The Effects on Reliability of Integration of Aircraft Systems Based on Integrated Modular Avionics

Dominick Rehage[1], Udo B. Carl[1], Maximilian Merkel[1], and Andreas Vahl[2]

[1] Hamburg University of Technology,
Institute for Aircraft Systems Engineering, 21071 Hamburg, Germany
{rehage,carl,merkel}@tuhh.de
http://www.tuhh.de/fst
[2] Airbus Deutschland GmbH,
Kreetslag 10, 21129 Hamburg, Germany
andreas.vahl@airbus.com

Abstract. The integration of aircraft systems – based on INTEGRATED MODULAR AVIONICS (IMA) – has significant effects on reliability. This paper presents the state of development of a software–tool for interactive reliability analysis and evaluation of aircraft system configurations on the IMA platform. For this, a hybrid system model of each aircraft system, being composed of a reliability block diagram model and a model of hierarchical, concurrent finite state machines, is essential. Within the area of reliability, different aircraft system models can be analyzed after they have been logically combined. This novel functionality provides a platform for systems engineers, enabling the evaluation of the effects of system integration by reliability calculations as well as redundancy management in a fault–free state and in cases of component failures.

1 Introduction

The objective pursued with the concept of INTEGRATED MODULAR AVIONICS (IMA) is the integration of the application–specific control and monitoring functions of different aircraft systems on standardized electronic computing modules ("horizontal integration"). This leads to a more hardware–economic concept than the typical function specific LINE REPLACEABLE UNITS (LRU) used nowadays, arranged in single lane channels consisting of computing and peripheral systems (actuation, sensors etc.). This integration of different aircraft systems on modules consequently causes many common points, resulting in dependencies between those systems.

The design of aircraft systems based on IMA is a very complex and multidisciplinary process in the fields of avionic, communication and peripheral systems. System reliability is an essential part of aircraft system design and has to be considered from the very beginning of the design phase to reach an optimum for the product in costs and time. In this context, high reliability requirements drive the capabilities of aircraft systems to be fault tolerant and the invested degree of redundancy to fulfill these requirements is an indicator for the system complexity, which is concerning the IMA on a very high level.

During the design of aircrafts, systems engineers are confronted with the effects of system integration and they have to develop their system under questions like:

M. Heisel et al. (Eds.): SAFECOMP 2004, LNCS 3219, pp. 224–238, 2004.

- *"What is the effect of a component failure on integrated aircraft systems assuming that the failure occurs on the IMA platform and induces the degradation of the system reliability or affects the failure propagation and reconfiguration?"*
- *"What effect has the integrated aircraft system on reliability of physically dependent systems?"*

Addressing these development challenges of aircraft systems this paper presents the state of development of the software–tool SyRelAn™ (**Sytem Reliability Analysis**). This tool provides systems engineers with a computer aided development environment for reliability synthesis and analysis of aircraft systems based on IMA.

Basis for the aircraft system analysis and evaluation is a hybrid system model. The structural architecture of the fault tolerant aircraft systems are modelled in independent Reliability Block Diagram (RBD) in *positive* logic. *Positive* logic means that the RBD–blocks are arranged to fulfill the system function and this leads to a mapping of the real system architecture. In order to represent the behavior of integrated systems under the event of component failures Hierarchical, Concurrent Finite State Machines (HCFSM) are operated in the background of each block within the RBD–model. This second modelling environment is used for visualization of failure propagation and reconfiguration processes within the redundancy management of a fault tolerant systems under the event of component failures.

During the system analysis various system states are to be analyzed in the hybrid system models (RBD, HCFSM) concurrently; starting from the nominal state without any component failure via several degraded system states caused by component failures until the state of system failure. For each of these states the failure probabilities are calculated in the RBD–models and the redundancy management is visualized by coloring the RBD–blocks with colors representing the current component states of the HCFSMs.

For IMA purposes the visualization of failure propagation and reconfiguration within the redundancy management is fulfilled integrative. This means, that failures of IMA components propagate across systems containing IMA components used in common. Furthermore, SyRelAn™ provides a novel functionality in this context making the logical combination of any aircraft systems possible. This functionality is essential for IMA systems, because it enables the evaluation of integration effects on reliability in a comfortable way. That means, that each of the aircraft systems based on IMA is modelled independently in RBD and HCFSMs. In order to analyze the reliability of whether physically dependent aircraft systems can be integrated on the same IMA module, SyRelAn™ provides the logical combination of RBD–models for any independent modelled aircraft systems, composed by the logical linking (**AND**, **OR**) of system blocks.

2 Models of Aircraft Systems Based on IMA

The software–tool SyRelAn™ provides system engineers with a RBD and an HCFSM environment for interactive system modelling of all aircraft systems of one aircraft type. This leads to a large number of hybrid system models where each of the models takes integration aspects of commonly used IMA resources into account. The logical

combination of independently modelled hybrid system models is the basis for reliability analysis of integrated systems.

2.1 Hybrid System Model

In the first step a fault tolerant aircraft system architecture is modelled in the RBD–environment in the nominal state by linking RBD–blocks of components logically according to their functional dependency in the system architecture. In addition to this, the HCFSMs will be placed in the background of the RBD–model. The coupling of the two models occurs in both directions. From the RBD point of view the coupling exists in assignments of current component states of the HCFSMs to the RBD–blocks (Fig. 1). From the HCFSM point of view component failures are transferred from the RBD–blocks to the state machines that trigger the redundancy process.

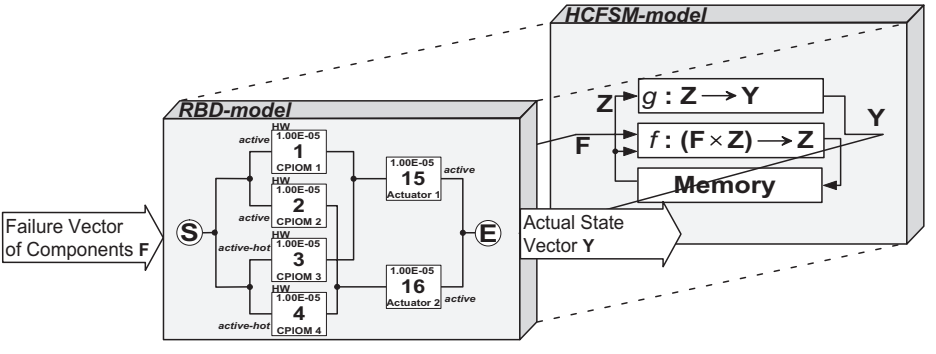


Fig. 1. Hybrid system model: RBD–model and HCFSM–model

RBD–Model
For fault tolerant aircraft system modelling in RBD it is necessary to determine a Top Event depending on which the reliability modelling and analysis can be performed. This event specifies system states that are to be analyzed. Boolean algebra describes the system model mathematically by using stochastically independent Boolean indicator variables for each component [Schnee01]

$$K_i = 1 \qquad \text{component } K_i \text{ is up,} \tag{1}$$

$$K_i = 0 \qquad \text{component } K_i \text{ is down.} \tag{2}$$

The expected value of the indicator variable K_i is the *survivor function*

$$E[K_i] = 0 \cdot P[K_i = 0] + 1 \cdot P[K_i = 1] = P[K_i = 1]. \tag{3}$$

The reliability R_i of a component i is defined as the probability $P[K_i = 1]$ that component is in functional state. Using an *exponential* distribution by considering a constant component *failure rate* λ_i per hour [1/h], the reliability is [VAH98]

$$R_i(t) = \mathrm{e}^{\lambda_i t}. \tag{4}$$

In general, the component failure rate λ_i is a function of time (BATHTUB CURVE [VAH98]), but in case of aircraft systems the component failure rate λ_i is sufficiently constant between two periodical component checks. Therefore failure of components are independent of age and stochastically distributed [VAH98]. Under the assumption of fulfilling monotony conditions and logical linking (**AND**, **OR**, **NOT**) of the variables K_i the system function ϕ is (see example in subsection 3.1) [VAH98]

$$\phi(\mathbf{K}) = 1 \qquad \text{system } \phi \text{ is up,} \tag{5}$$

$$\phi(\mathbf{K}) = 0 \qquad \text{system } \phi \text{ is down} \tag{6}$$

$$\text{with} \quad \mathbf{K} = \{K_1, \ldots, K_i, \ldots, K_m\}\,. \tag{7}$$

HCFSM–Model

The second modelling environment is the area of HCFSMs. This model can be built after the structural design of the system architecture is completed in the RBD–model. The complete HCFSM–model presentation is a 6–tuple and is composed of an input vector $\mathbf{F}$, an output vector $\mathbf{Y}$, a set of internal states in the elements of the state vector $\mathbf{Z}$, a set of initial states in the elements of the initial state vector $\hat{\mathbf{Z}}$, a next–state function f, and an output function g (Fig. 1) [GAJ94,TEI97]

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

The vector elements are MOORE–HCFSMs representatives for each component K_i (7) referring to a block in the RBD–model, which are described in detail in [REH03]. Vector $\mathbf{Z}$ contains in its rows $(i = 1, \cdots, m)$ the sets of internal states for each of the HCFSMs which are connected with component K_i. In this context it is important to assume that each component K_i is connected with at least one HCFSM and each of the applied HCFSMs has at least two ("*active*", "*isolated*") and up to five states (Fig. 2). These states can be reached by starting at the failure–free state $\hat{\mathbf{Z}}$ at initial operation time $(t_0 = 0)$, via several degraded system states $(t_s \geq t_0)$, up to system failure. Input vector $\mathbf{F}$ contains the injected failures of components K_i. This condition "**NOT** K_i" leads to the activation of the next–state function f of the HCFSMs of that component K_i and cause transitions from the current HCFSM states into states "*isolated*". The output vector $\mathbf{Y}$ of a system represents the current states of the MOORE–HCFSMs which are forwarded to the blocks above, by use of color assignments for each of the HCFSM states.

For the purpose of modelling the redundancy management, various HCFSMs of a fault tolerant system have to be coupled. The couplings exist by means of dependencies on the next state function as function of internal system states, as well as a function of component failures of multiple used components. It allows failure propagation and reconfiguration processes in the system model.

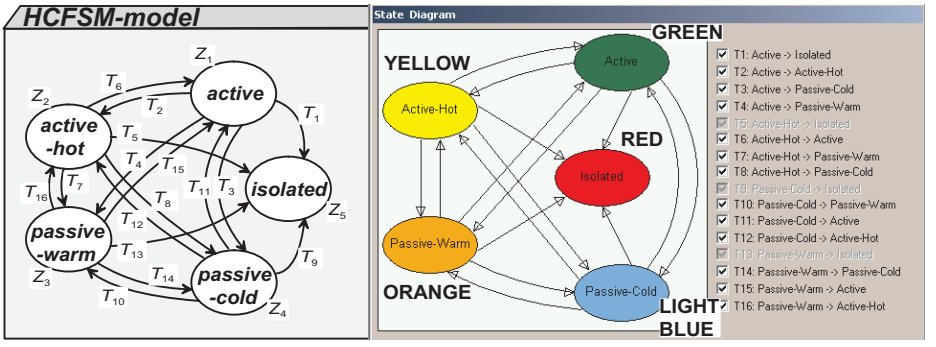


Fig. 2. States and transitions of an HCFSM and SyRelAn™ State Diagram

Each single HCFSM–model in the background of a RBD–block consists of up to five internal states $\{Z_1, \ldots, Z_5\}$ and up to 16 transitions $\{T_1, \ldots, T_{16}\}$ between the states, which define the next state functions using logical expressions as functions of states of HCFSMs neighbours (Fig. 2). In order to model the application specific HCFSM–model of an aircraft system, it is necessary to choose the transitions of each single HCFSM of the complete model in the State Diagram editor of SyRelAn™ in Fig. 2.

The variety of the internal states of the HCFSMs is motivated by stages of degradation from the reliability point of view. The next paragraph describes this context depending on the *failure rate* λ, which indicates the load of a stand–by component [VDI86]. It also contains the colors and *endings* representing the states of the HCFSMs. In case of current states of HCFSMs these states are transferred to the blocks above by assigning the corresponding colors in order to visualize the system states in the RBD–model.

"active" ← **GREEN**: From the start of the mission, the working component **a** is subjected to full stress. The failure rate is λ_a. The *ending* is "**a**".

"active–hot" ← **YELLOW**: From the beginning of the mission, reserve element **h** is subjected to the same stress as the actual working component **a**. For the failure rate, the following applies: $\lambda_h = \lambda_a$. The *ending* is "**h**".

"passive–warm" ← **ORANGE**: The reserve element **w** is subjected to less stress until failure of working component **a**, (or until **w** itself fails in advance). For the failure rate, the following applies: $0 < \lambda_w < \lambda_a$. The *ending* is "**w**".

"passive–cold" ← **LIGHT BLUE**: Until failure of working component **a**, reserve element **c** is not subjected to any stress. For the failure rate, the following applies: $\lambda_c = 0$. The *ending* is "**c**".

"isolated" ← **RED**: Failure state of component. The *ending* is "**i**".

The next–state function f, which contains the conditions for changing the actual state of an HCFSM to a succession state in the event of a component failure underlies a special syntax in SyRelAn™. In the corresponding transitions the equations, which

combine states of several HCFSMs logically (**AND**: "&", **OR**: "|", **NOT**: "$\sim$") must be "**TRUE**" to fulfill the state transition.

To address the states of HCFSMs it is necessary to distinguish between blocks, which operate only one or multiple HCFSMs in the background. The following equations provide the syntax for addressing a state of a single HCFSM in the background of a block (9) and a state of one of several HCFSMs in the background of a block (10)

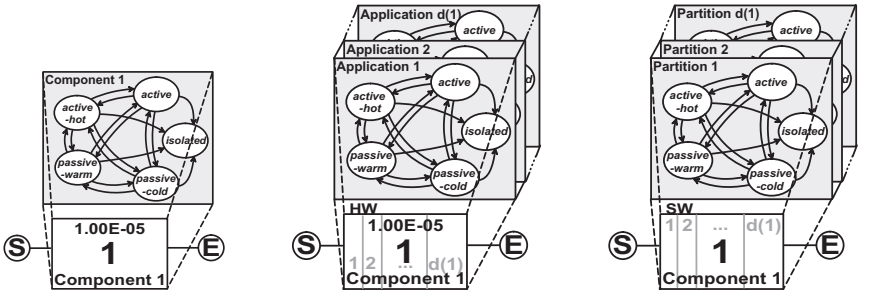
$$component : i\,,ending : \{\text{a, h, w, c, i}\} \quad \forall \quad K_i \in \mathbf{K}\,, \tag{9}$$

$$component : i\,,HCFSM : l\,,ending : \{\text{a, h, w, c, i}\} \tag{10}$$

$$\forall \quad K_i \in \mathbf{K} \quad \text{and} \quad l \in [1, d(i)] \quad \text{with} \quad d(i) \in I\!N\,.$$

Two examples are subsequently represented to clarify this syntax. $2, h$ addresses the state "*active–**h**ot*" of component K_2 related to a RBD–block with a single HCFSM in the background and $3, 7, c$ addresses the state "*passive–**c**old*" of HCFSM 7 of component K_3 in the background of its related RBD–block with several HCFSMs.

To model a fault tolerant aircraft system under the aspects of reliability and redundancy management various hardware and software components have to be represented. Therefore, SyRelAn^{TM} provides three categories of blocks. Fig. 3 shows the modelling options for two hardware blocks and one software block.



(a) Hardware block

(b) Multifunctional hardware block

(c) Multifunctional software block

Fig. 3. Three RBD–block categories with its HCFSMs

The use of these blocks depends on the specific application of the component modelled by this block. The simple *hardware block* is used in aircraft system modelling for single used components (e.g. actuators, sensors etc.) and represents them with a constant *failure rate* λ (Fig. 3(a)). Within the redundancy management this block contains one HCFSM with its states and transitions in the complete system context.

A specific version of a *hardware block* is a *multifunctional hardware block*. This type of block incorporates the same reliability characteristics as a *hardware block* but has the advantage of components used in common (e.g. bus, ethernet switch etc.) to separate

states of different applications by use of multiple HCFSMs. In case of a component failure all HCFSMs pass into the state "*isolated*" and the reliability reduces to zero.

The third category specifies the *multifunctional software block*. This block enables the modelling of different software applications within the RBD and further supports the characteristics of aircraft systems based on IMA. This is accomplished by separation of HCFSMs in the background of each *multifunctional software block*, which addresses the partitioning aspect of computing modules of the IMA systems. In the field of reliability the software blocks are failure–free ($R = 1$) or failed ($R = 0$) with respect to their HCFSMs. In contrast to the *multifunctional hardware block* an HCFSM of the *multifunctional software block* can be declared as failed independently. For this reason every HCFSM is associated with another RBD hardware block in an aircraft system model (e.g. Fig. 7: HCFSM 1 of K_7 is associated with K_{23}, see dashed arrow in system $\phi(\mathbf{K}_{aileron\,control})$). An HCFSM of a *multifunctional software block* in state "*isolated*" leads to a degraded system function (7) concerning the *minimal path* of associated RBD hardware block and, of course, the HCFSM of the *multifunctional software block*.

2.2 Superposition of Hybrid System Models

In order to take IMA specific characteristics of aircraft systems into account it is necessary to distinguish between components, which are used in a single aircraft system only, and those, which are used in various aircraft systems. Therefore SyRelAn™ offers different component lists. All components within an aircraft project, e.g. A380 or 7E7, are contained in the set of aircraft components

$$\mathbf{K_{AC}} = \{K_1, \ldots, K_i, \ldots, K_m\}\,. \tag{11}$$

All system models within an aircraft project access a subset of aircraft components (11), which is expressed by the transpose of system component vector

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

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

The corresponding transpose of the system vector with application of formula (5) is

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

An important property of various aircraft system models is that IMA based system models are able to access so-called *global blocks* (every *global block* is one of the three block types in figure 3). All of these *global blocks* are integral part of different system models. This means, that the *global blocks* represent characteristics of IMA components used common and thus have effects on the reliability of all RBD–models as well as all HCFSM–models of different systems using them (Fig. 4). Hence, current state variations of the *global block* HCFSMs lead to activation of the redundancy management of all systems using this blocks. If current state variations of the *global blocks* cause the activation of an HCFSM transition into the state "*isolated*", the reliability of systems, which apply these, will be reduced. This is because the *global block* components are

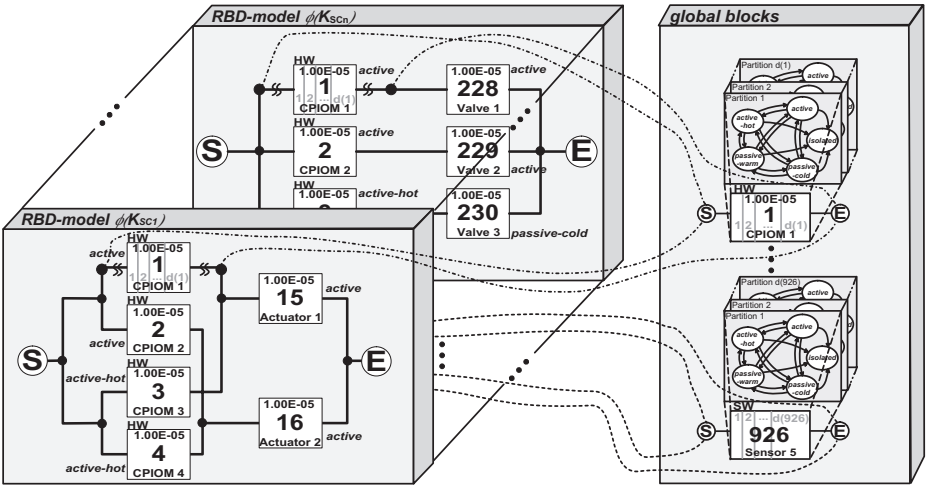


Fig. 4. Coupling of hybrid system models by using *global blocks*

treated as components, which are mapped in different systems (Fig. 4: K_1 of $\phi(\mathbf{K_{SC1}})$ and $\phi(\mathbf{K_{SCn}})$), but their existence in the context of all system models is unique according to their physically occurrence. The transpose of vector $\mathbf{K_{GC}}$ (15) consists of the *global block* components of each aircraft system within the aircraft project. The *global block* components are generated by building up the intersection of the sets of aircraft system components (16) with each other, because the condition of a *global block* component demands a component occurrence in more than one aircraft system.

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

$$\text{with} \quad \mathbf{K_{GCj}} = \{\mathbf{K_{SCj}} \cap \mathbf{K_{SCq}}\} \quad \forall \quad j, q = 1, \ldots, n \quad \text{and} \quad j \neq q\,. \tag{16}$$

2.3 Logical Combination of Hybrid System Models

In order to analyze the effects on reliability of integration of aircraft systems based on IMA, it is necessary to combine integrated systems logically in the case of dependency of functional effects. Regarding aircraft systems with independent functional effects, integration has no significant effects on reliability, which is comparable to the reliability of an aircraft system operated on LRU computing resources – except for architectural differences of both avionic systems. The reliability becomes a crucial factor of system analysis in case of different aircraft systems are dependent on their functional behaviour. An example is the reliability analysis of an aircraft *rudder control* and *engine control* system. These two aircraft systems have to be analyzed independently from each other, as well as combined in a second analysis. The dependency between both systems leads to higher reliability requirements than the requirement of each single system, since a loss of both systems causes the loss of aircraft control ("*catastrophical*" failure event). In this context it is necessary to analyze whether both systems can be integrated on

IMA computing resources with appropriate redundancy level or are the IMA computing resources the origin of too low system reliability, because of its common point characteristic. Within the reliability analysis, the integration and diversification aspect of aircraft systems has to be discussed considering reliability analysis of logically combined aircraft systems with IMA components used in common used or on separated IMA components.

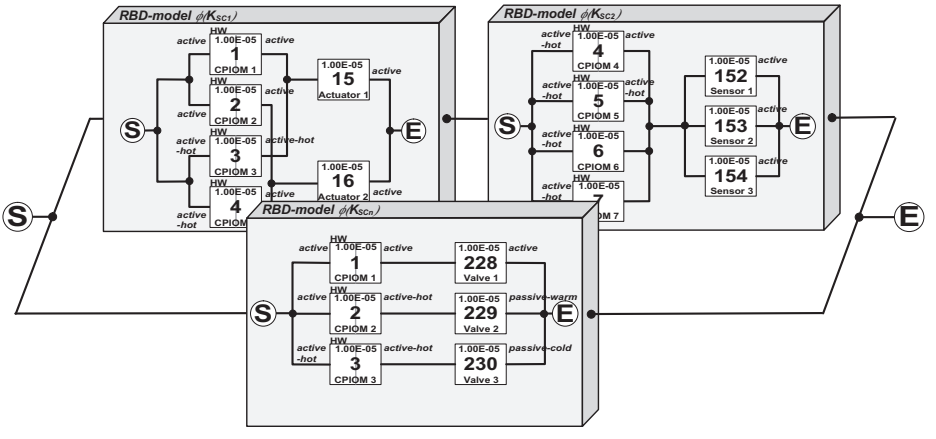


Fig. 5. Logical combinig of system models

Fig. 5 shows the possibilities to combine aircraft systems logically. In this case, three systems are combined on RBD system level, following the syntax of logic **AND** ($\wedge$) or **OR** ($\vee$) by depending on elements of the system vector (14). The set of components of logically combined aircraft systems $\mathbf{K_{LC}}$ is the union of the sets of system components $\mathbf{K_{SCj}}$ (13), which are involved in the combining process. Referring to Fig. 5 this is

$$\phi(\mathbf{K_{LC}}) = [\phi(\mathbf{K_{SC1}}) \wedge \phi(\mathbf{K_{SC2}})] \vee \phi(\mathbf{K_{SCn}}) \tag{17}$$

$$\text{with} \quad \mathbf{K_{LC}} = \{\mathbf{K_{SC1}} \cup \mathbf{K_{SC2}} \cup \mathbf{K_{SCn}}\}\,. \tag{18}$$

3 Analysis of Aircraft System Models Based on IMA

The analysis of RBD-models and HCFSM-models is performed separately for both model areas. However, the effects of component failures and state transitions of HCFSMs are interchanged.

3.1 Reliability Analysis

For reliability analysis of single and logically combined aircraft systems the CAOS (COMPUTER AIDED ORTHOGONALISATION SYSTEM) algorithm is applied for orthogonal-

isation processes of their BOOLEAN system functions $\phi(\mathbf{K_{SC}})$ (14) [VAH98]. Orthogonalisation means, in this case, that products of all disjunctive terms of a BOOLEAN system function (*minimal paths* M_r) are exclusive and thus zero [VAH98]. In case of system $\phi(\mathbf{K_{SC1}})$ in figure 5 the system function is

$$\phi(\mathbf{K_{SC1}}) = \phi(K_1, K_2, K_3, K_4, K_{15}, K_{16})\,, \tag{19}$$

$$\phi(\mathbf{K_{SC1}}) = K_1K_{15} \vee K_2K_{16} \vee K_3K_{15} \vee K_4K_{16} = M_1 \vee M_2 \vee M_3 \vee M_4\,. \tag{20}$$

After application of the CAOS orthogonalisation algorithm with its condition of orthogonalisation

$$M_r \cdot M_s = 0 \quad \text{with} \quad r, s = 1, 2, 3, 4 \quad \text{and} \quad r \neq s \tag{21}$$

the system function is in an unique linear form, which enables the application of real algebraic operators. By considering indicator variables as binary stochastical variables with the probability distribution (4), this leads to ($F_i = 1 - R_i$, see formula (4))

$$\begin{aligned} E[\phi(\mathbf{K_{SC1}})] = E[&K_1K_{15} + K_2K_{16}\overline{K_1K_{15}} + K_3K_{15}\overline{K_1}\ \overline{K_2K_{16}} + \cdots \\ &\cdots + K_4K_{16}\overline{K_2}\ \overline{K_{15}} + K_4K_{15}K_{16}\overline{K_1}\ \overline{K_2}\ \overline{K_3}\ \overline{K_3}]\,, \end{aligned} \tag{22}$$

$$\begin{aligned} R_{SC1} = &R_1R_{15} + R_2R_{16}F_1 + R_2R_{16}F_{15} + R_3R_{15}F_1F_2 + \cdots \\ &\cdots + R_3R_{15}F_1F_{16} + R_4R_{16}F_2F_{15} + R_4R_{15}R_{16}F_1F_2F_3 \end{aligned} \tag{23}$$

A major advantage of the orthogonalisation process is, that multiple used blocks of the same component within a RBD–model are only considered as a single physical component in the reliability calculations.

Furthermore, SYRELAN^{TM} enables the analysis of *degraded* system states, which defines the minimal operational requirements as well as k–out of–n systems, where n components exist in "*active*" redundancy, of which k are necessary to perform the required function [VAH98]. To take k–out of–n into account in the reliability analysis there is a dialog in SYRELAN^{TM} in order to enter logical equations Γ, which represent operational conditions of components. Thus, these logically combined components must be available in *minimal path* of the system functions $\phi(\mathbf{K}_{SC})$ (14) [VAH98].

3.2 Redundancy Management

The redundancy management of integrated aircraft systems based on IMA is to be considered as an important task within the system analysis. In general the objective of the redundancy management is to support systems engineers with a software–tool environment to simulate different strategies of reconfiguration (e.g. *priorities*) in a fault tolerant system before applying them in the target system as well as special discussion of IMA related problems as failure propagation process in the integrated system. For this purpose, SYRELAN^{TM} enables separate RBD and HCFSM modelling of each IMA resource and each aircraft system operating on this resource (Fig. 9: "SYSTEM TREE"). This supports systems engineers in analyzing the effects of IMA component failures by visualizing the impact within the failure propagation and reconfiguration processes on aircraft system

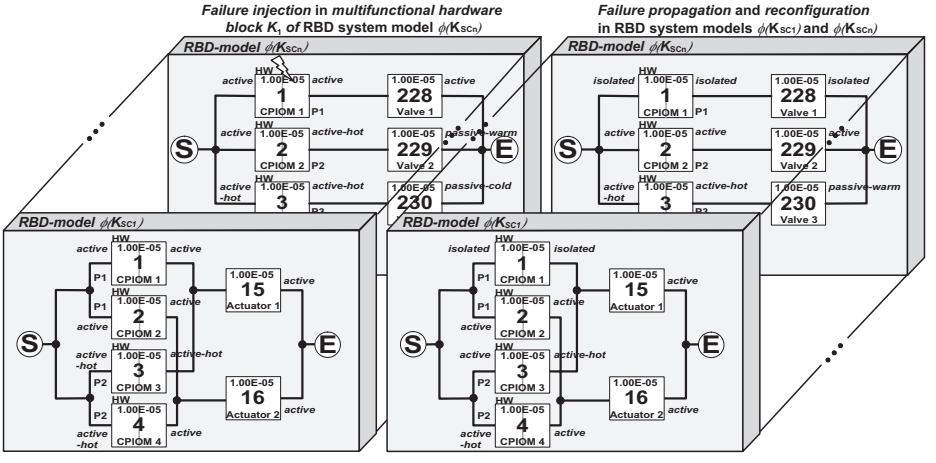


Fig. 6. *Redundancy management* on integrated aircraft systems

level. That means, that each state transition to a new current state of an HCFSM will be displayed in the RBD–model by a change of color of the corresponding RBD–block.

In this context Fig. 6 provides an example of the mode of operation of the *redundancy management*. As one can see, two systems ($\phi(\mathbf{K_{SC1}}), \phi(\mathbf{K_{SCn}})$) are modelled in their nominal system state on the left side. The use of IMA components $\{K_1, K_2, K_3\}$ (**Computing Input Output Module**, CPIOM) leads to dependencies of both systems in the event of component failures of this entities used in common. This is demonstrated by *failure injection* in IMA component K_1 of system $\phi(\mathbf{K_{SCn}})$. It triggers the *redundancy management* process in system $\phi(\mathbf{K_{SCn}})$ in a first step, where both HCFSMs of K_1 pass over to current state "*isolated*" (Fig. 6: right side).

Afterwards, the *failure propagation* follows by state transition of the HCFSM of K_{228} to "*isolated*". The *reconfiguration* has to be fulfilled in consideration of *priority* P2 of CPIOM 2 to control the system. The transition T_1, from state "*active–hot*" to "*active*" of the second HCFSM of component K_2, describes this context in the following logical equation

$$\text{P2}: \;\; T_1(K_2, \text{HCFSM 2}) = (1, 2, \text{i} \;\&\; 228, i) \;\&\; (2, 2, \text{h} \;\&\; 229, \text{w})\,. \qquad (24)$$

This means equation (24) is "**TRUE**", because only the first control channel $\{K_1, K_{228}\}$ is "*isolated*" (condition of P2) and not the first and the second channel $\{K_2, K_{229}\}$ which is the condition of *priority* P3. After *reconfiguration* of system $\phi(\mathbf{K_{SCn}})$ the *redundancy management* propagates to system $\phi(\mathbf{K_{SC1}})$ in a second step, because HCFSM 1 of K_1 of this system is also in an "*isolated*" state. This leads to a *reconfiguration* process wherein redundant CPIOM 3 takes over control of actuator 1.

4 Application

The synthesis and analysis of fault tolerant aircraft systems based on IMA is related to nominal system state via degraded system states caused by component failures up to system failure. The example presented in this paper is the *roll control* system of a civil aircraft in the nominal state. The *roll control* consists of two systems: *aileron control* and *spoiler control*. The design question is whether both systems can be integrated on redundant CPIOMs of the IMA resource or is the implementation on separated redundant CPIOMs is necessary to fulfill the reliability requirement in the nominal system state of both systems.

The reliability requirement is related to the system classification of *roll control*. This is according to JAR 25 to be considered as "*catastrophic*" [JAA89]. The loss of this system in the low speed range can yield to fatal effects on the passengers and on fatal damage on aircraft and has a maximum failure probability of $F = 10^{-9}$ per flight hour. The TOP EVENT defines the system state, which is to be analysed in the RBD–model:

"*Functionality of fault tolerant aircraft roll control system.*"

The RBD–model of an aileron control system is shown in Fig. 7. The HCFSM–model representation is shown by the block attributes, which describe the current states of the RBD–blocks. Usually, this is presented by colors of the RBD–blocks, which change in the event of component failures within the redundancy management process.

The system consists of two aileron hydraulic servo actuators on each wing. For pressurization, there are three hydraulic systems available (yellow, green, blue). As one can see there are two CPIOMs (CPIOM1: $\{K_1, K_7, K_{13}\}$ and CPIOM2: $\{K_2, K_8, K_{14}\}$) with their software blocks $\{K_7, K_8\}$ implemented. CPIOM1 controls the left and right outer aileron actuators (LO and RO) which are in an "*active*" mode in the nominal state. The first two of six partitions are occupied with the control applications represented by two HCFSMs (*multifunctional software block* of CPIOM1: K_7). CPIOM2 controls the

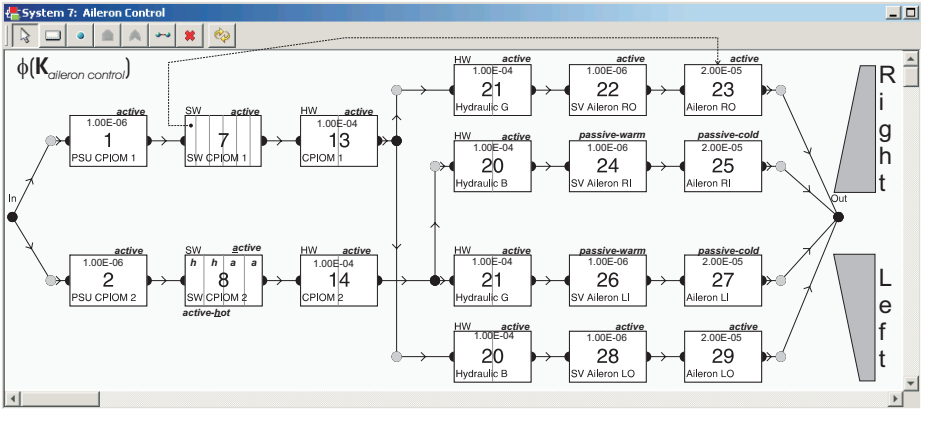


Fig. 7. *Aileron control*

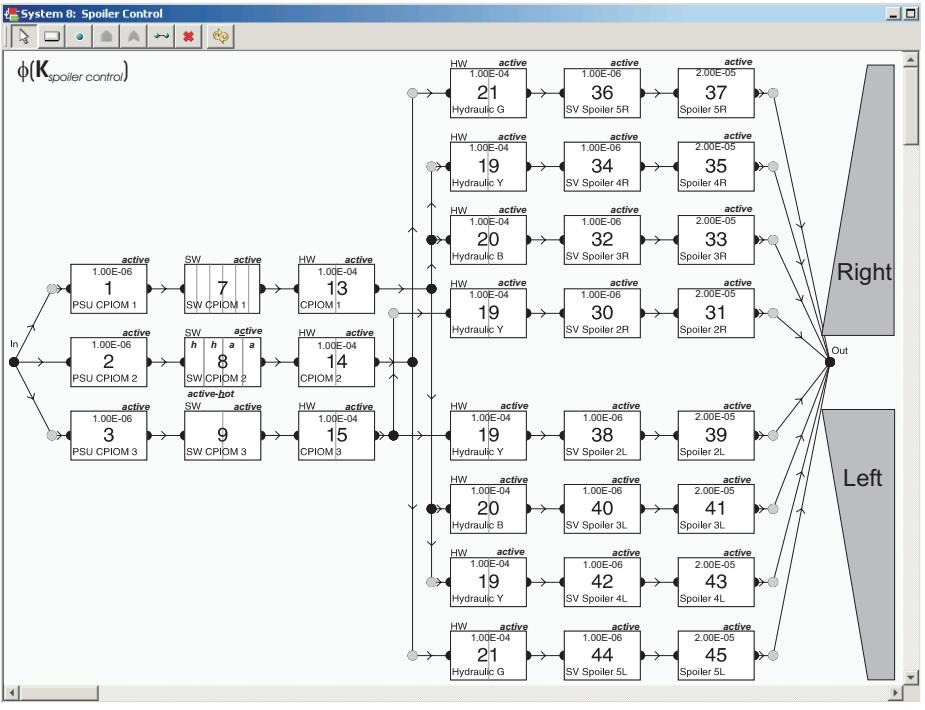


Fig. 8. *Spoiler control*

left and right inner aileron actuators (LI and RI), which are redundant in relation to the outer actuators. The controls of LI and RI actuators are located in the first two of four partitions of *multifunctional software block* K_8 of CPIOM2. These redundant actuator control channels are in the HCFSM current state "*active–hot*" from the software point of view and in the HCFSM current state "*passive–cold*" from the actuator point of view.

Fig. 8 shows that the spoiler control system is implemented on three CPIOMs (CPIOM1, CPIOM2 and CPIOM3: $\{K_3, K_9, K_{15}\}$). The responsibilities for controlling spoiler actuators are: left and right spoiler actuator 2 by CPIOM3, left and right spoiler actuator 3 and 4 by CPIOM1 and left and right spoiler actuator 5 by CPIOM2. It is obvious that CPIOM1 and CPIOM2 each control both spoilers and ailerons. Therefore, the CPIOM1 (K_7, a *multifunctional software block*) contains four spoiler HCFSMs and the CPIOM2 (K_8, a *multifunctional software block*) two spoiler HCFSMs each of them in "*active*" mode. This yields two hybrid system models, which consider the aspect of integration of commonly used IMA components. For operational purposes it is important to consider that the left and right spoiler actuators degrade in pairs. In the area of reliability the formulation of minimal operational requirements is necessary

$$\Gamma = [(K_{31} \wedge K_{39}) \vee (K_{33} \wedge K_{41}) \vee (K_{35} \wedge K_{43}) \vee (K_{37} \wedge K_{45})] \ . \qquad (25)$$

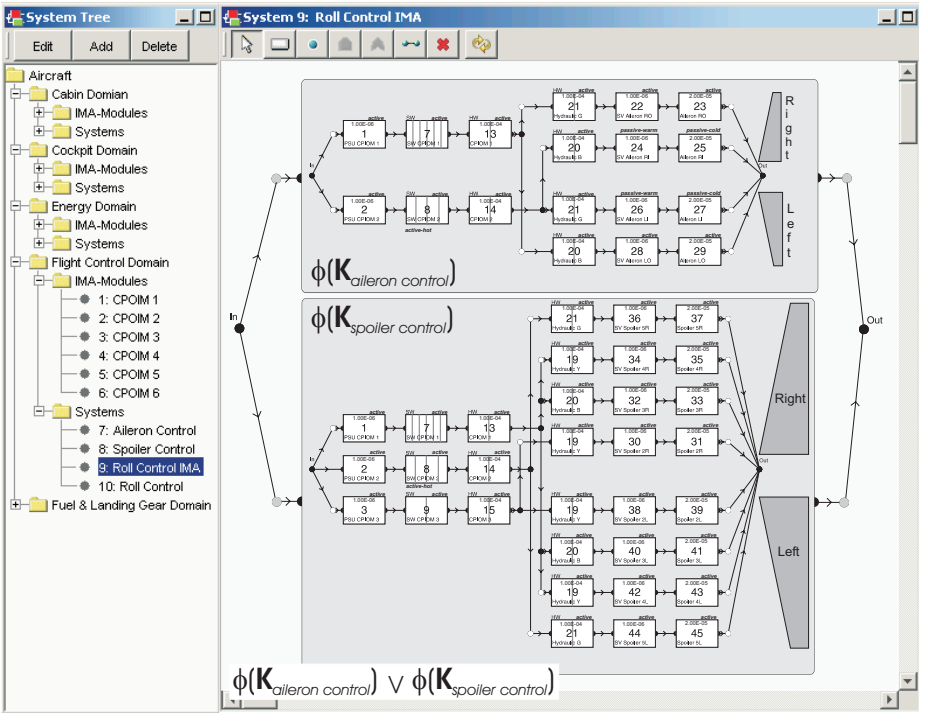


Fig. 9. Logical combining of *aileron control* and *spoiler control* in *roll control* system

In order to attain an answer whether the integration of *aileron control* and *spoiler control* on IMA resources fulfills the reliability requirements the systems must be logically combined (Fig. 9)

$$\phi(\mathbf{K_{LC}}) = [\phi(\mathbf{K}_{\text{aileron control}}) \vee \phi(\mathbf{K}_{\text{spoiler control}})] \ . \tag{26}$$

The reliability analysis of both logically combined systems based on the applied failure rates λ in Fig. 7 and 8 result in a failure probability of $F(t_s = 1\text{h}) = 3.47 \cdot 10^{-12}$. The conclusion of this failure probability is that the *aileron control* and *spoiler control* systems can be integrated on IMA resources used in common, because the reliability requirements are fulfilled. In this system the integration has no significant effect on reliability. The separation of these systems (e.g. *aileron control* on CPIOM 5 and 6) leads to less failure probability ($F(t_s = 1\text{h}) = 1.00 \cdot 10^{-12}$), but it is, nevertheless, not necessary to separate them.

5 Conclusion

This paper presents the approaches for a software–tool that can be applied for analysis and synthesis of fault tolerant aircraft systems based on IMA at a very early stage in

system design. In this scope, SyRelAn™ provides with its hybrid system models a very suitable tool environment for system engineers to evaluate the effects of aircraft systems integration on reliability.

This is realised in SyRelAn™ by the extension of analyzing logically combined aircraft systems in the field of reliability and the further development of the redundancy management for aircraft systems based on IMA, which means failures of IMA components propagated throughout the relevant aircraft systems.

Further extension in the field of reliability calculations under consideration of redundancy characteristics is in progress. Additionally work has been done on an optimization of calculation time within the orthogonalisation process of system functions by calculating these functions in server client computer arrangements.

References

[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.