Failure Mode Error Analysis (FMEA)

KHBO, Hobufonds SAFESYS
ing. Alexander Dekeyser
ing. Kurt Lintermans

IEC 812 Analysetechnieken voor systeem-betrouwbaarheid Procedure voor falende mode en effecten-analyse (FMEA)

1. Algemeen

Er zijn twee methoden : FMEA en FMECA (+ criticiteit)
Deze zijn bedoeld om een betrouwbaarheidsanalyse te doen zodat falingen kunnen geïdentificeerd worden die significante konsekwenties kunnen hebben op de systeemperformantie

Er kunnen kwantitatieve en kwalitatieve analysemethodes worden toegepast.
Kwantitatieve methodes laten toe een berekening of een voorspelling te maken van de performantie-indicatoren bij de uitvoering van een specifieke taak (of taken) tijdens langdurige werking van het systeem.
Typische indicatoren zijn betrouwbaarheid , veiligheid , beschikbaarheid , faalrata , MTTF (mean time to failure) , enz.

De FMEA is gebaseerd op het componentniveau of assemblage-niveau waarvan de faalcriteria (primaire faalmodes) beschikbaar zijn.
Startende vanuit de faalkarakteristieken van de basiselementen en de functionele systeemstructuur , legt de FMEA vast wat de relatie is tussen de componentfalingen en de systeemfalingen , de defecten , operationele beperkingen en degradatie van de performantie of integriteit.

De graad van de gevolgen van het falen wordt beschreven door de ‘criticiteit’.
De criticiteit wordt aangeduid door categoriëen of niveaus die functies zijn van de gevaren en het verlies van systeem-capaciteiten en soms door de kans van haar optreden.

De criticiteitsanalyse van de geïdentificeerde faalmodes is bekend als FMECA.

1.1 Doel van de analyse

Belangrijk voor het garanderen van de betrouwbaarheid.
De analyse wordt beknopt uitgevoerd tijdens de conceptvorming , de planning en de definitie-fase maar wordt meer uitgebreid gebruikt tijdens de ontwerpfase.
FMEA is een inductieve methode voor het uitvoeren van een kwalitatieve systeem-betrouwbaarheidsanalyse .

Het ontwikkelen van ‘ Reliability Block Diagrams (RLBs) ‘ en ‘ State Diagrams ‘ , afgeleid van de systeem- structuur , is gerelateerd met de FMEA
Afzonderlijke diagramma’s zijn nodig voor :
- *verschillend geïdentificeerde criteria voor falen van het systeem*
- *degradatie van de functies of reductie van betrouwbaarheid van de functies*
- *de veiligheid*
- *alternatieve operationele fases*

Men maakt een FMEA of een FMECA-analyse voor :

a) de evaluatie van de effecten en de gevolgen van gebeurtenissen veroorzaakt door elke geïdentificeerde faalmode , door welke reden dan ook veroorzaakt , op verschillende niveaus van de functionele hyrarchie van het systeem.
b) het vastleggen van de significantie of criticiteit van elke faalmode t.o.v de correcte functie of de performantie van het systeem en de impact op de betrouwbaarheid en/of veiligheid van het betrokken proces
c) klassificatie van de geïdentificeerde faalmodes volgens hun detecteerbaarheid , diagnoseerbaarheid , testbaarheid , item vervangbaarheid , voorzieningen voor compensatie tijdens bedrijf (herstelling , onderhoud , logistiek) en andere.
d) het schatten van de mate van de significantie en de kans op falen , afhankelijk van de beschikbare data

1.2 Toepassing

1.2.1 FMEA – veld van toepassing

Een FMEA is een methodiek die in de eerste plaats wordt gebruikt voor de studie van het gebruikte materiaal en het falen ervan , het kan toegepast worden op verschillende categoriëen systemen (op basis van technologie zoals electrisch , mechanisch , ..)
De FMEA kan ook gebruikt worden voor de studie van software en menselijk presteren.

1.2.2 FMEA – toepassing in het kader van een project

De gebruiker moet vastleggen hoe en voor welke redenen hij een FMEA gebruikt in zijn technische discipline.
Het kan alleen gebruikt worden of in combinatie met andere betrouwbaarheidsanalyses.
De noodzaak voor een FMEA vindt zijn oorsprong in de noodzaak voor het begrijpen van het gedrag van de hardware en de implicaties voor de operatie van het systeem

FMEA is een techniek die voor het nazicht van het ontwerp , de garantie en beoordeling van correct ontwerp , vanaf de ontwerpfase van het systeem gebruikt wordt.
FMEA is geschikt voor alle niveaus van het systeemontwerp.
FMEA moet bijgehouden worden via updates naarmate het project vordert en het ontwerp verandert.
Aan het eind van het project wordt de FMEA gebruikt om het project-ontwerp te controleren en kan het essentieel zijn voor de demonstratie van het conform zijn van het ontworpen systeem aan de vereiste standaarden, regelgevingen en gestelde eisen van de gebruiker.

Gewonnen informatie via de FMEA identificeert prioriteiten voor procescontroles en inspectie-testen tijdens het vervaardigen en de installatie en voor kwalificatie , akkoord gaan en aanvaarden van start-up tests.
Het levert essentiële informatie voor diagnostische procedures en onderhoud-procedures.

Voor de beslissing tot in welke mate en de manier waarop de FMEA moet worden toegepast op een item of een ontwerp , moet men de specifieke doelstellingen waarvoor de FMEA-resultaten nodig zijn in acht nemen , alsook de tijdsynchronisatie met andere activiteiten en controle over ongewenste faalmodes - en effecten.
Dit leidt tot de planning van de FMEA in kwalitatieve termen op specifieke niveaus (systeem , subsysteem , component , item) volgens het ontwikkelingsproces.

1.2.3 Gebruik van FMEA

a) identificeren van falingen die , wanneer ze alleen optreden , niet-accepteerbare of significante effecten hebben , en het vastleggen van de faalmodes die de bedoelde werking serieus kunnen beïnvloeden.
b) het bepalen van de nood aan :
- redundantie
- ontwerp-kenmerken die de 'fail-safe' status na falingen bewerkstelligen
- verdere ontwerp-simplifiëring
c) het bepalen van de noodzaak voor het selecteren van alternatieve materialen , onderdelen en componenten
d) het identificeren van ernstige faalkonsekwenties en daaruitvloeiend de noodzaak voor ontwerp-nazicht en revisie.
e) het logisch model verschaffen , nodig voor het evalueren van de kans op anomalische werkingstoestanden van het systeem
f) het inzicht verschaffen in veiligheidsrisicos en probleemgebieden , of niet-conformiteit met regelgevende voorschriften
g) het verzekeren dat het testprogramma potentiële faalmodes kan detecteren
h) verkrijgen van duty-cycles die anticiperen op en het optreden verhinderen van 'wear-out ' - falingen
i) het focusseren op kerngebieden betreffende kwaliteit ,inspectie en vervaardigingsproces-controles
j) het vermijden van kostelijke wijzigingen door het vroeg identificeren van ontwerp-afwijkingen
k) het creëren van de noodzaak om data te registreren en het monitoren tijdens testen , check-out en gebruik
l) het leveren van informatie voor de selectie van preventieve of correctieve onderhoudspunten en het ontwikkelen van trouble-shooting richtlijnen , testapparatuur en geschikte testpunten
m) vergemakkelijken van testcriteria , testplannen en diagnostische procedures , bvb. performantie-testen , betrouwbaarheids-testen
n) het identificeren van circuits die een worst-case analyse nodig hebben (regelmatig nodig voor faalmodes met betrekking tot parameterdriften)
o) het steunen van het ontwerp door fout-isolatie sekwenties en het steunen van de planning door alternatieve modes van operatie en reconfiguratie
p) het vergemakkelijken van de communicatie tussen : algemene en gespecialiseerde ingenieurs , de fabrikant van apparatuur en zijn leveranciers en de systeemgebruiker en de ontwerper
q) het verbeteren van de kennis van de analyst en zijn begrip van het gedrag van het bestudeerde materiaal
r) het leveren van een systematische en rigoureuze aanpak bij de studie van systeem-faciliteiten

1.2.4 Beperkingen en minpunten van FMEA

FMEA is extreem efficiënt als het wordt toegepast op de analyse van elementen die een fout veroorzaken op het gehele systeem.
Maar , FMEA kan moeilijk en uitgebreid zijn in het geval van complexe systemen die meerdere functies hebben en bestaan uit verschillende componenten .
Dit is door de kwantiteit , gedetailleerde systeem-informatie , dat onderzocht moet worden.

Deze moeilijkheid kan toenemen door de verschillend mogelijke operationele modes , en door de beschouwingen op het gebied van herstel en onderhoud.

Studies van mens – machine interacties zijn het onderwerp van specifieke methodes (bvb. de taak-analyse methode)
Als menselijke fouten optreden tijdens het gebruik van machines in een sekwentiële mode dan moet een studie van hun impact gemaakt worden door methodes zoals , bvb. oorzaak – gevolg analyses.
Niettemin kan de FMEA componenten identificeren die het meest gevoelig zijn aan menselijke factoren.
Een verdere beperking komt naar voor als de gevolgen van de omgeving significant zijn.
Het rekening houden met deze effecten vereist een grondige kennis van de karakteristieken en werking van de verschillende componenten van het systeem.

2. Basisprincipes van FMEA

2.1 Concept

FMEA vereist :

- het opsplitsen van het systeem in elementen
- diagramma's van de functionele structuur van het systeem en de data die nodig zijn om de FMEA te maken
- het concept van de faalmodes
- het concept der criticiteit (als een criticiteits – analyse nodig is)

2.2 Definiëring van de functionele systeemstructuur

De analyse begint met het laagste niveau van interesse (gebruikelijk het onderdeel , circuit of module – niveau) waarvan voldoende informatie beschikbaar is.
Op dit niveau worden de verschillende faalmodes die kunnen optreden voor dat item opgesomd (in tabelvorm).
Het faal-effect wordt per item vastgesteld en geïnterpreteerd als een faalmode voor het volgende hogere functionele niveau.
Opeenvolgende iteraties resulteren in de identificatie van het falende effect met betrekking tot specifieke faalmodes op alle noodzakelijke functionele niveaus tot op het hoogste niveau.
Het is belangrijk om het niveau van opbreken vast te leggen dat zal gebruikt worden voor de analyse. , bvb. tot op subsysteem-niveau , minst vervangbare items of detailcomponenten.
Als kwantitatieve resultaten nodig zijn , dan moet het gekozen niveau er een zijn waarbij het mogelijk is om doeltreffende faalrata data van elke faalmode of error-mode te krijgen , of om redelijke veronderstellingen te kunnen maken van deze faalrates.
Het gekozen breakdown-niveau vereist een gedetailleerde kennis van de faalmodes van de elementen.

2.3 Nodige informatie voor het uitvoeren van een FMEA

2.3.1 Systeem-structuur

Volgende informatie is vereist :
- de verschillende systeemelementen met hun karakteristieken , performanties , rol en functies
- de connecties tussen elementen
- redundantie-niveau en het soort redundantie-systeem
- lokatie van het systeem binnen de ganse faciliteit

2.3.2 Systeem-initiatie , werking , controle en onderhoud

De status van de verschillende operationele condities van het systeem moeten gespecifieerd zijn , ook de wijzigingen in de configuratie of de positie van het systeem en de componenten tijdens de verschillende operationele fases.
De minimumprestaties van het systeem moeten gedefinieerd zijn en specifieke voorschriften zoals beschikbaarheid en veiligheid moeten beschouwd worden in termen van gespecifieerde niveaus van performantie en niveaus van schade.

Het is noodzakelijk om te weten :

- de duur van elke taak
- de tijdsduur tussen periodische testen
- de beschikbare tijd voor correctieve aktie vooraleer serieuze konsekwenties kunnen optreden aan het systeem
- de complete faciliteit , de omgeving en/of het personeel
- herstelvoorwaarden , inclusief correctieve akties en de tijd , materiaal en/of personeel om ze te bereiken
- lopende procedures tijdens opstarten
- controle tijdens operationele fases
- preventief en/of correctief onderhoud
- procedures voor routine testen

2.3.3 Systeem-omgeving

De omgevingstoestand van het systeem moet gekend zijn , inclusief degene door andere systemen in de faciliteit gecreëerd.
Het verband , relatie , afhankelijkheid en interconnecties met andere systemen en menselijke interfaces moet uitgetekend worden.
Tijdens de ontwerpfase zijn deze gegevens waarschijnlijk niet gekend en daardoor moeten gissingen en veronderstellingen gedaan worden , naargelang het project vordert zal de data aangepast worden en de FMEA gewijzigd om deze wijzigingen te reflecteren.
FMEA of andere analyses vereisen een zekere modellering van het systeem , m.a.w. een simplificatie van de relevante informatie van het systeem.
Sommige veronderstellingen kunnen gemaakt worden i.v.m. de natuur van faalmodes en de graad van hun konsekwenties.
Bijvoorbeeld , in veiligheidstudies kunnen conservatieve hypotheses toegepast worden om de impact van bepaalde falingen op het systeem na te gaan.

Een FMEA die uitgevoerd wordt op hardware kan resulteren in beslissingen op effecten , criticiteit en conditionele kansen die bepalen dat software-elementen en hun gedrag , sekwentie van optreden en timing moeten geïdentificeerd worden
Als dit het geval is moeten de feiten duidelijk geïdentificeerd worden want enige verandering van de software kan de FMEA wijzigen en de ervan afgeleide beoordelingen.

2.4 Representatie van de systeem-structuur

Symbolische representaties van de systeemstructuur en werking , in het bijzonder diagramma's kunnen gebruikt worden.
Gewoonlijk worden blokdiagramma's gebruikt die de functies , belangrijk voor het systeem , in de verf zetten.
In het diagram worden de blokken met elkaar gelinkt door lijnen , deze stellen de in – en uitgangen voor van elke functie.
Van elke functie en elke ingang wordt de aard precies beschreven.
Er kunnen ook verschillende diagramma's zijn voor de verschillende fasen van het systeem.
In het algemeen dragen grafische presentaties , inclusief deze nauw verwant aan analytische methodes zoals 'FTA' of ' cause – consequence diagramma's ' , ertoe bij tot een beter begrijpen van het systeem , de structuur en de werking.
Hun gebruik , geeft aanleiding tot het probleem : relatie FMEA - deze methodes , dit wordt later behandeld.

2.5 Faalmodi

Een faalmode is het effect waarbij een faling geobserveerd wordt van een systeemcomponent.
Het is belangrijk dat alle mogelijke of potentiële faalmodes van een systeem opgesomd worden in een lijst , dit is de basis van de FMEA.
Vervaardigers van componenten of materiaal moeten deelnemen in de identificatie van de faalmodes van hun producten , in de context van :

- voor nieuwe componenten , referentie kan gemaakt worden naar andere componenten met gelijkaardige functies en structuren en tests die erop zijn gedaan
- voor veel voorkomende componenten kunnen gegevens over de performantie , gerapporteerde falingen en labo-testen geconsulteerd worden
- complexe componenten die kunnen opgebroken worden in subelementen kunnen kwalitatief geanalyseerd worden , elk afzonderlijk als een systeem behandelend
- potentiële faalmodes kunnen afgeleid worden van functies en fysische parameters , die typisch zijn voor de werking van de component

Er moet een klassificatie van de faalmodes gedaan worden.
Twee veel-voorkomende manieren voor het klassificeren van faalmodes zijn :

- identificatie van de algemene faalmodes , afgeleid van de definitie van betrouwbaarheid (tabel I)
- door opsomming , zo volledig mogelijk , van alle optredende faalmodes (tabel II)

2.5.1 Common mode falingen (CMF)

In een betrouwbaarheids-analyse , is het niet genoeg om enkel random en onafhankelijke falingen te beschouwen.

Sommige ‘ common-mode ‘ falingen kunnen optreden , die systeemperformantie-degradatie kunnen veroorzaken of een falen door simultane defecten van verschillende systeem - componenten , te wijten aan een enkele bron zoals een ontwerpfout , menselijke fout , etc.
Een CMF is het resultaat van een gebeurtenis die , wegens afhankelijkheden , toevallige faalstates veroorzaakt in twee of meer componenten (tweederangs falingen uitsluitend veroorzaakt door de effecten van een primaire faling)
CMF’s kunnen onderworpen worden aan kwalitatieve analytische technieken , gebruik makende van FMEA.
Omdat FMEA een procedure is om opeenvolgend elke faalmode en geassocieerde oorzaken te onderzoeken , maar ook voor alle periodische testen , preventieve onderhouds-maatregelingen ..., laat dit dus een studie van alle oorzaken die een potentiële CMF kan induceren toe.
De oorzaken kunnen in vijf categoriëen onderverdeeld worden :

a) omgevingsfactoren (normaal , abnormaal en accidenteel)
b) tekortkomingen in het ontwerp
c) vervaardigings – defecten
d) assemblage – fouten
e) menselijke fouten (tijdens bedrijf en/of onderhoud)

Een checklist gebaseerd op deze categoriëen kan gebruikt worden om alle mogelijke oorzaken die een CMF kunnen veroorzaken te identificeren.
Redundantie alleen kan het probleem van CMF niet oplossen .
Een combinatie van verschillende methodes is nuttig bij het aanpakken van dit soort falingen : functionele diversiteit , redundanties van verschillende types , fysische afscheiding , testen ,...
Check-lists zoals hierboven , kunnen gebruikt worden om de relevantie en effectiviteit te onderzoeken van elke methode.
Het onderzoek van preventieve maatregelingen valt buiten het doel van een FMEA.

2.5.2 Menselijke factoren

Sommige systemen moeten ontworpen worden om menselijke fouten toe te laten , bvb. paswoorden bij computer gebruik .
Waar zulke voorzieningen ingebouwd zijn in het systeem , zal het effect van faling van de voorziening afhankelijk zijn van het type van fout.
Sommige modes van menselijke fout moeten ook in beschouwing worden genomen voor een anderzijds foutenvrij systeem , om de effectiviteit van de voorzieningen te controleren.
Alhoewel incompleet is zelfs een gedeeltelijke opsomming van deze modes gunstig.

2.5.3 Softwarefouten

Een verkeerde werking , te wijten aan software-fouten zullen gevolgen hebben , waarvan de criticiteit zal vastgelegd worden door hard- en software ontwerp.
Het opnoemen van zulke fouten en de analyse van de effecten is alleen mogelijk tot een beperkte reikwijdte en valt buiten het doel van een FMEA.
Hoewel de gevolgen voor de betrokken hardware vanwege de foute software kan geschat worden.

2.6 Criticiteits- concept

De mate van aandacht geschonken aan een faaltoestand , is duidelijk gerelateerd aan de kans van haar optreden en de graad van haar gevolg.
Het 'criticiteits-concept' kwantificeert de analyse en complementeert de FMEA.
Er zijn geen algemene criteria voor criticiteit toepasbaar op een systeem , omdat het concept fundamenteel gelinkt is aan de graad van konsekwenties en hun kans van optreden.
Het concept van 'mate - van - gevolg ' kan op verschillende manieren gedefinieerd worden , afhankelijk van als het objectief gerelateerd is aan de veiligheid van een mensenleven , gebeurlijke schade of verlies of buiten dienst-stelling.

Het criticiteits-concept steunt goed de voordelen van de FMEA door rekening te houden met :
- items die meer intensieve studie moeten gegeven worden om een bepaald risico te elimineren , het vergroten van de kans op een fail-safe resultaat of verminderen van de faal-ratio
- items die speciale aandacht nodig hebben tijdens het vervaardigen en stringente kwaliteitscontrole
- speciale eisen bij de specificaties voor het aankopen betreffende ontwerp , performantie , betrouwbaarheid , veiligheid of kwaliteits-garandering
- standaarden voor het accepteren van produkten van sub-contractors ', de parameters inbegrepen die nauwgezet moeten getest worden
- speciale procedures , aandachtspunten , beschermend materiaal , monitors , waarschuwings-systemen
- de meest cost-effective applicatie van preventieve ongeval-maatregelingen

Om criticiteit te definiëren , is een waardeschaal nodig om de graad van de konsekwenties te beoordelen van de beschouwde criteria.
Appendix B geeft een voorbeeld van een classificatie van de graad van konsekwenties in vier niveaus .
Het eigenlijke nummer van de geselecteerde niveaus is arbitrair .
In betreffende voorbeeld is het nummer van de niveaus gebaseerd op de combinatie van criteria die als relevant worden beschouwd en te maken hebben met :
- schade aan personeel (verwonding , dood)
- verlies van systeemfuncties
- invloed van de omgeving en schade aan het materiaal

De termen ' katastrofe ' , ' kritisch' , 'aanzienlijk' , 'mineur' worden uitgebreid gebruikt maar hun definities in IEC Publicatie 271 kunnen of kunnen niet het voor FMEA bedoelde gebruik rechtvaardigen.

2.7 Relatie tussen FMEA en andere analysemethodes

Het is noodzakelijk om te discussiëren over hoe de verschillende analytische methodes van systeem-betrouwbaarheid en beschikbaarheid gecombineerd worden in een projekt.
De FMEA of FMECA kan alleen worden gebruikt.
Als een systematische inductieve analysemethode, wordt FMEA het meest gebruikt om andere aanpakmethodes te complementeren , in het bijzonder de deductieve methodes.
Tijdens het ontwerp is het vaak moeilijk om te beslissen of nu de inductieve of de deductieve aanpak het best is , omdat beide gecombineerd worden tijdens gedachteverwerking en analyse.

Waar graden van risico geïdentificeerd zijn in industriële faciliteiten en systemen , wordt de voorkeur gegeven aan de inductieve aanpak en daardoor is de FMEA een essentieel ontwikkeltool.
Het moet echter aangevuld worden door andere methoden , in het bijzonder waar meerdere falingen en opeenvolgende effecten bestudeerd worden.
Tijdens de prille ontwerpfase , waar alleen functies , de algemene systeem-structuur en subsystemen gedefinieerd zijn , kunnen goede performantie of faalpaden van het systeem afgebeeld worden door een ‘ reliability block diagram ‘ of door een FTA.
Maar , om te assisteren bij het tekenen van deze diagramma’s van het systeem , moet een FMEA- inductief proces toegepast worden op de subsystemen vooraleer ze ontworpen worden.
Onder deze omstandigheden kan de FMEA-aanpak geen vast-uitvoerbare procedure zijn maar een gedachte-proces die niet zomaar kan gegoten worden in een tabelvorm.
In het algemeen ,als een complex systeem wordt onderzocht met meerdere functies , vele componenten en interrelaties tussen deze componenten , is de FMEA-methode essentieel maar niet voldoende.

3. Procedure

De grote variatie in de complexiteit van systeemontwerpen en toepassingen kunnen de ontwikkeling van sterk geïndividualiseerde FMEA procedures opleveren , dat consistent is met de beschikbare informatie.

Dit zijn de fundamentele stappen , gebruikt in FMEA studies :

a) definitie van het systeem en de functionele en minimale werkings-eisen
b) ontwikkeling van ‘ reliability block diagrams ‘ en andere diagramma’s of mathematische modellen en beschrijvingen
c) het vastleggen van de basis-principes en de corresponderende documentatie bij het maken van de analyse
d) identificatie van de faalmodes , hun gevolg en effecten , hun relatieve belang en opeenvolging
e) identificatie van faaldetectie en voorzieningen voor het isoleren en methoden
f) identificatie van ontwerp en werkingstoestand – voorzieningen tegen ongewenste gebeurtenissen
g) vastleggen van de criticiteit van de gebeurtenis (enkel FMECA)
h) evaluatie van de kans op falen (enkel FMECA)
i) aanbevelingen

3.1 Definiëring van het systeem en zijn eisen

3.1.1 Definiëren van het systeem

Een complete definitie van het systeem omvat de primaire en secundaire functies , het gebruik , de verwachte performantie , systeembeperkingen en expliciete condities die aanleiding tot een faling geven.
Omdat elk systeem ontworpen is voor een of meerdere operationele modes en aktief kan zijn tijdens verschillende periodes van systeem - operationele tijd , moet de systeemdefinitie ook bepalen wat de operatie van het systeem voor elke mode en de tijdsduur is.

3.1.2 Definiëren van de functionele eisen

Het is noodzakelijk om de toelaatbare functionele performantie van het systeem als een geheel en van zijn constitutionele elementen te definiëren evenals de performantiekarakterisiteken die als onaanvaardbaar worden beschouwd.
De functionele eisen zouden een definitie van de toelaatbare performantie voor alle gewenste of specifieke karakteristieken moeten bevatten , in alle werkings - en niet - werkings modes voor alle relevante tijdsperiodes en voor alle omgevingstoestanden.

3.1.3 Definiëren van de omgevings-eisen

De omgevingen waarin het systeem verondersteld is aan onderworpen te worden , moeten duidelijk gedefiniëerd worden en de verwachte performantie in die bepaalde omgeving moet gespecifiëerd worden.
Omgevingen moeten rekening houden met factoren als temperatuur , vochtigheid , radiatie , vibratie en druk.
Voor cybernetische systemen moet ook rekening worden gehouden met factoren als psychologische , fysiologische en van de omgeving , voor zover ze menselijke performantie en systeem-ontwerp of werking kunnen beïnvloeden.

3.1.4 Regelgevende eisen

Bij het definiëren van de systeem-eisen , moet beschouwing worden gegeven aan van toepassing zijnde eisen betreffende het gebruik van het produkt , bijprodukten tijdens gebruik en andere factoren die het ontwerp van het systeem kunnen beïnvloeden.

3.2 Ontwikkelen van de ‘ block diagrams ‘

Diagramma’s die de functionele elementen van het systeem tonen zijn noodzakelijk voor zowel het technisch begrijpen van de functies en voor de subsequente analyse.
De diagramma’s moeten series van elementen en hun redundante relaties met elkaar tonen evenals de onderlinge wisselwerking.
Dit laat toe om de falingen te traceren in het systeem .
Er kan meer dan één diagram nodig zijn om alternatieve modes van systeemoperatie te tonen.
Afzonderlijke logische diagramma’s kunnen nodig zijn voor elke operationele mode.
Minimaal moet het ‘ block diagram ‘ bevatten :

a) opsplitsing van het systeem in subsystemen , inclusief functionele relaties
b) de benoemde inputs en outputs en identificatie-nummers waarbij elk subsysteem consistent gerefereerd wordt
c) alle redundanties , alternatieve signaalpaden en andere technische methodes die ‘fail-safe’ garanderen

3.3 Het vastleggen van basisregels

3.3.1 Niveaus van analyse

Basisprincipes voor het selecteren van systeemniveaus hangen af van de gewenste resultaten en de beschikbaarheid van ontwerpinformatie.
Deze richtlijnen kunnen helpen :

a) het hoogste systeemniveau wordt geselecteerd vanuit het ontwerp-concept en de gespecifieerde output-eisen
b) het laagste systeemniveau waarbij de analyse effectief is , is dat niveau waarvoor informatie beschikbaar is om definiëring en beschrijving van functies te doen.Keus van het laagste systeemniveau wordt beïnvloed door ervaring.Minder gedetailleerde analyse kan gerechtvaardigd worden voor elk systeem die een volwassen ontwerp , goede betrouwbaarheid , onderhoudbaarheid en een ‘ veiligheid-zijn ‘ status draagt. Voor een nieuw systeem of een systeem met ongekende betrouwbaarheidsgegevens zal men dan meer detail geven en een lager systeem-niveau toekennen.
c) de gespecifieerde of bedoelde graad van onderhoud en herstel kan een waardevolle gids zijn bij het vastleggen van lagere systeemniveaus.

Het laagste systeemniveau waarbij systeemonderhoud kan gedaan worden moet eerst geïdentificeerd worden (identificeer het minst vervangbare element) .
Een analyse wordt dan gemaakt van het niveau net boven het laagste systeemniveau waarbij onderhoud zal gedaan worden.
Bij kritische systemen wordt de analyse gedaan tot aan het minst vervangbare element.

3.3.2 FMEA documentatie

Het is raadzaam om bij de FMEA-studie van een systeem dit op een model-exemplaar te doen ,
worksheets genaamd , zoals in appendix A is weergegeven , en consistent met de gestelde objectieven.

3.4 Faalmodes , oorzaken en gevolgen

Het succesvol werken van een systeem is afhankelijk van bepaalde kritische systeemelementen.
De sleutel voor het evalueren van systeemperformantie is de identificatie van deze kritische elementen.
De procedures voor het identificeren van faalmodes , hun oorzaken en gevolgen kunnen effectief verbeterd worden door de bereiding van een lijst met faalmodes , inspelend op de vraag van :

- systeemgebruik
- betrokken systeem-element
- mode van werking
- relevante operationele specificaties
- tijdbeperkingen
- omgeving

In de FMEA zijn de definities van de faalmodes , de faaloorzaken en het falend effect afhankelijk van de graad van analyse.
Naarmate de analyse vordert , kunnen de geïdentificeerde faaleffecten op lager niveau faalmodes op hoger niveau worden.
Gelijkaardig kunnen faalmodes op lager niveau de faling-oorzaken worden op hoger niveau , enz.

3.4.1 Faalmodes

1	te vroege werking
2	falen om te werken op het voorgeschreven tijdstip
3	falen om te stopppen op voorgeschreven tijdstip
4	falen tijdens werking

Tabel 1 : Algemene faalmodi

Praktisch elk type faalmode kan geklassificeerd worden in een of meer van deze categoriëen. Deze algemene faalmodecategoriëen zijn nochtans te breed voor het vizier van een definitieve analyse , ze zijn dan ook meer uitgebreid in tabel 2
De faalmodes in tabel 2 kunnen de faling beschrijven van elk systeem-element in voldoende specifieke termen.
Als het gebruikt wordt in combinatie met performantie-specificaties betreffende de inputs en de outputs op het reliability block diagram , kunnen alle potentiële faalmodes geïdentificeerd en beschreven worden.

1	structurele faling	18	valse actuatie
2	fysische binding of vastzitten	19	faalt om te stoppen
3	vibratie	20	faalt om te starten
4	faalt om te blijven (in positie)	21	faalt om te schakelen
5	faalt om te openen	22	te vroege werking
6	faalt om te sluiten	23	uitgestelde werking
7	faalt bij open	24	foutieve input (vermeerderd)
8	faalt bij gesloten	25	foutieve input (verminderd)
9	intern lek	26	foutieve output (vermeerderd)
10	extern lek	27	foutieve output (verminderd)
11	faalt buiten tolerantie (hoog)	28	verlies van input
12	faalt buiten tolerantie (laag)	29	verlies van output
13	onaangekondigde werking	30	kortgesloten (electrisch)
14	niet-constante werking	31	open (electrisch)
15	foutieve werking	32	lek (electrisch)
16	foutieve indicatie	33	andere
17	beperkte vloei		

Tabel 2

3.4.2 Faaloorzaken

De mogelijke oorzaken geassocieerd met elke genoemde faalmode zijn geïdentificeerd en beschreven.
De oorzaken van elke faalmode zijn geïdentificeerd om te schatten wat de kans op optreden is , om secundaire effecten bloot te leggen en om een aanbevolen correctieve aktie uit te voeren.
Omdat een faalmode meer dan één oorzaak kan hebben , moeten alle onafhankelijke oorzaken voor elke faalmode geïdentificeerd en beschreven worden.
De faaloorzaken in naastliggende systeemniveaus worden ook beschouwd.
De lijst in tabel 2 laat een meer specifieke definitie van zowel faalmodes als faaloorzaken toe.
Een power supply kan bvb. een algemene faalmode hebben die beschreven is als een ‘ faling tijdens werking ‘ maar de specifieke faalmode‘ verlies van output ‘ en de faaloorzaak ‘ kortsluiting (electrisch) ‘

3.4.3 Faaleffecten

De konsekwenties van elke veronderstelde faalmode op de systeem-element werking , functie of status zijn geïdentificeerd , geëvalueerd en opgeslagen.
Onderhoud , personeel en systeemobjectieven moeten ook beschouwd worden als die relevant zijn.
Faaleffecten focussen op het specifieke systeem-element in het block diagram dat geanalyseerd wordt en die beïnvloed is door de faling in beschouwing genomen.
Een faaleffect kan ook het volgende hogere niveau en ultiem het hoogste niveau beïnvloeden die geanalyseerd wordt , daarom moeten de faaleffecten op elk hogere niveau geëvalueerd worden.

3.4.3.1 Lokale effecten

De uitdrukking ‘ lokale effecten ‘ slaat op de effecten van de faalmode op het systeemelement in beschouwing.
De konsekwenties van elke gepostuleerde faling op de output van het item zijn beschreven samen met de secundaire effecten.
Het doel van het definiëren van de lokale effecten is het leveren van een basis voor het oordelen
als het evalueren van bestaande alternatieve voorzieningen wordt gedaan of bij het samenstellen van aanbevolen correctieve acties.
In bepaalde gevallen is er geen lokaal effect behalve de faalmode zelf.

3.4.3.2 Eindeffecten

Bij het identificeren van eindeffecten , is de impact van een gepostuleerde faling op het hoogste systeemniveau gedefinieerd en geëvalueerd door de analyse van alle tussenliggende niveaus.
Het beschreven eindeffect kan het resultaat zijn van een meervoudige faling.
Bijvoorbeeld , faling van een veiligheidstoestel resulteert in een catastrofisch eindeffect , slechts in het geval dat het veiligheidstoestel faalt en de primaire functie waarvoor het toestel gemaakt is , buiten zijn grenzen gaat.

Deze eindeffecten die resulteren van een meervoudige faling zijn weergegeven op de worksheet.

3.5 Faaldetectie-methodes

De detectiemethodes van de faalmode zijn beschreven.
Faalmodes , anders dan degene die beschouwd worden , die aanleiding geven tot een identieke indicatie zijn geanalyseerd en opgesomd.
De nood aan afzonderlijke faaldetectie van redundante elementen tijdens de werking moeten in beschouwing worden genomen.

3.6 Kwalitatieve uitdrukking van de faalsignificantie en alternatieve voorzieningen

De relatieve significantie van de faling moet genoteerd worden in de worksheet.
Alsook de identificatie en evaluatie van alle kenmerken van het ontwerp op elk systeemniveau opdat andere voorzieningen het effect van de faalmode kunnen verhinderen of reduceren.
Deze worksheet toont dus het werkelijke gedrag van van het materiaal in aanwezigheid van een interne fout.
Andere voorzieningen zijn :
- redundante items die werking verzekeren als een of meer elementen falen
- alternatieve manieren van werking
- monitoren of alarmtoestellen
- elke andere manier die effectieve werking verzekerd of schade beperkt

Tijdens de ontwerpfase kunnen de functionele elementen van het materiaal (hard – en software) opnieuw gerangschikt of geconfigureerd worden om haar capaciteit te wijzigen.
Volgens dit gegeven moeten de relevante faalmodes opnieuw bekeken worden vooraleer de FMEA te herhalen.

3.7 Opmerkingen i.v.m. de worksheets

Als een criticiteits - analyse niet wordt gedaan , dan moet het laatst genoteerde punt relevante informatie geven om de opgesomde punten te verduidelijken.
Aanbevelingen voor verbetering van het ontwerp worden genoteerd en verder uitgewerkt in de samenvatting.
Dit laatste punt mag ook bevatten :
- ongewone omstandigheden
- effecten van redundante element-falingen
- herkenning van speciale kritische ontwerp-kenmerken
- verwijzingen naar andere punten voor sequentiële faalanalyse

4. Criticiteits- analyse

Het kan wenselijk zijn om de criticiteit van een falend effect te kwantifiëren en het schatten van de kans van het optreden van de relevante faalmodus.
De kwantifiëring van de criticiteit en de kans op falen wordt gedaan als een hulp bij het beslissingnemen van de resulterende correctieve akties en hun prioriteiten , en voor het verwezenlijken van een duidelijke afscheiding tussen een aanvaardbaar en niet-aanvaardbaar risico.
Elk falend effect dat beschouwd wordt is geklassificeerd door de criticiteit op de ganse systeem-performantie in het teken van de systeem-eisen , het objectief en de beperkingen.

Een opsomming van kritische falingen zal gedefinieerd worden voor elk item van uitrusting.
Er zijn echter algemeen aanvaarde categoriëen en klassificaties die van toepassing zijn op het meest voorkomende materiaal , gebaseerd op de konsekwenties die hieronder beschreven zijn , deze zijn kwalitatief geklassificeerd volgens hun graad van schade ;

- dood of ongeval aan het werkend personeel of het publiek
- schade aan extern materiaal of het materiaal zelf
- economisch verlies wegens gebrek aan output of functie
- faling om een taak te volbrengen wegens inabiliteit van het materiaal om het tet doen

Het voorbeeld van een criticiteits- schaal in appendix B is gebaseerd op verwonding , materiaal- schade en degradatie van functie
De keus van criticiteit-categoriëen vereist voorzichtige en overwogen beslissingen.
Alle relevante factoren moeten beschouwd worden wegens hun impact op de systeem-evaluatie met betrekking tot factoren als performantie , kost , schema , veiligheid en risiko.

4.1 Kans op een falende modus

De kans van optreden van elke gepostuleerde falende mode wordt beoordeeld in kwantitatieve termen , gebruik makend van analytisch afgeleide schattingen.
Schattingen van de kans op een specifieke falende mode in een specifiek werkingsomgeving vereist een statistisch significante betrouwbaarheids database.
Voorspellingen worden gedaan in parallel met de FMEA en gebruik makende van data van de directe bronnen afkomstig.

4.2 Evaluatie van de criticiteit

De evaluatie van de criticiteit kan gedaan worden gebruik makende van een criticiteit-rooster die op een handige manier de criticiteits-categoriëen als ordinaat en de faalkansen of frekwenties als absis weergeeft.
Zie het voorbeeld in fig.1
Als de faalmodes geklassificeerd zijn en een kans of frekwentie zijn toegewezen , zijn ze geïdentificeerd in de gepaste rechthoek van de grafiek.
Hoe verder de rechthoek boven de oorsprong uitkomt , de groter de criticiteit en des te sneller er correctieve aktie moet worden ondernomen.
Voor elke criticiteits-analyse gaat men een specifieke reeks kansen of frekwenties identificeren voor elke klassificatie.

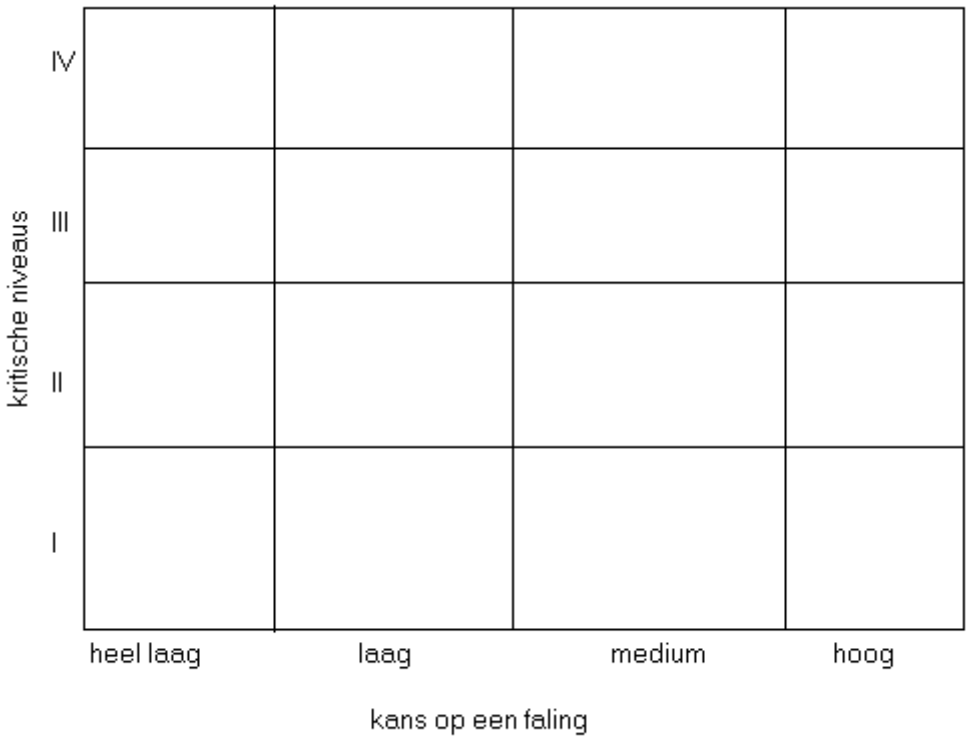


fig.1 Voorbeeld van een criticiteits-rooster

5. Analyse rapport.

Het rapport over de FMEA of FMECA mag in een ruimere studie worden bijgevoegd of kan op zichzelf worden gebruikt.
In elk geval moet het rapport een samenvatting bevatten en een gedetailleerde weergave van de analyse.
De samenvatting moet een korte beschrijving van de analyse-methode en het niveau tot waar het is uitgevoerd bevatten , de veronderstellingen en de grondregels.
In surplus moet het opsommingen bevatten van

- aanbevelingen voor de aandacht van ontwerpers , onderhoudspersoneel en gebruikers
- falingen die , als ze initieel alleen optreden , resulteren in serieuze effecten
- ontwerpveranderingen die reeds zijn uitgevoerd als het gevolg van FMEA (of FMECA)

Appendix A

Voorbeeld van een falende modus , effecten en criticiteits – analyse worksheet.

Datum : ...../...../.....
Code no. Naam v/d analyst : .....Naam v/d ontwerp-ingenieur : .....

naam materiaal
functie
ident nr.
faalmode
faling oorzaak
faling effect - lokaal
effect

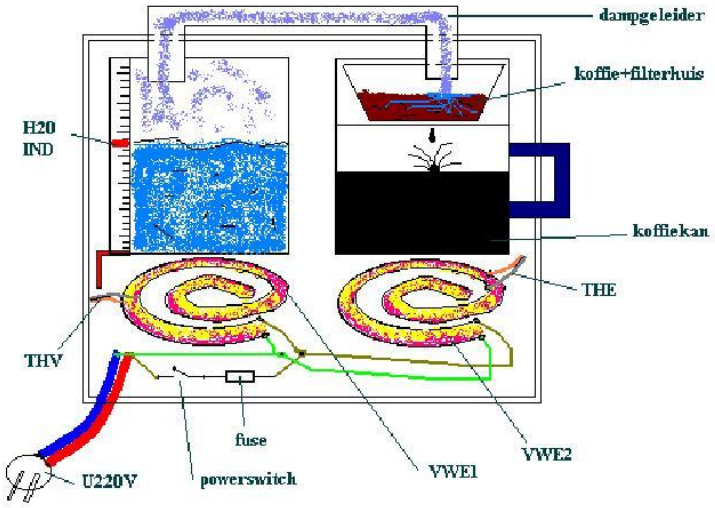
faling effect - eind effect
faling detectie
alternatieve voorzieningen
kans op falen
criticiteits - niveau
opmerkingen

Appendix B

Criticiteitsniveaus - condities

Criticiteits - niveau	*Criticiteits – condities*
IV	Elke gebeurtenis die potentieel het verlies van de primaire systeemfuncties kan veroorzaken , resulterende in significante schade aan het systeem of zijn omgeving en het verlies van leven of ledematen
III	Elke gebeurtenis die potentieel het verlies van primaire systeemfuncties kan veroorzaken , resulterende in significante schade aan het systeem of zijn omgeving en verwaarloosbaare blootstelling aan leven of ledematen
II	Elke gebeurtenis die de systeemperformantie-functies kan degraderen zonder aanzienlijke schade aan het systeem of leven of ledematen
I	Elke gebeurtenis die degradatie aan systeemperformantie – functies kan veroorzaken , resulterende in verwaarloosbare schade aan ofwel systeem als omgeving , zonder schade aan leven of ledematen

Het systeem – koffiemachine



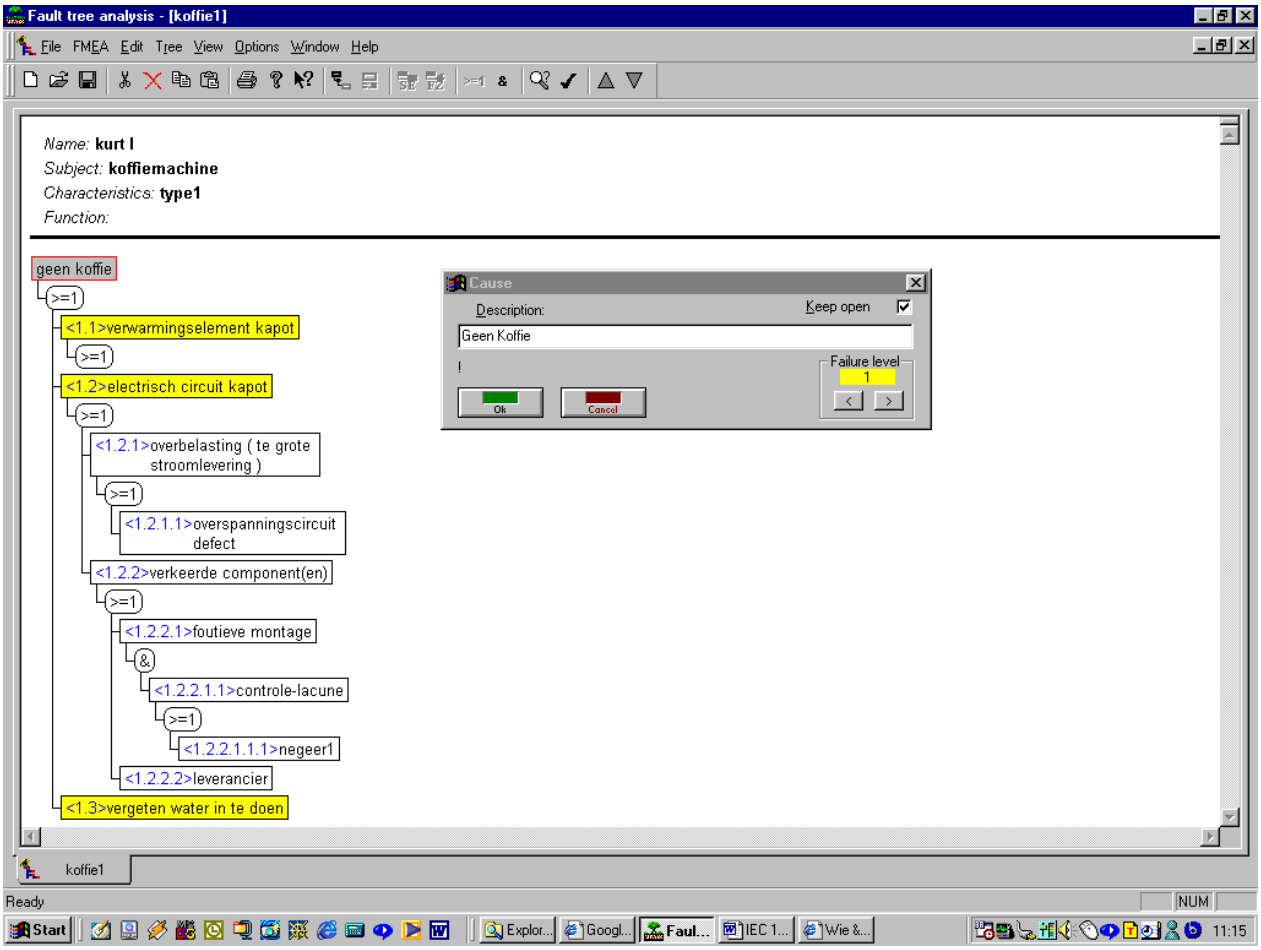
Principiële werking.

Water wordt in het reservoir gegoten.
Na aanzetten van de spanning via de schakelaar (Powerswitch) zullen de verwarmingselementen VWE1 en VWE2 opwarmen,op voorwaarde dat de fuse functioneert en dit zal zo zijn indien er geen fouten in het verwarmcircuit zijn en de spanning nominaalverloop heeft.
De eerste verhit het water en geleidt de ontstane damp via de dampgeleider naar het filterhuis waarin een hoeveelheid gemalen koffiebonen geschept is in een filter.
Na filtratie wordt het ontstane koffiemengsel opgevangen in een koffiekan.
Het tweede verwarmingselement houdt de koffie op een constante temperatuur.
Als beveiliging is er een THermische Veiligheid opgenomen in het eerste verwarmingselement om te verhinderen dat men lucht zou verhitten bij H_2O- niveau INDicatie = 0.
Een THErmostaat is aanwezig om de koffie op de juiste temperatuur te houden

7 Uitwerking

7.1 FTA

We passen een analyse toe op het systeem met koffiemachine.
Hiervoor maken we gebruik van het pakket FTA-analyse van softwarefabrikant Plato GmbH.

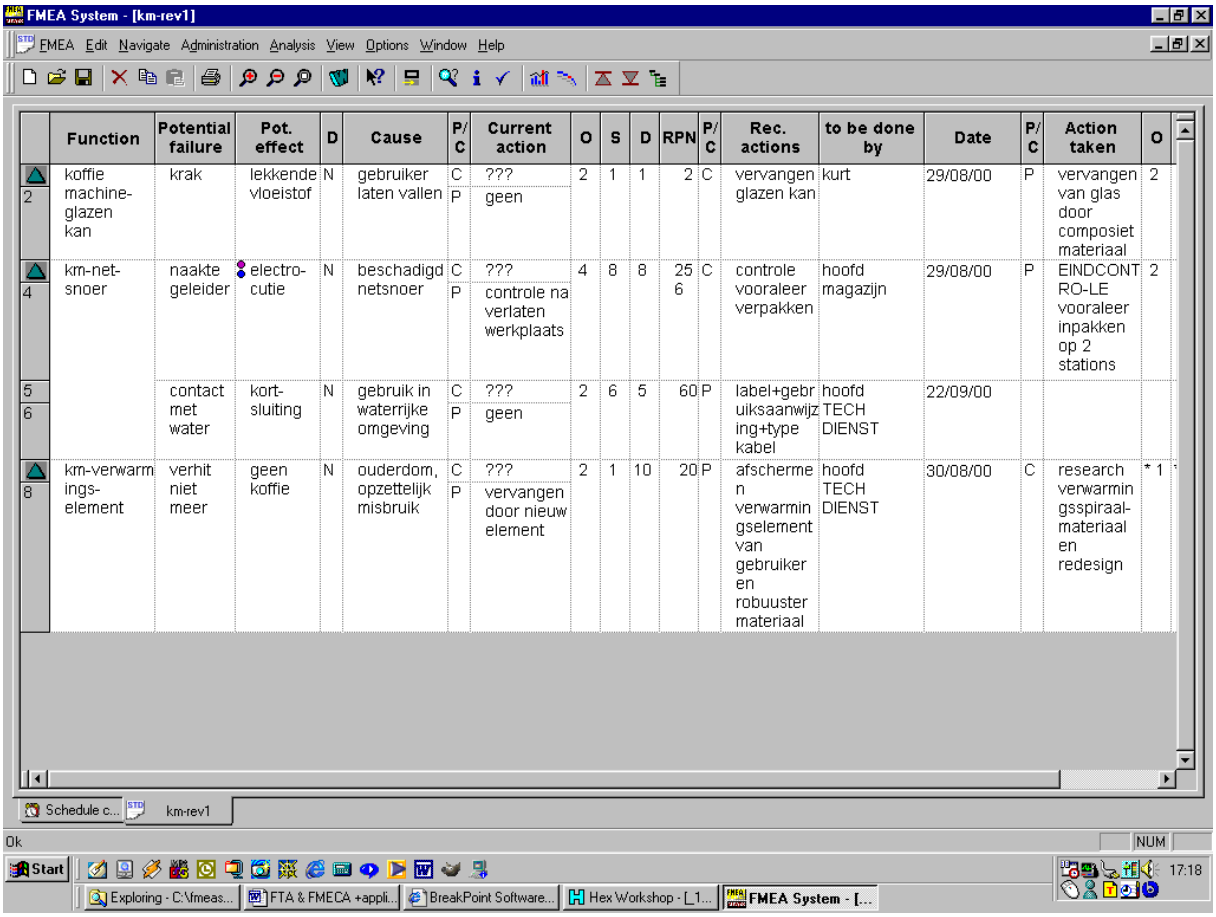


Bespreking

Via logische bouwstenen wordt het systeem kwalitatief deductief geanalyseerd,zoals verwacht wordt van een FTA.
Het programma laat toe om de gedachtegang van een systeem uit te schrijven , met de juiste symboliek , in een grafische vorm.
Er is de mogelijkheid om de gegevens te exporteren naar de FMEA-database zodat tijd wordt bespaard bij het uitschrijven ,het FMEA-pakket is eveneens van de firma Plato.
Verder zijn er een aantal mogelijkheden met de takken,er kunnen ‘copy and paste’ operaties worden gebruikt.

7.2 FMEA

We passen een analyse toe op het systeem koffiemachine.
Eveneens maken we gebruik van het risiko-analyse pakket van softwarefabrikant Plato GmbH., nu het onderdeel FMEA analysis.



	Function	Potential failure	Pot. effect	D	Cause	P/C	Current action	O	S	D	RPN	P/C	Rec. actions	to be done by	Date	P/C	Action taken	O
2	koffie machine-glazen kan	krak	lekkende vloeistof	N	gebruiker laten vallen	C P	??? geen	2	1	1	2	C	vervangen glazen kan	kurt	29/08/00	P	vervangen van glas door composiet materiaal	2
4	km-net-snoer	naakte geleider	electro-cutie	N	beschadigd netsnoer	C P	??? controle na verlaten werkplaats	4	8	8	256	C	controle vooraleer verpakken	hoofd magazijn	29/08/00	P	EINDCONTRO-LE vooraleer inpakken op 2 stations	2
5 6		contact met water	kort-sluiting	N	gebruik in waterrijke omgeving	C P	??? geen	2	6	5	60	P	label+gebruiksaanwijzing+type kabel	hoofd TECH DIENST	22/09/00			
8	km-verwarmings-element	verhit niet meer	geen koffie	N	ouderdom, opzettelijk misbruik	C P	??? vervangen door nieuw element	2	1	10	20	P	afschermen verwarmingselement van gebruiker en robuuster materiaal	hoofd TECH DIENST	30/08/00	C	research verwarmingsspiraal-materiaal en redesign	* 1

Bespreking

Met FMEAsys kunnen functies worden ingegeven ,de optredende falingen ,het effect ervan.
Verder de oorzaak,P/C (past of current) ,huidige aktie ,gewichten aan optreden , zwaartegraad , detecteerbaarheid.
Het produkt van de laatste drie factoren ,aangewezen akties,wie ervoor instaat.
Dan wordt de nieuwe waarde berekend van RPN na akties.
Er kunnen aan bepaalde gebeurtenissen bestanden worden gekoppeld ,er bestaat een exportfunctie naar de tekstverwerker Word en men kan grafisch de RPN-waarden uittekenen i.f.v. de systeemcomponenten.

7.3. De voor- en nadelen van FMEA en FTA van het softwarepakket PLATO.

	FMEASys	**FTA**
Voordelen	➜ grafische interface ➜ dienstverlening ➜ bijgeleverde documentatie ➜ Pareto/Landscape voorstelling ➜ data (communicatie) bijvoegen aan entries	➜ koppeling mogelijk met database van FMEASys ➜ grafische interface
Nadelen	➜ codes database vereist telefonisch contact ➜ helpfunctie Duitstalig ➜ kostprijs ➜ taalfouten ➜ geen mogelijkheid om gedistri–bueerd te werken ***<u>Opmerking</u>:*** ***Exporteerfunctie naar Word for Windows***	➜ helpfunctie Duitstalig ➜ kostprijs ➜ geen mogelijkheid om meerdere gebruikers toe te laten ➜ enkel verticale structuur

<u>Opmerking</u>: FTA analyse heeft geen gewichten, alleen kwalitatieve analyse en geen kwantitatieve.