ZUVERLÄSSIGKEITSANALYSE UND REDUNDANZMANAGEMENT FEHLERTOLERANTER FLUGZEUG–SYSTEMARCHITEKTUREN AUF BASIS VON INTEGRIERTER MODULARER AVIONIK

D. Rehage, ***U. B. Carl***, ***M. Merkel***, ***A. Vahl***
Technische Universität Hamburg–Harburg
Arbeitsbereich Flugzeug–Systemtechnik, D-21071 Hamburg

ÜBERSICHT

Dieser Artikel präsentiert den Entwicklungstand eines Software–Tools, welches sich an den Entwurfsherausforderungen von Flugzeugsystemen auf Basis von INTEGRIERTER MODULARER AVIONIK (IMA) orientiert. Hierbei werden besonders diejenigen Fragestellungen adressiert, die sich auf die *Fehlerausbreitung* ausgefallener IMA Komponenten („*common point*“ Komponenten) auf verschiedene, integrierte Flugzeugssysteme beziehen, sowie deren *Rekonfiguration* im Rahmen des *Redundanzmanagements*. Darüber hinaus ist das *Redundanzmanagement* mit der zuverlässigkeitstechnischen Analyse dieser Systeme gekoppelt, so daß den Systemingenieuren unter dem Gesichtspunkt der Fehlertoleranz ein geeignetes Werkzeug für den Entwurf dieser komplexen und hochgradig vermaschten Systeme zur Verfügung gestellt wird.
Die zur Analyse notwendigen Systemmodelle sind hybrid und bestehen aus Zuverlässigkeitsblockdiagrammen zur strukturellen Systemmodellierung und hierarchischen, nebenläufigen endlichen Automaten zur zustandorientierten Systemmodellierung des *Redundanzmanagements*. Neuartig ist die Ausrichtung des Software–Tools auf IMA spezifische Fragestellungen, welches die Analyse der *Fehlerausbreitungen* von IMA Komponenten auf davon abhängige Flugzeugsysteme ermöglicht.

SCHLAGWORTE

Endlicher Automat; degradiertes System; Fehlertoleranz; Integrierte Modulare Avionik; Redundanzmanagement; Systementwurf; Zuverlässigkeitsanalyse; Zuverlässigkeitsblockdiagramm

1 EINLEITUNG

Mit dem Einsatz der neuesten Generation von Avionniksystemen, der INTEGRIERTEN MODULAREN AVIONIK (IMA), wird das Ziel verfolgt, hardware–ökonomischer und auf der Basis standardisierter elektronischer Module, systemspezifische Regelungs–, Steuerungs– und Überwachungsfunktionen (Software-Applikationen) verschiedenster Flugzeugsysteme zu integrieren („horizontale Integration“). Bei den Flugzeugsystemen, deren Software-Applikationen auf diesen IMA–Modulen betrieben werden, besteht gerade durch die Integration ein erhöhtes Auswirkungspotential von Fehlern der Modulkomponenten auf eine Mehrzahl gleichzeitig betriebener Funktionen, so daß umfangreiche Redundanzen zur Fehlerdiagnose und Funktionserhaltung zu implementieren sind, um ein hohes Maß an Fehlertoleranz bereitzustellen.
Für den Entwurf und die Analyse solcher komplexen Systeme wurde am Arbeitsbereich Flugzeug–Systemtechnik das Software–Tool SYRELAN^{TM} (**SY**STEM **REL**IABILITY **AN**ALYSIS) entwickelt, welches schon in der Frühphase der konzeptionellen Systementwicklung eingesetzt werden kann, um die nachfolgenden Fragestellungen in einem angemessenen Zeit– und Kostenrahmen beantworten zu können:

- *„Auf welche Flugzeugsysteme wirken sich IMA Komponentenausfälle aus?“*,
- *„Wie rekonfigurieren die Flugzeugsysteme nach IMA Komponentenausfällen?“*,
- *„Welche Restzuverlässigkeit haben die Flugzeugsysteme nach IMA Komponentenausfällen?“*.

Dieses Tool basiert auf einer hybriden Systemmodellierung, bei dem die einzelnen Systeme strukturell auf Basis von ZUVERLÄSSIGKEITSBLOCKDIAGRAMMEN (RBD, *engl.* RELIABILITY BLOCK DIAGRAM) und zustandsorientiert über HIERARCHISCHE, NEBENLÄUFIGE ENDLICHE AUTOMATEN (HCFSM, *engl.* HIERARCHICAL, CONCURRENT FINITE STATE MACHINES) abgebildet werden. In der RBD–Modellebene werden die Systemkomponenten (Hardware und Software) logisch miteinander verknüpft (positive Logik, d. h. RBD in Funktionserfüllung) und zuverlässigkeitstechnisch unter Verwendung konstanter Ausfallraten von Hardwarekomponenten bewertet. Hinterlegt werden die RBD–Blöcke mit einem oder auch mehreren anwendungsspezifischen HCFSMs. Diese HCFSMs repräsentieren das Zustandsverhalten der jeweiligen Komponente (*„aktiv“*, *„aktiv–heiss“*, *„passiv–warm“*, *„passiv–kalt“* oder *„isoliert“*) im Gesamtsystemkontext, d.h. sie beschreiben in ihren Transitionen zwischen den Zuständen das Verhalten im *Fehlerausbreitungs-* und *Rekonfigurationsprozeß*. Dieses Verhalten, das soge-

nannte *Redundanzmanagement*, wird über logische Gleichungen definiert, die aufgrund von *Fehlerinjektionen* in Komponenten „**WAHR**“ sind und damit die Prozesse aus *Fehlerausbreitung* und *Rekonfiguration* anstoßen.
Im Hinblick auf IMA werden in SYRELAN^{TM} Funktionalitäten bereitgestellt, um die Auswirkungen ausgefallener IMA Komponenten auf sämtliche Flugzeugsysteme, die diese *„common point“* Komponenten verwenden, zu analysieren. SYRELAN^{TM} unterstützt in diesem Zusammenhang, neben der vollständigen Abbildung der Flugzeugsysteme auf Basis von IMA, eine zusätzliche Modellierung der IMA Module getrennt von den Systemen. Diese zusätzliche Modellierung wird durchgeführt, um die Effekte ausgefallener IMA Modulkomponenten in Wirkungsrichtung von den Modulen zu den Systemen zu analysieren.

2 MODELLE IMA BASIERTER SYSTEME

Bei den Systemmodellen handelt es sich um hybride Modelle in hierarchischer Anordnung. Hierarchisch bedeutet in diesem Zusammenhang, daß die RBDs in der oberen und die HCFSMs in der unteren Modellebene miteinander gekoppelt sind. In Bild 1 ist die Verbindung durch den Komponentenfehlervektor bzw. durch den aktuellen Ausgangsvektor dargestellt. D. h. aus Sicht der HCFSMs besteht die Kopplung durch die Weiterleitung der *Fehlerinjektionen* in RBD–Systemkomponenten an das HCFSM–Modell und aus Sicht des RBD–Modells besteht die Kopplung durch Zuweisungen aktueller Zustände der HCFSMs an die darüberliegenden Blöcke. Diese Zustandszuweisungen an die RBD–Blöcke wird auf RBD–Ebene durch Farben dargestellt, um das Systemverhalten im Rahmen des *Redundanzmanagements* visuell abbilden zu können.

2.1 Hierarchisches Systemmodell

Die Vorgehensweise in der Modellierung IMA basierter Flugzeugsysteme sieht vor, daß jedes der hybriden Flugzeug–Systemmodelle in einer eigenen Systemumgebung abgebildet wird, sowie eine zusätzliche Abbildung der IMA Module, gesondert von den Systemmodellen, optional durchgeführt werden kann.
In einem ersten Schritt werden System– bzw. Modulstruktur über RBDs zuverlässigkeitstechnisch abgebildet. Zur Berücksichtigung IMA charakteristischer Eigenschaften wie den *„common point“* Komponenten, werden sogenannte *globale Blöcke* eingeführt, d. h. RBD–Blöcke, die in der Modellierung mehrfach verwendet werden, jedoch ein und dieselbe physikalische bzw. virtuelle Komponente repräsentieren. Dem schließt sich in einem zweiten Schritt die Modellierung des Systemverhaltens unter Komponentenausfalleinflüssen im *Redunanzmanagement* an. Hierzu werden die RBD–Blöcke mit einem oder mehreren HCFSMs hinterlegt.

RBD–Model

Die strukturelle Modellierung der Flugzeugsysteme wird in RBDs realisiert. Die Abbildung erfolgt aufgrund der Definition sogenannter TOP EVENTS in Systemfunktionalität, welches den zu analysierenden Systemzustand spezifiziert. Dazu werden Blöcke, die die realen Komponenten des System repäsentieren, entsprechend ihrer Abhängigkeit im System, logisch miteinander verknüpft. Die Systemkomponenten werden im BOOLSCHEN Modell über die binäre, stochastisch unabhängige Indikatorvariable K_i beschrieben, und es gilt [SCHNEE01]

(1) $K_i = 1$ Komponente K_i ist funktionsfähig,
(2) $K_i = 0$ Komponente K_i ist ausgefallen.

Die Bildung des Erwartungswertes (3) der zweitwertigen Indikatorvariablen K_i führt auf Zuverlässigkeit R_i einer Systemkomponente i

$$(3) \quad E[K_i] = 0 \cdot P[K_i = 0] + 1 \cdot P[K_i = 1] = P[K_i = 1].$$

Diese ist definiert als die Eintrittswahrscheinlichkeit $P[K_i = 1]$ der Komponentenfunktionsfähigkeit [VAH98]. Unter Verwendung einer *Exponentialverteilung* der statistisch bestimmten *Komponentenausfallrate* λ_i (pro Stunde, [1/h]), ist die Zuverlässigkeit R_i [VAH98]

$$(4) \quad E[K_i] = P[K_i = 1] = R_i(t) = e^{\lambda_i t}.$$

Im Allgemeinen ist die Ausfallrate eine Funktion der Zeit (BADEWANNENKURVE), jedoch im Bereich der Flugzeugsysteme ist sie hinreichend konstant zwischen zwei periodischen Komponentenkontrollen, so daß Komponentenausfälle altersunabhängig und rein zufällig sind [VAH98].

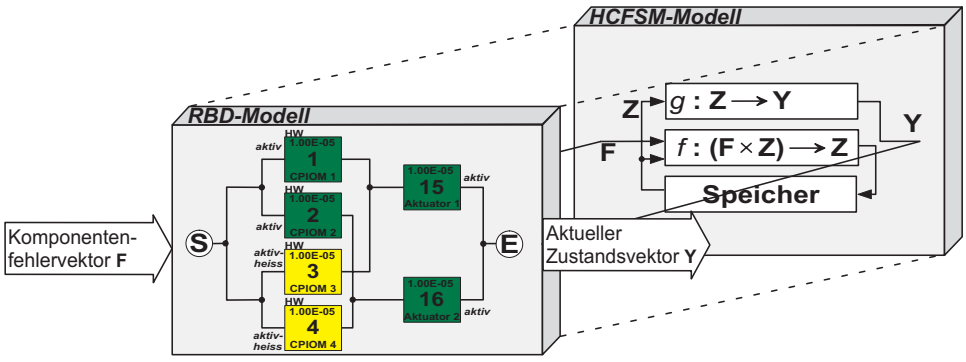


BILD 1: Hierarchische Systemmodelle: RBD–Modell und HCFSM–Modell

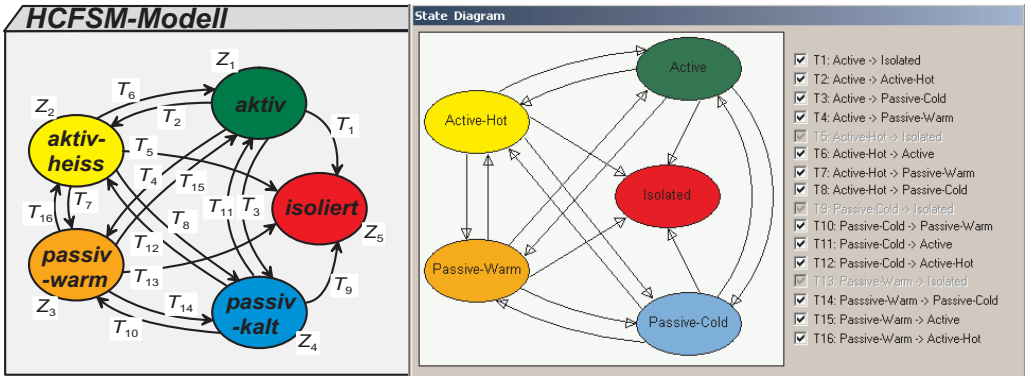


BILD 2: Zustände und Transitionen der HCFSMs und der SYRELAN^{TM} STATE DIAGRAM Editor

Unter der Annahme, daß die BOOLSCHEN Systeme die Monotoniebedingungen erfüllen, kann die Systemfunktion ϕ auf Basis logisch verknüpfter Systemkomponenten **K** (7) gebildet werden [VAH98]

(5) $\phi(\mathbf{K}) = 1$ System ϕ ist funktionsfähig,

(6) $\phi(\mathbf{K}) = 0$ System ϕ ist ausgefallen

(7) mit $\mathbf{K} = \{K_1, \ldots, K_i, \ldots, K_m\}$.

HCFSM–Model

Das Zustandsverhalten der fehlertoleranten Systeme wird über die HCFSM–Modelle beschrieben. Dazu wird in der zweiten Modellebene jeder Block im RBD–Modell mit einem bzw. mehreren HCFSMs hinterlegt, um das Verhalten bestehend aus *Fehlerausbreitung* und *Rekonfiguration* im Rahmen des *Redundanzmanagements* abbilden zu können. Das HCFSM–Modell setzt sich aus einem 6–Tupel zusammen, der aus einem Eingangsvektor **F**, einem Ausgangsvektor **Y**, einer Menge von internen Zuständen in den Elementen des Zustandsvektors **Z**, einer Menge von Initialzuständen in den Elementen des initialen Zustandsvektors $\hat{\mathbf{Z}}$, einer Übergangsfunktion f, und einer Ausgangsfunktion g besteht (Bild 1) [GAJ94, TEI97]

(8) $\left(\mathbf{F}, \mathbf{Y}, \mathbf{Z}, \hat{\mathbf{Z}} \subseteq \mathbf{Z}, f : \mathbf{F} \times \mathbf{Z} \to \mathbf{Z}, g : \mathbf{Z} \to \mathbf{Y}\right)$.

Die Vektorelemente des HCFSM 6–Tupels (8) enthalten in ihren Zeilen die HCFSM–Repräsentanten für die Systemkomponenten K_i $(i = 1, \ldots, m)$, die in [REH03] im Detail beschrieben sind.

Die HCFSMs, die im Hintergrund der RBD–Systemkomponenten betrieben werden, bestehen in Minimalkonfiguration aus den zwei Zuständen *„aktiv“* und *„isoliert“* (Bild 2). In Maximalkonfiguration sind es fünf Zustände $\{Z_1, \ldots, Z_5\}$, die über die Auswahl der Transitionen $\{T_1, \ldots, T_{16}\}$ zwischen den Zuständen im SYRELAN^{TM} STATE DIAGRAM in Bild 2 angesprochen werden. Die Auswahl der HCFSM–Zustände beruhen auf Degradationstufen fehlertoleranter Systeme, die aus zuverlässigkeitstechnischer Sicht sinnvoll sind und im nachfolgenden Abschnitt beschrieben werden [VDI86]:

„aktiv“ ← **GRÜN**: Die Arbeitskomponente **a** ist von Missionsbeginn an der vollen Belastung ausgesetzt. Die Ausfallrate ist λ_a. Die *Endung* ist „**a**“.

„aktiv–heiss“ ← **GELB**: Reserveelement **h** ist von Missionsbeginn an der gleichen Belastung ausgesetzt wie die eigentliche Arbeitskomponente **a**. Für die Ausfallrate gilt $\lambda_h = \lambda_a$. Die *Endung* ist „**h**“.

„passiv–warm“ ← **ORANGE**: Reserveelement **w** ist bis zum Ausfall der Arbeitskomponente A (oder bis zum eigenen vorzeitigen Ausfall) einer geringeren Belastung ausgesetzt. Für die Ausfallrate gilt $0 < \lambda_w < \lambda_a$. Die *Endung* ist „**w**“.

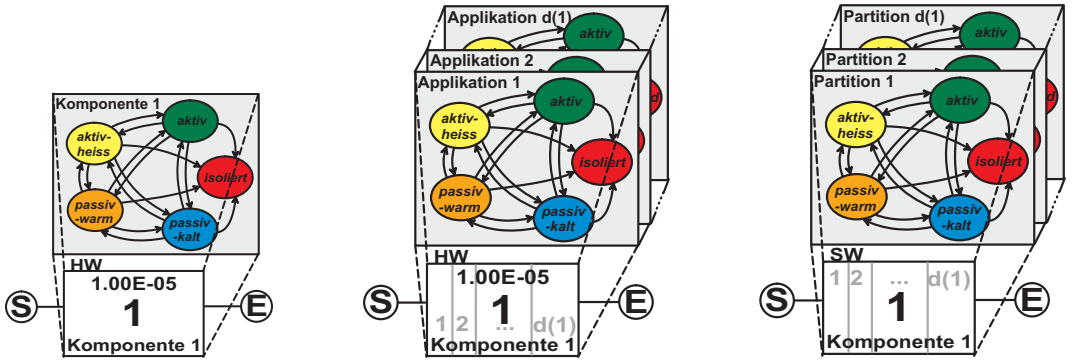
„passiv–kalt“ ← **HELLBLAU**: Reserveelement **k** ist bis zum Ausfall der Arbeitskomponente **a** keiner Belastung ausgesetzt. Für die Ausfallrate gilt $\lambda_k = 0$. Die *Endung* ist „**k**“.

„isoliert“ ← **ROT**: Ausfallzustand der Komponente. Die *Endung* ist „**i**“.

Die Modellierung des *Redundanzmangements* ist anwendungspeziefisch und abhängig von den RBD–Systemen. Hierzu stehen aus Sicht der RBDs drei verschiedene Blocktypen zur Verfügung, die jeweils mit einem oder mehreren HCFSMs hinterlegt werden können (Bild 3). Diesen RBD–Blöcken werden zur Visualisierung des *Redundanzmanagements* die im vorangegangenen Abschnitt präsentierten Zustandsfarben zugeordnet, sofern es sich um aktuelle Zustände handelt.

Der einfache *Hardware–Block* in Bild 3a wird bei Flugzeugsystemen zur Modellierung einmalig eingesetzter Komponenten verwendet. Es handelt sich dabei um Komponenten wie bspw. Aktuatoren und Sensoren, denen eine konstante Ausfallrate zugeornet ist. Zur Zustandsdarstellung wird im Hintergrund des RBD–Blocks eine einzelne HCFSM betrieben.

Im Gegensatz zum einfachen *Hardware–Block* können beim *multifunktionalen Hardware–Block* mehrere HCFSMs im Hintergrund betrieben werden (Bild 3b). Dies ermöglicht die getrennte Abbildung des Zustandsverhaltens von Komponenten, die in verschiedenen Anwendungen genutzt werden. Es handelt sich hier um Hardware–Komponenten wie bspw. Bussysteme, Ethernetswitches. Der Mehrfachbetrieb der HCFSMs dient ausschließlich einer übersichtlicheren Modellierung, weil die zuverlässigkeitstechnische Eigenschaft dieser RBD–Blöcke, der des einfachen *Hardware–Blocks* entsprechen. D. h. in diesem Fall die Zuweisung einer konstanten Komponentenausfallrate an den RBD–Block sowie den Simultanausfall



(a) *Hardware Block* (b) *Multifunktionaler Hardware–Block* (c) *Multifunktionaler Softwar–Block*

BILD 3: Drei RBD–Blockkategorien mit ihren hinterlegten HCFSMs

aller HCFSMs, wenn ein Fehler in den RBD–Block injeziert wird.
Der dritte Blocktyp ist der *multifunktionale Software–Block* in Bild 3c. Dieser zeichnet sich dadurch aus, daß mehrere unabhängige HCFSMs im Hintergrund des RBD–Blocks betrieben werden können. Eingestetzt wird dieser Blocktyp zur Abbildung des Zustandsverhaltens von Regelung–, Steuerungs– oder Überwachungsfunktionen, die in Partionen auf Rechnereinheiten betrieben werden. Dieser Blocktyp zeichnet sich schon durch die IMA spezifische Eigenschaft aus, da mehrere Applikationen parallel und auf einem Rechner betrieben werden können. Die Unabhängigkeit der HCFSMs bedeutet in diesem Zusammenhang, daß diese unabhängig voneinander als ausgefallen deklariert werden. Darüber hinaus sind die HCFSMs dieses Blocktyps jeweils mit einem weiteren RBD–Block verbunden, zu dem sie in funktioneller Abhängigkeit stehen, wie bspw. die HCFSM einer Aktuatorregelung mit dem RBD–Block des Aktuators. Die Zuverlässigkeit der Software–Applikationen, abgebildet über HCFSMs, nimmt die beiden Zustände funktionsfähig ($R = 1$) und ausgefallen ($F = 1$) ein.
Zur Modellierung des *Redundanzmanagements* ist es notwendig, die Transitionen der HCFSMs über logische Gleichungen zu definieren, in denen die Bedigungen für einen Zustandsübergang enthalten sind. Diese Gleichungen bestehen aus der logischen Verküpfung (**UND**: „&“, **ODER**: „|“, **NICHT**: „∼“) von HCFSM–Zuständen entsprechender Komponenten. Zur Adressierung der HCFSMs–Zustände wird die nachfolgend aufgeführte Syntax verwandt

$$(9)\quad \mathit{Komponente}: i\,,\mathit{Endung}: \{\mathrm{a,\,h,\,w,\,k,\,i}\}\ \forall\ K_i \in \mathbf{K},$$

$$(10)\quad \mathit{Komponente}: i\,,\mathit{HCFSM}: l\,,\mathit{Endung}: \{\mathrm{a,\,h,\,w,\,k,\,i}\}\ \forall\ K_i \in \mathbf{K}\quad \text{and}\quad l \in [1, d(i)]\quad \text{with}\quad d(i) \in I\!N.$$

Die Gleichung (9) beschreibt dabei den Zugriff auf den Zustand eines einfachen *Hardware Blocks*. Bspw. adressiert $2,h$ den HCFSM–Zustand „*aktiv–heiss*“ von Komponente 2. Die zweite Gleichung richtet sich an die HCFSM–Zustandsadressierung derjenigen RBD–Blöcke, die mehrere HCFSMs im Hintergrund betreiben können. Um in der logischen Gleichung einer Transition den HCFSM–Zustand „*passiv–kalt*“ in HCFSM 7 von Komponente 3 anzusprechen, muß $3,7,k$ im entsprechenden SYRELAN^{TM} Editor eingegeben werden.
Die Voraussetzung zum Betrieb des *Redundanzmanagements* ist, daß die HCFSMs der Systemkomponenten miteinander gekoppelt sind. Diese Kopplungen werden über die Transitionen der HCFSMs hergestellt, bei denen diese in ihren logischen Gleichungen funktionelle Abhängigkeiten zu den HCFSMs–Zuständen benachbarter Komponenten aufweisen. Deshalb wirkt sich ein Komponentenausfall über die HCFSM dieser Komponente auf benachbarte seriell liegende Komponenten aus und bei Fehlertoleranz über die *Rekonfigurationen* parallel liegender.

2.2 Überlagerung hierarchischer Systemmodelle

Das entscheidene Merkmal IMA basierter Flugzeugsysteme ist die Integration von Software–Applikationen verschiedenster Flugzeugsysteme auf Rechnermodulen. Dies hat zur Konsequenz, daß die Systeme von denselben Rechnermodulen abhängig sind und damit Vielzahl von *„common point“* Komponenten existieren, die im Rahmen der RBD– und HCFSM–Systemmodelle berücksichtigt werden müssen. SYRELAN^{TM} sieht hierfür zunächst eine Unterscheidung zwischen den Komponenten aller Systeme $(i = 1,\ldots,m)$ eines Flugzeugs vor, wie bspw. A380 oder 7E7, welches über die Menge $\mathbf{K_{AC}}$ beschrieben wird

$$(11)\quad \mathbf{K_{AC}} = \{K_1,\ldots,K_i,\ldots,K_m\}$$

und derjenigen Komponententeilmengen $\mathbf{K_{SCj}}$ bzgl. aller Systemkomponenten (11), die den Flugzeugsystemen $(j = 1,\ldots,n)$ zuzuordnen sind und über den tranponierten Vektor $\mathbf{K_{SC}}$ ausgedrückt werden

$$(12)\quad \mathbf{K_{SC}} = \left(\mathbf{K_{SC1}},\ldots,\mathbf{K_{SCj}},\ldots,\mathbf{K_{SCn}}\right)^{\mathrm{T}}$$

$$(13)\quad \text{mit}\quad \mathbf{K_{SCj}} \subseteq \mathbf{K_{AC}}\quad \forall\quad j = 1,\ldots,n.$$

Unter Anwendung von Formel (5) auf den Systemkomponentenvektor (12) ergibt sich für die BOOLSCHE Systemdarstellung

$$(14)\quad \phi(\mathbf{K_{SC}}) = \left(\phi(\mathbf{K_{SC1}}),\ldots,\phi(\mathbf{K_{SCj}}),\ldots,\phi(\mathbf{K_{SCn}})\right)^{\mathrm{T}}.$$

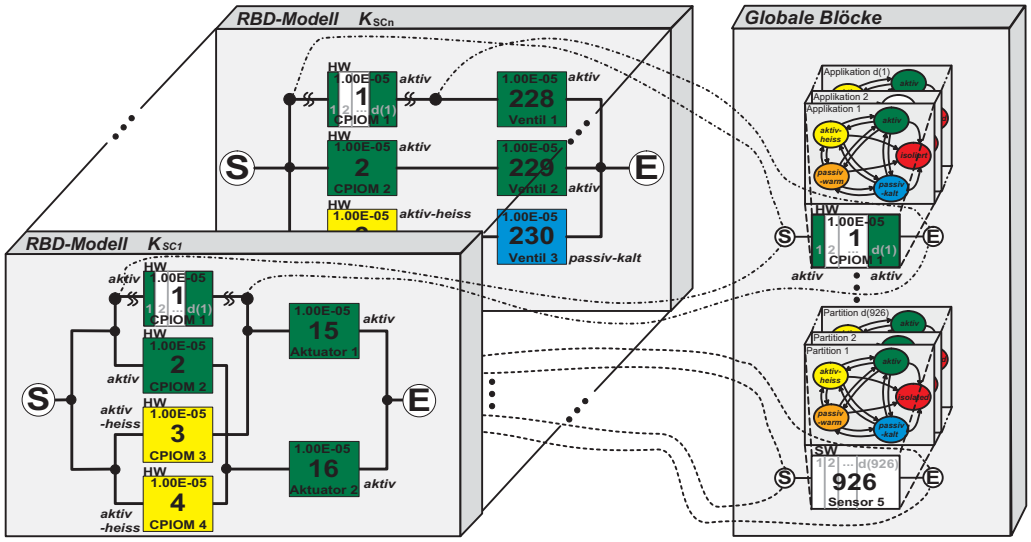


BILD 4: Kopplung der hybriden Systemmodelle durch Verwendung von *globalen Blöcken*

Zur Modellierung dieser IMA basierten *„common point“* Komponenten werden in SYRELAN^{TM} sogenannte *globale Blöcke* eingeführt (Bild 4). Jeder dieser *globalen Blöcke* ist einem der drei Blocktypen aus Bild 3 zugeordnet. Besonderes Merkmal dieser RBD–Blöcke ist, daß sie in verschiedenen Flugzeugsystemen abgebildet werden, jedoch nur als physikalisch einmalig auftretend gelten, wie die Komponente K_1 in den Systemen $\phi(\mathbf{K_{SC1}})$ und $\phi(\mathbf{K_{SCn}})$ (Bild 4). Dieses Merkmal ist besonders wichtig im Rahmen des *Redundanzmanagements* der integartiv betriebenen Flugzeugsysteme, da über die *globalen Blöcke Fehlerausbreitungen* systemübergreifend abgebildet und analysiert werden. Zur Bestimmung der *globalen Blöcke* in den Flugzeug–Systemmodellen $\mathbf{K_{GCj}}$ $(j = 1,\ldots,n)$ wird die Eigenschaft dieser RBD–Blöcke ausgenutzt, daß sie mindestens in zwei verschiedenen Flugzeugsystemen auftreten. Gebildet werden die *globalen Block* Mengen (16) je Flugzeugsystem über den Durchschnitt der Komponentenmengen von Flugzeugsystemen untereinander.

$$(15) \qquad \mathbf{K_{GC}} = \left(\mathbf{K_{GC1}},\ldots,\mathbf{K_{GCj}},\ldots,\mathbf{K_{GCn}}\right)^{\mathrm{T}}$$

$$(16) \quad \text{mit} \quad \mathbf{K_{GCj}} = \left\{\mathbf{K_{SCj}} \cap \mathbf{K_{SCq}}\right\}$$
$$\forall \quad j,q = 1,\ldots,n \quad \text{and} \quad j \neq q\,.$$

3 ANALYSE IMA BASIERTER SYSTEME

Die Analyse der hybriden Flugzeug–Systemmodelle erfolgt getrennt in beiden Modellebenen. Im Bereich der RBD–Modelle sind dies die Zuverlässigkeitsananlysen auf Basis orthogonalisierter Systemfunktionen. Das *Redundandanzmanagement* erfolgt ebenfalls lokal durch Suche schaltbarer Transitionen nach injeziertem Komponentenausfall, jedoch kommt an dieser Stelle die Eigenschaft IMA basierter Systemmodelle zum Tragen, so daß die Fehlerausbreitung der IMA Komponenten auf verschiedene integrierte Flugzeugsysteme erfolgt. Zwischen den beiden Modelleben findet der Austausch injezierter Komponentenausfälle und aktueller Komponentenzustände statt.

3.1 Zuverlässigkeitsanalyse

Die Zuverlässigkeitsanalyse wird bei den RBD–Modellen durch Orthogonalisierung der in den BOOLSCHEN Systemfunktionen (14) enthaltenen *Minimalpfade* (M_r) realisiert [VAH98]. Die Orthogonalisierungsbedingung besagt, daß die Produkte aller disjunktiven Terme (M_r) der BOOLSCHEN Systemfunktion sich gegenseitig ausschließen und somit null sind [VAH98]. Bei System $\phi(\mathbf{K_{SC1}})$ aus Bild 4 lautet die Systemfunktion

$$(17) \quad \phi(\mathbf{K_{SC1}}) = \phi(K_1,K_2,K_3,K_4,K_{15},K_{16})\,,$$
$$(18) \quad \phi(\mathbf{K_{SC1}}) = K_1K_{15} \vee K_2K_{16} \vee K_3K_{15} \vee K_4K_{16}$$
$$(19) \quad \phi(\mathbf{K_{SC1}}) = M_1 \vee M_2 \vee M_3 \vee M_4\,.$$

Der in SYRELAN^{TM} implementierte CAOS–Algorithmus (COMPUTER AIDED ORTHOGONALISATION SYSTEMS) leistet die Orthogonalisierungsbedigung (20) [VAH98]

$$(20) \quad M_r \cdot M_s = 0 \quad \text{with} \quad r,s = 1,2,3,4 \quad \text{and} \quad r \neq s\,.$$

Die Anwendung des CAOS–Algorithmus auf die Systemfunktion (18) überführt diese in eine orthogonale disjunktive Normalform sich gegenseitig ausschließender Terme [VAH98]. Aufgrund der Linearität des Erwartungswertoperators und der Berücksichtigung der Indikatorvariablen als binäre, stochastische Variablen mit der Wahrscheinlichkeitsverteilung (4), führt dies auf die Systemzuverlässigkeit ($F_i = 1 - R_i$, siehe Formel (4)) [VAH98]

$$(21) \quad E[\phi(\mathbf{K_{SC1}})] = E\left[K_1K_{15} + K_2K_{16}\overline{K_1K_{15}} + \ldots\right.$$
$$\ldots + K_3K_{15}\overline{K_1}\,\overline{K_2K_{16}} + K_4K_{16} \cdot \ldots$$
$$\ldots \cdot \left.\overline{K_2}\,\overline{K_{15}} + K_4K_{15}K_{16}\overline{K_1}\,\overline{K_2}\,\overline{K_3}\,\overline{K_3}\right],$$
$$(22) \quad R_{SC1} = R_1R_{15} + R_2R_{16}F_1 + R_2R_{16}F_{15} + \ldots$$
$$\ldots + R_3R_{15}F_1F_2 + R_3R_{15}F_1F_{16} + \ldots$$
$$\ldots + R_4R_{16}F_2F_{15} + R_4R_{15}R_{16}F_1F_2F_3$$

Ein wesentlicher Vorteil der Berechnung von Systemfunktionen auf Basis orthogonanlisierter *Minimalpfade* ist de-

ren Eigenschaft, physikalisch einmalig vorhandene Komponenten im System, durch mehrfach auftretende RBD–Blöcke mit identischer Komponentennummer abzubilden, ohne das dies zu geringeren Zuverlässigkeiten führt. Gerade bei hochgardig komplexen und vermaschten Systemen, ist dies ein immenser Vorteil im Rahmen der RBD–Modellierung solcher Systeme.
Darüber hinaus stellt SYRELAN^{TM} noch weitere zuverlässigkeitstechnische Analysefunktionalitäten für fehlertolerante Systeme auf RBD–Basis zur Verfügung. Dabei handelt es sich um die Analyse *degradierter* Systemzustände, die über Festlegung von Mindestanforderungen an die Systemfunktionalität gestellt werden [VAH98]. Ähnlich wie bei den *degradierten* Systemzuständen werden bei den Systemen mit *k*–aus–*n* Bedingungen Anforderungen an Komponenten gestellt, bei denen *n* Komponenten in „*aktiver*“ Redundanz existieren und mindestens *k* von ihnen die benötigte Funktionalität leisten müssen. Gemein haben beide Analysefunktionalitäten, daß die Eingabe in SYRELAN^{TM} über einen Dialog verläuft, bei dem die logische Gleichung Γ (**UND**, **ODER**) in Abhängigkeit notwendiger Systemkomponenten K_i (11) eingegeben werden, die in der Zuverlässigkeitsanalyse in den entsprechenden *Minimalpfaden* der Systemfunktionen $\phi(\mathbf{K}_{SC})$ (14) vorhanden sein müssen [VAH98].

3.2 Redundanzmanagement

Das *Redundanzmanagement* integrierter Systeme auf Basis von IMA ist ein wichtiger Bestandteil der Systemanalyse. Die Implementierung der HCFSM–Modellumgebung in der zweiten Modellebene in SYRELAN^{TM} wird dazu genutzt, um Systemingenieure mit einem Software–Tool auszustatten, mit dem unterschiedliche Strategien der *Rekonfiguration* (bspw. *Prioritäten*) in fehlertoleranten Systemen modelliert und simuliert werden können, bevor sie auf dem Zielsystem angewandt werden. Ein weiterer Aspekt richtet sich speziell an IMA basierte Flugzeugsysteme. Bei diesen Systemen werden die Ausfallauswirkungen von IMA Komponenten auf die davon entsprechend abhängigen Flugzeugsysteme analysiert. Dazu besteht die Option in SYRELAN^{TM}, die IMA Rechnermodule zusätzlich zu den Flugzeugsystemen zu modellierten. Dies hat zur Folge, daß eine gezielte Analyse der IMA Komponentenausfälle in Wirkungsrichtung von den IMA Modulen hin zu den Flugzeugsystemen erfolgen kann (Bild 7).
D. h. in IMA Komponenten injezierte Ausfälle führen dazu, daß dem entsprechenden RBD–Block die Zuverlässigkeit $R = 0$ zugewiesen wird und der Ausfall an das/die HCFSMs weitergeleitet wird, welches den *Fehlerausbreitungs* und *Rekonfigurationsprozeß* der *globalen Blöcke* im *Redundanzmanagement* anstößt. Das *Redundanzmanagement* wird zunächst lokal in dem System, in das der Komponentenausfall injeziert wurde, durchgeführt und breitet sich anschließend über die *globalen Blöcke* auf abhängige Flugzeugsysteme aus. Die mit dem *Redundanzmanagement* verbundenen aktuellen Zustandsänderungen in den HCFSMs der Systeme, werden für den Anwender durch Farbzuweisungen an die RBD–Blöcke visuell abgebildet.
Um diese Vorgehensweise in einem Algorithmus zur Anwendung zu bringen, müssen die *globalen Blöcke* aus den Systemen extrahiert werden. Die Bedingung für einen *globalen Block* ist, daß dieser mindestens einmal in zwei verschiedenen Flugzeugsystemen verwendet wird. Ist dies der Fall bei Komponente K_i $(i = 1,\ldots,m)$, dann enthält die Matrix (23) in mindestens zwei Zeilen ihrer Spalte *i* den Eintrag der Komponente K_i. Die Informationen über *globalen Blöcke* in den Systemen wird aus der Matrix (23)

$$(23)\quad \mathbf{K_{SM}} = \begin{pmatrix} (K_1 \cap \mathbf{K_{GC1}}) & \ldots & (K_i \cap \mathbf{K_{GC1}}) & \ldots & (K_m \cap \mathbf{K_{GC1}}) \\ \vdots & & \vdots & & \vdots \\ (K_1 \cap \mathbf{K_{GCj}}) & \ldots & (K_i \cap \mathbf{K_{GCj}}) & \ldots & (K_m \cap \mathbf{K_{GCj}}) \\ \vdots & & \vdots & & \vdots \\ (K_1 \cap \mathbf{K_{GCn}}) & \ldots & (K_i \cap \mathbf{K_{GCn}}) & \ldots & (K_m \cap \mathbf{K_{GCn}}) \end{pmatrix} \quad \forall\ i = 1,\ldots,m \text{ und } j = 1,\ldots,n.$$

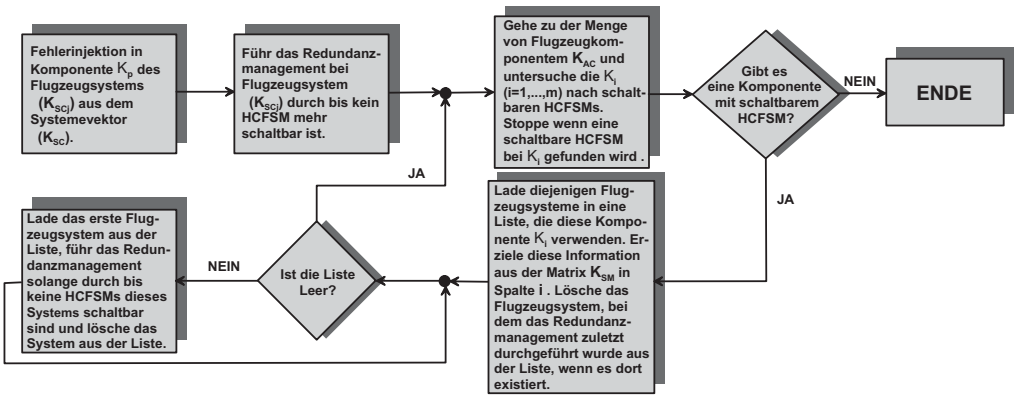


BILD 5: *Redundanzmanagement*–Algorithmus im Rahmen integrierter Systemmodelle

gewonnen und im *Redundanzmanagement*–Algorithmus für IMA basierte System verwandt (Bild 5). Dieser Algorithmus verfolgt die Strategie, daß das *Redundanzmanagement* lokal in den Systemen durchgeführt wird, bis ein stabiler Zustand erreicht ist, bei dem keine logische Gleichung in den HCFSM–Transitionen des Systems erfüllt wird. Nach Vollendung des lokalen *Redundanzmanagements* wird aus der Matrix (23) diejenige Information gewonnen, in welche Systeme der Komponentenausfall hineinpropagieren kann. Der gesamte Prozeß ist erst dann abgeschlossen, wenn bei keiner HCFSM–Transition die logische Gleichung „**WAHR**“ ist.

4 ANWENDUNG

Bei der Modellierung IMA basierter Flugzeugsysteme wird jedes der hybriden Flugzeug–Systemmodelle in einer eigenen Systemumgebung abgebildet. Um die Auswirkungen von IMA Komponentenausfällen analysieren und bewerten zu können, werden zusätzlich zu den Flugzeugsystemmodellen die IMA Module unabhängig abgebildet.
Ausgangspunkt der Systemmodellierung ist die Definition der TOP EVENTS, die es im Rahmen der Systemdesigns zu analysieren gilt. Für die Flugzeugsysteme der primären Flugsteuerung müssen diese in Systemfunktionalität definiert werden, da auf deren Grundlage die Modellierung der RBD–Modelle in positiver Logik erfolgt (Bild 6). Jedoch erfolgt die Klassifizierung der Systeme nach JAR 25 bzgl. ihrer Auswirkungen auf das Flugzeug sowie deren Insassen bei Verlust der einzelnen Systeme, so daß im Rahmen der RBD–Analyse nach der Ausfallwahrscheinlichkeit F gesucht wird [JAA89]. Die in Bild 6 aufgeführten Systeme der primären Flugsteuerung sind alle als *„major“* klassifiziert (TAB 1), so daß die Systemausfallwahrscheinlichkeit jeweils nicht höher als $1E-5$ pro Flugstunde liegen darf.
Im Rahmen der Zuverlässigkeitsanalyse bei der *Spoiler*– und der *Höhenrudersteuerung* sind die logischen Nebenbedingungen Γ zu berücksichtigen (TAB 1). Die Betriebsanforderungen der *Spoilersteuerung* sehen einen paarweises degradieren der Aktuatoren vor. Beim Ausfall eines *Spoileraktuators* wird der entsprechende Aktuator auf der gegenüberliegenden Tragflächenseite vom Systembetrieb isoliert. Im Bereich der *Höhenrudersteuerung* beschreibt die Nebenbedingung Γ die minimale Betriebsanforderung an das System. Diese besagt, daß ein Systembetrieb nur dann möglich ist, wenn mindestens ein Aktuator je Stellfläche zur Verfügung steht, um einen symmetrischen Systembetrieb zu gewährleisten.
Die in den zuverlässigkeitstechnischen Systemanalysen erzielten Ausfallwahrscheinlichkeiten bei einer Flugstunde bzgl. der nominalen Systemzustände aus Bild 6 sind in Tabelle 1 in der Spalte F_{nom} aufgeführt. Die Wahrscheinlichkeitswerte zeigen, daß die fehlertolerante Auslegung der Systeme hinreichend ist und die mit der Ausfallklasse *„major“* verbundene maximale Ausfallwahrscheinlichkeit von $1E-5$ pro Flugstunde nicht überschritten wird.
Die Arbeitsweise des *Redundanzmanagements* im Bereich der Integrierten Modularen Avionik wird anhand der Fehlerinjektion in die IMA Komponente K_{13} bespielhaft erläutert (Bild 7). Diese Fehlerinjektion führt zunächst zum Ausfall des CPIOM 1 in System 1 und breitet sich anschließend auf die weiteren von dieser Komponente abhängigen Flugzeugsysteme aus.
Um eine Vorstellung davon zu bekommen, wie die Übergangsbedingungen in den logischen Gleichungen der HCFSM–Transitionen lauten, wird exemplarisch für das System der *Höhenrudersteuerung* die Transition T_{12} von HCFSM 3 des *multifunktionalen Software–Blocks* K_9 beschrieben. Diese Transition definiert den Übergang vom Zustand *„passiv–kalt“* zu *„aktiv–heiss“* und wird im Rahmen der Rekonfigurationen nach der Fehlerinjektion in IMA Komponente K_{13} vollzogen (Bild 7).
Ausgangspunkt ist zunächst der Nominalzustand der *Höhenrudersteuerung*, bei dem beide Steuerflächen über je eine Software–Applikation auf CPIOM 2 (K_8, HCFSM 5 und 6) mit der Priorität P1 angesteuert werden (Bild 6). Zur schnellen *Rekonfiguration* des Systems werden zwei Software–Applikation mit der Priorität P2 auf CPIOM 1 (K_7, HCFSM 7 und 8) im Zustand *„aktiv–heiss“* betrieben.

TAB 1: Systemanalysen

System	TOP EVENT	Γ	Klasse	F_{nom}	F_{deg}
Querrudersteuerung	Verlust der *Querrudersteuerung*	–	*Major*	2.02E-8	1.01E-4
Spoilersteuerung	Verlust der *Spoilersteuerung*	$(K_{31} \wedge K_{39}) \vee (K_{33} \wedge K_{41}) \vee (K_{35} \wedge K_{43}) \vee (K_{37} \wedge K_{45})$	*Major*	9.41E-12	5.90E-8
Höhenrudersteuerung	Verlust der *Höhenrudersteuerung*	$(K_{47} \wedge K_{51}) \vee (K_{47} \wedge K_{53}) \vee (K_{49} \wedge K_{51}) \vee (K_{49} \wedge K_{53})$	*Major*	4.15E-8	7.63E-8
THS Steuerung	Verlust der elektronischen *THS Steuerung*	–	*Major*	2.14E-7	2.15E-7
Seitenrudersteuerung	Verlust der elektronischen *Seitenrudersteuerung*	–	*Major*	1.20E-7	1.01E-4

BILD 6: Primäre Flugsteuerungssysteme im Nominalzustand

BILD 7: *Rekonfigurierte* primäre Flugsteuerungssysteme nach Ausfall von CPIOM 1

Bei einem Komponentenausfall in den Steuerkanälen dieser Software–Applikation muß jedoch gesichert sein, daß weiterhin eine schnelle *Rekonfiguration* möglich ist, wenn in den *„aktiven“* Steuerkanälen ein Ausfall zu verzeichnen ist.
Die IMA Software Komponente K_9 enthält in der Transition T_{12} von HCFSM 3 die Bedingung zur Steuerung des rechten äußeren Aktuators (K_{47}). Deshalb ist zu berücksichtigen, daß die mit P3 priorisierte CPIOM 3 Software nur dann in den Systemzustand *„aktiv–heiss“* wechseln darf, wenn **keine** höher priorisierte Software–Applikation zur Steuerung der rechten *Höhenruder*–Stellfläche im Systemzustand *„aktiv–heiss“* ist. Beschrieben wird dies durch die logische Gleichung (24) mit der in SYRELAN^{TM} implementierten Syntax

$$(24)\quad T_{9,3,12} \;=\; \underbrace{(\sim 8,5,\mathrm{h})}_{\text{P1: CPIOM 2}} \;\mid\; \underbrace{(\sim 7,7,\mathrm{h})}_{\text{P2: CPIOM 1}}.$$

Ausgehend von den Nominalzuständen der Flugzeug–Systemmodelle in Bild 6 wird die *Fehlerinjektion* in der IMA Hardwarekomponente K_{13} des Systems CPIOM 1 in Bild 6 durchgeführt. Dies hat zur Folge, daß zunächst sämtliche HCFSMs der IMA Komponente K_{13} simultan in den Zustand *„isoliert“* übergehen und sich im System CPIOM 1 ausbreiten, was den Verlust des Systems zur Folge hat.
Da es sich aber bei der Komponenten K_{13} um eine IMA Komponente des CPIOM 1 handelt, die von sämtlichen Systemen der primären Flugsteuerung verwandt wird, sind auch diese Systeme vom den *Fehlerausbreitungs–* und *Rekonfigurationsprozeß* im Rahmen des *Redundanzmanagements* betroffen (Bild 7). Gerade diese SYRELAN^{TM} Fähigkeit unterstützt die im Systementwurf auftretende Fragestellung, wie sich die IMA Komponentenausfälle auf die darauf integrierten Flugzeugsysteme ausbreiten.
Betrachtet man nun die Wirkung des IMA Komponentenausfalls, gehen in sämtlichen Systemen die Software–Applikationen in den HCFSMs des CPIOM 1 (K_7) in den Zustand *„isoliert“* über. In allen Systemen, außer der *Spoilersteuerung*, hat dies keinerlei Wirkung auf die *„aktiven“* Systemkanäle, so daß hinsichtlich der CPIOMs der Redundanzgrad gemindert bzw. bei der *Höhenrudersteuerung* und der *Seitenrudersteuerung* ganz aufgehoben wird. Hingegen fallen bei der *Spoilersteuerung* zwei Aktuatorpaare (Aktuator 3 und 4) weg. Die Restausfallwahrscheinlichkeiten der degradierten Systeme sind in der Spalte F_{deg} von Tabelle 1 aufgeführt und zeigen gerade bei der *Höhenrudersteuerung* und der *Seitenrudersteuerung* eine hohe Ausfallwahrscheinlichkeit, da im Bereich der CPIOMs keine Fehlertoleranz mehr existiert.

5 ZUSAMMENFASSUNG

Dieser Artikel beschreibt die Methoden des Software–Tools SYRELAN^{TM}, daß von Systemingenieuren schon mit Begin der Vorentwurfsphase von Flugzeugsystemen auf Basis von Integrierter Modularer Avionk eingesetzt werden kann. Es handelt sich um ein Software–Tool, welches auf Basis von interaktiv erstellten RBD– und HCFSM–Modellen gekoppelter Flugzeugsysteme sowohl die zuverlässigkeitstechnische Analyse als auch die Analyse injezierter Komponentenfehler hinsichtlich der *Fehlerausbreitungs–* und *Rekonfigurationsprozesse* im Rahmen des *Redundanzmanagements* bereitstellt. Besonders hervorzuheben ist hierbei die Analyse von IMA Komponentenausfällen bzgl. ihrer Wirkung bei *Fehlerausbreitung* und *Rekonfiguration* auf die davon abhängigen Flugzeugsysteme. In SYRELAN^{TM} wird dies gerade durch die zusätzliche und separate Abbildung der IMA Module, unabhängig von den Flugzeugsystemen, unterstützt.
Weitere Entwicklungsstufen des Tools sehen die zuverlässigkeitstechnische Analyse logisch kombinierter Flugzeug–Systemmodelle vor, sowie die Berücksichtigung der Komponenten–Redundanzmerkmale in der Zuverlässigkeitsanalyse, die in der aktuellen SYRELAN^{TM} Version auf Basis *„aktiver“* Redundanzen implementiert ist.

DANKSAGUNG

Die Autoren danken AIRBUS DEUTSCHLAND, Hamburg für die Finanzierung und freundliche Unterstützung des Forschungprojektes *Modellierung und zuverlässigkeitstechnische Analyse fehlertoleranter, vernetzter Systemarchitekturen auf Basis von IMA*.

SCHRIFTTUM

[GAJ94] GAJSKI, D. D.; VAHID, F.; NARAYAN, S.; GONG, J.: *Specification and Design of Embedded Systems.* Prentice Hall, Englewood Cliffs, New Jersey, 1994.

[JAA89] JOINT AVIATION AUTHORITIES: *1 to JAR 25.1309 – Advisory Circular Joint to Aviation Requirements.* Civil Aviation Authority, London, 1989.

[REH03] REHAGE, D., CARL, U. B., VAHL, A.: *Redundanzmanagement fehlertoleranter Flugzeug–Systemarchitekturen – Zuverlässigkeitstechnische Analyse und Synthese degradierter Systemzustände.* Deutscher Luft- und Raumfahrtkongress 2003, München, November 2003.

[SCHNEE01] SCHNEEWEISS, W. G.: *Reliability Modeling.* LiLoLe–Verlag, Hagen, 2001.

[TEI97] TEICH, J.: *Digitale Hardware/Software–Systeme.* Springer Verlag, Berlin Heidelberg, 1997.

[VAH98] VAHL, A.: *Interaktive Zuverlässigkeitsanalyse von Flugzeug–Systemarchitekturen.* Dissertation, Arbeitsbereich Flugzeug–Systemtechnik, Technische Unversität Hamburg–Harburg, Fortschritt–Berichte VDI, Reihe 10, Nr. 565, Düsseldorf, 1998.

[VDI86] VEREIN DEUTSCHER INGENIEURE (HRSG.): *Mathematische Modelle für Redundanz.* VDI–Richtlinie 4008, VDI–Handbuch Technische Zuverlässigkeit, VDI–Verlag Düssledorf, 1986.