DOCUMENT CONTROL SHEET

	ORIGINATOR'S REF. NLR-TP-98333		SECURITY CLASS. Ongerubriceerd

ORIGINATOR
National Aerospace Laboratory NLR, Amsterdam, The Netherlands

TITLE
Het veiligheidssysteem van ERA (In Dutch, based on NLR TP 97155 U)

PUBLISHED IN
het blad Ruimtevaart, februari 1998, uitgegeven door de Nederlandse Vereniging voor Ruimtevaart en gebaseerd op de publicatie "Failure detection and recovery system concept for the European Robotic Arm", oorspronkelijk gepubliceerd in de Proceedings van de International Conference on Safety and Reliability"(ESREL'97),Lisbon,Portugal,June 17-20'97

AUTHORS	DATE	pp ref
J.F.T. Bos en M.J.A. Oort	februari'99	13

DESCRIPTORS

Errors	Robot dynamics
Extravehicular activity	Robot sensors
Failure	Robotics
International space station	Robots
Robot arms	Safety
Robot control	Space tools

ABSTRACT
Momenteel wordt de European Robotic Arm (ESA) door Fokker Space BV ontwikkeld in opdracht van de European Space Agency (ESA). ERA zal in de loop van het jaar 2000 worden gelanceerd. Zijn eerste missie is het helpen van Russische kosmonauten bij het samenbouwen van het Russische segment van het International Space Station (ISS). Verder zal ERA een rol spelen in de bevoorrading, de inspectie en het onderhoud van het ruimtestation. Eén van de onderdelen van ERA is het Failure Detection, Isolation and Recovery (FDIR) systeem. In opdracht van Fokker Space BV levert het Nationaal Lucht- en Ruimtevaartlaboratorium een belangrijke bijdrage in het ontwerp van dit systeem. Dit artikel beschrijft hoe de veiligheidseisen, gegeven de specifieke mogelijkheden en besprekingen van een ruimterobot, hebben geresulteerd in het concept voor het FDIR-systeem. Allereerst wordt ERA kort beschreven, en worden de algemene uitgangspunten van het onderwerp behandeld. Daarna worden de elementen van het FDIR-systeem in meer detail beschreven.

NLR-TP-98333

Het veiligheidssysteem van ERA

J.F.T. Bos en M.J.A. Oort

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-98333

Het veiligheidssysteem van ERA

J.F.T. Bos en M.J.A. Oort*

* *Fokker Space BV*

Dit rapport is gebaseerd op een artikel in het blad Ruimtevaart, februari 1998, uitgegeven door de Nederlandse Vereniging voor Ruimtevaart.

Het artikel is gebaseerd op de publicatie "Failure detection, isolation and recovery system concept for the European Robotic Arm" dat reeds is verschenen als NLR-rapport TP 97155 L. Het oorspronkelijke artikel is gepubliceerd in de Proceedings van de "International Conference on Safety and Reliability" (ESREL '97), Lisbon, Portugal, June 17-20, 1997.

Hoofdafdeling:	Informatica
Datum:	februari 1999
Rubricering van de titel:	ongerubriceerd

Samenvatting

Momenteel wordt de European Robotic Arm (ERA) door Fokker Space BV ontwikkeld in opdracht van de European Space Agency (ESA). ERA zal in de loop van het jaar 2000 worden gelanceerd. Zijn eerste missie is het helpen van de Russische kosmonauten bij het samenbouwen van het Russische segment van het International Space Station (ISS).
Verder zal ERA een rol spelen in de bevoorrading, de inspectie en het onderhoud van het ruimtestation. Eén van de onderdelen van ERA is het Failure Detection, Isolation and Recovery (FDIR) systeem. In opdracht van Fokker Space BV levert het Nationaal Lucht- en Ruimtevaart-laboratorium een belangrijke bijdrage in het ontwerp van dit systeem. Dit artikel beschrijft hoe de veiligheidseisen, gegeven de specifieke mogelijkheden en beperkingen van een ruimterobot, hebben geresulteerd in het concept voor het FDIR-systeem. Allereerst wordt ERA kort beschreven, en worden de algemene uitgangspuntenvan het ontwerp behandeld. Daarna worden de elementen van het FDIR-systeem in meer detail beschreven.

Inhoudsopgave

3 Figuren

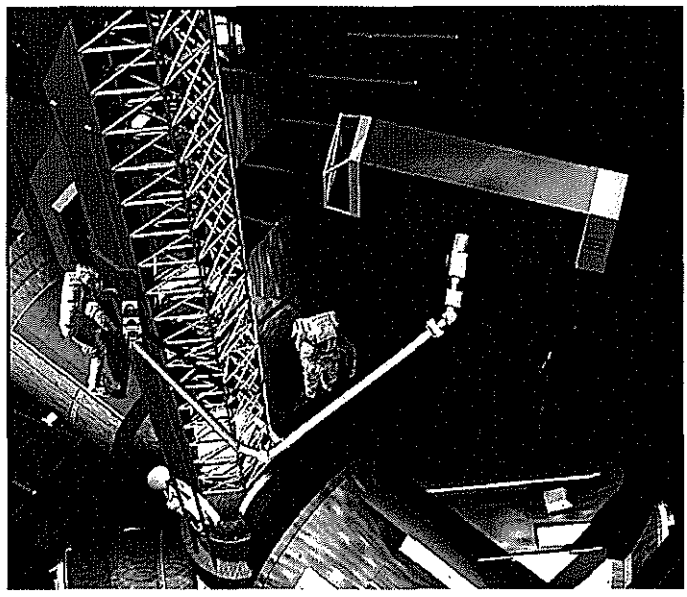
(13 pagina's totaal)

De robotarm ERA

ERA is een robotarm met zeven graden van vrijheid. De totale lengte bedraagt ongeveer 11 meter. De robotarm is in staat om zijn schoudergewricht op verschillende posities aan het ruimtestation te bevestigen: de zgn. "basepoints". In zo'n situatie grijpt de hand van de robotarm het nieuwe "basepoint", en laat de schouder het oorspronkelijke "basepoint" los, zodat de rollen van oorspronkelijke hand en schouder nu omgedraaid zijn. ERA is in staat om in de ruimte objecten met een massa van maximaal 8000 kg te manipuleren.

Het totale ERA-systeem bestaat uit een vluchtsegment en een grondsegment. Het vluchtsegment bestaat uit de robotarm zelf en twee Man-Machine Interfaces (MMIs). De robotarm kan op twee manieren worden bestuurd: tijdens een Extra Vehicular Activity (EVA), alsmede vanuit het ruimtestation zelf. Omdat de kosmonaut tijdens een EVA een ruimtepak aan heeft, zijn het beeldscherm en de bedieningsorganen van de EVA-MMI beperkt. De IVA-MMI (Intra Vehicular Activity MMI) daarentegen bestaat uit een laptop, en tevens kan de kosmonaut ook over TV-beelden van externe Russische camera's beschikken.

Het grondsegment bestaat uit een door het NLR te realiseren faciliteit om een missie voor te bereiden en te trainen, een "WET-model" dat gebruikt wordt in een zwembad om de kosmonauten in de besturing van ERA onder gewichtsloosheid te trainen, en ondersteunende testfaciliteiten voor de verificatie van het ERA-ontwerp.



De robotarm bestaat uit meerdere subsystemen: ledematen (limbs), gewrichten (joints), camera's (Camera Lighting Units, CLUS), handen (Basic End-Effectors, BEEs) en een (hoofd)computer, de ERA Control Computer (ECC). [Fokker Space]

Uitgangspunten voor het ontwerp

Het feit dat ERA in de ruimte door kosmonauten wordt bestuurd en actief kan zijn in een omgeving waar mensen aanwezig zijn, maakt dat er stringente eisen gelden met betrekking tot de veiligheid, de robuustheid en de flexibiliteit van de robotarm. In principe kan een fout snel resulteren in een levensgevaarlijke situatie: zonder voorzorgsmaatregelen kan de arm tijdens een EVA een kosmonaut raken, of kan dusdanige schade aan het ruimtestation aanbrengen, dat er indirect levensgevaar dreigt.

De strikte veiligheidseisen vragen om het veiligstellen van de situatie bij twee foutdetecties, en het behoud van functionaliteit na een foutdetectie. Vanwege deze veiligheidseisen zijn er voor elke kritische fout (hardware- dan wel softwarematig) twee automatische en volledig onafhankelijke detectiemechanismen ingebracht. Er is voor gekozen om ERA te stoppen na elke ontdekte fout, zonder vooraf te controleren of de fout terecht gedetecteerd is. Met andere woorden, ook onterechte foutmeldingen leiden tot het stoppen van de robotarm. Dit is een valide uitgangspunt: ERA is geen autonoom systeem. zodat het werk weer snel hervat kan worden. Tevens geldt dat het voorkomen van menselijk letsel belangrijker is dan operationele onderbrekingen, al dienen deze wel zo weinig mogelijk op te treden. Als de fout wel terecht gedetecteerd is zijn er maatregelen mogelijk om de fuctionaliteit te handhaven.

Een tweede uitgangspunt is een gespreide verantwoordelijkheid voor detectie en ingrijpen. De verantwoordelijkheden worden gedeeld door de centrale ERA Control Computer (ECC) en de ERA-subsystemen. Als een subsysteem een fout ontdekt, deactiveert hij allereerst zichzelf. Vervolgens wordt de fout gerapporteerd aan de ECC. De ECC zorgt daarna voor het deactiveren van de overige subsystemen, met als resultaat dat ERA als geheel wordt gestopt.

Het derde uitgangspunt is het streven om het ontwerp zo simpel mogelijk te houden. Dit is met name gedaan uit overwegingen t.a.v. de robuustheid. De verantwoordelijkheid voor diagnose en herstel ("recovery") is derhalve bij de operators gelegd: hetzij de kosmonauten, hetzij de mensen in het grondstation. Een ander argument voor deze keuze is dat de kracht van de computers in de ruimte zeer beperkt is, waardoor de algoritmes relatief eenvoudig en de rekenfrequenties beperkt moeten blijven. Overwegingen t.a.v. robuustheid leiden al snel tot een voorkeur voor bewezen technologiën. ERA is echter een compleet nieuw product, waardoor er niet aan de introductie van veel nieuwe technologie viel te ontkomen. Voor het FDIR-systeem is gebruik gemaakt van een aantal bewezen concepten uit de satelliet ISO.

Omwille van de gewenste flexibiliteit kunnen de autonome functies m.b.t. detectie en stoppen door de operator worden uitgeschakeld.

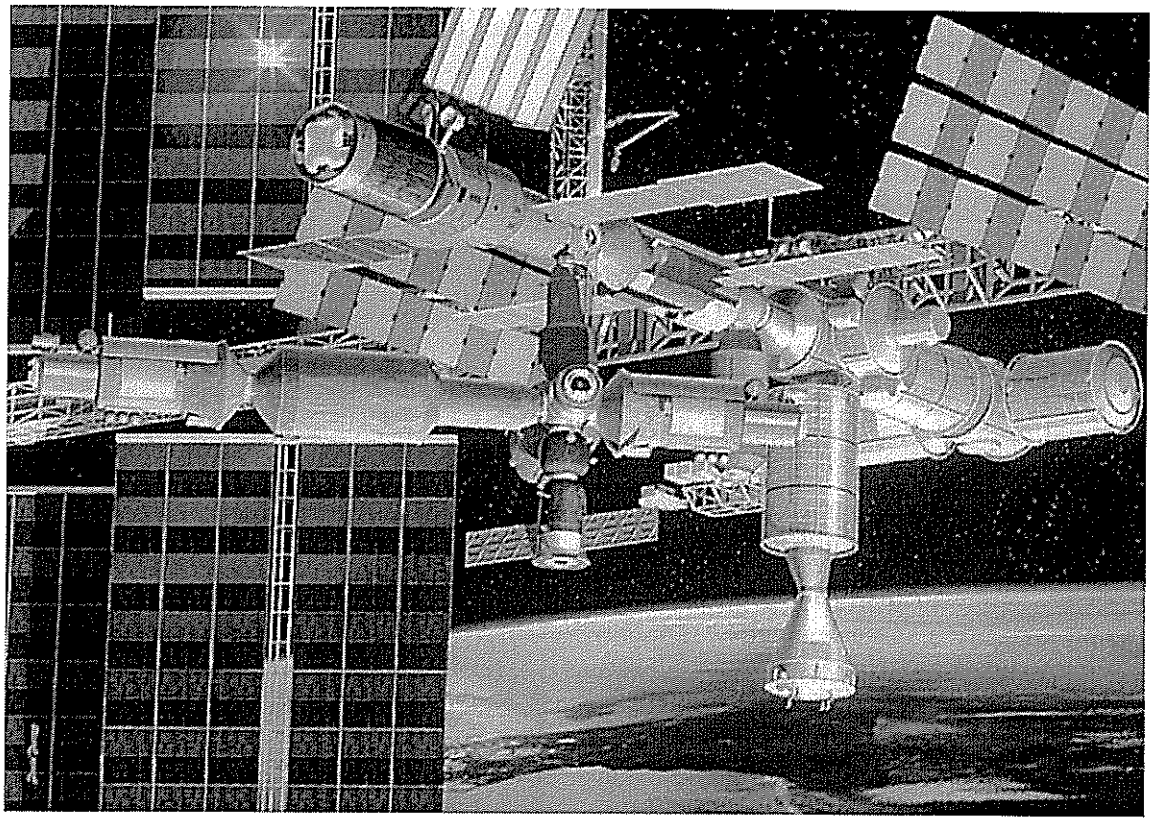
In principe stellen de typerende eigenschappen van de ruimte (thermische omgeving, gewichtsloosheid, vacuüm en kosmische straling) een grote uitdaging voor het ontwerp van een willekeurig ruimteobject. Alhoewel deze factoren in belangrijke mate het totale ERA-ontwerp beïnvloeden, is hun invloed op het FDIR-systeem zeer beperkt. Echter, doordat de EVA-kosmonauten een ruimtepak dragen en vanwege het feit dat de EVA-MMI bestand moet zijn tegen de zojuist genoemde ruimte-aspecten, zijn de informatie en de commandeer-mogelijkheden van de EVA-MMI beperkt. Hierdoor kunnen de EVA-kosmonauten geen rol van betekenis hebben in het stellen van de diagnose van eventuele problemen. Tevens geldt dat de reparatiemogelijkheden in de ruimte zeer beperkt zijn. Dit heeft uiteraard z'n weerslag op de mogelijkheden voor herstel (redundante kanalen etc.).

Detectie

Om te voorkomen, dat de ERA-operator verrast wordt door een automatische actie ten gevolge van een door het systeem geconstateerde fout, worden twee detectieniveaus gebruikt: een Waarschuwingsniveau en een Gevaarniveau. Het eerste niveau geeft aan dat de situatie zich verkeerd ontwikkelt, maar nog niet gevaarlijk is. Hier wordt volstaan met een waarschuwingsbericht aan de operator. Als vervolgens het Gevaarniveau wordt overschreden (een indicatie dat de operator niet heeft kunnen of willen optreden) grijpt het automatische systeem onmiddellijk in, en brengt ERA in een veilige toestand.
Een van de belangrijkste veiligheidsrisico's is een ongecontroleerde beweging, bijvoorbeeld veroorzaakt door een fout in een gewricht. In het gewricht zelf bevindt zich een zeer snel, analoog uitgevoerd detectiemechanisme, dat gebaseerd is op het meten van de stroomsterkte door de motor. Omdat deze stroomsterkte een lineair verband heeft met de versnelling, beperkt het detectiemechanisme de maximale versnellingen die mogelijk zijn na een fout. Andere detectiemiddelen zijn de "Velocity Tracking Error Check" (300 Hz) en de "Joint Angle Tracking Error Check" (20 Hz). De detectiemechanismen zijn zoals gezegd vrij eenvoudig vanwege de beperkte rekenkracht in de gewrichten. De Waarschuwings- en Gevaarniveaus zijn instelbaar.

In de ECC bevindt zich de "Path Deviation Check", waarmee gecontroleerd wordt of het punt dat bestuurd wordt (meestal het uiteinde van ERA) niet teveel afwijkt van het gewenste pad (zowel positie als oriëntatie). Als ERA zich vlak bij het ruimtestation bevindt, hetgeen de meest kritieke situatie is, worden de volgfouten bepaald uit het camerabeeld, dat onafhankelijk is van de hoekmetingen in de gewrichten. De "Path Deviation Check" is het meest gevoelig, en vindt plaats op de lage frequentie van 2 Hz. Dit is acceptabel vanwege de langzame beweging van de "vrije" hand. Ook hier zijn de toetsingsparameters instelbaar. Alle vier detectiemechanismen (stroom-, snelheids-, hoek- en padafwijking) zijn nodig om veiligheid te kunnen garanderen, zelfs in de situatie van twee (onafhankelijke) fouten.

Voorbeeld foutdetectie
Stel dat de sensor die de rotatiesnelheid van het gewricht meet kapot is, en een vaste maar foutieve waarde afgeeft. Als reactie op de steeds groter wordende fout in de snelheid zal de regelaar steeds hogere versnellingen proberen te realiseren. Als de volgfout en de versnellingen te groot worden zullen de "Joint Velocity Tracking Error Check" en het detectiemechanisme gebaseerd op stroommeting de fout detecteren. De gewenste ERA-beweging in Cartesiaanse coördinaten kan dusdanig zijn dat een bijna constante snelheid van het gewricht vereist is. Indien nu de foutieve waarde toevallig ongeveer gelijk is aan de gewenste waarde, zal de fout slechts langzaam propageren. Ondanks het feit dat de "Path Deviation Check" op de laagste frequentie werkt, zal deze toch de fout als eerste detecteren omdat op Cartesiaans niveau de toegestane volgfouten het kleinst zijn.



Het ruimtestation omvat Amerikaanse, Russische, Japanse en Europese modules. De totale afmetingen zijn circa 100 x 30 x 30 meter. [ESA]

Het veiligstellen van de robotarm

Afhankelijk van de gedetecteerde fout moet ERA in een veilige toestand gebracht worden. In feite komt dit neer op het stoppen van alle motoren en het uitschakelen van de laser van de camera, die zorgt voor het benodigde licht om iets met de camera te kunnen zien. Ook is een situatie denkbaar waarin de arm bijvoorbeeld een luchtsluis blokkeert, waardoor kosmonauten het ruimtestation niet meer in kunnen. Voor dit soort situaties kunnen de gewrichten handmatig (mechanisch) worden verdraaid.

De belangrijkste automatische manier om de arm in een veilige toestand te brengen ("safing") is de Soft Emergency Stop (SES). Deze zorgt ervoor dat de bewegingscommando's worden stopgezet, de remmen worden bekrachtigd, en de motorstromen geblokkeerd worden. Als al deze acties niet naar behoren worden uitgevoerd (althans voorzover de ECC dat kan beoordelen), kan de ECC een verzoek doen aan de kosmonaut en de centrale Russische computer om de stroom van ERA als geheel af te sluiten.

Voorbeeld uitschakeling
Stel dat in het voorbeeld van de vorige sectie de fout is gedetecteerd door een controle in de elleboog. Dan deactiveert de elleboog zichzelf, en rapporteert hij de fout aan de ECC. De ECC commandeert een SES om de andere subsystemen te deactiveren.

Rapportage

Nu de arm veilig is, is het nodig de oorzaak te melden en te verhelpen. Om de fout te kunnen corrigeren is de mens nodig. Het ontwerp moet rekening houden met het probleem dat een kosmonaut weinig mogelijkheden heeft tot detailanalyse, maar wel ter plekke is. Het grondstation daarentegen heeft alle faciliteiten om een probleem te analyseren, maar heeft geen directe toegang tot ERA. Sterker nog, het is heel wel mogelijk dat er geen grondcontact is als het probleem zich voordoet. Derhalve is het ontwerp gebaseerd op de volgende richtlijnen:

- De kosmonaut moet alleen in hoofdlijnen geïnformeerd worden over het probleem: hoe serieus is het probleem (Waarschuwing of Gevaar) en welk detectiemechanisme heeft het probleem ontdekt.
- Fouten mogen niet over het hoofd gezien worden. Zowel visuele als hoorbare signalen moeten worden gebruikt om de aandacht van de kosmonaut te trekken, zelfs als hij in een ruimtepak zit, kijkend door een dikke helm. De situatie is in zekere zin te vergelijken met die in een vliegtuig, waar een piloot soms "doof' lijkt te zijn voor alarmsignalen met alle kwalijke gevolgen van dien.
- Meer gedetailleerde informatie over de fout moet opgeslagen worden in de ECC, zodat die later beschikbaar is voor analyse, hetzij door het grondstation hetzij door een kosmonaut in het ruimtestation. De ECC slaat informatie op over de laatste honderd gebeurtenissen (niet alleen een fout, maar ook het starten of stoppen van een beweging wordt hier beschouwd als "gebeurtenis").

Doordat de kosmonaut slechts beperkte middelen heeft om een foutrapportage af te handelen (de EVA-kosmonaut kan maar één foutboodschap zien), moeten er prioriteitsregels gesteld worden:

- Gevaarboodschappen hebben uiteraard prioriteit boven waarschuwingsboodschappen.
- Boodschappen van de ECC hebben prioriteit boven die van een MMI.
- Als er meerdere boodschappen van dezelfde prioriteit zijn, wordt alleen de meest recente verstuurd.
- De boodschap blijft bestaan tot het probleem is opgelost, waarna deze wordt vervangen door een ander nog openstaand probleem (indien aanwezig).

Diagnose en foutcorrectie

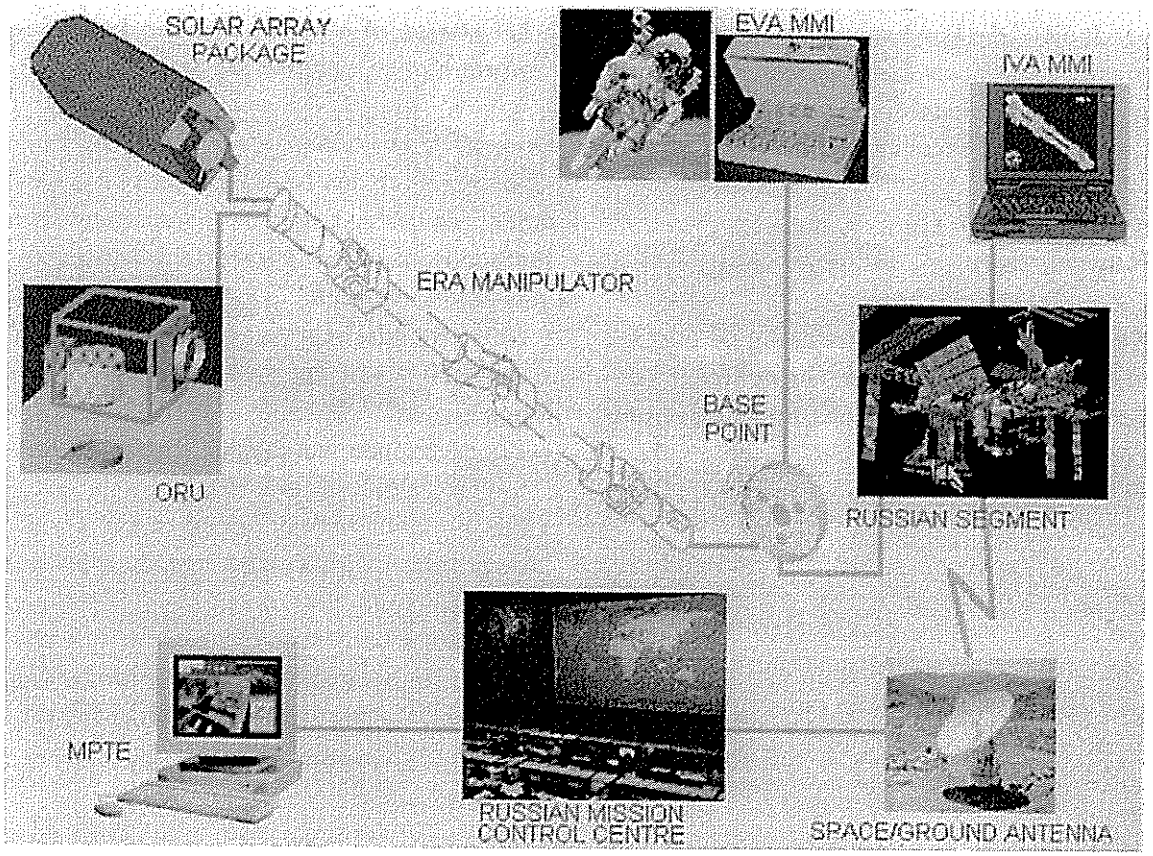
Diagnose heeft tot doel de oorzaak van de fouten te vinden tot op het niveau dat men de gewenste maatregel kan bepalen. ERA kent een aantal mogelijke correcties: men kan overschakelen naar het redundante elektrische kanaal, gebruik maken van redundante communicatiekanalen, herstarten, of complete subsystemen vervangen.

Conclusies

De beslissing om het FDIR-systeem niet volledig te centraliseren, maar om de subsystemen zèlf een zekere mate van autonomie te geven. leidt zowel tot het gevaar van "over-design" als ook tot dat van "under-design" (omdat elke partij denkt dat de ander wel een beveiliging heeft gerealiseerd). Een strikte aansturing en controle door de hoofdaannemer is essentieel om deze gevaren te ondervangen. Een voordeel van een decentrale foutdetectie t.o.v. een volledige centrale controle, is dat een gedetailleerdere foutdiagnose mogelijk is. Een centraal detectie-mechanisme controleert vaak meerdere functies tegelijk (zodat er minder detectiemiddelen nodig zijn), terwijl voor een decentrale aanpak geldt dat elke afzonderlijke functie een eigen detectiemechanisme heeft (waardoor er veel detectiemiddelen nodig zijn).

Zoals gebruikelijk bij ESA-projecten, zijn de veiligheidseisen die gesteld worden aan ERA onafhankelijk van de kans op een bepaalde fout: "No single ERA failure shall lead to catastrophic, serious or major consequences". De huidige eisen houden alleen rekening met de consequenties van een fout. Ook indien een mogelijke fout een zeer kleine kans van optreden heeft met minimale consequenties, zijn er toch preventieve maatregelen nodig danwel is een detectiemechanisme vereist. Dit alles kan leiden tot een kostbaar ontwerp en vertragingen.

Een manier om hiermee om te gaan is risico-management: hier wordt het risico vastgesteld door de kans van optreden te vermenigvuldigen met een maat voor de consequenties. Slechts als het totale risico onaanvaardbaar is, moeten er maatregelen genomen worden. Een dergelijke ontwerpfilosofie is echter niet perfect. Immers, het zal bijvoorbeeld moeilijk zijn om realistische schattingen voor de faalkansen te verkrijgen. Risico-gebaseerd ontwerpen is echter een valide alternatief om een project sneller en tegen geringere kosten te kunnen uitvoeren. Het zal duidelijk zijn dat er nog veel weerstand overwonnen moet worden voordat dit bij een echt project tot uitvoer gebracht kan worden.



In het ERA-project wordt niet alleen de robotarm zelf geproduceerd. De andere producten zijn de IVA-MMI, EVA-MMI, Mission Preparation and Training Equipment (MPTE), en grondsystemen ter verificatie van het ontwerp (EGSE etc.). [Fokker Space]