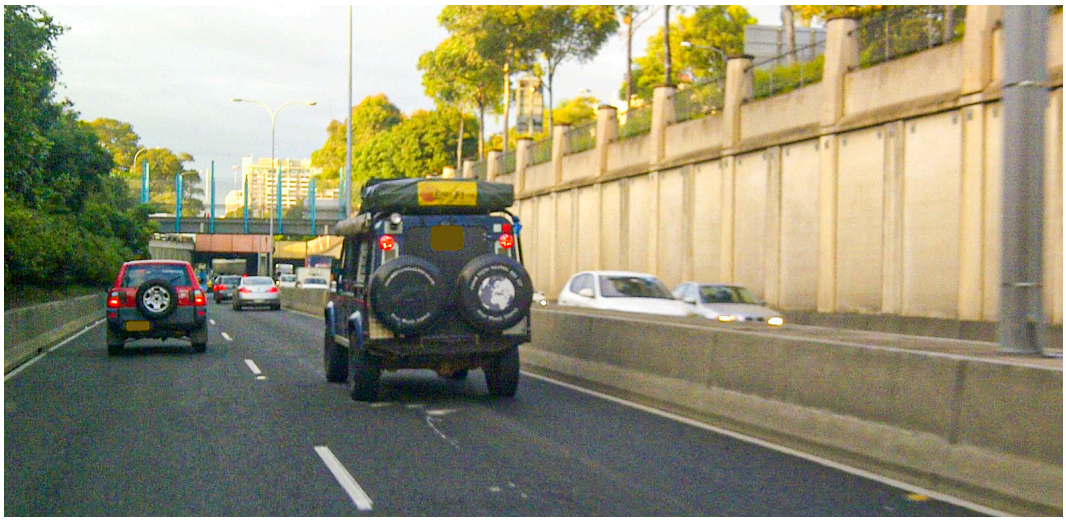
Inleiding

Tijdens een zakentrip naar Oostenrijk viel in het vliegtuig een kop koffie over de broek van een collega. Als wijs man had hij een reserve-broek meegenomen. Als nog wijzer man had hij in plaats van het gebruik van een redundante broek (twee over elkaar) een cold stand-by broek meegenomen (een reservebroek in de handkoffer).

Niemand denkt erover na in het natuurlijke leven: je trekt geen twee broeken over elkaar heen: in de eerste plaats zitten de twee broeken elkaar in de weg en hinderen elkaar en jezelf. Maar de nog belangrijker reden is dat iedereen zich bewust is van 'afhankelijk falen': het kopje koffie treft de tweede broek als je hem al aan hebt net zo goed als de eerste, terwijl de broek in de koffer veilig is.

In Nepal, waar de auteur een aantal jaren heeft gewerkt, werden Landrovers gebruikt voor de 'Camps'. Bij deze Camps ging een team naar afgelegen plaatsen om in een week of drie enkele honderden mensen te behandelen, opereren, etc. Er waren o.a. KNO-camps en gynaecology camps. De Landrovers met aanhangers namen zes reservewielen mee: 1x op de motorkap, 1x op achterdeur, 2x op het dak en 2x binnen.

Veel moderne auto's hebben helemaal geen reservewiel meer, maar alleen een spuitflesje. Als je een grote reis naar afgelegen gebieden maakt met een Landrover is het zinnig om reservewielen mee te nemen. Als je alleen maar op nederlandse snelwegen rijdt, is dat helemaal niet voor de hand liggend. De bestuurder (m/v) van de onderstaande Landrover gaat waarschijnlijk niet iedere dag zo op weg naar zijn/haar dagelijkse werk:



In tunnels wordt meestal een redundant netwerk gebruikt. Dit artikel gaat in op de effecten op de betrouwbaarheid en op het project als geheel bij het toepassen van redundante netwerken.

Het artikel hoopt bij te dragen aan bewustzijn van het nut en noodzaak (of het ontbreken daarvan) van redundante netwerken in tunnels.

1. Problemen in tunnels

Wat gaat er specifiek mis met netwerken?

Gebaseerd op ervaringen bij veel tunnelprojecten heeft Movares RAMS-berekeningen gemaakt van de prestaties van netwerken. Er is naar aanleiding van tegenvallende prestaties in de praktijk bekeken of de redundante netwerken zoals die vaak worden toegepast nu echt nodig zijn. Sommige veel-gebruikte vormen van redundantie blijken namelijk soms meer kwaad dan goed doen.

Verdere navraag bij een aantal tunnelprojecten maakte duidelijk dat bij al deze tunnels[1] dezelfde problemen optraden: verhoogde tot extreem verhoogde niet-beschikbaarheid door netwerkproblemen (het mechanisme hierachter wordt later besproken). Het probleem blijkt vrij universeel te zijn. De netwerken van de bevraagde tunnels hadden verschillende leveranciers en verschillende uitvoerende/ontwerpende aannemers.
Het is bekend dat het bijzonder moeilijk is om op langere termijn complexe redundante netwerken en systemen probleemloos te laten werken. Dit geldt ook voor tunnels.

"I know it's yesterday's ticket! That's when I got on this bloody train!"

Er is een verschil tussen systemen in tunnels en bijvoorbeeld in het spoor en in vliegtuigen op het gebied van veiligheid. Bij spoorbeveiligings-PLC's worden door Movares redundante netwerken en veiligheids-PLC's gebruikt. Bij bijvoorbeeld timings-problemen tussen de netwerken -en dus twijfel over de correctheid van wat de PLC ziet- wordt bijvoorbeeld direct het treinverkeer stilgelegd.
Bij vliegtuigen is de situatie anders: de start wordt niet afgebroken bij twijfel over het al of niet correct zijn van een input: men gaat door met starten, omdat dit niet anders kan. Dit is voor een startend vliegtuig het veiligst.
Bij tunnels is de situatie weer anders: de tunnel wordt veilig gemaakt door hem af te sluiten; de tunnel zelf is het veiligst als er geen verkeer is. Een netwerkprobleem in een tunnel levert overigens niet direct een gevaarlijke situatie op: de meeste systemen werken nog en de auto's kunnen in eerste instantie gewoon blijven rijden. Ook is er de mogelijkheid om de tunnel af te sluiten met een noodbediening.

'correctness' versus 'availability'

Bij 'correctness' gaat het programma/de installatie uitsluitend verder als er zekerheid is over de juistheid van de verkregen input en de correcte werking van het gehele systeem. Bij twijfel wordt het proces of de installatie in een veilige toestand gebracht (bij tunnels: verkeerslichten op rood en afsluitbomen dicht).

Bij 'availability' is de hoofdzaak het doorgaan van het proces en wordt zoveel mogelijk informatie gebruikt om het proces doorgang te laten vinden.

Eigenlijk het verschil tussen 'perfect' en 'better done than perfect.'.

Bij een tunnel kan afgewogen worden welk type PLC geschikt is: een veiligheids-PLC, een 'H-systeem', een redundante 'gewone' PLC, een enkele PLC, of een soft-PLC.
Vanzelfsprekend is de auteur zich bewust van het mogelijke effect van uitval van het netwerk: een verkeersinfarct en de boetes tot €100.000 per kwartier bij het sluiten van de tunnel door uitval van de besturing tijdens de spits. Deze effecten zijn zeker een probleem. De vraag is echter of 'redundantie' het probleem oplost (of juist groter maakt). Uiteindelijk blijft iedere 'oplossing' een afweging van risico's, kosten en baten.

1: In alle onderzochte tunnels (twaalf tunnels en een grote zeehaven) was sprake van door redundantie-problemen veroorzaakte storingen. Dit specifieke storingsmechanisme was in één geval verantwoordelijk voor 110 uur niet-beschikbaarheid per jaar (ieder jaar opnieuw). In deze tunnels is het netwerk uiteindelijk omgebouwd naar een enkelvoudig systeem.

De in dit artikel onderbouwde stelling luidt als volgt:
De besturing van tunnels zonder redundantie draaien veel stabieler en met minder problemen dan tunnels met redundante systemen. Ze zijn sneller te ontwerpen, gemakkelijker te testen, sneller in bedrijf te stellen, gemakkelijker te onderhouden. Ook worden storingen sneller opgelost. Tunnels zonder redundantie kosten substantieel minder in ontwerp, aanleg, testen, inbedrijfstellen, onderhoud en reparatie en bij vervanging.

Bij een extreem goed ontworpen en gemaakt systeem (zeer zeldzaam!) zal een redundant systeem op tunnel-niveau op papier een marginaal betere RAMS-performance laten zien (tegen zeer hoge kosten). Echter, hierbij blijft altijd het projectrisico bestaan dat ondanks de inspanningen en kosten de RAMS-performance van het redundante systeem in de praktijk lager uitpakt dan bij een enkelvoudig systeem. De lagere kosten van een enkelvoudig systeem zijn een zekerheid. Het rekenen met de marginaal betere RAMS-performance van een redundant systeem is een onzekerheid, omdat deze gemakkelijk kan omslaan naar een slechtere RAMS-performance. Een tunnel zonder redundantie geeft bij de bouw en over de levensduur een lager projectrisico.

Er mogen meestal ook een aantal storingen optreden zonder boete. Als de RAMS-performance van een enkelvoudig systeem voldoende goed is, is er geen reden om het projectrisico van een veel complexer systeem te nemen.

2. Hoe bereik ik een hoge betrouwbaarheid?

In dit hoofdstuk wordt betrouwbaarheid uit elkaar getrokken naar de RAMS-aspecten Reliability en Availability. Om het onderscheid aan te geven worden de engelse termen gebruikt.

Reliability gaat over de zekerheid dat een actie zal worden uitgevoerd als we daarom vragen: het sluiten van een waterkering, het openen van een brug, het sluiten van een afsluitboom.

Availability gaat over de verwachting dat we een minimaal aantal uren per jaar kunnen beschikken over de functie, zoals -in ons geval- het open zijn voor verkeer van een tunnel. Dat is (buiten veiligheid) het eerste doel van de tunnel: altijd doorgaan met verkeer, ondanks alles (zoals de Sinterklaas in een heet Nepal in het onderstaande plaatje)[2]:

Hoge betrouwbaarheid bereiken

In het algemeen gelden de volgende richtlijnen om tot een hoge betrouwbaarheid te komen:
1. Beperk het aantal componenten tot een minimum;
2. Verminder de afhankelijkheid;
3. Maak de downtime klein.[3]

Ad 1. Beperk het aantal componenten tot een minimum

Alles wat er niet is, kan ook niet defect raken. Het vermijden van niet-essentiële apparatuur, functies, software-features, complexe systeemarchitectuur en dergelijke verhoogt de betrouwbaarheid. Bepalende vraag: hoe kan ik met een minimum van robuuste functies en robuuste apparaten mijn doel bereiken? Het gaat om de **kunst** van het weglaten!
Hier geldt het KISS-principle: keep it smart & simple.

Ad 2. Verminder de afhankelijkheid

In de RAMS-berekeningen is afhankelijk falen een belangrijk verschijnsel. Wat heeft het voor zin om een vliegtuig van vier motoren te voorzien als het dominante faalmechanisme het vormen van ijsafzetting op de inlaat is? Als dit bij één motor gebeurt, gebeurt het bij allemaal. Er ontstaat geen voordeel bij vier motoren ten opzichte van een enkele motor. Als er sprake is van een dominant beschadigingsmechanisme, zoals het opgraven van een glasvezelkabel, of het doorknagen van de kabel door muizen, dan heeft het geen zin om twee kabels direct naast elkaar te leggen. Als softwarefalen het dominante faalmechanisme is, dan heeft het geen zin om twee parallele apparaten te hebben met dezelfde software.

2: Locatie: Pokhara, Nepal.Locatie: Pokhara, Nepal. Het is warm in de zon, de baard zit niet geweldig, de staf is een plastic bezemsteel, máár, de kindertjes zitten vol spanning te wachten! Ik heb geen perfecte staf en zo, maar ik ga door! Want de kindertjes zitten te wachten: 'availability'.

3: De 'downtime' is de tijd dat de functie niet vervuld kan worden en bestaat bijvoorbeeld uit de tijd benodigd voor: opmerken van de storing; oproepen van de storingsdienst; aanrijdtijd van de monteur en verkeerregelaars; creëren veilige situatie voor reparatie; storingzoeken; oplossen van storing of maatregelen nemen voor tijdelijk functieherstel (voldoende reservedelen zijn aanwezig op locatie); testen van de reparatie en in bedrijf nemen; opheffen tijdelijke situatie en veiligheidsmaatregelen; opstellen van de tunnel.

Immers, bij dezelfde slechte combinaties van omgevingsinvloeden gaan ze allebei op hetzelfde moment fout.[4]
Bij een hoge mate van afhankelijkheid wordt de betrouwbaarheid van het geheel vooral bepaald door één of enkele factoren of faalvormen. Complexe systemen zullen al snel meer afhankelijkheden in zich hebben, die soms moeilijk te zien zijn, maar wel de betrouwbaarheid van het geheel negatief beïnvloeden.

Ad 3. Maak de downtime klein

Alles zal uiteindelijk eens defect raken; daar is niets aan te doen.
Om een hoge availability te bereiken, is het nodig dat een defect snel hersteld kan worden (downtime klein maken). Dat is mogelijk door een combinatie van:

- snel storingen kunnen localiseren;
- defecte delen snel kunnen vervangen (of resetten) en weer opstarten;
- de juiste reservematerialen op voorraad hebben of beschikbaar kunnen maken.

Hier komt tevens de versterkende werking van de punten 1. t/m 3. naar voren (minimum aantal componenten, afhankelijkheid klein en downtime klein). Immers, een eenvoudig systeem maakt storingzoeken eenvoudiger en daarmee sneller. Bij weinig kans op afhankelijk falen is de kans dat er veel tegelijk defect raakt door een gemeenschappelijke oorzaak ook kleiner. Dit maakt het weer gemakkelijker om de enkele storing te localiseren.
Juist op dit punt komt het venijn van redundantie boven: men is al snel geneigd om het probleem van de downtime in tunnels (lage availability) op te lossen door redundantie. Echter, dit is juist een grote bedreiging voor de punten 1. en 2. waardoor het effect in de praktijk tegenvalt, of zelfs tegengesteld is.

Op een Movares-dag voor studenten was er een wedstrijd tussen studenten wie het beste en snelste een treinbeveiliging kon ontwerpen op een Arduino-microprocessor voor een modelspoorlijn die daar opgebouwd was. Het winnende groepje had een goed werkend ontwerp gemaakt. Hierbij was de 'positieve' kanttekening dat er een stukje extra handige functionaliteit ingebouwd was. Eigenlijk had de kanttekening negatief moeten zijn: het inbrengen van ongevraagde extra functionaliteit is sterk kostenverhogend door meer programmeerwerk, een grotere testinspanning voor het aantonen van de vereiste betrouwbaarheid. Ook vergroot het de faalkans van het geheel door verhoogde omvang en complexiteit van de software, want software is sowieso al fragiel.

Een slecht idee dus. Bij studenten is het verzinnen van 'slimme' extra functionaliteit misschien een positief punt en leidt het tot een hoger cijfer. In de dagelijkse praktijk kan deze keuze het project juist beschadigen.

4: Bij de landelijke '112-storing' van midden 2019 was dit het probleem. De hardware was viervoudig uitgevoerd (super-redundant), maar op alle redundante machines was dezelfde software geïnstalleerd. Bij het falen van de software faalden alle machines. De software was identiek en was het 'single point of failure'.

Frustratie en illusie van controle, een psychologische invalshoek.

Petra Heijnsbroek, Psychotherapeut/GZ-psycholoog

Ieder mens heeft behoefte aan competentie (ook wel mastery genoemd). Dit is een psychologische basisbehoefte die motiveert (en daarmee activeert) te blijven proberen en te leren totdat beheersing van het resultaat ervaren wordt. Bij een succesvol resultaat wordt aan deze behoefte voldaan. Dit geeft een goed gevoel.
We willen graag ons leven (en onze techniek) beheersen en hier controle over houden. De realiteit is echter dat dingen mis gaan -bij onszelf, bij de ander en ook in de techniek. Dat geeft frustratie (geen prettig gevoel). Het liefst staan we hier niet te lang bij stil.
Het is makkelijker ervan uit te gaan dat alles maakbaar is en dat we controle hebben.
Leven en werken vanuit dit denken wordt 'illusie van controle' genoemd.

Frustratie is geen aangenaam gevoel. Actief worden – iets gaan doen – helpt om een ander, prettiger gevoel te verkrijgen. Dit gebeurt op verschillende manieren. Het doen op zich geeft al een beter gevoel: minder onmachtig omdat je wat hebt gedaan. Verder genereert actief worden vaak ook waardering van een ander (en zeker van je baas die je tenslotte betaalt om wat te doen 😀)
Helaas is niet iedere actie even zinnig en effectief. Het is fijn als je je minder gefrustreerd of onmachtig voelt, maar is het werkelijke levens- of technische probleem nu minder geworden?
Er is niets mis met het nemen van actie om een beter resultaat te bereiken. Wel is het de vraag of de actie het werkelijke probleem aanpakt, of dat slechts de illusie van controle vergroot wordt. In het laatste geval is het vooral een actie gericht op beter voelen geweest.

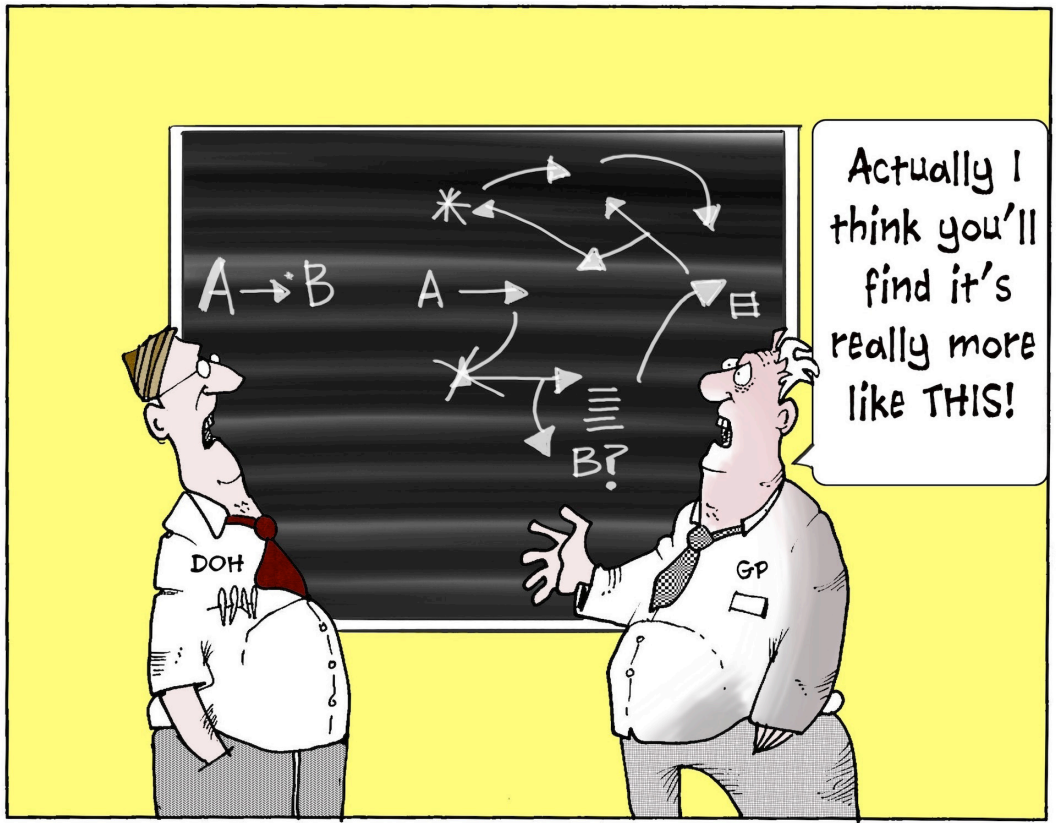
Gedrag wordt aangestuurd door twee verschillende systemen met twee kwalitatief verschillende denkprocessen.[5]
1. Reflectief systeem. Dit bestaat uit trage, gecontroleerde denkprocessen die moeite kosten en die onderhevig zijn aan bewuste overwegingen en regels. Hier is denktijd voor nodig en een niet te hoog stressniveau.
2. Impulsief systeem. Dit werkt associatief. Dit is een snelle en automatische denkprocessor. Gevoelens spelen hier een belangrijke rol in.

Het is nodig de illusie van controle los te laten en om frustratie te kunnen verdragen - frustratie dat er iets mis gaat. Soms is minder of iets anders doen effectiever dan (dezelfde soort) actie in te zetten. Hierover nadenken en overwegen vraagt een extra inspanning. Juist op stressvolle momenten ruimte maken voor nadenken en overwegen over het effect op het probleem, helpt hierbij.

5: Bron: Kinderen uit de Knel. Justine van Lawick & Margreet Visser.
B.V. Uitgeverij SWP Amsterdam. 3e druk 2019.

3. Het venijn van redundantie

In de leeswijzer is 'redundantie' als volgt omschreven: 'Redundancy is a system design in which a component is duplicated so if it fails there will be a backup.'
Dit klinkt zeer aantrekkelijk (en is het soms ook), maar helaas is het niet altijd zo eenvoudig in een complexe omgeving.



Slechts beperkt positief effect van redundantie.

Bij 'afhankelijk falen' zorgt een verschijnsel/verstoring er voor dat de hoofdcomponent en de redundante component beiden tegelijk, of kort na elkaar, falen.
Bij gebruik van redundantie zorgt 'afhankelijk falen' er in het algemeen voor dat we ten hoogste een factor 10 verbetering in betrouwbaarheid van dat systeemdeel kunnen bereiken.[6]

Introductie van extra faalmechanismen

Als gekozen wordt voor een oplossing met twee tegelijk werkende en elkaars werking controlerende systeemdelen, bestaat de kans dat er (momentaan) verschillen ontstaan tussen de toestand van die delen. Dit verschil wordt gedetecteerd, met een foutmelding of systeem-actie tot gevolg.
Een veiligheids-PLC is hier een goed voorbeeld van. Een timings-verschil tussen inputs of een netwerk-ingang wordt geïnterpreteerd als mogelijk defect. Een veiligheids-PLC zal dan in het algemeen stoppen en naar een veilige toestand gaan. Echter: er was misschien niets aan de hand, maar het zou kunnen. Voor de zekerheid wordt een actie ingezet: veilige

6: Als bijvoorbeeld de koeling van een schakelkast uitvalt, dan zullen redundante componenten in dezelfde kast snel na elkaar defect raken, omdat de resulterende oververhitting beide componenten tegelijk treft. Vergelijkbare situaties treden op bij componenten van dezelfde serie (waar dezelfde zwakke punten in zitten), dezelfde onderhoudsmonteur die dezelfde fouten heeft gemaakt en dergelijke.
Afhankelijk falen is een complex onderwerp. Echter, een maximaal bereikbare verbetering bij normale, zorgvuldige toepassing van redundantie met een factor 10 is een goede vuistregel. Voor verdieping wordt verwezen naar de literatuur.

stand aannemen en stoppen.
Dit is veilig bij een spoorwegovergang; maar storend bij een tunnel.

Extra factoren die de beoogde werking van 'de redundantie' negatief kunnen beïnvloeden:
- de software die de redundantie regelt is een storingsbron op zich. 'Redundantie-softwareprobleem' is een faalmechanisme dat een enkelvoudig systeem simpelweg niet heeft;
- meerdere redundante (sub-)systemen in het netwerk;
- extra benodigde (soms zeer kritische) instellingen van machines en randapparatuur;
- DIP-switches die goed moeten staan;
- configuratie-tabellen in het netwerk;
- firmware-onvolkomenheden in de redundantiefunctie van de PLC's zelf;
- bijhouden van de juiste configuraties van alle systeemdelen over de jaren heen (na vervanging van delen van het systeem, firmware-updates, software-updates, uitbreidingen, etc.);
- gebrek aan mogelijkheden voor het af en toe testen van de redundantie-functionaliteit, zodat ingeslopen fouten onopgemerkt blijven;
- fout-maskering: een fout wordt in een redundant systeem minder snel opgemerkt, omdat de fout 'opgevangen' wordt door de redundante componenten. Een (gedeeltelijk) defecte component kan dus lange tijd 'overleven' in het geheel, maar bij falen van de nog wel goed werkende component blijkt dat de defecte component waarop gerekend werd al lange tijd niet meer actief was en het systeem alsnog uitvalt;
- bij redundante servers wordt dit probleem nog verergerd. Een server is gevoeliger voor timings-problemen, omdat een server inwendig veel "drukker" en onvoorspelbaarder is dan een PLC.

Het stabiel krijgen van een redundant systeem is zeer lastig en zeer kostbaar. Het stabiel houden van een redundant systeem over de jaren is nog veel lastiger. Een probleem met redundantie blijkt vaak pas in extreme situaties: juist de tijd waarin men storingen het minst kan gebruiken.
Voor de algemene aanduiding van de extra geïntroduceerde faalvormen en bijkomende problemen die optreden bij het gebruik van redundantie in een netwerk is gekozen voor: 'instabiliteit' van het netwerk.
Bij de onderzochte tunnels bleek dit faalmechanisme over het algemeen verantwoordelijk voor ongeveer de helft van het aantal ernstige netwerk-storingen die het sluiten van de tunnel tot gevolg hadden. Bij enkele tunnels was het probleem extreem en bovendien niet oplosbaar.

Complexiteit

Complexe systemen, waar veel gebeurt, worden door redundantie bijna onmogelijk complex. Er is simpelweg niet meer te overzien wat er op een bepaald moment gebeurt en hoe gebeurtenissen op elkaar ingrijpen.
In tunnels waar bijna alle subsystemen ook redundant zijn uitgevoerd wordt het probleem exponentieel groter.

Is dit het juiste middel?

De vraag is of redundantie het juiste middel is voor de kwaal (storingen). De volgende vragen verkennen dit:
- Is redundantie echt nodig voor dit (sub-)systeem?
- Pakt de redundantie het dominante probleem aan?
- Is de vorm van redundantie zodanig dat substantiële winst te behalen is?
- Kan ik mijn probleem op een andere manier oplossen (availability-budget wat verhogen en elders wat verlagen)? Hoe veel draagt dit systeem bij aan de totale niet-beschikbaarheid?
- Introduceert het geen niet-merkbaar falen in mijn systeem?

Bij een grote leverancier van PLC-systemen werd discussie gevoerd over redundante systemen voor het tunnel-project. De leverancier had geclaimd dat de PLC's speciaal ontworpen waren op hoge beschikbaarheid bij redundante configuratie en dat dat niet fout kon gaan. Bij het koffie-halen op de gang kon het projectteam (inclusief de auteur) echter een gesprek van mede-koffiehalers volgen over redundantie-problemen die optraden bij het betreffende systeem die al een tijdje speelden en ook door het hoofdkantoor tot op heden niet opgelost waren.

Samenvattend:

- De winst in betrouwbaarheid van een redundant netwerk is veel lager dan vaak wordt gehoopt (en berekend);
- De introductie van extra faalmechanismen door redundantie verdubbelt het aantal storingen van het netwerk bij de onderzochte tunnels (of erger);
- Het toepassen van redundantie zondigt tegen de eerste twee basisregels voor een betrouwbaar systeem (aantal componenten tot een minimum beperken en afhankelijkheid verminderen);
- De gewenste winst in betrouwbaarheid van de tunnel als geheel kan wellicht goedkoper en effectiever op een andere manier bereikt worden;
- De ontwerp- en onderhoudsinspanning voor een effectief redundant systeem is zeer veel groter dan voor een enkelvoudig systeem.

4. De uitwerking van een rekenvoorbeeld in een tunnel

In dit hoofdstuk wordt een getallenvoorbeeld uitgewerkt als illustratie van het gestelde in de voorgaande hoofdstukken. De performance van een enkelvoudig systeem wordt vergeleken met de performance van hetzelfde systeem, maar dan redundant uitgevoerd.

Er wordt gestart met de uitgangspunten voor een hoge beschikbaarheid:
1. Beperk het aantal componenten tot een minimum;
2. Verminder de afhankelijkheid;
3. Maak de downtime klein.

Bovenstaande uitgangspunten leveren een enkelvoudig netwerk op:
- 1 enkelvoudige glasvezelring;
- 1 centrale besturings-PLC (geen veiligheids-PLC);
- 1 SCADA-server;
- enkelvoudige voedingen (via een UPS);
- aanvullende maatregelen om de downtime klein te maken (niet verder behandeld).

Enkelvoudig systeem

Voor het enkelvoudige systeem is het volgende vereenvoudigde schema opgesteld voor 'het netwerk'. Hiervoor zijn praktijkgetallen gebruikt (zie kader).

Apparaat	Faalkans per uur (tunnel dicht)
SCADA-server software	5,7E-5
SCADA-server hardware	7,76E-6
Voeding UPS	7E-6
Switch + voeding 24V	3,04E-6 + 7E-7 = 3,74E-6
Glasvezelkabel, dubbel, gescheiden gelegd, 10km	10E-5 // 10E-5 = 10E-6
Switch + voeding 24V	3,74E-6
centrale PLC software	5,7E-5
voeding UPS	7E-6
centrale PLC hardware	6,7E-6
glasvezel	verwaarloosbaar, zeer kort en beschermd
switch + voeding 24V	3,74E-6
glasvezel in ring gelegd, 2km	2E-6
Switch + voeding 24V	3,74E-6
glasvezel	verwaarloosbaar, zeer kort en beschermd
RIO + voeding 24V	2,86E-7 + 7E-7 = 1E-6
Subtotaal hardware	5,6E-5
Subtotaal software	11,4E-5
Totaal faalkans netwerk	17E-5

De faalkans per uur voor het enkelvoudige netwerk is 17E-5, wat overeenkomt met 1,5 storingen per jaar.
Voor de tunnel als geheel komt hier nog de faalkans van de andere tunnelsystemen bij. In de praktijk is de faalkans van alle andere tunnelsystemen bij elkaar ongeveer gelijk aan de faalkans van het netwerk. Deze twee (netwerk en andere installaties) bij elkaar opgeteld geeft 1,5+1,5= 3 storingen per jaar.

De getallen voor de software-betrouwbaarheid zijn berekend met TOPAAS (Task Oriented Probability of Abnormalities Analysis for Software), een RWS-methodiek) en vervolgens vergeleken met de prestaties van een grote verkeerstunnel op één van de drukste punten in NL. Het bleek dat de schatting volgens TOPAAS zeer goed overeenkwam met de prestaties van de tunnel in de praktijk.
NB TOPAAS geeft de faalkans op aanspraak. Via een veel-gebruikte methode (via tabellen in de IEC61508-1) kan dit 'omgerekend' worden naar de faalkans per uur.

De hardware betrouwbaarheidsgetallen zijn ontleend aan een RWS-overzicht met praktijk-getallen. Voor het gemak is aangenomen dat de SCADA-server software net zo betrouwbaar is als de PLC-software.

Systeem met redundantie

Bij het volgende overzicht zijn zoveel mogelijk delen van het netwerk redundant gemaakt, met de volgende uitgangspunten:

- afhankelijk falen is gesteld op 0,1, dus een verbetering van een factor 10 voor een redundant systeem;
- voor de faalvorm 'instabiliteit netwerk' is een faalkans genomen die gelijk is aan de faalkans voor de bijbehorende software;
- faalvorm 'instabiliteit' is bij het subtotaal gerekend onder de software.

Apparaat	Faalkans per uur (tunnel dicht)
SCADA-server software	5,7E-5
blijft zo: identieke software op beide servers	
SCADA-server hardware	7,76E-6 → 7,76E-7
factor 10 verbetering	
Extra faalvorm 'instabiliteit'	5,7E-5
Voeding UPS	7E-6
blijft zo: één UPS	
Switch + voeding 24V	3,74E-6 → 1E-6
bijna factor 10 verbetering, maar 2x zo veel switches	
Glasvezelkabel, dubbel, gescheiden gelegd, 10km	10E-5 // 10E-5 = 10E-6
Blijft zo: was al dubbel.	
Switch + voeding 24V	3,74E-6 → 1E-6
Extra faalvorm 'instabiliteit'	5,7E-5
centrale PLC software	5,7E-5
blijft zo: identieke software op beide servers	
voeding UPS	7E-6
centrale PLC hardware	7,76E-6 → 7,76E-7
factor 10 verbetering	
glasvezel	verwaarloosbaar, zeer kort en beschermd
switch + voeding 24V	3,74E-6 → 1E-6
glasvezel in ring gelegd, 2km	2E-6 → 1E-6
(afhankelijk falen groot, want beide ringen liggen altijd naast elkaar)	
Switch + voeding 24V	3,74E-6 → 1E-6
glasvezel	verwaarloosbaar, zeer kort en beschermd
RIO + voeding 24V	2,86E-7 + 7E-7 = 1E-6 → 1E-7
Subtotaal hardware	3,1E-5
Subtotaal software	22,8E-5
Totaal faalkans netwerk	26,6E-5

De faalkans per uur voor het redundante netwerk is 26,6E-5, wat overeenkomt met 2,3 storingen per jaar.
Het tunneltotaal komt hiermee (netwerk + andere installaties) op 2,3+1,5= 3,8 storingen per jaar.

Conclusie

De betrouwbaarheid van het netwerk is in dit rekenvoorbeeld bij toepassing van redundantie juist afgenomen. Dit wordt in zijn geheel veroorzaakt door introductie van het extra faalmechanisme 'instabiliteit'.
De tunnel-performance als geheel is door toepassing van een redundant netwerk verslechterd van 3 storingen per jaar voor een enkelvoudig netwerk naar 3,8 storingen per jaar voor een redundant netwerk.
Een 'storing' is in dit verband: tunnelsluiting door een technische storing.

5. Praktijkvoorbeelden en illustraties

Tunnel A

Deze tunnel was de aanleiding voor de interesse in het onderwerp. Mijn collega Adriaan Eigenraam merkte op, dat de RAMS berekeningen aangaven dat een redundant netwerk helemaal niet nodig is om de vereiste betrouwbaarheid van de tunnel te realiseren. Dit is dan ook niet gedaan.
De tunnel draait probleemloos met dit enkele (ring-)netwerk.
Een andere tunnel is daarop ook enkel uitgevoerd (behalve helaas de MMI-server). Ook deze tunnel draait al een aantal jaren probleemloos.

Tunnel B

Deze tunnel (of aantal tunnels) is uitgerust met een geheel dubbel glasvezelnetwerk, met dubbele PLC's, servers, etc. Dit geheel was (ook met hulp van het hoofdkantoor van de PLC-leverancier) niet stabiel te krijgen, wat resulteerde in een jaarlijks terugkomende niet-beschikbaarheid van 110 uur door redundantie-fouten. Uiteindelijk is na een jaar of 10 besloten om het gehele redundante deel te verwijderen.

Tunnel C

Deze tunnel (één van de drukste verkeerstunnels) is gebruikt om de werkelijke betrouwbaarheid van de tunnel met betrekking tot de bediening en besturing te onderzoeken. De gegevens zijn afkomstig van de onderhoudsafdeling. Pijnlijk is, dat de ontwerpafdeling niet op de hoogte was van de performance tijdens de gebruiksfase. Diverse claims van de aannemer over het al of niet optreden van storingen bleken in de praktijk niet te kloppen. Bij deze tunnel bleek het aantal storingen door redundantiefouten in aantal ongeveer overeen te komen met de storingen van het bedienings- en besturingssysteem. Het toevoegen van redundantie leidde in dit geval dus tot twee maal zoveel storingen dan het geval zou zijn geweest als de redundantie er niet geweest was.
Opvallend was, dat een TOPAAS-berekening precies de uitkomst aangaf die ook in de praktijk gerealiseerd werd.

Tunnel D

Deze tunnel is interessant, omdat vanaf het begin is overlegd over redundantie.
De opdrachtgever adviseerde om een enkelvoudig systeem toe te passen. De opdrachtnemer koos er echter voor om toch een (beperkte) redundantie toe te passen. Er zijn extra maatregelen genomen en er is door de opdrachtnemer speciale aandacht aan redundantie besteed. Er zijn door een expert van de opdrachtgever diverse aanvullende tips en maatregelen voorgesteld om de goede werking van het systeem te borgen.

De omstandigheden voor de realisatie van een redundant netwerk bij deze tunnel waren bijna ideaal:

- Bij zowel de opdrachtnemer als de opdrachtgever waren goede professionals betrokken met veel kennis en ervaring;
- Er werd goede kwaliteit apparatuur toegepast;
- Er was een goed onderhoudsplan;
- Alle ondersteuning van de apparatuur was aanwezig door het moederbedrijf (leverancier van het betreffende systeem);
- Er was sprake van een meedenkende opdrachtgever, die ook actief hulp inbracht.

Met de (in een later stadium) berekende RAMS-getallen viel de RAMS-performance van een geheel enkelvoudig systeem ruimschoots binnen de vereiste grenzen en waren bij deze tunnel, ook bij een sterk tegenvallend aantal storingen, geen boetes te verwachten.

Kosten bij tunnel D vanwege deze -op grond van betrouwbaarheid onnodige- redundantie

Voor de meer-kosten zijn geen berekeningen gemaakt. De gegeven getallen zijn orde-grootes en geven slechts een ruw idee.

Het gehele project had een waarde van ongeveer 25 miljoen euro. De gekozen bedragen zijn conservatief ingeschat en zullen eerder hoger zijn geweest dan lager. De kosten zijn uitsluitend de meerkosten voor het realiseren van de redundantie en oplossen van problemen met de gerealiseerde redundantie:

- Extra apparatuur, inclusief voorzieningen (kasten, koeling, voedingen, aanleg, controles bij IBS): €100.000
- Meerkosten ontwerp (tekeningen, ontwerp, inkoop, berekeningen): €20.000
- Meerkosten instellen apparatuur (dip-switches, 'vinkjes', configuratietabellen, problemen oplossen, etc.) en om de FAT (Factory Acceptance Test) te laten slagen (na 6 maanden na de eerste mislukte redundantie-FAT was het redundantieprobleem nog niet opgelost): €10.000
- Meerkosten problemen oplossen bij de inbedrijfstelling, SAT (Site Acceptance Test) en SIT (Site Integration Test): €100.000
- (Dit is buiten de organisatorische kosten voor de ondersteuning, bijhouden restpunten, her-SATs, etc.)
- Meerkosten voor opdrachtgever voor extra ondersteuning van de opdrachtnemer: €20.000
- Meerkosten bij onderhoud: storingzoeken is lastiger, er zullen meer storingen zijn, omdat er ook redundantiestoringen bijkomen, er gaat meer apparatuur stuk, etc.: €50.000
- Meerkosten bij vervanging van apparatuur aan einde levensduur, inclusief alle instellingen, extra testen, etc: €100.000

Met al deze kosten was op het moment van openstelling nog geen stabiel systeem verkregen. De redundantie-problemen waren dusdanig disruptief, dat er geen tijd meer was om vóór openstelling alle andere problemen grondig op te lossen. Na openstelling was nog veel tijd nodig om het systeem stabiel te krijgen. Het is onbekend of het systeem inmiddels stabiel is. Het lijkt er op dat een 'rock-stable' systeem niet aan de orde zal zijn.

Interessant: bij het uitzetten van redundante servers bleken de systemen opeens veel beter te lopen. Er is zelfs overwogen om een aantal redundante servers permanent uit te schakelen, omdat de problemen niet oplosbaar leken in de beschikbare tijd. Dit is tot één dag vóór openstelling nog een laatste optie gebleven.
De redundantieproblemen hebben de oplossing van de andere netwerkproblemen (o.a. samenwerking met andere subsystemen) zeer gehinderd en vertraagd. Het oplossen van problemen is zonder bijkomende redundantieproblemen al moeilijk genoeg.

Baten voor tunnel D van de toegepaste redundantie op tunnelniveau

Het berekende aantal storingen van de tunnel is verminderd:

- 1,36 storingen per jaar voor een geheel enkelvoudig systeem;
- 1,31 storingen per jaar voor het huidige redundante systeeem.

Het aantal toegestane storingen zonder boete is 4 per jaar.

Conclusie

De meerkosten voor het redundante systeem van tunnel D zijn in de orde-grootte van €400.000 (en veel hoofdpijn).
De baten zijn een toename van de tunnelbetrouwbaarheid van minder dan 4% t.o.v. een geheel enkelvoudig systeem.
Deze toename van de tunnelbetrouwbaarheid heeft geen invloed op het aantal boetes, zelfs niet als het werkelijke aantal storingen drie maal zo groot wordt als berekend.

6. Eindconclusie en aanbeveling

Aanleiding van dit artikel waren de problemen in tunnels die ontstaan ten gevolge van het vaak onnodige gebruik van redundantie in het netwerk. Het is de mening van de auteur dat redundantie beter zoveel mogelijk vermeden kan worden. Bij het toch willen toepassen van redundantie is een zorgvuldige overweging benodigd, zodat de redundantie niet de bananenschil is waar een project over uit kan glijden. Het spreekt overigens voor zich dat ook het ontwerp van een enkelvoudig systeem de nodige aandachtspunten kent.
Voor de faalkans van de faalvorm 'instabiliteit' adviseert de auteur om deze gelijk te houden aan de faalkans van de software, zoals berekend met TOPAAS. Het lijkt er op dat dit een redelijke aanname is.[7]

7: RAMS-getallen zijn statistische getallen en hoeven dus niet voor uw of mjin specifieke systeem 'waar' te zijn. Echter, in de onderzochte gevallen zijn wel grote afwijkingen in negatieve zin geconstateerd, maar geen grote afwijkingen in positieve zin. De aanbevolen faalkans lijkt dus aan de veilige kant. Met andere woorden: bij het gebruiken van de geadviseerde faalkans zal het redundante systeem er in sommige gevallen nog (te?) gunstig uitkomen. Deze faalkans moet in rekening gebracht worden bij ieder redundant (sub-)systeem apart. Bij redundantie van server, van PLC en van een subsysteem moet deze faalkans dus drie maal in rekening gebracht worden, op de juiste plaats. Gezien de exponentieel stijgende problemen bij het combineren van meerdere op zich redundante systemen lijkt ook dit zeer behoudend (i.e. wellicht te gunstig uitvallend voor het redundante systeem).