Bogusław DOŁĘGA
POLITECHNIKA RZESZOWSKA,
Al. Powstańców Warszawy 8, 35-959 Rzeszów

Some remarks about aircraft control and navigation system as reliable fault tolerant system

PhD. eng. Bogusław DOŁĘGA

Professor Assistant on Avionics and Control Systems Department at Rzeszow University of Technology. Research interests: Fault Tolerant Avionic Systems, with special interest in Aircraft Control and Navigation Systems. Publications: Over 60 scientific articles.

e-mail: dolbog@prz.edu.pl

Abstract

This paper presents some remarks about making more reliable aircraft control and navigation system. On simple examples the author presents the influence of architecture of a fault tolerant system on its reliability. The proposed description of fault diagnosis procedures and control reconfiguration enables preparation and analysis of a fault tolerant system.

Keywords: reliability, fault tolerant system, fault localisation, aircraft control and navigation system.

Wybrane uwagi dotyczące lotniczych systemów sterowania i nawigacji, jako niezawodnych systemów tolerujących uszkodzenia

Streszczenie

Artykuł przedstawia wybrane uwagi związane z tworzeniem lotniczych systemów sterowania i nawigacji, które powinna cechować podwyższona niezawodność działania. Nie podjęto analizy konkretnego przykładu rozwiązań stosowanych w lotnictwie, ale poprzez proste przykłady architektury możliwych do zastosowania w lotnictwie rozwiązań przedstawiono ich wpływ na niezawodność i tolerowanie pojawiających się uszkodzeń. Podjęto w ten sposób próbę uzasadnienia wprowadzania wymagań tolerowania uszkodzeń w tych systemach ze względu na uzyskane wskaźniki niezawodności. Przywołując ogólną postać formuły wnioskowania deontycznego opisującą proces rekonfiguracji zaprezentowano rolę lokalizacji uszkodzeń w poprawnym działaniu takich systemów. Zaproponowany opis stosowanych procedur diagnostyki i rekonfiguracji, poprzez wykorzystanie elementów teorii zbiorów przybliżonych umożliwia zarówno przygotowanie, jak i przeprowadzenie analizy tworzonego systemu z uwzględnieniem właściwości tolerowania pojawiających się uszkodzeń.

Słowa kluczowe: niezawodność, system tolerujący uszkodzenia, lokalizacja uszkodzeń, lotniczy system sterowania i nawigacji.

1. Introduction

Aircraft Control and Navigation Systems (ACNS) are very important in flying safety. The effects of their failures are catastrophic and as requirements and recommendations of FAR/CS-23 and AC 23.1309 present, must be shown to reach the probability of less than 10^{-6} for small aircraft per flight hour [1, 2]. The designer draws his attention to flight – while aircraft is airborne, faults appearing cannot interrupt the mission or can bring it to halt prior to safe landing. The high reliability of aircraft flight can be achieved by control architecture which can react to fault appearance. That theme is important for various groups of researchers like Wu [3] and Li [4]. The first inspiration for this paper was Sha paper [5]. He presented the general remarks about reliability of a control system. This paper, after showing the point of using the fault tolerant idea, presents the proposal of modelling and analysis of such systems.

2. Introduction to aviation reliability

It is well known, that aircrafts and other products of aviation industry are goods of high reliability. The general appreciation of reliability as in Oxford Dictionary of the US Military [6] involves ability of the system to perform its required functions under states conditions for a specified period of time. In aviation it means the ability to carry out a mission and not to lose the ability for safe landing. From the beginning of aviation history, the perfectionism in materials and technology which are used is the main way of realising the requirements of high reliability. Unfortunately, despite the wide spectrum of aviation reliability research, the faults occurrence cannot be eliminated at all. This pessimistic observation is the main reason for appearance of the fault tolerance idea. Fault tolerance ensures proper realisation of the required system functions despite of fault occurrence. Requirements of fault tolerance can be really realised by using different kinds of redundancy and could be implemented in ACNS when the digital technology was employed in this field. A lot kinds of redundancies, implementations of different methods and other specific features of an airplane as the object of control make that system complex. Moreover, as was earlier mentioned, the ACNS are complex system with high reliability, availability and safety requirements. As Prasad [7] defined, we can notice that it is complex system with requirements of dependability. The design process of ACNS, taking into consideration the dependability requirements, generates a lot of tests from laboratory, through ground and flight as finalised. We must remember that reliability is connected with analysis, of course, but the high reliability there is obtained consequently during the synthesis process. Equally, some general remarks of fault tolerant systems could be very useful during the ACNS design process. To make deeper consideration, there is proposed the reliability analysis of a few basic examples o the feedback loop control system.

3. Reliability analysis of a feedback loop system

Let us consider a very simple example, in which the goal γ_i could be achieved, when the binary information $y_i(t)$ about the goal realisation is known (Fig. 1). If we assume perfect process realisation of goal achieving, then the reliability of the whole system is the function of reliability of y_i correct access – $R_{sysI}(t)=R_{yi}(t)$.

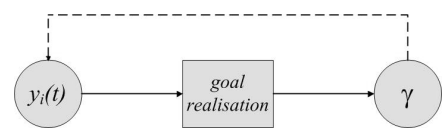

Fig. 1. Goal γ_i realisation by knowledge about y_i.
Rys. 1. Informacja y_i o realizacji celu γ_i.

Looking at the passive approach of fault tolerant realisation of a system, we can triple the access to $y_i(t)$ by signals $y_{i1}(t)$, $y_{i2}(t)$ and $y_{i3}(t)$. The realisation of the goal γ_i is performed with use of the signal whose value will be in accordance with the most of $y_{ii}(t)$ values. We can assume the signals $y_{ii}(t)$ to be synchronised. The logic of its realisation could be presented like in Fig. 2.

It is the typical Triple Modular Redundancy system and its reliability with perfect logical circuits and equal reliability distribution for each $y_{ii}(t)$ access ($R_{yi1}=R_{yi2}=R_{yi3}=R_{yi}$) is given by:

$$R_{TMR}(t)=R_{yi}(t)^3+3R_{yi}(t)^2[1-R_{yi}(t)]$$

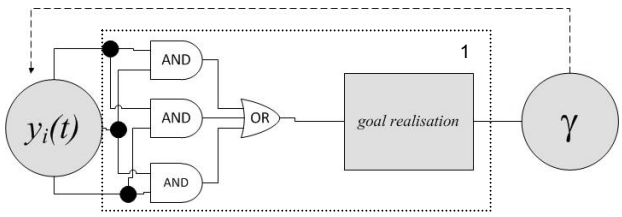

Fig. 2. Tripled goal γ_i realisation schema.
Rys. 2. Potrojenie informacji o realizacji celu γ_i

The reliability $R_{TMR}(t)$ of that system is greater than previous $R_{sys1}(t)$ for t in which $R_{yi}(t)>0.5$ but the mean time to failure (MTTF) is less then MTTF for a single component system. If we want to cover reliability of logical circuits, the time in which the value of the system reliability distribution is greater than that of the reliability of a single component will be shorter, because the system reliability must be multiplied by a product of the reliability of all circuits. We assume that subsystem realisation (area signed as 1 in Fig. 2) is realised perfectly.

The active approach of fault tolerance can be designed with the usage of fault detection and reconfiguration modules. We know that a lot of system architectures can realise the previous task, but it will not be essential for the general conclusion to make analysis of the example presented in Fig. 3.

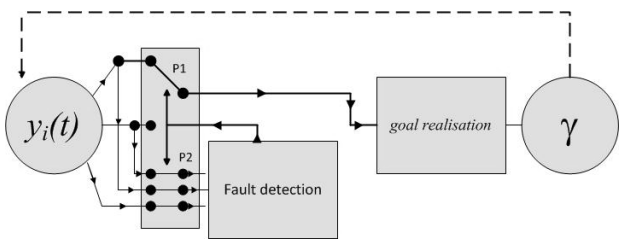

Fig. 3. General schema with fault detection module
Rys. 3. Schemat z modułem detekcji uszkodzeń

The reconfiguration module consists of two switches: P2 which turns off fault detection process and P1 which switches the output signal from signal $y_{i1}(t)$ into $y_{i2}(t)$ if fault in $y_{i1}(t)$ appears as the first fault in the system and is detected. Fault detection process will be turned off when the first difference in signals $y_{ii}(t)$ will be found. It is because in this example it is impossible to make fault localisation process during multiple faults. We can isolate five states: the 1st - all is ok, fault detection is on (FD=on) and realisation of γ_i goal is based on $y_{i1}(t)$ (realise($y_{i1}(t)$) and there is not fault - FD=on∧realise($y_{i1}(t)$)∧fault_in(not); the 2nd - FD=off ∧ realise($y_{i2}(t)$) ∧ fault_in($y_{i1}(t)$); the 3rd - FD=off ∧ realise($y_{i1}(t)$) ∧ fault_in($y_{i2}(t)$); the 4th - FD=off ∧ realise($y_{i1}(t)$) ∧ fault_in($y_{i3}(t)$); and the 5th – system does not work properly. The diagram of changes among the states can be expressed as in Fig. 4.

Comparing the reliability analysis of this solution (Fig. 3) to the previous one (Fig. 2), we can find new proper system states with double failures mode (failures in $y_{i2}(t)$ and $y_{i3}(t)$). We can see that the sequence of faults is important in the final state of the system. For example, if fault of $y_{i1}(t)$ is the first failure in the system and the second is fault of $y_{i3}(t)$, then the system will realise the goal but the system cannot realise the goal. It is the consequence of single fault supposition and turning off the reconfiguration process after the first fault occurrence. Using the Markov model we can estimate the system reliability distribution which is higher than the reliability distribution of the considered earlier systems:

$$R_{reconf}(t)=R_{yi}(t)^3+3R_{yi}(t)^2[1-R_{yi}(t)]+1.5R_{yi}(t)[1-R_{yi}(t)]^2$$

If in our system additional reliable diagnostic information is provided, the system structure will be aimed at parallel structure. We obtain the parallel structure if a diagnostic system can generate information about each signal $y_{ii}(t)$ separately.

$$R_{par}(t)=1-[1-R_{yi}(t)]^3$$

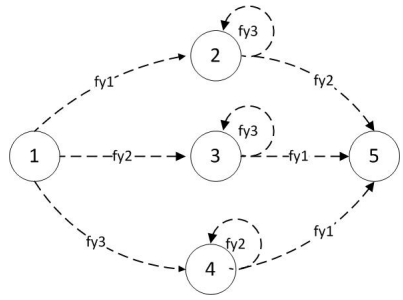

Fig. 4. Diagram of failure state changes
Rys. 4. Diagram zmian stanów zdatności

Finally, we must also make one remark. In process control we cannot activate parallel functioning regulators with integration action, e.g. two parallel connected PI regulators. In these redundancies we must use the standby architecture, but in these we lose some diagnostic information which could be necessary in activation reconfiguration process. From reliability point of view, the standby architecture is very interesting considering its distribution function. For one standby component:

$$R_{s\tan d2}(t)=R_{yi}(t)+\int_0^t R_{yi}(t-t')\frac{d}{dt'}R(t')dt'$$

In Fig. 5 there are shown reliability distribution functions for the presented systems, parallel system and standby system with one standby component. In all cases there was assumed to the exponential distribution of the component.

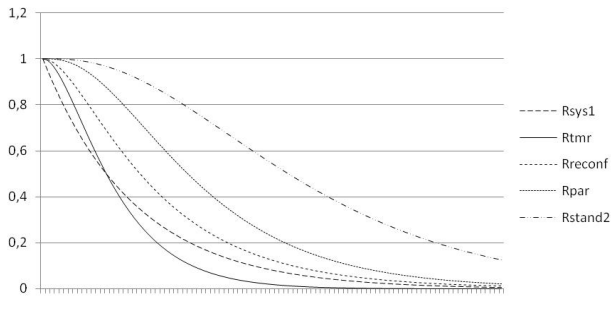

Fig. 5. Reliability distribution
Rys. 5. Rozkłady niezawodności

The basic conclusion for design of ACNS process is usage of active redundancy schema (with FD and reconfiguration) to increase the system reliability. The general ACNS reconfiguration formula was presented by Dolega in the paper [8] published in 2011. It is the deontic formula: "*if* system diagnosis is equal **xx** *do* **yy** *to achieve* **zz**". During ACNS designing we must prove, by theoretic and experimental approach, the paraphrase of this formula: "*if* system diagnosis had been equal **xx** *and* **yy** was done *then* **zz** is achievable". The zz is the goal realised by the designed

system and for ACNS it can be graded by different values of the quality index. These values are conditional on chosen actions **yy**. During reconfiguration process we can use only available in actual moment actions as **yy.** For these reason the trustworthy of fault localisation is very important. Unfortunately, in the real ACNS the fault localisation process is strongly connected with different type of information uncertainty. Moreover, it is a dynamic process because we must remember about system degradation after fault occurrence. Those remarks bring up a question: how to prepare the diagnosed system model to make trustworthy fault localisation decision?

4. Conditions of fault localisation

To make correct reconfiguration process we must possess true fault localisation information. The theme is difficult because we must consider different types of failures. Moreover, the same type of faults can be different in its parameters values. For the most precise fault localisation process we must take several fault detection modules because each of them is sensitive not only to one fault. Additionally, each of them has different parametric sensitivity to that fault. Usually, we can set the minimal parametric value of fault which always is detected by each module. It must be done not only by a theoretic way, but also in practice tests, because this value is dependent not only on the used methods, but also on many specific for the diagnosed object things like the disturbance characteristic, exploitation conditions etc.. Most of the used modules can be classified as dynamic systems. They vary in the time detection delay for the same faults. Creating the correct fault localisation information we can present it as a process of two steps:

- after assumption of occurrence of the localised fault we must collect all its symptoms – *E->S*
- we must make the analysis of correctness of the inverse relationship to the previous one *S->*$\hat{E}$

The inverse relationship can be expressed as the rule: *if S then* $\hat{E}$. The set of symptoms will be created from the results of fault detection modules - *R*, but also different flight parameters represented by aircraft inputs and outputs – *U*, *Y*. As was presented in the previous section, the fault tolerance is realised by dynamic process. This means that actual diagnostic knowledge $\hat{E}(t)$ must be taken into consideration.

5. Fault localisation decision as informatic system

As Dolega suggested in [9] that diagnostic localisation is the dynamical process and can be presented as a rule:

$$\textit{if } S(t) \textit{ then } \hat{E}(t+1), \tag{1}$$

with the set of conditions $S(t) = \{R(t), U(t), Y(t), \hat{E}(t)\}$ and the set of decisions $\hat{E} = \{\hat{E}(t+1)\}$.

The analysed system is a 4-tuple:

$$IS = (X, S \cup \hat{E}, V, f), \tag{2}$$

where: X - is a nonempty, finite set of objects, called *universe*; $Q = S \cup \hat{E}$ - is a finite set of *attributes*; S - is a set of condition (observable) attributes; $\hat{E}$ - is a set of decision attributes; $V = \bigcup_{q \in S \cup \hat{E}} V_q$, where V_q is a domain of attribute q; f - is an *information function* assigning a value of attribute to every object and every attribute, i.e., $f: X \times Q \rightarrow V$, such that for every $x \in X$ and for every $q \in Q$, $f(x,q) \in V_q$.

In the system we cannot distinguish two states $x, y \in X$ using attributes $P \subseteq Q$ if $f(x,a) = f(y,a)$ for each $a \in P$**.** It is defined by Pawlak [10] as the indiscernibility relation - *IND(P)*. This relation is an equivalence relation over X. Hence, it partitions X into equivalence classes. Such partition (classification) is denoted by *X/IND(P)*. When knowledge about our system is represented by the value of attributes, an important problem is to find and express relationships among the attributes. In Pawlak [10] rough sets theory a measure of dependency of two sets of attributes is defined for that purpose. The measure is called a *degree of dependency* of $\hat{E}$ on S (where $\hat{E}$ and S are sets of attributes) and denoted $\gamma_S(\hat{E})$. It is defined as:

$$\gamma_S(\hat{E}) = \frac{card(POS_S(\hat{E}))}{card(X)} \tag{3}$$

The set $POS_S(\hat{E})$ is called *positive region of classification X/IND(*$\hat{E}$*)* (denoted by fault) for the set of condition attributes S. Informally speaking, the set $POS_S(\hat{E})$ contains those objects of X which may be classified as belonging to one of the equivalence classes of $IND(\hat{E})$, employing attributes from the set S:

$$POS_S(\hat{E}) = \bigcup_{Z \in X / IND(\hat{E})} \underline{S}Z \tag{4}$$

where: $\underline{S}Z$ – *S-lower approximation* of $Z \subseteq X$:

$$\underline{S}Z = \cup \{Y \in X/IND(S): Y \subseteq Z\}$$

The coefficient γ expresses numerically objects which can be properly classified. If $\gamma_S(\hat{E})=1$, we say that $\hat{E}$ is *totally* dependent on S in X (the diagnostic localisation rule *if S then* $\hat{E}$ is true). For $0<\gamma_S(\hat{E})<1$ we say that $\hat{E}$ depends to degree $\gamma_S(\hat{E})$ on S (the diagnostic localisation rule is not true).

6. Analysis of fault localisation and system reconfiguration reasoning

Having information system *IS* presented in the previous section, for some faults E and diagnostic methods (attributes S) we are able to analyse $\hat{E}$ - fault localisation reasoning for each fault. The usage of indiscenibility relation in that reasoning allows separating the set $POS_S(\hat{E})$ of well diagnosed states. The set $X \backslash POS_S(\hat{E})$ includes the states with uncertain diagnose. There cannot be detectable or localisable states both for single and for multiple faults. Regardless of that, we can make the optimisation analysis of the whole or of a part of the information system.

If the degree of dependency for one group of condition attributes S_1 is equal $\gamma_1(\hat{E})$ and it is equal the degree of dependency $\gamma_2(\hat{E})$ for the other group S_2, which includes the first group ($S_2 \subset S_1$), then we can find relative reducts of this system. According to Pawlak's definition - a relative reduct T with respects to P **(**$P, T \subseteq Q$**)** is such a minimal subset of the set of attributes R ($T \subset R$, $R \subseteq Q$) which preserves its relation to some classification of subjects:

$$POS_T(X/IND(P)) = POS_R(X/IND(P)) \tag{5}$$

These rules can be allowed during designing the optimal fault diagnosis system. The problem of minimising the number of diagnostic subsystems is equivalent to finding relative reducts of the information system. We can return to wrong diagnosable states included in set $X \backslash POS_S(\hat{E})$**.** We can see that linking the next diagnostic subsystem will supply additional information if the degree of dependency $\gamma_S(\hat{E})$ of decision attributes $\hat{E}$ on condition attributes S will be increased.

When we applied this information during design and analysis of an aircraft control and navigation diagnostic system we decreased the number of residual generators which detected faults in different subsystems. During this process we wanted to find the system, which could provide the maximum quantity of diagnostics information, and also could be the most sensitive to detected faults and quickly functioning. The example of the design of the fault detection system for longitude aircraft control system was presented by Dolega [9]. The system was composed of several residual generators with different fault sensitivity and different delays of detected faults.

The last remark is associated with reconfiguration process. In some aircraft emergency procedures, we allow the system to be degraded. The theoretic design of the system in some of these states is very difficult or impossible, but if we hold the experimental data for different faults and different reconfiguration actions, we can make analysis of the rule "*If* **diagnosis xx** *and* **do reconfiguration action yy** *then* **goal zz is achieved**". After appearance of the faults, the degree of dependency of this formula for the previous goal "**zz**" of the non-faulty system is less than one in most cases. We must change the goal "**zz**" into another one which will be reached by the degraded system. For that goal the degree of dependency must be equal to one, which assures the suitable level of safety. In that way we can analyse the performability properties of the system.

7. Conclusions

The required reliability can be achieved by using different architectures of ACNS. Despite the fault occurrence, the redundancy, fault detection and localisation as well as proper reconfiguration process can assure aircraft safety. Using the presented method of analysis we can design the optimal aircraft fault tolerant control and navigation system for the above-mentioned requirements.

8. References

[1] Advisory Circular AC 23.1309-1C. Equipment, Systems, and Installations in Part 23 Airplanes. Federal Aviation Administration, Washington D.C. 1999, www.faa.gov.

[2] FAR Part 23. Airplanes Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes. Federal Aviation Administration, Washington D.C. 2002, www.faa.gov.

[3] Wu N. E.: Reliability of fault tolerant control system: Part I and II. Proceedings of the 40th IEEE Conference on Decision and Control, Orlando, USA, pp. 1460-1471, 2001.

[4] Li H., Zhao Q. and Yang Z.: Reliability modeling of fault tolerant control systems, International Journal of Applied Mathematics and Computer Science. Vol.17 No.4, pp.491-504, 2007.

[5] Sha L.: Using Simplicity to Control Complexity, Software IEEE. Vol. 18/4 pp.20-28, 2001.

[6] Oxford Dictionary of the US Military, Oxford University Press, 2001.

[7] Prasad D., McDermid J. and Wand I.: Dependability Terminology: Similarities and Differeinces, IEEE Aerospace and Electronic Systems Magazine, Vol.11/1 pp. 14-21, 1996.

[8] Dołęga B.: Some remarks about aircraft control and navigation systems during their subsystems failures presence (in polish) in J. Gruszecki (Eds) Wybrane zagadnienia sterowania obiektami latającymi, Oficyna Wydwnicza Politechniki Rzeszowskiej, Rzeszów 2011.

[9] Dołęga B.: The Rough Sets Theory in Diagnostic Aircraft Control and Navigation Systems, Guidance, Navigation and Control Conference and Exhibit, Monterey, USA 2002.

[10] Pawlak Z.: Rough Sets. Theoretical Aspects of Reasoning about Data. Kluwer Academic Publishers, 1991.

otrzymano / received: 03.07.2011
przyjęto do druku / accepted: 05.08.2011 *artykuł recenzowany*

INFORMACJE

Newsletter PAK

Wydawnictwo PAK wysyła drogą e-mailową do osób zainteresowanych Newsletter PAK, w którym są zamieszczane:
- spis treści aktualnego numeru miesięcznika PAK,
- kalendarz imprez branżowych,
- ważniejsze informacje o działalności Wydawnictwa PAK.

Newsletter jest wysyłany co miesiąc do osób, które w jakikolwiek sposób współpracują z Wydawnictwem PAK (autorzy prac opublikowanych w miesięczniku PAK, recenzenci, członkowie Rady Programowej, osoby które zgłosiły chęć otrzymywania Newslettera).

Celem inicjatywy jest umocnienie w środowisku pozycji miesięcznika PAK jako ważnego i aktualnego źródła informacji naukowo-technicznej.

Do newslettera można zapisać się za pośrednictwem:
- strony internetowej: www.pak.info.pl, po dodaniu swojego adresu mailowego do subskrypcji,
- adresu mailowego: wydawnictwo@pak.info.pl, wysyłając swoje zgłoszenie.

Otrzymywanie Newslettera nie powoduje żadnych zobowiązań ze strony adresatów. W każdej chwili można zrezygnować z otrzymywania Newslettera.

Tadeusz SKUBIS
Redaktor naczelny Wydawnictwa PAK