



Divisie Technologie in de  
Gezondheidszorg  
Gaubius gebouw  
Zernikedreef 9  
Postbus 2215  
2301 CE Leiden

[www.tno.nl](http://www.tno.nl)

T 071 518 18 18  
F 071 518 19 02  
[info-TG@pg.tno.nl](mailto:info-TG@pg.tno.nl)

**TNO-rapport**

**PG/TG/2003.310**

**Risicomangement**

Datum 28 november 2003

Auteur(s) Ir. M. Schoone  
Ir. C.J.P.M. Teirlinck  
Ir. H.E.F. Vos  
Dr. M.W.M. Oostenbrug  
Dr. J.A.M. van Bossel

Exemplaarnummer  
Oplage  
Aantal pagina's 77  
Aantal bijlagen 3  
Opdrachtgever ZonMw  
Projectnaam  
Projectnummer 011.50984

Alle rechten voorbehouden.

Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, foto-kopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor onderzoeksopdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.

Het ter inzage geven van het TNO-rapport aan direct belang-hebbenden is toegestaan.

© 2003 TNO

## Samenvatting

Fabrikanten van Medische Hulpmiddelen zijn op grond van de Europese Richtlijn Medische Hulpmiddelen wettelijk verplicht om, voordat zij een product op de markt brengen, van dit product een risicoanalyse uit te voeren. Het uitvoeren van de risicoanalyse moet passen in een geheel traject van risicomanagement. Dit is conform de nieuwe norm voor risicomanagement ISO 14971, die de norm voor risicoanalyse, de ISO 1441 is opgevolgd.

Alhoewel de methode zoals beschreven in de norm zeer systematisch is opgebouwd, zijn aan de uitvoering van een goede risicoanalyse de nodige moeilijkheden verbonden. Zo is het moeilijk, zo niet onmogelijk om alle mogelijke ongewenste situaties, die met een medisch hulpmiddel kunnen optreden, te voorzien. Embedded software maakt het voorspellen van ongewenste gebruikssituaties zo mogelijk nog complexer. Ook laat de methodebeschrijving uit de norm nog zodanig veel ruimte voor eigen invulling, dat het zelfs voor een expert, maar zeker voor een producent met weinig ervaring hierin, een moeilijke taak is om een dergelijke risicoanalyse goed uit te voeren. Daarnaast is het zo dat het uitvoeren van de risicoanalyse slechts een onderdeel is van het gehele risicomanagement proces, dat als geïntegreerd onderdeel van de kwaliteitsborging processen een plaats binnen de bedrijfsvoering zou moeten hebben. Het blijkt in de praktijk dat de kwaliteit van risicomanagement en risicoanalyse door fabrikanten van medische hulpmiddelen het nodige te wensen overlaat.

Het doel van dit project was dan ook om een instrumentarium te ontwikkelen waarmee fabrikanten beter in staat zouden zijn om zelfstandig dit risicomanagement proces te beheersen en ten uitvoer te brengen. Ter ondersteuning van het proces van risicomanagement en het uitvoeren van een risicoanalyse is door TNO Preventie en Gezondheid met subsidie van ZonMw een project uitgevoerd dat ten doel had hiervoor een softwarepakket te ontwikkelen.

De stappen die in het risicomanagement proces van ISO 14971 worden onderscheiden zijn:

- Risicoanalyse
- Risico-evaluatie
- Risicocontrole
- Post-productie informatie

Ten behoeve van de stappen in dit proces moeten gegevens worden verzameld en analyses worden uitgevoerd volgens een vooropgesteld plan. Alle resultaten moeten worden gebundeld in een risicomanagement-dossier.

In het ontwikkelde softwarepakket wordt ten eerste het raamwerk geboden voor de stappen in het risicomanagement proces zoals beschreven in ISO 14971. Daarnaast worden voor een aantal onderwerpen ondersteuningsmodules uitgewerkt. Er is een methodewijzer die de gebruiker helpt bij het selecteren van de juiste methode voor het uitvoeren van de risicoanalyse. Er wordt een database van ongevalgegevens van werkelijk gebeurde ongevallen aangeboden die als referentie kan dienen bij het opsporen en genereren van mogelijke ongewenste situaties met een nieuwe medisch hulpmiddel. En er is een link naar diverse checklists van normen en richtlijnen onder andere op het specifieke gebied van de softwareveiligheid.

Begonnen is met een uitgebreide inventarisatie om alle informatie te verzamelen die behulpzaam kan zijn bij het uitvoeren van een risicoanalyse en bij risicomanagement. Op basis van de verzamelde informatie is een eerste invulling op papier gegeven aan het raamwerk en de modules. Deze stappen zijn uitgebreid besproken met een breed samengestelde Klankbordgroep met vertegenwoordigers uit industrie, de onderzoekswereld en de gebruikers van medische hulpmiddelen. Vervolgens is met behulp van dit materiaal een eerste versie van het softwarepakket gebouwd, een demonstratieversie. Daarbij is nog niet gestreefd naar compleetheid, maar primair naar het representeren van de functionaliteit van het softwarepakket als geheel en naar een optimale inzet van de modules bij de verschillende stappen van de risicoanalyse en het risicomanagement.

Deze demonstratieversie is beoordeeld door een panel van experts, met veel en gevarieerde ervaring met risicoanalyse en risicomanagement. Dit panel heeft aan de hand van het werken met de demonstratieversie een inschatting gemaakt hoe de uiteindelijk beoogde versie van het software pakket zou gaan werken en welke activiteiten nodig zijn om deze versie te realiseren. Aan dit panel is ook de vraag voorgelegd met wat voor soort softwarepakket fabrikanten het meest geholpen zouden zijn. Dit panel heeft vraagtekens geplaatst bij de oorspronkelijke doelstelling en haar opinie gegeven over alternatieven.

In het licht van alle opgedane ervaringen en inzichten en van de waardering van de verschillende opties, is bij de afronding van het project de voorkeur gegeven aan een softwareversie met een aangepast doel en focus. Het meeste rendement valt te verwachten van een instrument dat zich richt op de fabrikanten die apparatuur produceren in risicocategorie I (waar zelfregulering van toepassing is) en vooral een informatief karakter heeft. Dit wil zeggen dat het de fabrikant een goed inzicht biedt in de structuur van risicomanagement volgens ISO 14971 en deze ondersteunt bij het nemen van beslissingen welke onderdelen van de risicoanalyse en risicomanagement hij zelf uit kan voeren en voor welke onderdelen deskundige ondersteuning dienstig kan zijn. Resultaten zijn een groei van de *awareness* voor risicomanagement in het veld en een betere vraagarticulatie bij fabrikanten bij het inschakelen van hulp bij specifieke onderdelen van het risicomanagement proces.

Eindproduct van het project is, naast een uitgebreid dossier met alle verzamelde informatie, een verbeterde versie van de demonstratieversie van het risicomanagementinstrument en globale specificaties van het informatieve software-instrument t.b.v. producten in klasse I. Feitelijke bouw zal in een vervolgproject moeten plaatsvinden. Naar financiering hiervoor wordt nog gezocht.

## Inhoud

Samenvatting .....	3
Inhoud .....	6
1 Inleiding.....	8
2 Projectopzet .....	11
2.1 Projectinrichting.....	11
2.2 Uitgangspunten .....	11
2.3 Fasering .....	12
3 Inventarisatie.....	13
3.1 Bestaande methoden voor risicoanalyse en ongevalanalyse .....	13
3.2 Bestaande ongevalgegevens .....	14
3.3 Bestaande wettelijke regelingen, normen en richtlijnen.....	20
4 Analyse van de verzamelde gegevens .....	22
4.1 Methoden voor risicoanalyse en ongevalanalyse .....	22
4.2 Ongevalgegevens .....	23
4.3 Achtergronden software veiligheid .....	27
5 Methode ontwikkeling .....	29
5.1 Uitgangspunt: de bestaande norm voor risicoanalyse .....	29
5.1.1 Risicomanagement plan .....	29
5.1.2 Algemene beschrijving.....	29
5.1.3 Eigenschappen van het medische hulpmiddel.....	29
5.1.4 Identificatie van mogelijke gevaren .....	30
5.1.5 Schatting van het risico voor een gevaar.....	30
5.1.6 Aanvaardbaarheid van de risico's .....	30
5.1.7 Risicobeheersing .....	31
5.1.8 Het ontstaan van nieuwe gevaren.....	31
5.1.9 Evaluatie van het risicobeheersingproces .....	31
5.1.10 Risicoanalyserapport .....	31
5.1.11 Herziening van de risicoanalyse.....	31
5.1.12 Post-production informatie.....	32
5.2 Uitwerking van de modules.....	32
5.2.1 Methodewijzer.....	32
5.2.2 Database ongevalprofielen .....	33
5.2.3 Checklist documenten .....	33
5.2.4 Checklist Software Risicoanalyse .....	35

6	Softwarepakket voor risicomanagement: Risicoanalyse database.....	39
6.1	Step by Step .....	39
6.2	Incident Database .....	40
6.3	Risk analysis methods .....	41
6.4	Overig.....	41
7	Beoordeling demonstratieversie softwarepakket voor risicomanagement: Risk Analysis Database .....	42
8	Conclusies en aanbevelingen .....	48
9	Ondertekening .....	53
10	Geraadpleegde literatuur.....	55
Bijlage A	Samenstelling Klankbordgroep.....	59
Bijlage B	Samenstelling Panel van experts risicomanagement .....	61
Bijlage C	Ongevalanalyse- en risicoanalysemethoden .....	63

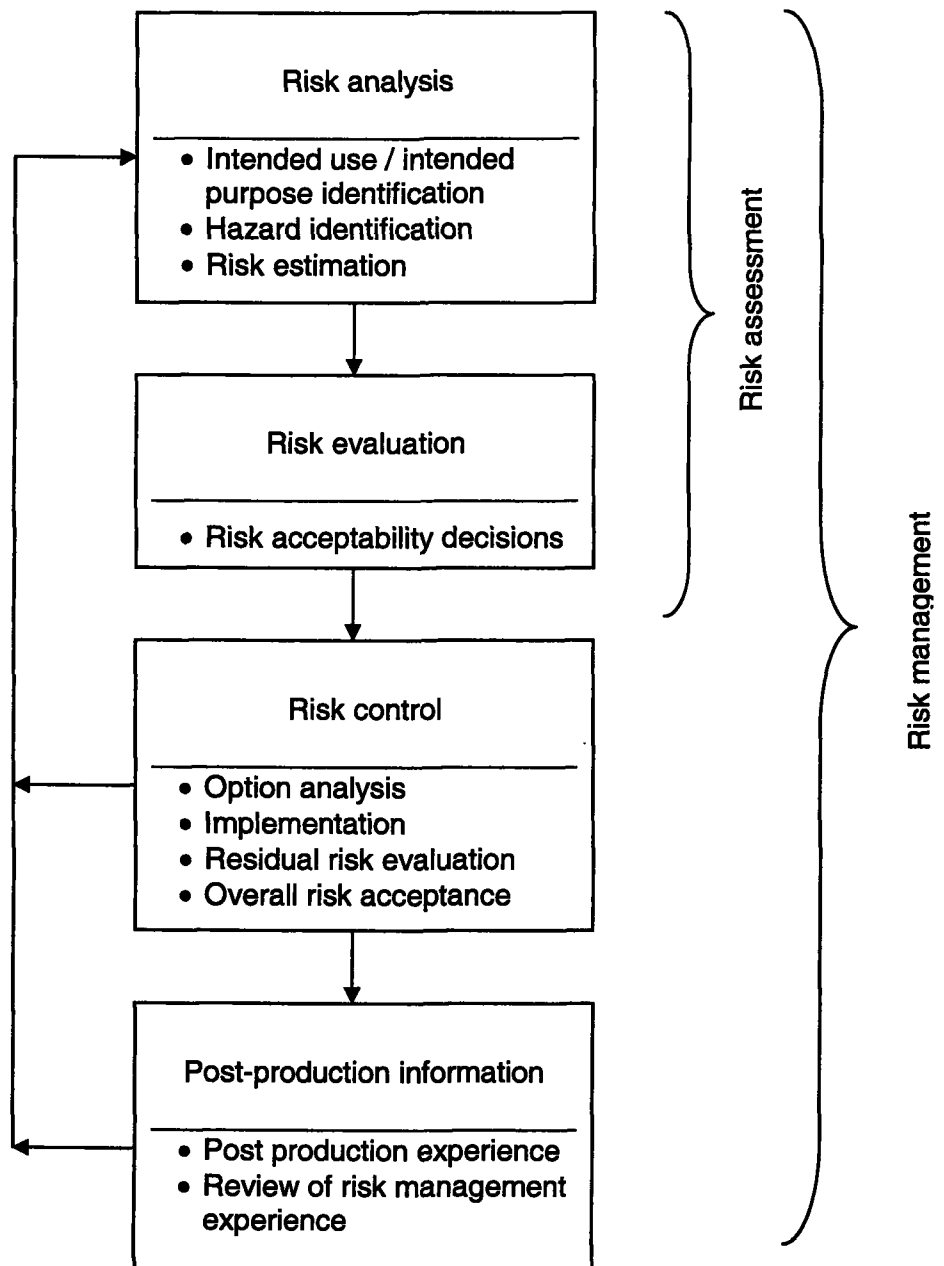
Apart bijgevoegd: Softwarepakket voor Risicomanagement "Risk Analysis Database"

## 1 Inleiding

Deze rapportage bevat het verslag van een project dat is uitgevoerd met subsidie van ZonMw. Doel van het project was om een softwarepakket te ontwikkelen waarmee fabrikanten van medische hulpmiddelen en apparatuur zelfstandig in staat zouden zijn een risicoanalyse uit te voeren van een medisch hulpmiddel. Voor toelating van een medisch hulpmiddel op de Europese markt moet het medisch hulpmiddel voldoen aan de Richtlijn Medische Hulpmiddelen. Onderdeel van het op te bouwen dossier is een risicoanalyse en risk management report. Dit dient opgebouwd te worden volgens ISO 14971. Producenten van Medische Hulpmiddelen van risicoklasse I mogen dit geheel zelfstandig doen. Fabrikanten van Medische Hulpmiddelen van klasse IIa, IIb of III moeten dit dossier laten toetsen door een bevoegde instantie.

Hoewel het basisschema van het risicomangement volgens ISO 14971 (zie schema volgende bladzijde) er relatief eenvoudig uitziet, betreft het toch een complex proces omdat het innovatieproces van een nieuwe medische product beslist niet als een simpel lineair proces verloopt.

Aan allerlei aspecten die uiteindelijk noodzakelijk zijn voor een succesvolle introductie in de markt en het voor het competitief blijven gedurende de rest van de levenscyclus van het product, wordt vaak parallel op verschillende momenten en verschillende plaatsen in (en buiten) het bedrijf gewerkt. Aspecten die soms al goed geregeld leken, kunnen later toch weer onverwacht ter discussie komen. In de praktijk is het een hele opgave uiteindelijk een compleet risicomangement-dossier op te bouwen, waarmee toelating op de markt en acceptatie in de zorg gegarandeerd zijn. Met de introductie van een nieuw product start ook een proces van verbetering en uitbreiding naar nieuwe toepassingen. Deze veranderingen kunnen op eigen initiatief plaatsvinden (productverbetering, efficiënter productieproces of indicatieverbreding), maar ook kunnen incidenten, of ontwikkelingen in de zorg of bij concurrerende technologieën dwingen tot herontwerp. Bij iedere verandering in het product dient steeds ook het risicomangement opnieuw bekeken te worden. Het is daarom van het grootste belang het risicomangement transparant en gemakkelijk wijzigbaar en aanvulbaar te houden. Indien men dit proces goed beheerst, komt dit uiteindelijk de gehele bedrijfsvoering ten goede.



*Figuur: schematische voorstelling van het risicomanagement proces (ISO 14971)*

In hoofdstuk 2 wordt de oorspronkelijke opzet van dit project toegelicht, wie bij de uitvoering en begeleiding van het project betrokken zijn geweest, wat de uitgangspunten waren en welke stappen zijn doorlopen.

Hoofdstuk 3 beschrijft de uitgevoerde inventarisatie. De inventarisatie heeft zich toegespitst op de onderwerpen: beschikbare analysemethoden voor risico en onge-



vallenanalyse, aard en inhoud van beschikbare ongevalgegevens en bestaande richtlijnen, normen en checklists gerelateerd aan veiligheid van medische hulpmiddelen en de bijbehorende software.

In hoofdstuk 4 zijn de verzamelde gegevens geanalyseerd en beoordeeld op hun bruikbaarheid. Op grond van de analyseresultaten is een begin gemaakt met de theoretische invulling van 3 ondersteunende modules:

- een methodewijzer nader beschreven in paragraaf 4.1;
- de ongevalprofielen nader beschreven in paragraaf 4.2, en
- de checklist softwareveiligheid en andere algemene ondersteunende informatie nader beschreven in paragraaf 4.3.

Hoofdstuk 5 beschrijft de ontwikkeling van de methode gebaseerd op de stappen uit de norm ISO 14791, uitmondend in een raamwerk en een drietal modules.

Hoofdstuk 6 beschrijft de opzet van het softwarepakket en de bouw van een demonstratie versie daarvan.

In hoofdstuk 7 worden de uitkomsten weergegeven van een beoordeling door een panel van experts, op basis van het werken met de demonstratieversie en aanvullende informatie, van de verwachte bruikbaarheid van het uiteindelijke instrument.

Hoofdstuk 8 bevat de conclusies van het project en de aanbevelingen voor de toekomst.

Aan het eind van het rapport is informatie te vinden over de geraadpleegde literatuur, en bijlagen met de samenstelling van de Klankbordgroep en van het panel van experts, en informatie over ongevalanalyse- en risicoanalysemethoden.

## 2 Projectopzet

### 2.1 Projectinrichting

Voor de uitvoering van het project is een kernteam samengesteld van vier medewerkers van de divisie Technologie in de Gezondheidszorg van TNO Preventie en Gezondheid. De leden van het kernteam waren:

- Ir. M. Schoone (projectleider), industrieel ontwerper, met expertise op het gebied van productveiligheid, ergonomie en risicoanalyse;
- Dr. W. Oostenbrug, informaticus, met expertise op het gebied van kwaliteitsborging van software en kwaliteitsmanagement
- Ir. C.J.P.M. Teirlinck, klinisch fysicus, met expertise op het gebied van incidentanalyse en productimplementatie
- Ir. H. Vos, industrieel ontwerper, met expertise op het gebied van productontwikkeling en productbeoordeling (tot juli 2002).

In de afrondingsfase (september-november 2003) is het projectteam aangevuld met dr. J.A.M. van Boxxel (deskundige op het gebied van technology assessment, i.h.b. betreffende technologie in de gezondheidszorg).

Voor uitvoering van diverse werkzaamheden zijn ook andere deskundigen ingeschakeld, zowel van binnen TNO Preventie en Gezondheid als daarbuiten.

Ter ondersteuning van het onderzoeksproject is tevens een klankbordgroep samengesteld uit vertegenwoordigers van verschillende instellingen die met medische hulpmiddelen en/of risicoanalyse te maken hebben, waaronder producenten van medische hulpmiddelen, de Inspectie van de Gezondheidszorg, gebruikers van medische hulpmiddelen en onderzoekers op dit terrein. Als bijlage is een lijst opgenomen van de deelnemers aan deze klankbordgroep met vermelding van de instelling die zij vertegenwoordigen.

### 2.2 Uitgangspunten

Uitgangspunt voor dit project is de verplichting, die geldt voor producenten en leveranciers van medische hulpmiddelen, voor het uitvoeren van een risicoanalyse in het kader van een risico managementproces. Deze verplichting is vastgelegd in de Richtlijn Medische Hulpmiddelen (RMH) en de Richtlijn In Vitro Diagnostica (IVD). Voor het uitvoeren van een risicoanalyse wordt in deze richtlijnen verwezen naar de norm ISO 14971: Medical devices – Application of risk management to

medical devices. Deze norm heeft de oude norm EN1441 vervangen die beperkt was tot risicoanalyse. In de norm ISO 14971 wordt het uitvoeren van een risicoanalyse geplaatst in een groter geheel van risicomangement.

Het implementeren van risicomangement en het uitvoeren van een risicoanalyse is echter geen eenvoudige zaak en de aangereikte normen leiden niet zonder meer tot een gedegen aanpak. In dit project is gezocht naar manieren om het uitvoeren van een risicoanalyse gebaseerd op de systematiek van de genoemde normen met een aantal praktische hulpmiddelen te ondersteunen. Bij de uitwerking van de ondersteunende instrumenten is tevens aandacht geschonken aan het proces van risicomangement, waar het uitvoeren van een risicoanalyse deel van uitmaakt.

### **2.3 Fasering**

In het eerste deel van het project was de aandacht gericht op het nader definiëren van de werkzaamheden en de aandachtsgebieden waarvoor ondersteunende modules zouden kunnen worden ontwikkeld.

Vervolgens zijn, gericht op deze modules, relevante gegevens verzameld betreffende risico- en ongevallenanalysemethoden, ongevalgegevens, relevante normen en richtlijnen betreffende softwareveiligheid en andere ondersteunende checklists. De gegevens zijn geanalyseerd op bruikbaarheid en bewerkt, zodat zij de basis konden vormen voor de ondersteunende modules.

In het tweede deel van het project zijn de modules uitgewerkt in elektronische vorm en geplaatst in een raamwerk voor het stappenplan van het risicomangement, zoals dat in de norm wordt beschreven. Het eindresultaat was een demonstratieversie van een softwarepakket waarmee de uitvoering en implementatie van risicomangement kan worden ondersteund.

Deze demonstratieversie is naar aanleiding van een toetsing door experts herzien tot de huidige opgeleverde versie.

### 3 Inventarisatie

Tijdens het eerste deel van het onderzoek is de aandacht gericht geweest op het verzamelen van gegevens rondom analysemethoden, ongevalgegevens, wettelijke regelingen, normen en richtlijnen en softwareveiligheid. In dit hoofdstuk is beschreven op welke wijze is gezocht en wat de resultaten zijn.

#### 3.1 Bestaande methoden voor risicoanalyse en ongevalanalyse

Uit de literatuur zijn zoveel mogelijk risicoanalysemethoden verzameld. Van elke gevonden methode is een korte beschrijving gemaakt van de werkwijze, (rand)voorwaarden voor gebruik, te verwachten resultaten, voor en nadelen van de methode, een verwijzing naar literatuur en eventuele andere achtergrondinformatie en indien van toepassing de overlap of connectie met andere analysemethoden.

De methoden kunnen worden onderverdeeld in twee groepen, enerzijds de methoden die geschikt zijn voor het inventariseren van risico's en het analyseren van incidenten op oorzaken en anderzijds de methoden waarmee een uitspraak kan worden gedaan over ernst en waarschijnlijkheid van het optreden van een ongeval.

**Inventariseren en identificeren van risico's:**

- Checklists: lijsten van mogelijke gevaren, mogelijke fouten, mogelijke letsel worden nagelopen om risico's te identificeren.
- FMEA/HAZOP: systematische techniek voor identificatie van gevaren en het identificeren van afwijkingen van normaal gebruik of falen van een productonderdeel die aanleiding kunnen geven tot risico's; de HAZOP beschouwd ook de bijbehorende processen.
- Preliminary Hazards Analysis: eerste beoordeling van een productontwerp op systeemniveau. Risico's worden geïdentificeerd met behulp van checklists en de onderdelen van het systeem die gevaar opleveren worden benoemd.
- Incident analyse: historische gegevens van incidenten worden geanalyseerd.

**Inschatten van risico (waarschijnlijkheid/ ernst):**

- FMECA: een FMEA met inschatting van risico, kans op optreden en mogelijkheid om incident te voorkomen
- Fault Tree Analysis: in een grafische presentatie worden oorzaken en gevolgen die leiden tot een incident in kaart gebracht. Oorzaken en combinaties van oorzaken worden zo inzichtelijk gemaakt.
- Event Tree Analysis: gebeurtenissenboom die wordt gebouwd rond de centrale vraag "wat gebeurt er als...". Hiermee wordt vooruitgekeken naar de mogelijke gevolgen van een fout.

Daarnaast is er nog een aantal specifieke methoden gericht op het analyseren van taken en handelingen tijdens het gebruik:

- Usability Study: observatie van gebruik in een zoveel als mogelijk op het echte gebruik lijkende situatie met als doel risico's tijdens het gebruik te identificeren.
- Task analysis: observatie van taken die door mensen worden uitgevoerd, met als doel informatie te ordenen en een oordeel over onveilige handelingen te vormen.
- Human Reliability Analysis: methode om de betrouwbaarheid van het menselijk handelen in kaart te brengen.

## 3.2 Bestaande ongevalgegevens

### A. Gegevens medische hulpmiddelen voor gebruik in instellingen

Er is een inventarisatie gemaakt van mogelijke bronnen van ongevallen met medische hulpmiddelen. Eerst staan enkele Nederlandse bronnen genoemd en daarna ook een serie buitenlandse.

#### **Registratie IGZ** (informatie uit jaarverslag)

**Beschrijving:** Het gaat hier om registratie van officieel gemelde incidenten met medische hulpmiddelen.

**Gegevens:** Per incidentmelding staan minimaal geregistreerd datum van het incident, plaats van het incident, betrokken hulpmiddel, betrokken personen, gevolgen (schade/ letsel). Daarnaast leveren de incidentonderzoeken, die worden uitgevoerd als de ernst van het voorval daartoe aanleiding geeft, een dusdanig beeld op van het incident dat kan worden vastgesteld hoe een schuldvraag moet worden beantwoord.

**Toegankelijkheid:** De gegevens zijn niet openbaar. In het jaarverslag van de IGZ worden wel geanonimiseerde overzichten van deze gegevens weergegeven. Voor bijv. 1999 gaat het daarbij om 434 meldingen, een verdubbeling met het voorgaande jaar. In het overgrote merendeel van de gevallen (ca. 300) waren er geen nadelige gevolgen voor de patiënt. In ca. 100 gevallen gaat het om niet-blijvend letsel. De overige 33 incidenten hebben geleid tot blijvend letsel, waarvan 18 met een dodelijke afloop. In het jaarverslag is tevens aangegeven welke categorie producten zijn betrokken. Hier vallen *disposables*, *re-usables*, actieve en niet actieve transplantaten en elektromechanische apparatuur op, doordat zij vaak bij de incidentmeldingen voorkomen.

Door de Inspectie wordt ook nader onderzoek gedaan naar speciale onderwerpen op het gebied van de geneesmiddelen en de medische hulpmiddelen.

### ***CIBZ overleg***

**Beschrijving** In het overleg van de Werkgroep Coördinatie Instrumentatie Beheer Ziekenhuizen (CIBZ) worden via afgevaardigden van de verenigingen NVKF (klinische fysici), VZI (ziekenhuis instrumentatietechnici) en NVTG (technici in de gezondheidszorg) en van de WIBAZ (Werkgroep Instrumentatie Beheer Academische Ziekenhuizen) ervaringen uitgewisseld over de apparatuur waarmee zij werken. Hierbij komen algemene ervaringen met de apparatuur aan de orde, maar ook eventuele andere ongewenste situaties die zich hebben voorgedaan. Deze uitwisseling heeft tot doel om elkaar op de hoogte te brengen.

**Gegevens:** Afhankelijk van de discussie komen hierbij vele details aan de orde.

**Toegankelijkheid:** De gegevens zijn niet openbaar.

### ***Registratie NVZ(Zorgsignaal)***

**Beschrijving:** Zorgsignaal is een communicatiesysteem via welke ziekenhuizen elkaar en de betreffende leverancier of fabrikant kunnen informeren over (bijna)incidenten waarbij medische hulpmiddelen zijn betrokken.

**Gegevens:** Een melding die via Zorgsignaal wordt verspreid bevat voor zover relevant onder meer de volgende gegevens:

- productsoort, merk, model, leverancier, batchnummer, leverdatum, uiterste gebruiksdatum
- aard van het incident, datum en beschrijving van gebeurtenis, maatregelen ter voorkoming van herhaling
- melding aan leverancier, commentaar van leverancier
- afzender van de melding

**Toegankelijkheid:** De gegevens zijn niet openbaar op het Internet beschikbaar.

Ziekenhuizen en leveranciers kunnen via aanmelding aan het communicatiesysteem deelnemen.

### ***Registratie van de FONA/FOBO commissies (ook MIP Melding Incidenten Patiëntenzorg)***

**Beschrijving:** Ieder ziekenhuis is verplicht een FONA commissie te hebben waar incidenten die binnen het ziekenhuis plaatsvinden, moeten worden gemeld. Een ziekenhuis is niet verplicht om alle incidenten die besproken worden in de FONA commissie naar buiten te brengen.

**Gegevens:** Per incidentmelding zijn diverse details bekend: betrokken product en de gevolgen.

**Toegankelijkheid:** De gegevens zijn niet openbaar.

### ***Registratie van de Arbeidsinspectie***

**Beschrijving:** Als bij een incident (potentieel) gevaar optreedt voor een werknemer moet dit worden gemeld bij de Arbeidsinspectie. Als daar aanleiding toe is zal een Inspecteur nader onderzoek instellen.

**Toegankelijkheid:** De gegevens zijn niet openbaar. Alleen in statistische zin is hiervan wel iets terug te vinden in het jaarverslagen van de Arbeidsinspectie.

## **BUITENLANDSE GEGEVENS**

### ***Registratie MHRA<sup>1</sup> (UK)***

**Beschrijving:** In Engeland worden incidenten, waar medische hulpmiddelen bij zijn betrokken, gemeld bij het Medicines and Healthcare products Regulatory Agency (MHRA) van het Engelse Ministerie van Gezondheid. Informatie over een deel van deze incidenten wordt per incident in afzonderlijke 'Medical Device Alerts' gepubliceerd. Daarnaast publiceert de MHRA jaarlijks een rapport met onder meer statistische gegevens en trends in vergelijking met voorgaande jaren.

**Gegevens:** De volgende gegevens worden in de hiervoor genoemde 'Medical Device Alerts' gepubliceerd:

- merk en model van het betrokken medisch hulpmiddel
- korte beschrijving van het probleem
- wie actie moet ondernemen
- te ondernemen actie
- distributielijst voor de melding
- contact personen bij de MDA en de betrokken fabrikant / leverancier
- noodzakelijke terugkoppeling (naar MDA)

**Toegankelijkheid:** De 'Medical Device Alerts' en de jaarrapporten zijn zonder kosten publiek toegankelijk, zowel op papier (via een verzendlijst) als via het internet.

### ***Registratie ECRI (VS)***

**Beschrijving:** ECRI is een in de Verenigde Staten gevestigde onafhankelijke non-profit onderzoeksorganisatie met een groot aantal producten en diensten ter ondersteuning van een veilige en doelmatige toepassing van de medische technologie in de gezondheidszorg. ECRI biedt haar producten en diensten wereldwijd aan. Eén van haar producten wordt gevormd door de Health Devices Alerts, samenvattingen van informatie over medische

---

<sup>1</sup> Het MHRA is een samenvoeging van het voormalige Medical Device Agency en het voormalige Medicines Control Agency.

hulpmiddelen uit diverse bronnen. Eén van de categorieën waarin de Health Devices Alerts zijn verdeeld betreffen de zogenaamde 'Action Items' of incidentmeldingen. De bronnen voor deze incidentmeldingen zijn onder meer gezondheidszorginstellingen, de Food and Drug Administration (FDA), fabrikanten, andere organisaties die incidentmeldingen registreren en publiceren etc. Ook geeft ECRI het maandblad Health Devices uit, waarin aan een enkele incidentmelding uitgebreider aandacht wordt besteed dan in de Action Items.

**Gegevens:** In de Action Items kan men per incidentmelding de volgende gegevens raadplegen:

- beschrijving van het product (soort, merk, model, uitvoering)
- identificatie (catalogusnummer, partijnummer, distributieregio)
- fabrikant (NAW gegevens)
- probleembeschrijving
- noodzakelijke actie
- bron van de melding
- suggestie voor interne distributie van de melding

**Toegankelijkheid:** Inzage in de Health Devices Alerts en het tijdschrift Health Devices kan via een abonnement worden verkregen. De informatie is zowel op papier als elektronisch op het Internet (via gebruikersnaam en wachtwoord) beschikbaar.

#### ***Registratie Hosmat (France)***

**Beschrijving:** Informatie over incidenten en besluiten over terugtrekkingen, gebruiksrestricties etc. van het Franse Ministerie van Gezondheid of het 'Agence Française de Sécurité Sanitaire des Produits de Santé' (AFSSAPS).

**Gegevens:** De informatie bestaat uit het noemen van merk, model en fabrikant met soms een uiterst summiere beschrijving van het probleem en het besluit van de AFSSAPS met betrekking tot terugtrekking en/of beperking van gebruik. Aan elke melding is echter een aan gebruikers gerichte brief van de fabrikant gehecht met meer gedetailleerde informatie.

**Toegankelijkheid:** De informatie is per jaar vanaf 1989 via de website [www.hosmat.com](http://www.hosmat.com) publiek toegankelijk. Ook biedt de website statistische gegevens vanaf 1996, is een zoekfunctie beschikbaar en kunnen gestelde vragen en gegeven antwoorden worden geraadpleegd.

#### ***Registratie TPD-Web (Canada)***

**Beschrijving:** Het 'Therapeutic Products Directorate' (TPD) publiceert op haar website 'TPD-web' onder meer informatie over incidenten betreffende medische hulpmiddelen en geneesmiddelen. Deze informatie bestaat voornamelijk uit brieven van betreffende fabrikanten aan zowel professionals van



de gezondheidszorg (Advisories for Health Professionals) als het publiek (Advisories for the Public).

**Gegevens:** De informatie bestaat naast het noemen van productsoort, merk en model, hoofdzakelijk uit een door de betreffende fabrikant opgesteld schrijven aan zorgverleners en indien relevant aan patiënten, met een beschrijving van het probleem en de te nemen acties.

**Toegankelijkheid:** De informatie voor professionals in de gezondheidszorg is per jaar vanaf 1991 via de website TPD-Web publiek toegankelijk. Voor het publiek is dit vanaf 2001 het geval. Men kan zich gratis abonneren op een e-mail service, waardoor men op nieuwe 'Advisories' wordt geattendeerd.

### ***Registratie TGA-news (Australië)***

**Beschrijving:** De 'Therapeutic Products Directorate' (TPD) van het Australische 'Department of Health and Ageing' publiceert driemaal per jaar 'TGA-news' met onder meer informatie over 'Medical Device Incident Investigations: Recommendations'

**Gegevens:** De informatie bestaat uit

- merk, model en productsoort
- probleembeschrijving
- aanbevolen maatregelen

**Toegankelijkheid:** De TGA-news edities zijn vanaf juni 1995 publiek toegankelijk via de TGA website

### ***Registratie FDA (USA)***

**Beschrijving:** De Amerikaanse 'Food and Drugs Administration'(FDA) publiceert via het web haar 'MedWatch' programma en haar 'FDA Enforcement Reports'. MedWatch geeft veiligheidsinformatie met betrekking tot drugs en andere medische producten. De Enforcement Reports geven informatie over de door de FDA opgelegde 'Class I, II and III Recalls'. Daarnaast verzorgt het FDA 'Centre for Devices and Radiological Health' de zgn. MAUDE database, de 'Manufacturer And User Facility Device Experience Database' met rapporten van incidenten met waarbij medische hulpmiddelen waren betrokken.

**Gegevens:** De 'Enforcement Reports' geven de volgende informatie:

- recall categorie
- productomschrijving (soort, merk, model, uitvoering)
- code (serienummers, partijnummers etc.)
- recall firma (NAW gegevens)
- reden van de recall
- aantal producten in de handel

- regio van distributie (nationaal, internationaal, land, staat).

De andere FDA bronnen geven gelijksoortige informatie met een wat uitgebreidere beschrijving van het probleem etc.

Toegankelijkheid: De FDA informatie is publiek toegankelijk via haar website: MedWatch met informatie sinds 1996, de Enforcements Reports sinds 1990 en de MAUDE database met gegevens sinds 1991.

## *B Gegevens medische hulpmiddelen voor privé-gebruik*

### ***Registratie Consument en Veiligheid***

Beschrijving: De registratie van Stichting Consument en Veiligheid bevat uitsluitend privé-ongevallen. Ook in de privé-sfeer zijn medische hulpmiddelen aanwezig. De registratie betreft ongevallen waarvoor behandeling in de eerste hulp afdeling van het ziekenhuis noodzakelijk was. De registratie wordt uitgevoerd door speciaal daarvoor getrainde medewerkers van de EHBO afdelingen.

Gegevens: Per incidentmelding staan onder andere geregistreerd datum, aard en plaats van het ongeval, betrokken product, gevolg (schade/ letsel) en een aantal slachtoffergegevens.

Toegankelijkheid: De gegevens zijn openbaar. In jaarverslagen staan algemene statistische overzichten. Specifieke gegevensanalyses zijn mogelijk tegen betaling, in overleg met de afdeling databeheer. In onderzoeksrapporten zijn de resultaten van dieptestudies beschreven.

Recent heeft de Stichting Consument en Veiligheid samen met TNO een onderzoek gedaan naar ongevallen in ziekenhuizen en verpleeghuizen. Meer informatie hierover is beschikbaar bij TNO Preventie en Gezondheid.

Tevens is er een onderzoek gedaan naar ongevalrisico's voor lichamelijk gehandicapten waarvan een interne rapportage is gemaakt (inhoudsopgave beschikbaar).

Voor meer gegevens over de inhoud kan contact opgenomen worden met de Stichting Consument en Veiligheid (020-5114511).

### ***Klachtenregistratie Nationale Ombudsman***

Beschrijving: Online kan worden gezocht in de klachten database van De Nationale Ombudsman ([www.ombudsman.nl](http://www.ombudsman.nl)). Incidenteel betreft dit een klacht over een medisch hulpmiddel.

Gegevens: De klacht wordt uitgebreid beschreven en in een achtergrond document is aangegeven wat de mogelijk relevante wetgeving is, die als referentie kan dienen voor het aanhangig maken van de zaak.

Toegankelijkheid: De gegevens via internet zijn openbaar. Aangezien de klachten volgens officiële (juridische) procedures worden afgehandeld zullen ongetwijfeld uitgebreidere dossiers aanwezig zijn.

### 3.3 Bestaande wettelijke regelingen, normen en richtlijnen

#### IEC 60601 Medical Electrical Equipment

- IEC 60601-1-1: elektrische veiligheid
- IEC 60601-1-4: veiligheid van software

#### EN 1441 Risk Analysis (deze norm is inmiddels vervallen en opgevolgd door de norm ISO 14971)

- stel bedoeld gebruik vast  $\Rightarrow$  referentiekader
- gevaar identificatie
- schatting van frequentie en mogelijke schade  $\Rightarrow$  risico
- aanvaardbaarheid
- maatregelen voor risico reductie
- gevolg risico's?
- rapport (eis voor CE certificaat)

#### ISO 14971 Risk Management

- risico analyse (analoog aan ISO 1441)
- risico evaluatie
- risico beheersing
- gebruikservaringen

#### IEC 60300-3-9 Application guide - Risk Analysis

#### ISO 9126 Quality Aspects of Software

- opstellen van meetbare parameters
- definiëren van meetmethoden
- andere software kwaliteitsborging

#### CMM - Capability Maturity Model

- kwaliteitssysteem om kwaliteit van het proces van ontwikkelen van software te sturen
- niveaus van beheersing 1 t/m 5. (Het hoogste niveau wordt slechts bij uitzondering behaald.)

#### ISO 15504: Software Process Assessment

- norm voor het beschrijven van software ontwikkeling
- bevat criteria voor uitvoering

- bevat criteria voor (externe) beoordeling

**ISO 9000-3: Richtlijn kwaliteitsborging medische software**

- gedeelte uit de oude ISO 9000 serie die nog geldig is
- geeft invulling van de ISO 9000-1 voor software ontwikkelproces
- richtlijnen voor documentatie van het proces

## 4 Analyse van de verzamelde gegevens

### 4.1 Methoden voor risicoanalyse en ongevalanalyse

De bedoeling was de informatie, die over risicoanalyse en ongevalanalyse was geïnventariseerd, op te nemen in een softwaremodule van het eindproduct van het risicomangementproject. Hiertoe zou de verzamelde informatie worden vertaald in een beslisboom voor methodeselectie. Via het stellen van vragen kan de gebruiker van de softwaremodule naar de juiste (selectie van) methode(n) worden geleid. Naast deze beslisboom zal het in de softwaremodule natuurlijk ook mogelijk moeten zijn om informatie over risicoanalysemethoden te vinden via zelf in te voeren zoektermen. Hieronder volgt een toelichting op de structuur van de beslisboom.

#### “Life-cycle”-model

Welke risicoanalysemethode gebruikt wordt is sterk afhankelijk van *de fase* waarin het product zich bevindt. In een vroeg stadium zal nog weinig vast staan of bekend zijn van eigenschappen van het product en zal de nadruk op het analyseren liggen, terwijl in een verder gevorderd stadium meer nadruk kan worden gelegd op het uitvoeren van praktijktesten. Het stadium van productontwikkeling zal dan ook als eerste ingang worden gebruikt voor de methodewijzer.

Een fabrikant wordt bijvoorbeeld de vraag gesteld: in welk stadium van ontwikkeling bevindt het product zich? Daarbij kan gekozen worden uit een aantal fasen, zoals:

- Conceptfase
- Ontwikkelfase
- Productiefase
- Gebruiksfase

Als een keuze is gemaakt zal doorgevraagd worden in welke vorm informatie beschikbaar is over het product (bijvoorbeeld: profiel, programma van eisen, schetsen, tekeningen, prototype, rapporten, duurproeven, incidentmeldingen, etc.). Aan de hand hiervan kan een selectie worden gepresenteerd uit de database.

#### Norm ISO 14971

Een tweede ingang voor de beslisboom is *het doel* van het uitvoeren van een risicoanalyse. Afhankelijk van het gewenste eindresultaat kan een methode worden geselecteerd. De ene methode is bijvoorbeeld beter geschikt voor het opsporen en identificeren van risico's bij gebruik, en andere methoden zijn bijvoorbeeld beter te gebruiken bij het kwantificeren of inschatten van de ernst van een risico. De struc-

tuur van de risicomangementnorm ISO 14971 kan hiervoor als uitgangspunt worden genomen. Er kan bijvoorbeeld de meerkeuzevraag gesteld worden: "Wat is het doel van de risicoanalyse?" Waarbij gekozen kan worden uit de risicoanalyse-activiteiten volgens de ISO 14971:

- Intended use identification
- Hazard identification
- Risk estimation
- Risk acceptability decision
- Risk control
- Post-production information

Wanneer gekozen is voor een activiteit kan een selectie uit de database worden gepresenteerd. Het lijkt op dit moment nuttig om de database wat dit punt betreft verder aan te vullen met ondersteunende informatie, aangezien de norm ISO 14971 vrij summiere ondersteuning geeft via checklists in de diverse bijlagen. Verdere uitdieping is wenselijk.

## 4.2 Ongevalgegevens

Uit de database van ECRI en MDA is een selectie van ongevalbeschrijvingen gekozen. Op grond van de beschrijvingen is gezocht naar een systematiek om deze ongevallen eenduidig in te delen, te categoriseren zodat een ongevalprofiel ontstaat. Het doel hiervan is om in bestaande gegevens met behulp van bijvoorbeeld trefwoorden te kunnen zoeken naar producten, gebruikssituaties of omgevingskenmerken die op enige wijze vergelijkbaar zijn met een nieuw product, waarvan de risicoanalyse moet worden uitgevoerd. De relevante incidenten die bekend zijn kunnen uit een database worden geselecteerd en dienen als referentie voor wat redelijkerwijs aan incidenten te verwachten is met het nieuwe product.

De selectie van ongevalgegevens die als basis heeft gediend voor de hierna beschreven indeling omvatten de volgende producten: Ademhalingbewakingsmonitor; Anesthesietoestellen; Bedden; Brancards; Chirurgische boormachines; Hartlong machines; Hechtapparatuur; Hoofdsteunen; Krukken; Loopbruggen; Loophek; MRI apparatuur; Oefentoestellen; Patiëntliften; Rollators; Rolstoelen; Schroeven; Zagen.

Om te beginnen worden een aantal algemene gegevens van het product en het incident benoemd, zoals: naam van product, type, fabrikant, UMDNS code, datum. Vervolgens wordt uit de ongevalbeschrijving een aantal andere kenmerken van het incident benoemd. Hiervoor worden 7 schijven (variabelen) onderscheiden, waarbij per schijf voor de van toepassing zijnde mogelijkheid (waarde) moet worden gekozen. De 7 schijven met hun respectievelijke keuzemogelijkheden zijn:

**1<sup>e</sup> Schijf: Waar is het product voor bedoeld?**

- Preventie;
- Diagnose;
- Bewaking;
- Behandeling / verlichting van ziekten of wonden;
- Compensatie voor een handicap.

**Toelichting op de eerste schijf**

De eerste schijf behandelt meteen de meest belangrijke vraag:

*Waar is het product voor bedoeld / Wat is de functie van het product?*

Om op deze vraag goed antwoord te kunnen beantwoorden, dient men eerst te weten wat men onder een medisch hulpmiddel verstaat.

De Europese Gemeenschap definieert (verkort) het medisch hulpmiddel als:  
*'elk instrument, toestel, apparaat of elk ander artikel, met inbegrip van de software die voor de werking ervan benodigd is, dat bestemd is om bij de mens voor de volgende doeleinden te worden aangewend: preventie, diagnose, bewaking, behandeling of verlichting van ziekten of verwondingen, of compensatie van een handicap.'*

In deze definitie van de Europese Gemeenschap zijn alle categorieën aanwezig waar men het product voor zou kunnen gebruiken. Deze categorieën zijn dan ook gekozen als categorieën voor de eerste schijf.

**2<sup>e</sup> Schijf: Tot welke klasse behoort het product?**

- Klasse I
- Klasse IIa
- Klasse IIb
- Klasse III

**Toelichting op de tweede schijf**

De Europese Gemeenschap heeft regels opgezet voor classificatie van medische hulpmiddelen. In het Besluit Medische Hulpmiddelen worden hulpmiddelen opgedeeld in klassen (I, IIa en IIb, III). De klasse geeft een indicatie voor de impact van het hulpmiddel op de gebruiker ervan en tevens een indicatie van potentiële gevaren die inherent zijn aan het hulpmiddel. Daarom geldt dat voor de verschillende klassen ook verschillende normen gelden en verschillende controle procedures voor de kwaliteit van een hulpmiddel en de productie ervan. Voor alle hulpmiddelen geldt dat de fabrikant/producent een dossier moet samenstellen waaruit blijkt dat het product volgens de vereiste kwaliteitsnormen is ontworpen en geproduceerd. Verplicht onderdeel van het dossier is het uitvoeren van een risicoanalyse. In hoofdstuk 6 worden richtlijnen gegeven waarmee de producent kan bepalen tot welke klasse zijn product behoort.

**3<sup>e</sup> Schijf: Waar wordt het product het meest gebruikt**

- thuis;
- buiten het huis;
- binnen het huis;
- laboratorium;
- extramurale praktijken;
- ziekenhuis;
- ambulancedienst;
- apotheek;
- operatiekamer;
- verpleegafdeling;
- verzorgingstehuis.

***Toelichting op de derde schijf***

Naast risico's van het product en zijn functie kunnen gevaren ook ontstaan door de omgeving waarin het product zijn functie uitoefent. Voor het bepalen van de gevaren is het daarom belangrijk dat risico's inherent aan de plaats waar het product het meest zal worden gebruikt, bekend zijn.

**4<sup>e</sup> Schijf: Betrokken personen / personeel**

- professioneel
- extramuraal (huis-, tandarts e.d.);
- intramuraal;
- thuiszorg;
- niet professioneel;
- patiënt;
- mantelzorg.

***Toelichting op de vierde schijf***

Het ontstaan van gevaren en incidenten kan vaak worden toegekend aan een fout in het product. Het is echter voor goed functioneren van het product van groot belang dat het product door voldoende opgeleid personeel wordt gebruikt en dat de gebruikers van het product de te verrichten handelingen goed kunnen uitvoeren.

**5<sup>e</sup> Schijf: Interactie tussen product en gebruiker**

- handleidingen;
- zichtbaarheid, hoorbaarheid, tastbaarheid (bijvoorbeeld van alarmsignalen);
- bedienen / begrijpen van een controlepaneel;
- reageren op / aflezen / interpreteren;
- manipuleren / handelingen met het product;
- kracht uitoefenen op het product.



### *Toelichting op de vijfde schijf*

In deze schijf wordt er gekeken naar de interactie van de gebruiker met het product. Wat voor handelingen moet de persoon verrichten om het product goed te laten functioneren. Wat voor risico's brengen deze handelingen met zich mee (kracht) of zijn bijvoorbeeld weergegeven resultaten wel goed leesbaar en worden ze goed geïnterpreteerd.

### **6<sup>e</sup> Schijf: Producteigenschappen**

- het product wordt meerdere keren gebruikt;
- het product zend straling of magnetische velden uit;
- het product moet steriel (verpakt) zijn;
- het product heeft elektriciteit / een energiebron nodig;
- het product werkt met (brand)gevaarlijke stoffen;
- het product is vatbaar voor storing door straling of magnetische velden;
- er wordt kracht geleverd door het product;
- er zijn bewegende onderdelen op het product aanwezig;
- er vindt een transfer van data plaats;
- er is een uiterste gebruiksdatum of levensduur van het product;
- het product werkt met andere apparaten samen;
- het product heeft scherpe randen en / of onderdelen;
- het product is brandgevaarlijk;
- het product is vatbaar voor vervuiling wat zijn functie hindert;
- het product is vatbaar voor vervuiling wat risico's oplevert voor de gebruiker / patiënt;
- het product bestaat uit materiaal (of onderdelen) dat gevaarlijke stoffen bevat;
- er zijn maximum waarden voor de mechanische belastingen en krachten waaraan het product moet voldoen.

### *Toelichting op de zesde schijf*

In de zesde schijf kan de producent kijken en nagaan of bepaalde producteigenschappen weergegeven in deze schijf van toepassing zijn op zijn product. Men kan hierbij denken aan de manier waarop het product wordt aangedreven, wat de gevaren zijn van eventuele veroudering van het product en of er bijvoorbeeld kracht wordt geleverd door of op het product. De categorieën uit deze schijf zijn voor het grootste deel afkomstig uit de norm EN 1414 Annex C.

### **7<sup>e</sup> Schijf: Wat voor soort letsel kan men bij een incident verwachten?**

- besmetting / infectie;
- brandwonden;
- elektrocutie / schok;
- fractuur;
- kneuzing;

- snijwonden;
- verstikking / vergiftiging;
- zenuwletsel.

#### *Toelichting op de zevende schijf*

De zevende schijf geeft de mogelijkheid voor de producent om te kijken wat voor gevolgen (letsel) een incident, waar zijn product bij betrokken kan raken, heeft op de gebruiker / patiënt. Dit wordt gedaan door middel van voorbeelden (cases) uit het verleden waarbij soortgelijke producten waren betrokken en wat de gevolgen waren voor de gebruiker / patiënt (lichte verwonding, serieuze verwonding, enz.).

Het eenduidig indelen van incidenten is geen eenvoudige zaak. Dit is gebleken toen, ter toetsing, aan een aantal onderzoekers werd gevraagd om 5 ongevalbeschrijvingen op bovenbeschreven wijze te scoren. Dit leverde een zodanige spreiding in scores op dat duidelijk is dat de vraagstelling en de scoringsmogelijkheden nog niet eenduidig genoeg zijn. Hier dient verder aan te worden gewerkt.

### **4.3 Achtergronden software veiligheid**

In principe geldt voor software of voor een medische hulpmiddel in combinatie met software geen andere eis dan voor medische hulpmiddelen in het algemeen. Bepalend is te voldoen aan de in Bijlage I van richtlijn 93/42/EEG genoemde zogenaamde essentiële eisen. De eerste alinea bevat de kern van de vereiste veiligheid:

De hulpmiddelen moeten zodanig zijn ontworpen en vervaardigd dat het gebruik er van geen gevaar oplevert voor de klinische toestand of de veiligheid van de patiënten, noch voor de veiligheid en de gezondheid van de gebruikers [...], wanneer ze gebruikt worden op de voorgeschreven wijze en voor de doeleinden die ervoor zijn vastgesteld, met dien verstande dat eventuele risico's die aan het gebruik ervan kunnen zijn verbonden, aanvaardbare risico's vormen ten opzichte van het nut van het hulpmiddel voor de patiënt en verenigbaar zijn met een hoog niveau van bescherming van de gezondheid en de veiligheid.

Hierin komt tot uitdrukking, dat risico's aanvaardbaar kunnen zijn in relatie tot het nut van het hulpmiddel. Er dient dus altijd een afweging plaats te hebben gevonden.

De tweede alinea van Bijlage I bevat bepalingen ten aanzien van de minimalisatie van de risico's, waarin een veilig ontwerp en een veilige constructie naar de algemeen erkende stand van de techniek als primaire eis geldt, gevolgd door passende maatregelen zoals alarmeringen, wanneer risico's niet uitgesloten kunnen worden.

Resterende risico's dienen gedocumenteerd te worden een aan de gebruiker bekend gemaakt.

Algemeen geldt dat een fabrikant door toepassing van relevante geharmoniseerde normen aannemelijk kan maken aan de essentiële eisen te voldoen. Dat zijn normen (zie artikel 5 lid 1), die door de EU zijn gepubliceerd. Aan deze geharmoniseerde normen is in het algemeen in nationale normen uitvoering gegeven.

Voor als (deel van een) hulpmiddel aan te merken software zijn de volgende normen van belang:

- CEN/IEC-60601-1-4: *Medical electrical equipment; deel 1: general requirements for safety*; 4<sup>e</sup> collaterale standaard: *programmable electrical medical systems*.
- ISO 9000-3:1991 *Quality management and quality assurance standards - Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software*.

Daarnaast zijn uiteraard als voor hardware de normen EN 1441, ISO 14971 en NEN-EN-46001 van toepassing. Voor specifieke producten zijn nog tal van specifieke productnormen van toepassing.

Met betrekking tot software betekent het bovenstaande, dat fabrikanten gehouden zijn CEN/IEC 60601-1-4 en ISO 9000-3 te implementeren, dan wel een vergelijkbaar kwaliteitssysteem te ontwerpen en in gebruik te nemen. Dat betekent dat bij software de nadruk komt te liggen op het voortbrengingsproces.

## 5 Methode ontwikkeling

### 5.1 Uitgangspunt: de bestaande norm voor risicoanalyse

De uit te werken modules zullen passen in het stroomschema van de bestaande norm, waarin de volgende stappen worden onderscheiden. Vanuit de stappen kan een verwijzing komen naar de relevante module. Onderstaande is gebaseerd op de ISO 14971.

#### 5.1.1 Risicomanagement plan

- beschrijving van product(en) waar het om gaat en het deel van de levenscyclus waar het plan op is gericht;
- een plan voor verificatie;
- toewijzen van de verantwoordelijkheden;
- eisen voor het beoordelen van de risicomanagement activiteiten;
- criteria voor risicoacceptatie.

#### 5.1.2 Algemene beschrijving

- een complete beschrijving van de apparaten en accessoires;
- beschrijving van de personen en organisaties die de risicoanalyse hebben uitgevoerd;
- datum dat de analyse is uitgevoerd.

#### 5.1.3 Eigenschappen van het medische hulpmiddel

Maak van het te bekijken apparaat of accessoires een lijst van alle eigenschappen die de veiligheid kunnen aantasten. Waar nodig, met vermelding van de gedefiniëerde limieten.

- Waarvoor is het product bedoeld en hoe moet het gebruikt worden?
- Komt het product in contact met de patiënt en/of personen?
- Uit welke materialen bestaat het product?
- Wordt er energie geleverd naar of energie afgevoerd van de patiënt?
- Wordt er een vloeistof geleverd naar of vloeistof afgevoerd van de patiënt?
- Worden er biologische materialen door het product gebruikt en/of hergebruikt?
- Is het apparaat steriel of moet het gesteriliseerd kunnen worden?
- Is het de bedoeling dat de omgeving van de patiënt wordt veranderd?
- Zijn er metingen gedaan?
- Interpreteert het product de meetwaarden correct?
- Is het de bedoeling dat het product controleert of samenwerkt met andere producten of medicamenten?
- Is er ongewenste productie van energie of vloeistoffen?

- Kan het product worden beïnvloed door zijn omgeving?
- Zijn er essentiële accessoires nodig voor het functioneren van het product?
- Is er onderhoud of calibratie nodig?
- Maakt het product gebruik van software?
- Zijn er mogelijke vertraagde of lange termijneffecten?
- Aan welke mechanische krachten is het product onderhevig?
- Wat bepaald de levensduur van het product?
- Is het product bedoeld voor eenmalig gebruik of hergebruik?

#### **5.1.4 Identificatie van mogelijke gevaren**

Vervaardig een lijst van mogelijke gevaren die betrekking hebben op het apparaat in zowel normale omstandigheden als tijdens falen. Maak hierbij gebruik van de voorbeelden van mogelijke gevaren die vermeld staan in diverse bijlagen.

#### **5.1.5 Schatting van het risico voor een gevaar**

Ga na hoe bovenstaande gevaren van toepassing zijn op zijn product door gebruik te maken van beschikbare informatie. Bij het voorspellen van een risico moet men kijken naar de normale situaties en situaties waarin er iets mis is gegaan.

- ontstaat er gevaar zonder dat er iets fout gaat?
- ontstaat er alleen gevaar als er iets fout gaat?
- ontstaat het gevaar alleen als er meerdere dingen fout gaan?

Informatie / data kan worden verkregen van bijvoorbeeld:

- relevante normen;
- onderzoeksgegevens;
- data uit het werkveld van vergelijkbare apparaten en gepubliceerde incidenten;
- klinisch bewijs;
- resultaten van andere onderzoeken.

#### **5.1.6 Aanvaardbaarheid van de risico's**

Van ieder risico moet worden bepaald in hoeverre dit acceptabel is of niet. Bij de acceptabele risico's kan de analyse worden vervolgd met 5.1.7. Als het risico voor het bepaalde gevaar onacceptabel is, vervolg de analyse dan met 5.1.5.

- kan het defect worden ontdekt door de gebruiker voordat het gevaar ontstaat?
- kan het defect worden opgelost door meer effectieve productiecontrole of preventief onderhoud?
- zal verkeerd gebruik leiden tot een toename van de kans op het defect?
- kunnen er alarmmeldingen worden toegevoegd?

### **5.1.7 Risicobeheersing**

#### *Risicovermindering*

Bepaal of risicovermindering noodzakelijk is. Zo ja, volg dan de volgende stappen.

#### *Analyse van de opties*

Risicoreductie kan op drie manieren geschieden:

- herontwerp met inherent in het ontwerp een grotere veiligheid
- beschermende maatregelen op of om het medische hulpmiddel of bij de productie
- informatie gericht op verhogen van de veiligheid (waarschuwingen)

#### *Implementeren van de risicobeheersingmaatregelen*

- het product of een deel hiervan wordt herontworpen;
- er worden afschermingskappen en dergelijke op het product aangebracht zodat het gevaar wordt afgeschermd;
- waarschuwingen of handleidingen worden toegevoegd;
- herdefinitie waarvoor het product bedoeld is.

### **5.1.8 Het ontstaan van nieuwe gevaren**

Ga na of de procedure voor het verminderen van risico's geen nieuwe gevaren heeft opgeleverd.

### **5.1.9 Evaluatie van het risicobeheersingproces**

- afweging van de risico's tegen het nut van het product;
- inschatting van nieuw ontstane risico's;
- evalueer de resterende risico's.

### **5.1.10 Risicoanalyserapport**

Maak een rapport van de resultaten van de risicoanalyse waardoor een beslissing kan worden genomen of de overgebleven risico met de geïdentificeerde gevaren acceptabel zijn, daarbij in acht genomen het bedoelde gebruik van het product.

### **5.1.11 Herziening van de risicoanalyse**

Ga na of op grond van nieuwe informatie een herziening van de risicoanalyse nodig is.

### 5.1.12 Post-production informatie

In het kader van het risicomanagementproces dient de fabrikant voortdurend op de hoogte te zijn van actuele feiten rondom het functioneren van zijn producten die in gebruik zijn. Uit gegevens van het gebruik valt af te leiden:

- of er tot nu toe onontdekte gevaren aan het product kleven;
- of het ingeschatte risico nog steeds acceptabel is;
- of de originele risicoanalyse om andere reden wellicht ongeldig is geworden.

## 5.2 Uitwerking van de modules

### 5.2.1 Methodewijzer

In paragraaf 4.1 is beschreven hoe de gevonden ongeval- en risicoanalysetechnieken kunnen worden getypeerd, zodat een zinnige selectie van de methode gemaakt kan worden met behulp van een beslisboom. Hoe meer elementen in het "profiel" van de methoden wordt toegevoegd, hoe selectiever het keuzeprocess kan worden gemaakt. Behalve de reeds genoemde twee ingangen: *fase van het productontwikkelingsproces* en *doel van de analyse* is het zinvol op dat moment nog een paar andere criteria toe te voegen.

Zeer bepalend voor het succes van de analyse is de *beschikbaarheid van de juiste materialen, mensen en middelen*. In een vroeg stadium wordt een product beschreven in tekst, programma van eisen of in tekeningen. Aan de hand van deze materialen blijven alle analyses noodgedwongen beschouwend en theoretisch. Pas in een stadium dat een eerste proefmodel van een product beschikbaar is kunnen ook de eerste hanterings-, bruikbaarheids- en technische veiligheidstesten gedaan worden. Omdat een proefmodel op bepaalde aspecten van het uiteindelijke product zal verschillen bijv. in vorm, grootte, materialen, wijze van fabricage, gewicht, uiterlijk en werking, zullen ook deze testen niet het definitieve antwoord kunnen geven op vele praktijkvragen. Pas in een nog later stadium kan sprake zijn van testen met gebruikers/patiënten, omdat dit vanzelfsprekend met de noodzakelijke zorgvuldigheid dient te worden voorbereid. In ieder van deze situaties zal een andere methode het meest aangewezen zijn om de dan heersende vragen te beantwoorden.

Tenslotte is het ook nuttig een ingang te maken naar *type van de methode*. In het simpelste geval zoekt men naar een methode die aanvullende informatie uit normen of state-of-the-art informatie toevoegt. Het doorlopen van een checklist kan op een ander moment een zeer gewenste (tussen)stap zijn die in relatief korte tijd nuttige toegevoegde inzichten kan bieden. Op weer een ander moment is de juiste keuze een uitgebreide veldevaluatie, waarmee uiteraard veel meer tijd, mensen en geld is gemoeid, maar waarmee heel andere vragen kunnen worden beantwoord. Elk van

de methoden geeft zijn eigen dynamiek aan het proces door de verschillen in tijd en inzet die zij vergt.

### 5.2.2 Database ongevalprofielen

Dat het eenduidig indelen van incidenten geen eenvoudige zaak is, is reeds gebleken toen, zoals eerder beschreven, aan een aantal onderzoekers werd gevraagd om ter toetsing 5 ongevalbeschrijvingen op bovenbeschreven wijze te scoren. Dit leverde een zodanige spreiding in scores op dat duidelijk is dat de vraagstelling en de scoringsmogelijkheden nog niet eenduidig genoeg zijn.

De database van ongevalbeschrijvingen en ongevalprofielen moet tenminste op twee geheel verschillende manieren te benaderen zijn: om de gegevens in te voeren (vullen van de database) en om gegevens te vinden (zoeken in de database). Voor het vullen van de database is het belangrijk dat eenduidig trefwoorden kunnen worden toegekend, die later voor het zoeken het juiste aanknopingspunt vormen (zie ook 4.2). Voor het zoeken naar "vergelijkbare" producten, "vergelijkbare" gebruikssituaties, "vergelijkbare" gebruikers, "vergelijkbare" letsels, etc. is een andere vraagstelling en koppeling tussen de gegevens nodig. Dit alles moet voor het uiteindelijk risicomangement-instrument verder worden uitgewerkt.

### 5.2.3 Checklist documenten

De fabrikant dient zorg te dragen voor de nodige documentatie (zie bijvoorbeeld Bijlage VI van 93/42/EEG, par. 3.1, 3.2 en 4.2). Deze documentatie dient beschikbaar en leesbaar te zijn.

Op basis van EN-60601-4 en ISO 9000-3 moeten we denken aan de volgende documenten:

Document	Betekenis
Programma van Eisen (PvE)	Dit document is de basis voor elke ontwikkeling. Het bevat de (functionele en kwaliteits-) eisen gezien vanuit de gebruiker. Dit document geldt voor het gehele hulpmiddel, dus waar van toepassing, het hardware en het software deel. Desgewenst kan het nader wordt uitgewerkt in twee afzonderlijke delen, voor hardware en software, maar dat kan ook pas gebeuren in de Functionele Specificaties.
Lifecycle model	Dit document geeft aan volgens welke principes de ontwikkeling en de productie van het hulpmiddel plaats vindt. Een beschrijving dus van het proces van ontwikkeling, de stappen, de niveaus en de momenten van iteratie en testen.
Risico analyse	Zie checklist (5.2.4) Bevat alle te nemen maatregelen, waarnaar in de Technische Specificaties kan worden verwezen.



<b>Document</b>	<b>Betekenis</b>
Validatie testplan	<p>Het PvE is de basis voor de validatie van het hulpmiddel aan het einde van de ontwikkel- en productiecyclus.</p> <p>De finale controle of het hulpmiddel voldoet aan het PvE heet de validatie. Hiervoor kan dus direct aan het begin aan de hand van het PvE een validatie testplan worden opgesteld.</p> <p>Gevalideerd wordt dus, dat het hulpmiddel (als black box beschouwd) voldoet aan hetgeen in het PvE wordt geëist.</p> <p>Het testplan bevat tevens aanwijzingen om te valideren, dat de maatregelen op grond van de risicoanalyse zijn geëffectueerd</p>
Functionele Specificaties	<p>De FS zijn een nadere uitwerking van het PvE, mogelijk, maar niet noodzakelijk, apart voor hardware en software.</p> <p>Het bevat een nadere uitwerking van de eisen in het PvE in technisch implementeerbare termen.</p> <p>Het onderscheid tussen PvE en FS is niet altijd nodig.</p>
Architectuur Ontwerp	<p>Dit is feitelijk een onderdeel van de Technische Specificaties.</p> <p>Het beschrijft de opsplitsing van het hulpmiddel in logische onderdelen en de wijze waarop die onderdelen met elkaar zullen interacteren.</p>
Systeem testplan (Integratie testplan)	<p>Dit testplan is noodzakelijk als er sprake is van een architectuur met meerdere onderdelen die worden samengevoegd in het gerede product.</p>
Technische Specificaties	<p>De TS bevatten exacte specificaties van technische aard, op grand waarvan nog slechts een engineering taak het product onderdeel kan fabriceren.</p> <p>Tevens bevat het een exacte specificatie van (eisen aan de) input en van de verwachte output. De interface parameters met de buitenwereld worden gespecificeerd. Alle fout condities worden gespecificeerd.</p> <p>Dit document bevat ook de maatregelen op grond van de risico analyse, zoals die in de onderhavige module zijn uitgevoerd.</p>
Verificatie testplan	<p>Elk van de TS documenten (voor elk onderdeel) is de basis voor een verificatie testplan, waarin de juiste en beoogde werking van het onderdeel wordt getest.</p> <p>Het testplan evolueert mee met de eventuele aanpassingen in de TS.</p>
Verificatie testrapport	<p>Elke iteratie in de productiecyclus van het onderdeel wordt gevolgd door een verificatie test, waarvan een testrapport het aantoonbaar resultaat is.</p>
Systeemtestrapport	<p>Als sprake is van een architectuur met onderdelen, die later worden samengevoegd in het gerede product, dan wordt een systeem of integratietest uitgevoerd.</p> <p>Hierin wordt het technisch functioneren van het hulpmiddel als geheel beoordeeld.</p>
Validatie testrapport	<p>Dit rapport is het finale testrapport, waarin getoetst is dat het hulpmiddel aan de in het PvE gestelde eisen voldoet, en dat de maatregelen genoemd in de risicoanalyse zijn geëffectueerd.</p>

Enkele termen vragen om een nadere definitie, omdat ze soms verwarring oproepen. Hieronder volgen bruikbare definities van verificatie en validatie:

**Verificatie** beoogt het bevestigen dat de software aan de voor dat onderdeel gespecificeerde eisen voldoet. Verificatie wordt dus uitgevoerd per gespecificeerd onderdeel (module) en is uitsluitend betrokken op de voor dat onderdeel gespecificeerde eisen.

**Validatie** beoogt het bevestigen dat het product aan de gespecificeerde eisen in relatie tot het beoogde gebruik voldoet. Validatie heeft daarom betrekking op de voor de gebruiker gespecificeerde functionaliteit, inclusief de veiligheid.

#### 5.2.4 Checklist Software Risicoanalyse

Hieronder volgt een lijst van aandachtspunten, die specifiek betrekking heeft op de risico's van software en van door software ondersteunde middelen. Aandachtspunten met betrekking tot puur mechanische of elektronische aspecten worden hier niet genoemd, maar moeten uiteraard in elk concreet geval aan de orde komen.

Onderscheid moet gemaakt worden tussen producten die uitsluitend bestaan uit software, waarbij alleen de voor het draaien van de software benodigde apparatuur (bijvoorbeeld PC) een rol speelt, en software die in zijn werking vooral tot uiting komt in de aansturing en/of het uitlezen van elektronische of mechanische onderdelen van een apparaat. De tweede situatie levert met betrekking tot deze interactie extra aandachtspunten op.

##### 5.2.4.1 Checklist software gebruikersinterface

De volgende aspecten hebben betrekking op software systemen en de interactie met de gebruiker. Er wordt een korte lijst gepresenteerd van algemene aspecten en de mogelijke gevaren. Daarbij is het aan de ontwikkelaar om de kans op de gevaren in te schatten.

Aspecten	Mogelijke gevaren
Is er sprake van berekeningen?	Foute uitkomsten door fouten in het algoritme Foute uitkomsten doordat invoerwaarden buiten de gespecificeerde grenzen vallen
Zijn berekeningen gebaseerd op intern vastgelegde (referentie)gegevens?	Foutieve referentiewaarden (zijn er consistentiecontroles mogelijk en ingebouwd?)
Zijn berekeningen gebaseerd op extern in te voeren gegevens?	Foutieve invoerwaarden (zijn er consistentiecontroles mogelijk en ingebouwd?)

Aspecten	Mogelijke gevaren
Zijn extern in te voeren gegevens afkomstig van andere bronnen?	Gebruik van verkeerde medium (bijvoorbeeld verkeerde floppy) Fouten in de elektronische interface tussen apparaten
Worden brongegevens ingevoerd door de gebruiker?	Foutieve invoerwaarden (zijn er consistentiecontroles mogelijk en ingebouwd?)
Worden uit de uitvoer van de software conclusies getrokken ten aanzien van de diagnose?	Verkeerde diagnose op basis van verkeerde of misleidende informatie
Worden uit de uitvoer van de software conclusies getrokken ten aanzien van de therapie?	Verkeerde therapie op basis van verkeerde of misleidende informatie
Is er sprake van de opslag, het bewaren en het teruglezen van geïdentificeerde gegevens?	Verloren gaan van de relatie tussen gegevens en identificatie Koppeling van gegevens aan de verkeerde identificatie

#### 5.2.4.2 Checklist interactie software en hardware

De volgende aspecten hebben betrekking op software systemen in interactie met mechanische of elektronische apparatuur. Eerst wordt een korte lijst gepresenteerd van algemene aspecten en de mogelijke gevaren. Daarbij is het aan de ontwikkelaar om de kans op de gevaren in te schatten.

Aspecten	Mogelijke gevaren
Is er sprake van de overdracht van mechanische signalen aan de software?	Onbeheerst gedrag van mechanische onderdelen of van de sensor bij belastingen buiten de specificaties
Is er sprake van de overdracht van elektrische of elektronische signalen aan de software?	Onbeheerst gedrag van elektrische of elektronische onderdelen of van de sensor bij belastingen of externe invloeden buiten de specificaties
Is er sprake van de besturing van mechanische onderdelen of de uitvoering van mechanische acties vanuit de software (al dan niet via elektronica)?	Fouten in de signaalverwerking bij aansturing Onbeheerst gedrag van de mechanische onderdelen bij aansturende waarden buiten de specificaties
Is er sprake van de besturing van elektrische onderdelen of de uitgifte van elektrische signalen vanuit de software (al dan niet via elektronica)?	Fouten in de signaalverwerking bij aansturing Onbeheerst gedrag van de elektrische onderdelen bij aansturende waarden buiten de specificaties
Is er sprake van de presentatie van uitvoer via mechanische, elektrische of elektronische onderdelen vanuit de software?	Presenteren van onjuiste of misleidende informatie bij falen van presenterende onderdelen of de aansturing daarvan. Niet kenbaar maken in de presentatie van storingen in de presenterende onderdelen of van het optreden van afwijkende waarden die niet correct kunnen worden gepresenteerd (bijv: door limitering wijzeruitslag of door aantal beschikbare cijfers op display).

### 5.2.4.3 Checklist gevaarpunten

Hieronder volgt een opsomming van aandachtspunten voor mogelijke specifieke gevaren en een aanduiding van de mogelijke aard van de te nemen maatregelen.

Gevaarpunten	Mogelijke maatregelen
Berekeningsalgoritme met keuzes	Is altijd een keuze 'overig' opgenomen en wordt deze correct afgehandeld?
Foutcondities	Is elke foutconditie beschreven en wordt deze op welomschreven wijze afgehandeld?
Inputparameters van modules	Zijn de eisen aan inputparameters welomschreven en is specifieke foutafhandeling voorzien voor elke afwijkende inputwaarde?
Outputparameters van modules	Zijn de eisen aan outputparameters welomschreven en krijgen outputparameters ook onder elke foutconditie een omschreven waarde?
Overdracht van gegevens tussen onderdelen	Zijn de eisen aan de gegevens vanuit het ontvangende onderdeel welomschreven en wordt geborgd dat het verzendende onderdeel onder alle omstandigheden aan deze eisen voldoet?
Ontvangst van gegevens van externe bron	Zijn de eisen aan de gegevens vanuit het ontvangende onderdeel welomschreven en wordt geborgd dat de bron onder alle omstandigheden aan deze eisen voldoet?  Zijn er formele of informele standaarden waarmee de bedoelde eisen vastliggen en waarin alle uitzonderings- en foutcondities zijn afgedekt?
Overdracht van gegevens aan externe ontvanger	Zijn de eisen aan de gegevens vanuit de ontvanger welomschreven en wordt geborgd dat de bron onder alle omstandigheden aan deze eisen voldoet?  Zijn er formele of informele standaarden waarmee de bedoelde eisen vastliggen en waarin alle uitzonderings- en foutcondities zijn afgedekt?
Invoer van basis informatie	Liggen de eisen aan de basis (referentie) informatie vast?  Is er effectief versie beheer van de betreffende informatie en is die inzichtelijk voor de gebruiker?  Zijn de rechten op het muteren van deze informatie beschreven en geïmplementeerd?
Invoer van parameters en identificerende gegevens	Zijn er controles op de toegelaten waarden en gegevenstypes van parameters geïmplementeerd?  Zijn er controles op de uniciteit en mogelijke andere eisen aan de identificerende gegevens geïmplementeerd?

Gevaarpunten	Mogelijke maatregelen
Opslag van geïdentificeerde gegevens in een bestandssysteem (bijv. bestanden per sessie met een identificerende bestandsnaam)	<p>Identificeer de mogelijkheden dat de relatie tussen identificatie en inhoud verloren gaat</p> <p>Welke afscherming is er voor gebruikers tot de rechtstreekse toegang tot de opslag?</p> <p>Hoe zijn de rechten tot de toegang tot het bestandssysteem buiten de software om beschreven en geïmplementeerd?</p>
Opslag van geïdentificeerde gegevens in een gegevensbank (bijv record(s) per sessie met een identificerende sleutel)	<p>Identificeer de mogelijkheden dat de relatie tussen identificatie en inhoud verloren gaat</p> <p>Welke afscherming is er voor gebruikers tot de rechtstreekse toegang tot de opslag?</p> <p>Hoe zijn de rechten tot de toegang tot de gegevensbank buiten de software om beschreven en geïmplementeerd?</p>
Presentatie van gegevens in tekstuele vorm	<p>Identificeer de mogelijkheden tot verminking van de tekst bij presentatie, zowel door fouten in de software als door fouten in de presentatiemiddelen (bijv LCD display)</p> <p>Zijn de te produceren teksten zodanig gedefinieerd dat verminking voor de gebruiker niet tot misleiding kan leiden?</p>
Presentatie van gegevens in grafische vorm	<p>Identificeer de mogelijkheden tot verminking van de grafische informatie bij presentatie, zowel door fouten in de software als door fouten in de presentatiemiddelen (bijv LCD display)</p> <p>Zijn grafische parameters duidelijk en niet voor misleiding vatbaar (assen, asindeling, normaalwaarden, betrouwbaarheidsintervallen)</p>

Deze en andere checklists uit de bijlagen van de normen en andere literatuur kunnen worden opgenomen in het ondersteunende instrument.

## 6 Softwarepakket voor risicomanagement: Risicoanalyse database

Bij het verzamelen van alle relevante informatie die zou kunnen dienen als ondersteuning voor het beter uitvoeren van risicomanagement voor medische hulpmiddelen, bleek reeds de grote diversiteit aan informatie en de gedeeltelijke onbruikbaarheid van die informatie voor het doel dat in dit project oorspronkelijk voor ogen stond: een volledig zelfstandig door fabrikanten uit te voeren risicomanagement.

In de fase van het verzamelen van de informatie (zie hoofdstuk 3) is een eerste keuze gemaakt voor de aandachtsgebieden: a) de tekst en stapsgewijze werkwijze van de norm ISO 14971:2000, b) ongeval- en risicoanalysemethoden, c) ongevalgegevens en d) checklists voor softwareveiligheid en andere aspecten.

Vervolgens is bij de analyse van de verzamelde informatie (zie hoofdstuk 4) voor de onderdelen b), c) en d) gezocht naar een structuur waarin de informatie in te passen is, zodat de aansluiting bij het ondersteunende karakter van de te ontwikkelen softwaremodules maximaal kan zijn. Hierbij bleek opnieuw, door de veelheid en diversiteit van informatie, hoe moeilijk dit toegankelijk te maken is voor relatief onervaren gebruikers. Bijvoorbeeld: achter het ongevalanalyse-model zit een complexe denkstructuur om te kunnen bepalen hoe ongevallen vergelijkbaar met elkaar zijn; de checklists op het gebied van softwareveiligheid vatten in enkele zinnen een heel kwaliteitsborgingsysteem voor softwareontwikkeling samen; de meeste ongeval- en risicoanalyse methoden vragen bij toepassing expertkennis en ervaring.

Tijdens de methode ontwikkeling (zie hoofdstuk 5) is de keus gemaakt voor het uitwerken van drie onderdelen in de vorm van een demonstratieversie van het software pakket. De onderdelen a t/m c zijn uiteindelijk in de demonstratieversie verwerkt.

### 6.1 Step by Step

De kern van het software pakket wordt gevormd door een stap voor stap toegang tot de werkwijze zoals die is beschreven in de norm ISO 14971. In hoofdstuk 5.1 zijn die stappen genoemd en toegelicht. De manier van navigeren die wordt aangeboden in deze module werkt via *roll-out menu's*. Iedere activiteit of stap in de werkwijze kent subactiviteiten, die in het roll-out menu worden genoemd. Indien een keuze wordt gemaakt voor een item en de zoektaak wordt gestart, komt men terecht in een achterliggend document. Dit kan een instructie zijn om de aanpak van de subactiviteit toe te lichten met additionele informatie en hulp. In de meeste

gevallen zal er naar worden gestreefd om dat in de vorm van een format of invulformulier te presenteren, die bij invulling vanzelf aanzet tot uitvoer van de gewenste actie en vergaren van de noodzakelijke informatie. Deze laatste laag is in de demonstratieversie niet geactiveerd.

Indien men al in het productontwikkelingsproces en bijbehorende risicomangementtraject op weg is kan via de roll-out menu's direct gekozen worden voor de activiteit waar men op dat moment aan toe is. Ook kan de Risk Analysis Database incidenteel tijdens het proces geraadpleegd worden als men voor een specifiek onderdeel ondersteuning behoeft. Ook dan kan via de roll-out menu's direct toegang worden verkregen tot de gewenste activiteit.

Het is de bedoeling dat door het uitvoeren van de activiteiten van de Step by Step module een dossier wordt opgebouwd zoals dat is vereist in het kader van risicomangement. Men kan op ieder punt (tijdelijk) ophouden met vullen van het dossier en op een later moment door de juiste subactiviteit te kiezen de draad weer oppakken waar men was gebleven. Dit systeem is vergelijkbaar met het invullen van een elektronische belastingaangifte.

## 6.2 Incident Database

Een afzonderlijk te benaderen module wordt gevormd door de Incident Database. De module Incident Database kan op ieder willekeurig moment in het proces worden geraadpleegd.

In de uiteindelijke versie is deze database gevuld met incidentbeschrijvingen, die gerubriceerd zijn aan de hand van de 7 schijven (zie paragraaf 4.2). De gebruiker van de database dient te bedenken wat de kenmerken van zijn nieuwe product zijn en welke van deze kenmerken aanknopingspunt kunnen vormen voor het zoeken naar vergelijkbare incidenten. De meest duidelijke ingang is hierbij is het product zelf (b.v. anesthesieapparaat), hiervoor bieden bestaande databases al wel ingangen. In het geval dat het gaat om een "nieuw" product, dan is deze uiteraard nog niet onder een productnaam terug te vinden in een lijst en moet op andere wijze worden gezocht. Daarom worden in deze module de keuzemogelijkheden van de 7 categorieën in roll-out menu's gepresenteerd. Men kan kiezen voor het benoemen van een enkele keuze mogelijkheid, b.v. alle incidenten op een bepaalde plaats (environment). Ook is het mogelijk de selectie meer specifiek te maken door voor meerdere categorieën een selectie in te vullen. Hoe meer wordt gespecificeerd, hoe kleiner het aantal incidenten dat aan de specificaties zal voldoen. Door keuzes te wijzigen en opnieuw te zoeken kan men uiteindelijk de selecties bepalen van incidentbeschrijvingen die het best de ideeën voor mogelijke gevaren voedt.

In de demonstratieversie zijn geen incidentbeschrijvingen toegevoegd, alleen een enkel voorbeeld.

### **6.3 Risk analysis methods**

De zoekstructuur van de methodewijzer, zoals beschreven in de paragrafen 4.1 en 5.2, is in het software pakket van de Risk Analysis Database te benaderen via een aantal roll-out menu's, op vergelijkbare wijze als de Incident Database.

Aan de beschreven ongevalanalysemethoden en risicoanalysemethoden zijn kenmerken gedefinieerd conform de keuzecategorieën: ontwikkelingsfase, doel van de analyse, beschikbare input en type methode. In de software module kan per categorie een keuze worden gemaakt. Bij het selecteren kan óf slechts één categorie nader worden gespecificeerd óf maximaal alle vier. In het eerste geval krijgt men waarschijnlijk een groter aantal "geschikte" methoden voorgeschoteld en kan men zelf een keuze daaruit maken.

Omdat het aantal methoden, dat nu is opgenomen nog overzichtelijk is, is tevens een direct op alfabet gerangschikte toegang op naam van de methode toegevoegd.

### **6.4 Overig**

Voor de gebruiker van de Risk Analysis Database is tevens een introductie (Start) en een mogelijkheid om in de Database te zoeken (Search) en assistentie te vragen en problemen te melden (Feedback). Ook is bij wijze van verantwoording een korte tekst over TNO opgenomen (About Us).



## 7 Beoordeling demonstratieversie softwarepakket voor risicomanagement: Risk Analysis Database

In hoofdstuk 6 is beschreven hoe op basis van het materiaal, verzameld in de eerdere fasen van het project, een demonstratieversie is gemaakt van een softwarepakket voor risicomanagement (in de vorm van een CD-ROM, ook direct te gebruiken als website of deel van een intranetsite), een instrument om het proces van risicomanagement te ondersteunen. Het reeds verzamelde materiaal was veel te uitgebreid en complex om direct in een volledig software model neer te laten slaan, waarmee complete risicoanalyses en het aansluitende risicomanagement gedaan kunnen worden. Daardoor was ook letterlijke validatie van het software pakket, waarvan aanvankelijk wel gehoopt werd dat dit tegen het eind van het project uitgevoerd zou kunnen worden, niet meer mogelijk. Dit leverde een complicatie op m.b.t. de beoordeling van het software pakket.

Een oplossing van dit probleem is in de volgende richting gezocht. Enerzijds is er naar gestreefd de uitvoering en de navigatie van de CD-ROM zodanig vorm te geven, dat de demonstratieversie een realistische beoordeling op deze aspecten mogelijk kon maken. Anderzijds zou in de vorm van toelichtende informatie duidelijk gemaakt moeten worden welke aanvullende informatie nog daarin verwerkt zou gaan worden en hoe het dan "in het echt" zou gaan worden. Op basis hiervan zou dan een oordeel gegeven kunnen worden over de praktische toepasbaarheid van het uiteindelijke instrument. Hiervoor is in eerste instantie de klankbordgroep, die eerder in het project een zeer nuttige sturende en becommentariërende rol had, benaderd voor een schriftelijke procedure met behulp van een toegestuurde CD-ROM. Hierop kwam echter maar een beperkt bruikbare reactie.

In verband met de planning van het project is daarom gekozen voor een alternatieve oplossing. TNO Preventie en Gezondheid en de aan TNO gelieerde, maar onafhankelijke organisatie TNO Certification Medical Devices BV, beschikken over een ruim aantal experts die op verschillende manieren met risicoanalyse te maken hebben. Een groep van 8 van deze experts (zie bijlage 3 voor de samenstelling van deze expertgroep) is bereid gevonden om aan de hand van een vragenlijst de demonstratieversie op CD-ROM of intranet (in uiterlijk en in gebruik vrijwel niet te onderscheiden) te beoordelen en er vervolgens op een workshop over te discussiëren. De schriftelijke reacties op het werken met de CD-ROM zijn gebruikt voor het structureren van de agenda van de workshop. Deze agenda concentreerde zich op drie clusters van vragen:

- vragen naar vormgeving, gebruiksgemak e.d. van de CD-ROM c.q. internetsite;
- vragen over de inhoud en structuur van de CD-ROM, namelijk welke naast de aangegeven elementen eventueel nog meer toegevoegd zouden moeten worden;

- vragen over de optimale toepassingswijze van een in deze lijn uitontwikkeld instrument.

Onderstaand volgen beknopte samenvattingen van de discussie op de drie clusters van vragen.

### ***Vormgeving en gebruiksgemak***

De vormgeving werd door deze groep van ervaren internetgebruikers zeer op prijs gesteld, evenals het gebruiksgemak. Het instrument ziet er professioneel uit, strak maar fraai, en de vormgeving leidt niet af van de inhoud. De navigatie tussen de verschillende onderdelen verloopt ook soepel en vraagt weinig afzonderlijke instructie. Wel werden enige suggesties voor verbeteringen gedaan:

- de navigatiemogelijkheden over de site als geheel nog wat verbeteren, door vanaf ieder scherm, ook bij frames die groter zijn dan één scherm en door scrollen bekeken moeten worden, direct naar alle andere onderdelen van de site te kunnen springen;
- de structuur van de site zou nog verbeterd kunnen worden door de, zeer overzichtelijke, goed in een stroomdiagram samen te vatten overall structuur van het risicomanagementproces, nauwer te volgen;
- de suggestie werd gedaan ook digitale formulieren toe te voegen aan de site waarin aan de hand van een eigen voorbeeldproduct "gescoord" zou kunnen worden, hoever men is met een risicoanalyse of waarmee een deelanalyse zou kunnen worden uitgevoerd. (N.B. met name deze suggesties hangen nauw samen met de beoogde toepassingswijze en kwamen later in de workshop opnieuw aan de orde).

Een groot deel van de gedane suggesties bleken op korte termijn te verwerken in een nieuwe versie van het softwarepakket. Op de bij dit rapport gevoegde CD-ROM staat de meest recente demonstratieversie van het software-instrument voor risicomanagement: de "Risk Analysis Database".

### ***Inhoud en structuur***

Voor de module Step by Step werd aanbevolen om de structuur van het risicomanagementproces conform de norm ISO 14971 nauwer te volgen. Dit werd ook om inhoudelijke redenen van groot belang geacht. Het helpt namelijk de gebruiker om de logica van risicomanagement beter te volgen. Aangegeven werd dat de afzonderlijke stappen zowel een goede toelichting behoeven, als extra schema's, invulformulieren e.d. om de risicoanalyse en de vervolgens te nemen risicomanagementstappen daadwerkelijk door de fabrikant uit te laten voeren.

De Incidents Database module moet gezien worden als hulpmodule dat op ieder moment in de analyse aangeroepen kan worden om het realiteitsgehalte van de (tussentijdse) resultaten te toetsen. Dit werd gezien als een zeer nuttig onderdeel. De ervaren experts onderstreepten dat het maken van een risicoanalyse en het toepassen van risicomangement geen puur logische, "mechanische" aangelegenheid is, of tenminste niet alleen, maar dat degene die een risicoanalyse uitvoert er zeer bij gebaat kan zijn om kennis te kunnen nemen van echte ongevallen en bijna-ongevallen. Om het zoekmechanisme te baseren op de 7 "schijven" werd als nuttig gezien. Zo kunnen incidenten op gespoord worden met voldoende verwantschap (op specifieke punten in meerdere dimensies). Dit is leerzaam voor de risicoanalyse van het onderhanden product. Wel werden twee mogelijke praktische bezwaren gezien. Het eerste bezwaar is het probleem om de database op te bouwen. Een tweede bezwaar is vervolgens het up-to-date te houden. Dit vereist een aanzienlijke inspanning en een goede organisatie. Mogelijk kan hiervoor samenwerking met organisaties worden aangegaan die ongevalgegevens verzamelen en bewerken, zoals ECRI, MDA of FDA.

De Risk Analysis Methods module is een andere hulpmodule. Deze module wordt specifiek aangeroepen op verschillende momenten in het proces. De vormgeving suggereert dat een selectie nodig is uit een omvangrijk aantal mogelijkheden. Dit werd echter overdreven gevonden: in werkelijkheid bestaat er maar een beperkt aantal relevante methoden, 20, hooguit 30, en deze zijn met een eenvoudiger zoekmechanisme te vinden. Deze constatering zou het uitwerken van het instrument vergemakkelijken. Er werd echter ook vastgesteld dat de beschrijving van de methoden uitgebreider zou moeten zijn en vergezeld zou moeten gaan van in te vullen formulieren of schema's (zoals waarmee bij de FMEA een begin is gemaakt). Een andere complicatie werd gezien in het feit dat zowel de argumenten voor het kiezen van een methode in die gevallen dat er uit meerdere methoden gekozen kan worden als voor het hanteren van de methode lastig volledig eenduidig te beschrijven zijn. Het zelfstandig uitvoeren van een goede risicoanalyse kan met deze module wel worden ondersteund, maar deskundigheid en ervaring is hierbij zeker nodig. De module reikt eigenlijk vooral suggesties aan voor het selecteren van de juiste methode plus een korte beschrijving van de methode. Dat is niet voldoende om zelfstandig uitvoeren door een onervaren fabrikant mogelijk te maken.

Voor de modules Search en Feedback werd gesteld dat deze als nuttig werden gezien, maar dat ook het opbouwen en onderhouden van deze onderdelen de nodige inspanning zou vergen om blijvend een goede bruikbaarheid te garanderen.

De algemene conclusie op dit punt kan als volgt worden samengevat: de uitwerking tot een volledig zelfstandig te gebruiken instrument is in principe langs de lijnen van de demonstratieversie mogelijk, maar vergt veel tijd voor opbouw en onder-

houd. Ook in deze uitgewerkte vorm blijven, om zelfstandig tot succesvolle toepassing te komen, oordeelsvermogen en ervaring onontbeerlijk.

### *Optimale toepassingswijze*

De discussie richtte zich in eerste instantie op de beoogde toepassing: zelfstandig gebruik door een fabrikant. Daartoe zou het instrument doorontwikkeld moeten worden tot een compleet zelfsturend instrument. De fabrikant zou erop moeten kunnen vertrouwen dat hij, als hij de instructies bij alle aangegeven stappen letterlijk volgt, aan het eind een dossier heeft opgebouwd waarmee het risicomangementdeel van de aan de toelatingsautoriteit te overleggen dossier op de juiste wijze is opgebouwd. Als dit zo precies wordt genomen, is dit, zo bleek uit de discussie bij de eerdere punten, om meerdere redenen wellicht een zwaardere taak en met een minder zekere garantie voor zelfstandig gebruik, dan mogelijk leek bij aanvang van het project.

Vervolgens werd met de experts bediscussieerd welke fabrikanten behoefte zouden hebben aan zo'n volledig zelfstandig te gebruiken instrument. Daarbij bleek een duidelijk onderscheid gemaakt te moeten worden tussen enerzijds fabrikanten die hulpmiddelen produceren in de categorie I (zelfregulering) en in de overige categorieën (IIa, IIb en III) anderzijds.

Fabrikanten die producten maken in deze laatste categorieën hebben over het algemeen een ruime ervaring met risicoanalyse en risicomangement en hebben hiervoor bestaande structuren (teams van ervaren deskundigen, aanwezige literatuur, onderdeel van kwaliteitssysteem of anderszins van bedrijfsprocedures, meetopstellingen etc.). Als zij ondersteuning zoeken dan betreft dat meestal een van twee vormen, of een combinatie daarvan:

- ondersteuning op een specifiek punt, waarvan zij het belang goed kunnen inschatten, maar dat zij om praktische redenen liever door een ervaren of op dat punt goed geëquipeerde derde partij laten uitvoeren en vervolgens in hun risicoanalyse en risicomangement integreren;
- ondersteuning die meer de vorm aanneemt van fungeren als “sparring partner” of “coach”, waarbij er regelmatig interactie is met een externe adviseur, maar waarbij de fabrikant uiteindelijk de regie houdt over het proces (ook in termen van te besteden tijd en middelen).

De situatie ligt geheel anders bij fabrikanten van medical devices in categorie I. Uit de beperkte ervaringen tot dusverre met de kwaliteit van zelfopgebouwde dossiers, blijkt dat hier veel ruimte voor verbetering is en dat er veel fabrikanten zijn die maar een beperkte ervaring hebben op dit terrein. Aangezien de ongevallen met deze categorie meestal niet zo ernstig zijn, is er tot dusverre geen grote druk geweest hierin verbetering te brengen. Toch blijkt uit de schaarse gegevens dat deze

categorie niet vergeten mag worden, en juist wellicht zeer geholpen zou kunnen zijn met een methode waar men zelf een eind mee komt en waarmee al een significante verbetering bereikt kan worden ten opzichte van de huidige werkwijze. Bij uitwerking specifiek voor deze categorie zal ook een ander probleem zichtbaar worden. Een wezenlijk onderdeel van het instrument is het kunnen vergelijken met gegevens over incidenten met vergelijkbare apparatuur, maar juist met betrekking tot deze categorie zijn er relatief weinig gedocumenteerde incidenten voorhanden. Met behulp van een schriftelijke enquête is getracht een beeld te krijgen van aantal en aard van incidenten in Nederland met hulpmiddelen in categorie I om te bezien of hierover nadere informatie te verkrijgen die bij de uitwerking van het instrument gebruikt zou kunnen worden. De reacties op deze enquête hebben echter zeer weinig extra informatie opgeleverd.

Het laatste agendapunt van de workshop betrof een discussie over andere mogelijke gebruiksvormen van een soortgelijk instrument. Twee mogelijkheden werden geselecteerd voor verdere discussie.

De eerste mogelijkheid betreft een expertsysteem voor risico-onderzoek bestemd voor externe deskundigen (bijvoorbeeld deskundigen van TNO), te gebruiken bij externe advisering. Het voordeel van een instrument als dit zou tweërlei zijn:

- het systematiseren en sneller bij de hand hebben van alle procedures en documenten die men nu al gebruikt;
- als een vergelijkbaar systeem door een groep experts gebruikt wordt, vergemakkelijkt dit de communicatie en samenwerking en kan men gemakkelijker informatie van anderen overnemen of aan anderen overdragen. Zo kunnen analyses gemakkelijker door breed samengestelde teams worden verricht, wat de kwaliteit en efficiëntie ten goede kan komen.

De experts zagen dit als een reële mogelijkheid tot verbetering, maar hadden hun twijfels over de verhouding tussen de hiervoor benodigde investeringen en de daarmee op korte termijn te realiseren kwaliteitsverbetering of efficiencywinst.

De tweede mogelijkheid betreft een instrument met een meer educatief karakter, een "awareness" bevorderend instrument. In dat geval wordt de doelstelling losgelaten om een instrument te ontwikkelen dat volledig zelfstandig gebruikt kan worden. De doelstelling van een educatief instrument is om de fabrikant die het gebruikt een compleet beeld te geven van de vereiste procedures en van de methodes die nodig zijn om de verschillende stappen uit te voeren. Maar de methode zou in deze vorm ook goed duidelijk moeten maken hoe complex een risicoanalyse of het proces van risicomangement kan worden en minder ervaren fabrikanten moeten adviseren voor welke onderdelen het verstandiger is externe hulp te vragen. Dit verhoogt de bewustwording voor de risicoproblematiek en helpt de fabrikant een

eventuele externe vraag om ondersteuning te articuleren. Het zou deze vorm zijn, die het beste ingezet zou kunnen worden bij hulpmiddelen in categorie I.

In de slotdiscussie van de workshop bestond consensus dat in het licht van de benodigde investeringen en de specifiek wenselijke verbeteringsmogelijkheden in de industrie, de voorkeur uitging naar een doorontwikkeling tot een informatief instrument, vooral bruikbaar voor fabrikanten van hulpmiddelen in categorie I. Het instrument kan de "awareness" deze groep verhogen en het inzicht in het proces zodanig vergroten dat men goed kan vaststellen welke onderdelen zelfstandig kunnen worden uitgevoerd en bij welke onderdelen de steun van een expert (intern of extern) noodzakelijk is. Bovendien kan de vraag voor die expert veel preciezer worden geformuleerd.

## 8 Conclusies en aanbevelingen

Het onderzoeksproject (in meer detail toegelicht in hoofdstuk 2) kan globaal in vier fasen worden ingedeeld:

- het verzamelen van de benodigde gegevens
- het integreren van de gegevens in een software instrument
- het beoordelen van de bruikbaarheid van het software instrument
- de conclusies van het project en aanbevelingen voor de toekomst.

In hoofdstuk 3 is beschreven welke gegevens zijn geïnventariseerd en met welke methoden. De volgende categorieën gegevens zijn geïnventariseerd:

- bestaande methoden van risicoanalyse en ongevalanalyse
- gegevens ongevallen medische hulpmiddelen voor gebruik in instellingen
- gegevens ongevallen medische hulpmiddelen voor privé-gebruik
- bestaande relevante wettelijke regelingen en normen naast de ISO 14971
- checklists voor veiligheid van software en andere specifieke aspecten.

De omvangrijke resultaten zijn in een dossier verzameld. Hierin is veel materiaal bijeengebracht. Slechts een beperkte selectie is opgenomen in deze rapportage en de demonstratieversie. Het materiaal is beschikbaar voor de verdere ontwikkeling van het software instrument.

### *Risicoanalysemethoden*

Vervolgens is in hoofdstuk 4 nagegaan op welke wijze de omvangrijke hoeveelheid gegevens m.b.t. risicoanalysemethoden in de vorm van een methodewijzer toegankelijk gemaakt zou kunnen worden voor iemand die risicoanalyse en risicomanaagement uit wil voeren.

De belangrijkste conclusie van deze analyse was dat de informatie die door het te ontwikkelen software instrument aan de risico-onderzoeker wordt toegeleverd afhankelijk moet zijn van twee aspecten:

- de fase waarin de productontwikkeling zich bevindt. Te onderscheiden zijn:
  - conceptfase
  - ontwikkelfase
  - productiefase
  - gebruiksfase.
- het doel van de betreffende risicoanalyse. Hoewel het zinvol bleek de database verder aan te vullen met gedetailleerde gegevens in aanvulling op de summiere checklists van de norm ISO 14971, is als hoofdindeling de indeling van risicoanalyse activiteiten uit deze ISO norm aangehouden:

- intended use identification
- hazard identification
- risk estimation
- risk acceptability decision
- risk control
- post-production information.

### *Ongevalgegevens*

Een soortgelijk probleem bestaat m.b.t. het toeleveren van ongevalgegevens over ongevallen die lijken op wat er met het onderhanden product zou kunnen gebeuren. Wat betreft de beschikbaarheid van gegevens bleek het hier te gaan om twee totaal verschillende gebieden:

- risico's en ongevallen met apparatuur gebruikt in ziekenhuizen
- risico's en ongevallen met apparatuur gebruikt buiten ziekenhuizen, met name hulpmiddelen gebruikt in de privé sfeer.

Over risico's en ongevallen met apparatuur in ziekenhuizen bestaan zeer veel gegevens, met name in de buitenlandse databases van het ECRI in de V.S. en het MDA in het Verenigd Koninkrijk. De primaire ingang voor zoeksystemen is het type apparatuur. Op basis hiervan kan effectief gezocht worden naar verwante typen van apparatuur. Andere typen apparatuur kunnen echter aspecten bezitten die ook van belang zijn voor het te onderzoeken nieuwe product. Hiertoe is een systeem van "schijven" ontwikkeld, dat het mogelijk maakt in meerdere dimensies te zoeken. Hierover is in 2001 al een eerste rapport opgesteld (R. de Jeu. "Risicoanalyse, nader bekeken"). Deze schijven zijn (voor de keuzemogelijk per schijf zie hoofdstuk 4):

- Waar is het product voor bedoeld?
- Tot welke klasse behoort het product?
- Waar wordt het product het meest gebruikt?
- Betrokken personen/personeel
- Interactie tussen product en gebruiker
- Producteigenschappen
- Wat voor soort letsel kan men bij een incident verwachten.

### *Softwareveiligheid*

Veiligheid van software, zowel van "embedded" software als software die wordt gebruikt via een afzonderlijke computer, is een terrein dat sterk in opkomst is. Hiervan is een afzonderlijke inventarisatie gemaakt. Een belangrijk aspect van softwareveiligheid is de nadruk hierbij op de kwaliteitsborging tijdens het ontwikkelingsproces van de software.

### *Ontwikkeling van het softwarepakket*

Vervolgens zijn in hoofdstuk 5 de hoofdlijnen beschreven waarmee het instrument



zou dienen te gaan werken. Op de hoofdlijnen wordt de risiconorm ISO 14971 nauw gevolgd. Om de verschillende stappen uit te kunnen voeren is echter gekozen voor het ontwikkelen van drie modules, die op ieder gewenst moment aangeropen kunnen worden in de vorm van checklists, formulieren of tabellen, en nadere toelichting en achtergrondinformatie:

- een stap voor stap ondersteuning van de werkwijze van de norm ISO 14971;
- een methode wijzer (met ingang voor fase van productontwikkeling en doel van de betreffende stap van de risicoanalyse);
- een database met ongevalprofielen (die het zoeken via de 7 schijven mogelijk maakt).

In hoofdstuk 6 is beschreven met welke dilemma's de onderzoekers en ontwerpers van het software instrument te maken kregen, toen concrete plannen werden gemaakt om het software-instrument te bouwen. Zowel de complexiteit van alle denkbare varianten van risicoanalyse die met het instrument gedekt zou moeten worden, als de pure hoeveelheid gegevens die op dat moment reeds verzameld c.q. toegankelijk was gemaakt, maken het tot een probleem deze informatie in een hanteerbaar instrument te integreren. Dit deed de onderzoekers en de ontwerpers van het software instrument ervoor kiezen eerst een demonstratieversie te bouwen. Op basis van een beoordeling hiervan zou dan beslist kunnen worden over de verdere bouw van het instrument. In het vervolg van hoofdstuk 6 wordt beschreven hoe de demoversie van het software-instrument is ontworpen en gebouwd.

In hoofdstuk 7 is beschreven hoe de demonstratieversie is getoetst. Daarbij is om logistieke redenen gekozen voor een andere opzet van toetsing dan aanvankelijk beoogd. De beoordeling heeft uiteindelijk plaatsgevonden met een panel van experts afkomstig van TNO en van TNO Certification Medical Devices BV. Deze beoordeling is in twee stappen verlopen: eerst een schriftelijke beoordeling van de demo na het zelfstandig uitvoeren van een serie activiteiten met de demo aan de hand van een schriftelijk instructie. Vervolgens zijn deze experts in een workshop bijeen geweest. Daarbij is eerst bekeken in welke mate consensus bereikt kon worden over de bruikbaarheid van het uiteindelijk te ontwikkelen instrument op basis van een extrapolatie van de ervaringen met de demo en een toelichting over de verwachte uitwerking van de demo die nodig zou zijn om uiteindelijk tot het beoogde instrument te komen. Vervolgens is met de experts bediscussieerd in welke mate men doorontwikkeling zinvol achtte tot een instrument waarmee een fabrikant volledig zelfstandig een risicoanalyse uit zou kunnen voeren van voldoende kwaliteit om in een toelatingsdossier op te nemen. Om meerdere redenen werd dit niet als zinvol beschouwd, met als belangrijkste reden dat de grote hoeveelheid werk die hiervoor nog nodig zou zijn, niet zou leiden tot een aanzienlijk vergrote vraag bij fabrikanten die bovendien hun eigen methoden gewend zijn. Een uitzondering werd gemaakt voor producten in klasse I. Tenslotte werd de experts gevraagd tot welke andere toepassingsvorm de demonstratieversie het beste zou

kunnen worden doorontwikkeld. Een andere mogelijkheid, die om inhoudelijke redenen mogelijk is, is het doorontwikkelen tot een expertsysteem. Dit zou met name interessant zijn om teams van externe risico-onderzoekers (bijv. van TNO zelf) efficiënter en meer gestandaardiseerd samen te laten werken bij het verwerken van externe opdrachten. Toch werd ook hier het bezwaar gezien dat de grote verder benodigde investeringen op korte termijn niet op zouden wegen tegen de verwachte extra opdrachten.

Als meest interessante optie bleef over het doorontwikkelen tot een instrument met een meer educatief karakter. Hierbij zou de doelstelling losgelaten moeten worden dat een fabrikant hiermee volledig zelfstandig een compleet risicomanagement-dossier op kan bouwen, maar wel dat deze een goed beeld krijgt wat dit inhoudt en welke onderdelen hij zelf uit kan voeren, dan wel beter aan deskundigen over kan laten. Gegeven de feitelijke situatie op dit terrein zou dit niet interessant zijn voor fabrikanten van apparatuur in de hogere risicoklassen (IIa, IIb en III), maar wel voor fabrikanten van apparatuur in risicoklasse I. Hier bestaat duidelijk ruimte voor verbetering, die ingevuld moet worden met praktische, kosteneffectieve instrumenten.

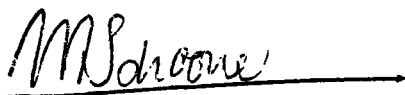
Na de workshop heeft het onderzoekteam de resterende projecttijd besteed aan een analyse van de uitkomsten van de workshop in het licht van alle eerder verzamelde gegevens en inzichten en in het laten neerslaan van deze conclusies en inzichten in het voorliggende rapport en in een dossier dat de alle gevonden gegevens beschikbaar houdt voor vervolgonderzoek.


Alles overziend komen de onderzoekers tot de aanbeveling dat doorontwikkeling zinvol is in eerste instantie tot een instrument waarmee fabrikanten van apparatuur in risicoklasse I geholpen worden een goed inzicht te krijgen in wat risicoanalyse inhoudt op klasse I niveau, en waarmee ze een verantwoorde inschatting kunnen maken welke onderdelen ze zelf uit kunnen voeren en voor welke onderdelen het nodig is of veel praktischer is hiervoor externe deskundigheid in te roepen. De snelheid waarmee de ontwikkeling van dit instrument ter hand genomen kan worden, zal afhangen van de belangstelling hiervoor in het veld. Deze zal gepeild worden. Als het instrument als bedoeld is ontwikkeld, dan kan op het raamwerk hiervan een informatief instrument worden gebouwd voor de hogere categorieën. De doelstelling hiervan moet niet zijn, om de in dit rapport aangegeven redenen, fabrikanten van apparatuur in de hogere categorieën "op te voeden" hoe risicoanalyses uitgevoerd moeten worden. Een informatief instrument kan wel behulpzaam zijn om efficiënte toegang te krijgen tot relevante gegevens over methoden en ongevalgegevens en zelf te beoordelen welke externe hulp om praktische redenen efficiënt kan zijn en in welke hoek die gezocht kan worden.



## 9 Ondertekening

Leiden, 28 november 2003

Auteur(s)	Handtekening
Ir. M. Schoone auteur	

Interne beoordeling door	Handtekening
Dr. J.A.M. van Boxsel hoofd sector Kwaliteit en Bruikbaarheid	

## 10 Geraadpleegde literatuur

### *Risicomanagement Algemeen*

- [1] Aken van et al., Handboek ontwerpen van veilige producten. Uitgeverij Lemma, 1996. ISBN 90-5189-566-6.
- [2] Dhillon B.S., Medical device reliability and associated areas. CRC Press LLC Florida, 2000, Page 110. ISBN 0-8493-0312-5.
- [3] Dolan Alfred M., Risk Management ISO 14971: The World Standard for Medical Devices. FDLI Update, July/August 2003.
- [4] Henley E.J., Kumamoto H., Reliability Engineering and risk assessment. Prentice-Hall, New York, 1981. ISBN -0-13-772251-6, p. 20.
- [5] ISO 14971:2000(E), Medical devices – Application of risk management to medical devices. First edition, 2000-12-15
- [6] ISO/CD 14971, Medical devices – Application of risk management to medical devices. Second edition, 2003-03-07.
- [7] Kornneef F., Organised learning from small-scale incidents. Delft, 2000.
- [8] Medirisk, Onderlinge Waarborgmaatschappij voor Instellingen in de Gezondheidszorg B.A., Juridisch Handboek.
- [9] Schmuland Carl, Creating a Value-Added Risk Management Process. Biomedical Instrumentation and Technology, September/October 2003
- [10] Wang J.X., Roush M.L., What every engineer should know about risk engineering and management, page 69–71. Marcel Dekker Inc, NY, 2000. ISBN 0-8247=9301-3.

### *Risicoanalysemethoden*

- [11] CEN/BT/WG113:20. CEN/CENELEC/ETSI JTAG 4. CLC/BTWG 101-5(sec)19. Guide for the risk analysis of products considering people with special needs.
  - Annex A/A.1. Hazard and Operability (HAZOP) study.
  - Annex A/A 5 Preliminary Hazard Analysis (PHA).
  - Annex A/A6 Human Reliability Assessment.
- [12] Gelderblom G.J. et al. Functionele analyse: eindrapportage van de projecten Utensils en Functionele analyse 1998 -1999, IRV, maart 2000.

- [13] Henley E.J., Kumamoto H. Reliability engineering and risk assessment. Prentice-Hall, New York, 1981, page 19 –22, 24-28. ISBN 0-13-772251-6.
- [14] IEC 60812. Analysis techniques for system reliability – Procedures for failure mode and effects analysis (FMEA).
- [15] IEC 61025: 1990. Fault Tree Analysis (FTA). International Standard.
- [16] IEC 61882. Guide for hazard and operability studies (HAZOP studies).
- [17] IEC Standard 812 85. Procedure for failure mode and effects analysis (FMEA)
- [18] ISO 14971:2000. Annex F.4. Hazard and Operability Study (HAZOP).
- [19] Kirwan B., Ainsworth L.K., A guide to task analysis. 1999 (First published 1992). ISBN 0748400583.
- [20] Spoomaker Prof. Ir. J.L., Ontwerpen op bedrijfszekerheid en veiligheid. Dictaat io36, Faculteit van het industrieel ontwerpen, TU Delft, augustus 1995.

### ***Ongevalgegevens***

- [21] ECRI diverse publicaties.
- [22] FDA diverse publicaties.
- [23] Jaarrapportages Inspectie voor de Gezondheidszorg, Den Haag. 1999 tot nu.
- [24] Jeu, Ronald de. Risicoanalyse, nader bekeken. TNO Preventie en Gezondheid. Leiden, maart 2003.
- [25] Medical Devices – Adverse Incident Reports 1999, diverse Safety Notices March 2000, MDA, UK.
- [26] Medical Devices – Repair and Maintenance Provision, diverse Safety Notices June 2000, MDA, UK.
- [27] Medical Devices – Reporting Adverse Incidents and Disseminating Safety Warnings, diverse Safety Notices 2000 tot nu, MDA, UK.
- [28] Nimwegen Chris van, Oostenbrug Wytze, Verplichtingen bij Incidentenmeldingen volgens de Europese Richtlijnen voor Medische Hulpmiddelen. Technologie in de Gezondheid, juni-2000.
- [29] Publicatieblad van de Europese Gemeenschappen Nr. L 169/36 Bijlage IX, Classificatie. 1993.
- [30] Stichting Consument en Veiligheid, diverse publicaties.

- [31] Stichting Consument en Veiligheid, Privé-ongevallen bij senioren. Amsterdam, 1998.
- [32] Weegels M.F., Accidents involving consumer products. Den Haag, 1996.  
Diverse websites over incidenten en klachten met medische hulpmiddelen.
- [33] MedPro, TNO Medische producten, Databank & Informatiedienst. Technologie in de Gezondheid, 2000. (CD-ROM)

#### ***Softwareveiligheid***

- [34] CMM - Capability Maturity Model, CMU/SEI-93-TR-24
- [35] ISO/IEC 15408: 1999. Common Criteria for Information Technology - Security Techniques - Evaluation Criteria for IT Security.
- [36] ISO 9126: 1996 Quality aspects of Software
- [37] ISO/IEC TR 15504-1/9 - Information Technology - Software Process Assessment.

#### ***Gerelateerde normen***

- [38] IEC 60300-3-9, Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems.
- [39] ISO 13485, Quality systems – Medical devices – Particular requirements for the application of ISO 9001.
- [40] ISO 13488, Quality systems – Medical devices – Particular requirements for the application of ISO 9002.
- [41] ISO 14969, Quality systems – Medical devices – Guidance on the application of ISO 13485 ISO 13488





**Bijlage A Samenstelling Klankbordgroep**

<b>Organisatie/instelling</b>	<b>Deelnemer [p.m. checken]</b>
Cardio Control NV	F. Kroon Technisch Directeur
CIBZ Coördinatie Instrumentatie Beheer Zieken- huizen	J.W.H. Gradussen UMC Radboud
Consument & Veiligheid	Mw. S. van Haastrecht Onderzoeker Technische Veiligheid
Gehandicaptenraad	Mw. T. Rooijen Mw. B.J. van den Boomgaard
IGZ Inspectie voor de Gezondheidszorg	drs. E.C.A. Stomph Inspecteur Regionale Inspectie
IRV, Hoensbroek	Dr. G.J. Gelderblom
RU Leiden werkgroep Veiligheid	Mw. S. Akerboom J. Groeneweg
TU Delft Faculteit Ontwerp & Constructie Mens-Machine Systemen	Mw. M. van der Vlugt
TU Delft Veiligheidskunde	F. Koornneef



## **Bijlage B Samenstelling Panel van experts risicomangement**

### **Panel van experts voor beoordeling demo-versie software instrument**

K.P. Barto	auditor TNO-C Medical Devices BV
Dr. J.A.M. van Boxsel	TNO-PG, hoofd sector Kwaliteit en Bruikbaarheid, deskundige Technology Assessment
Ir R. Hensbroek	TNO-PG, deskundige MDD richtlijn en elektrische veiligheid
G. van Keulen	TNO-PG, deskundige technologie voor zelfmonitoring en –toediening
Drs. R. van Melick, apotheker	directeur TNO-C Medical Devices BV, deskundige veiligheids- en kwaliteitsmanagement,
C. van Nimwegen	TNO-PG, deskundige incidentonderzoek/vigilantiesystemen
Ir. M. Schoone	TNO-PG, industrieel ontwerper, veiligheidsdeskundige
Ir. C.J.P.M. Teirlinck	TNO-PG, klinisch fysicus



## Bijlage C Ongevalanalyse- en risicoanalysemethoden

### Checklists

#### ■ Description

Checklists are mainly used for the identification of hazards. It is a useful tool to in an early design stage. Relevant checklists can be found in standards or companies can create their own checklists suitable for their specific situation and product.

#### ■ Examples

<i>Checklist specific for medical devices: ISO 14971: 2000</i>
Annex A: checklist with questions for identification of medical device characteristics that could impact on safety
Annex B: checklist for in vitro diagnostic medical devices
Annex C: checklist for toxicological hazards
Annex D: checklist for identification of possible hazards and contributing factors associated with medical devices
Annex A: checklist with questions for identification of medical device characteristics that could impact on safety

<i>Checklist of hazardous Energy sources</i>
1. Fuels
2. Propellants
3. Initiators
4. Explosive charges
5. Charged electrical capacitors
6. Storage batteries
7. Static electrical charges
8. Pressure containers
9. Spring-loaded devices
10. Suspension systems
11. Gas generators
12. Electrical generators
13. Rf energy sources
14. Radioactive energy sources
15. Falling objects
16. Catapulted objects

<i>Checklist of hazardous Processes and Events</i>
1. Acceleration
2. Contamination
3. Corrosion
4. Chemical dissociation
5. Electrical
- Shock
- Thermal
- Inadvertent activation
- Power source failure
- Electromagnetic radiation
6. Explosion
7. Fire
8. Heat and temperature
- high temperature
- low temperature
- temperature variations
9. Leakage
10. Moisture
- high humidity
- low humidity
11. Oxidation
12. Pressure
- high pressure
- low pressure
- rapid pressure changes
13. Radiation
- thermal
- electromagnetic
- ionizing
- ultraviolet
14. Chemical replacement
15. Mechanical shock
16. Acceleration

17. Heating devices
18. Pumps, blowers, fans
19. Rotating machinery
20. Actuating devices
21. Nuclear devices

17. Contamination
18. Corrosion
19. Chemical dissociation
20. Electrical
- Shock
- Thermal
- Inadvertent activation
- Power source failure
- Electromagnetic radiation
21. Explosion
22. Fire
23. Heat and temperature
- high temperature
- low temperature
- temperature variations
24. Leakage
25. Moisture
- high humidity
- low humidity
26. Oxidation
27. Pressure
- high pressure
- low pressure
- rapid pressure changes
28. Radiation
- thermal
- electromagnetic
- ionizing
- ultraviolet
29. Chemical replacement
30. Mechanical shock

#### ■ Sources and references

Henley E.J., Kumamoto H. Reliability Engineering and risk assessment. Prentice-Hall, New York. 1981. ISBN -0-13-772251-6, p. 20.

## **ETA – Event Tree Analysis**

### **■ Description**

The Event Tree Analysis (ETA) is a visual representation method that is used to identify possible outcomes when the occurrence of an initiating event is known. The basic question asked is: "What happens if...?". The approach is bottom-up and can both be used for analysis of system reliability as for the analysis of human reliability. It is also a method to quantify the probability of errors and the probability of sequences.

The starting point (initiating event) disrupts the normal system operation. From this event several other events will take place, because of the interaction with other parts of the system or because of the reaction from operators who discover that the event took place and try to solve the problem. In this way the initiating event can finally result in one or more outcomes or consequences. It is usually assumed that the outcome of each sequence is either a success or a failure. This is visually represented in an event tree.

To start building an event tree, it is important to have a logical and structured sequence of tasks or component functionality's. It is necessary (but sometimes difficult) to find the right level of detail of this sequence. These activities or sequential events are represented in a can be placed in a row, with the initiating event on the left and the outcome or final consequence at the right. Below this row the actual event tree can be drawn.

Whereas event trees work forwards to identify the consequences of errors, fault trees work backwards to identify the causes of errors. It can be useful to "hang" fault trees from the various nodes of an event tree.

## ■ Example

### Activities or sequential events

	Event or activity A	Event or activity B	Event or activity C	
--	---------------------	---------------------	---------------------	--

## ■ Sources and references

Kirwan B. and Ainsworth L.K. A guide to task analysis. Page 178 -184. 1999 (First published 1992). ISBN 0748400583.

Dhillon, B.S. Medical device reliability and associated areas. CRC Press LLC Florida, 2000, Page 110. ISBN 0-8493-0312-5.

Henley E.J., Kumamoto H. Reliability engineering and risk assessment. Prentice-Hall, New York, 1981, page 24-28.

Wang J.X., Roush M,L. What every engineer should know about risk engineering and management, page 69–71. Marcel Dekker Inc, NY, 2000. ISBN 0-8247=9301-3.



## FMEA – failure mode and effect analysis

### ■ Description

The FMEA is a method where every failure in a (sub)part of a system is checked to see whether it influences the functionality of this (sub)system and to see how critical this is with respect to the reliability and safety. Preferably this analysis is performed by the designer, together with people who are not directly involved with the design. It should be used and applied several times during the development of a product. The result of the analysis is a list with critical items, together with actions to reduce the probability of failure of the relevant parts.

The analysis starts at the part level of a product and goes up to the system level, and is therefore called a "bottom-up" procedure. Starting at the part-level the following questions can be asked:

- Which function does this (sub)part have?
- How does it work?
- In what way can it fail?
- What happens if it fails?

The FMEA should be seen as a starting point for discussion and should be repeated several times during the development of a product. After performing a FMEA the risks for critical parts must be quantified. The risk is defined as the *seriousness* of the effect multiplied by the probability of *occurrence* as well as the probability of *discovery* of a failure.

The seriousness of the effect of a failure	S (Seriousness)
The probability of occurrence of a failure	O (Occurrence)
The probability of the discovery of a failure before it is delivered to the user	D (Discovery)

These three dimensions are separately rated on a scale of 1 to 10. With this the quantification is reduced to ranking, and therefore easier to perform.

The expression for the risk (R) is:

$$R = S \times O \times D$$

### ■ Example

Part		Fail characteristics			Risk estimation				Action/ status of action				
Id. no.	Function	Failure mode	Causes of failure	Effects of failure	S	O	D	R	Recommendations	S	O	D	R
1													
2													

### ■ Sources and references

IEC Standard 812 85 Procedure for failure mode and effects analysis (FMEA).

CEN/BT/WG113:20 Guide for the risk analysis of products considering people with special needs.

Ontwerpen op bedrijfszekerheid en veiligheid. Prof. Ir. J.L. Spoormaker. Dictaat io36, Faculteit van het industrieel ontwerpen, TU Delft, augustus 1995.

## FTA – Fault Tree Analysis

### ■ Description

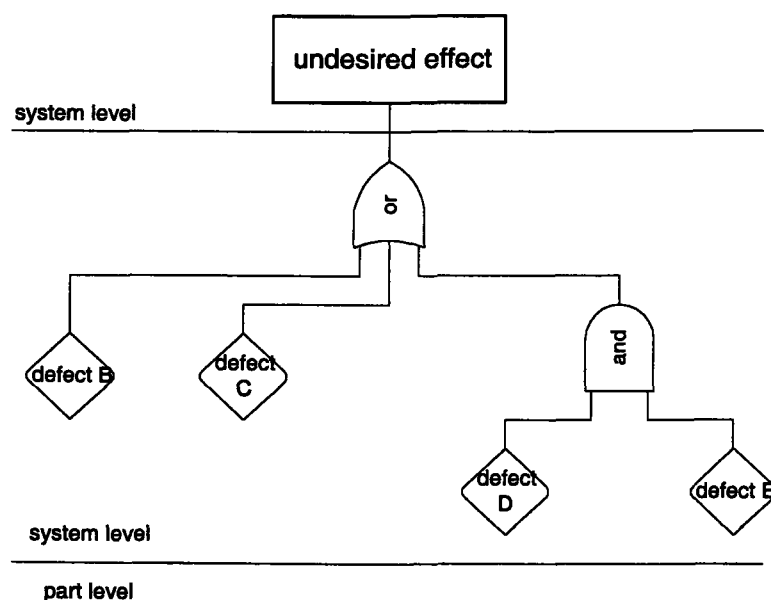
The Fault Tree analysis is an organised graphical presentation of the conditions and other factors that cause or contribute to the occurrence of a defined undesired effect. It is mainly a qualitative method for analysing hazards identified by other techniques (for example failure modes that are found by FMEA). The aim is to determine all the ways in which a specific failure mode can occur.

The FTA is a top-down approach where a product or system slowly breaks down into several subsystems and parts. The starting point of the analysis is a known, undesired failure mode and is called a "top event". From this undesired effect the system breaks down via logical operators, like and- ports and or- ports until the level of the so-called "basic events". The "and" port is used for a result that will occur only if more than one underlying failure took place. The "or" port is used for a resulting event that will occur when only one of the underlying defects take place.

A fault tree can be used to identify causes and combination of causes, which lead to the undesired effect, to find critical paths and to be able to say something about the independence of several subsystems or parts. At least the procedure consists of the following steps:

- Definition of the scope of the analysis
- Familiarisation with the design, functions and operation of the system
- Definition of the top event
- Construction of the fault tree
- Analysis of the fault tree logic
- Reporting on results of the analysis

### ■ Example



## ■ Sources and references

IEC 1025: 1990. Fault Tree Analysis (FTA). International standard.

Kirwan B. and Ainsworth L.K. A guide to task analysis. Page 188 -193. 1999 (First published 1992). ISBN 0748400583.

Ontwerpen op bedrijfszekerheid en veiligheid. Prof. Ir. J.L. Spoormaker. Dictaat io36, Faculteit van het industrieel ontwerpen, TU Delft, augustus 1995.

## HAZOP – Hazard and Operability Study

### ■ Description

The hazard and operability study (HAZOP) is a systematic technique for identifying hazards and operability problems. It is similar to a Failure Mode and Effect Analysis, but is based on a theory that assumes accidents are caused by deviations from the design or operation intentions. It identifies deviations from normal use and identifies whether the consequences of such deviations can lead to hazards or operability problems. In other words the HAZOP is an extended FMEA technique in the direction of including operability factors in addition to equipment fault modes. The HAZOP technique can be used in the initial design phase to provide a guide to safer detailed design. However, the most common use of HAZOP is the detailed design phase. After defining the scope and objectives of the study, the selection of a team and the collection of necessary data, the actual HAZOP examination can start. Preferably this study consists of the following steps:

1. Creation of a full description of the product:
  - divide the system into parts;
2. Systematic review of every part to discover how deviations from the intention of the design can occur:
  - identify deviation by using guide words on each element;
3. Decide whether these deviations can lead to hazards or operability problems:
  - identify consequences;
  - identify whether a significant problem exists;
  - identify protection, detection and indicating mechanisms;
  - Identify possible remedial/ mitigating measures (optional);

The conventional HAZOP studies were originally developed for the chemical industry. It starts with the identification of "property words" and "guide words". Common guide words are: not, no, more, less, as well as, part of, reverse, other than, etc. Typical HAZOP 'property words' are: flow, temperature, pressure, level, concentration, amount, etc. An example with the guide word 'no' and the property word 'flow' is given below. For the medical device industry this method can be used to analyse the operation of the medical device or a process used in the manufacture or maintenance of the medical device that may have significant impact on the function.

## ■ Example

Guide word	Deviation	Possible causes	Consequences	Action required
<i>Not, no</i>	<i>No flow</i>	1. No feed material available	Reduced output polymer will be formed	A. Ensure good communication with operator B. Provide low level alarm on setting tank.
		2. Pump fails	As for 1.	As for B.

## ■ Sources and references

IEC 61882 Guide for hazard and operability studies (HAZOP studies).

CEN/BT/WG113:20. CEN/CENELEC/ETSI JTAG 4. CLC/BTWG 101-5(sec)19.

Guide for the risk analysis of products considering people with special needs.

Annex A/A.1. Hazard and Operability (HAZOP) study.

Henley E.J., Kumamoto H. Reliability engineering and risk assessment. Prentice-Hall, New York, 1981, page 36-37.

Kirwan, B. A guide to task analysis. Taylor&Francis Ltd, London, 1992, page 194-201.

ISO 14971:2000. Annex F.4. Hazard and Operability Study (HAZOP).

## **Incident analysis**

### **■ Description**

To gain more insight in risks associated with a product a study can be performed on historical data of accidents with relevant existing products already on the market. Companies might have filled their own databases during the years and have this information available. There are also several commercially available databases for medical devices, for example the ECRI database.

Analysis of historical data is a good starting point to gain more insight in the risks associated with specific product characteristics and the results are useful input for new product design. However, a risk analysis can never be conducted on historical data only. A new or modified design should always be analysed to identify other, new risks.

## Preliminary Hazards Analysis (PHA)

### ■ Description

A preliminary hazard analysis is a first attempt to identify the (gross) system hardware and events, which can lead to hazards, while the system is still in a preliminary design stage. In this early step in the analysis the system is decomposed into subsystems to identify the sections or components, which are likely sources of hazardous situations. The study mainly uses methods like checklists and expert reviews. Good engineering judgement is crucial. At least the analysis consists of two steps:

1. Identification of hazards (checklists)
2. Identification of parts of the system, which give rise to the hazard(s)

The PHA is build mostly by using checklists and performing expert reviews. The end result is a list with possible hazards, hazardous situations and events, which can be used for further studies. The study can also be extended to a more formal manner, including the consideration of event sequences leading hazards to accidents, a qualitative evaluation of the consequences of these accidents and corrective measures.

The use of *checklists* and performing an *expert review* are explained elsewhere in the database.



■ **Sources and references**

E.J. Henley, H. Kumamoto. Reliability engineering and risk assessment. Prentice-Hall, Inc. N.J. 1981, ISBN 0-13-772251-6, pag. 19 –22.

CEN/CENELEC/ETSI JTAG4, CLC/BTWG 101-5(sec)19, CEN/BT/WG113:20. Guide for the risk analysis of products considering people with special needs, annex A/A 5 Preliminary Hazard Analysis (PHA).

## Task analysis

### ■ Description

Task analysis is a method that is used for the identification of human error, human reliability quantification or for the evaluation of human machine interfaces. It examines the tasks that must be performed by users when they interact with systems or products. It is a fundamental approach, which assists in achieving higher safety, productivity and availability standards. There are many task analysis techniques to help the analyst collect information, organise it and then use it to make various judgements or design decisions:

- Task data collection methods: collecting data on actual or proposed task performance
- Task description methods: representing such data in a pre-specified format
- Task simulation methods: creating simulations of the task
- Task behaviour assessment methods: assessing what can go wrong in task performance
- Task requirement evaluation methods: assessing the adequacy of the task environment and existing facilities available to carry out the task.

Observation, questionnaires and interviews are examples of data collection methods. Known task description methods are flow charts, operational sequence diagrams, etc. Examples of task simulation methods are studies that use simulators, mock-ups or computer models. Task behaviour assessment methods include event trees, FMEA's, Fault trees, HAZOP, etc. Task requirement evaluation methods include ergonomic checklists, interface surveys, etc.

### ■ Sources and references

Kirwan, B. A guide to task analysis. Taylor&Francis Ltd, London, 1992. ISBN 0748400575.

CEN/BT/WG113:20. CEN/CENELEC/ETSI JTAG 4. CLC/BTWG 101-5(sec)19. Guide for the risk analysis of products considering people with special needs. Annex A/A6 Human Reliability Assessment.

## Usability studies

### ■ Description

To identify risks related to usability and human error a test can be performed in actual or simulated conditions with representatives of future end users. There are several ways to perform this study, depending on the design stage and the availability of mock-ups or prototypes. Examples of the three most used methods are given below:

#### *Observation*

The selected 'users' are asked to perform several tasks with the product and observers or cameras register the behaviour of the user and the interaction with the product. An observation study can be performed with existing/related products or with mock-ups/ prototypes.

#### *Questionnaires*

Gathering of information about risks associated with the product by asking structured questions on paper. This method is mainly used as a way to get more insight in the opinion of a specific group of people, most of the times representatives of the end users of the product. The study can both result in qualitative or quantitative results. For a quantitative questionnaire analysis a large group of respondents will have to be present and a statistical analysis afterwards is necessary to get useful information.

#### *(Expert) interview or review*

Gathering of information by interviewing individuals with specific knowledge about the product or representatives of the group of end users. This method gains a qualitative insight in the risks associated with the product and can be used in any design stage. Questions can both be open or closed, improvised or previously structured via checklists.

### ■ Sources and references

Gelderblom G.J. et al. Functionele analyse: eindrapportage van de projecten Uten- sils en Functionele analyse 1998 -1999, IRV, maart 2000.

Kirwan, B. A guide to task analysis. Taylor&Francis Ltd, London, 1992. ISBN 0748400575.