International Conference
“NEW CHALLENGES IN AERONAUTICS”
ASTEC’07, August 19–23, 2007, Moscow

PRINCIPLE OF ACTIVE SYSTEM SAFETY FOR AVIATION: CHALLENGES, SUPPORTIVE THEORY, IMPLEMENTATION, APPLICATION AND FUTURE

V. Bukov*, V. Chernyshov*, B. Kirk **, I. Schagaev***
**FSUE NIIAO, Zhukovsky, Russia Email: v_bukov@mail.ru*
***ITACS Ltd Stevenage, UK Email: b.kirk@itactsltd.com*
**** London Metropolitan University, Email: i.schagaev@londonmet.ac.uk*

Abstract

Active system safety approach for aviation is presented. An implementation scheme using a typical aircrafts structure is discussed with requirements, models and algorithms, hardware and software features. A reliability gain of the active system safety approach is analyzed. It is shown how active system safety model of an aircraft is organized and features of the main dependency matrix are described. Challenges as well as further potential development and possible projects are briefly introduced.

KEYWORDS: *active safety, preventive maintenance, real time systems, dependency matrix, active black box, monitor of European system safety*.

1. Flight safety aspect

The current state of flight safety in the world has not been changed since 1998. Regretfully for both main players in commercial aviation: Boeing and Airbus the goal to reduce accident rate (from 5 down to 1 per million departures) has not been achieved so far. In turn, intensity of flights, number of aircrafts made, growth of their complexity, and intensification of aircraft fleet use and ageing of an aircraft in action combined do not give any optimism in safety improvement in foreseen future.

On of the reason of this situation is a conservative approach to an aircraft safety, when even existing flight data are used in terms of safety only after a flight. An example of Challenger accident timing (Fig.1) shows that much more could be done to save the situation if an active approach to safety applied [1, 2].

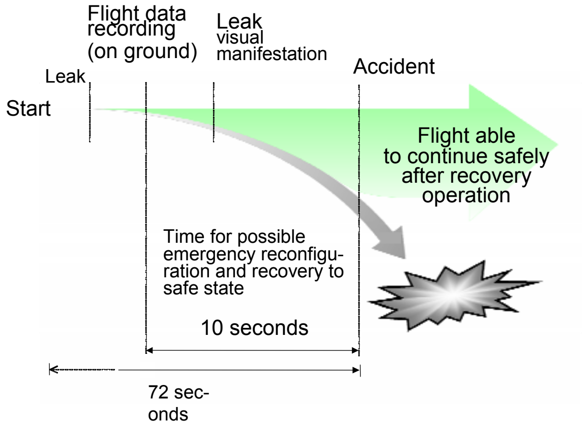

Flight data recording (on ground)
Leak visual manifestation
Accident
Leak
Start
Flight able to continue safely after recovery operation
Time for possible emergency reconfiguration and recovery to safe state
10 seconds
72 seconds

Fig.1. Timing of the Challenger accident

2. Active system safety definitions and scheme

An idea of dynamic (active) safety for an aircraft was discussed initially in early 90’s [3] by authors of this paper and an initial development was supported by ISTC [4] and presented ISSC on 1998, 1999 [1, 3] and currently the prototype development and research granted by EU FP6 [5].

The importance of an aircraft classification for the purpose of formation of a technical portrait including design, technological and management features became obvious. Rigorous classification and further model of mentioned features within one framework enable to analyze impact on aircraft reliability, maintainability, and, therefore, safety. As it was described in details in the project ONBASS (Deliverable 1.1 and Deliverable 1.2) [5]:

…Existing schemes of safety management in aviation are conservative and oriented on strategic goals of after flight (accident) analysis (CA, military) or do not exist (GA).

...All these schemes are easily avoidable by aircraft owners and users, as they depend upon 'human' factor (the weakest link in the chain can't be relied on to fix the chain)...

To avoid known drawback an approach called principle of active system safety (PASS) was introduced.

Definition 1. *PASS is as an approach to continuously evaluate and process the state of an aircraft in real time of flight to define when necessary appropriate RT recovery action or the most efficient scheme of graceful degradation.*

PASS proposes a description of an aircraft as a framework of process oriented information models. These models behave in real time of flight using existing objects, elements and flight data in terms of predicates. The last ones serve as safety guards. The monitoring aircraft safety actively in real time of flight requires an introduction of a special matrix of dependency (DM) between elements. For each element recovery actions (functionally dependent on respected DM elements and reasons of fault) were arranged as recovery matrix (RM).

Both matrices are placed in the specially designed hardware called On Board Active Safety System (ONBASS) together with algorithms of monitoring of active system safety. A generalized scheme of ONBASS is shown on Fig. 2 and in more details on Fig. 3 respectively.

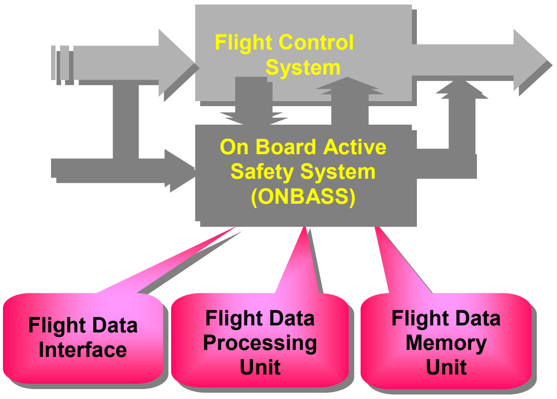

Flight Control System
On Board Active Safety System (ONBASS)
Flight Data Interface
Flight Data Processing Unit
Flight Data Memory Unit

Fig. 2. ONBASS conceptual scheme

Arrows from and to crew as well as from ONBASS to control system as well executive devices provides "activeness" of safety as well as gracefulness of degradation of the system (here aircraft) when a full recovery is impossible. Diagnostic and test hardware units provide automatic on-board and on-ground supportive reliability tests.

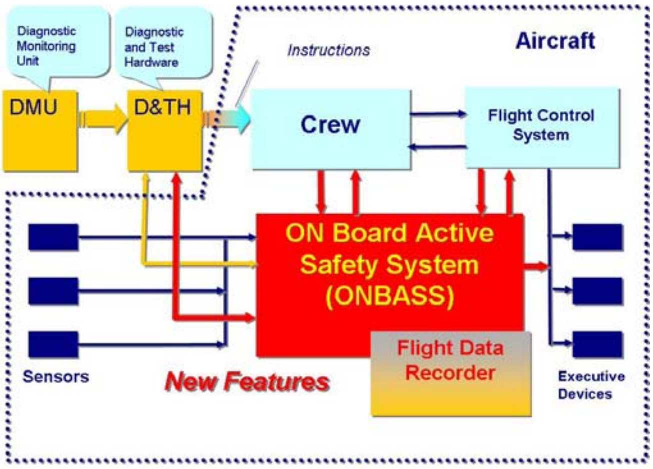


Fig. 3. ONBASS principal scheme

4. Active preventive maintenance

The use of information and communication technologies provides the best basis for introducing an unavoidable scheme of aircraft safety. Hardware/software safety monitors can be applied to exclude the possibility of cutting corners in aviation safety. There is no doubt, this improvement goes at some cost, and thus safety always conflicts with a commercial aspect of aviation. Here we briefly introduce how active safety approach fit the goal of a safety improvement at smaller cost.

A well-known approach of conditional maintenance [6] assumes that state of an aircraft is tested after flight to assure a level of reliability. When reliability reaches defined threshold maintenance takes place. Descending of reliability caused by two main factors: ageing of an aircraft and incomplete testing (denote *coverage* as α_c) of an aircraft conditions.

The *reliability function* with these assumptions is presented below on Fig. 4. The following assumptions were made:

Assumption 1: *Coverage percentage is 100α %, where 0<α<1 and is assumed to be constant over the lifespan of the aircraft for the purposes of this report.*

Assumption 2: *Maintenance is instantaneous and doesn't delay an aircraft use according to schedule.*

Assumption 3: *A threshold of acceptable reliability R_0 exists for R(t).*

Assumption 4: *T_{PM} is not a constant but a variable, actually, a function of several variables, includingα, λ and R_0.*

Reliability is then calculated according (1):

$$\begin{cases} R(t) = \alpha^{(n-1)} e^{-\lambda(t-\sum_{i=1}^{n} T_{PM}(i))}, & \sum_{i=1}^{n} T_{PM(i)} < t, \\ R(\sum_{i=1}^{n} T_{PM}(i)) = R_0, & n = 1,2,\ldots,m. \end{cases} \quad (1)$$

The conditional maintenance drawback is avoidable procedure of testing after flights and therefore there is low confidence in evaluation of aircraft conditions.

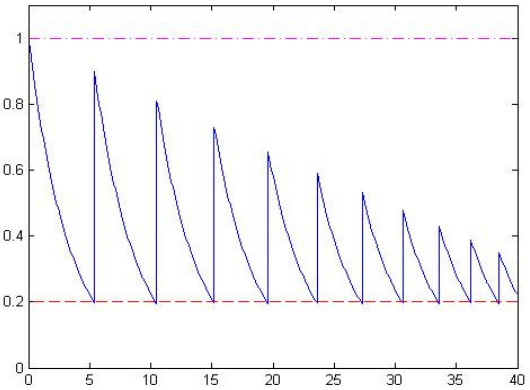


Fig. 4 Reliability assuming conditional maintenance

Activeness of safety is about constant monitoring and prognosis of aircraft state. Adding to the above an <u>Assumption 5:</u> *The period between two successive maintenance inspections is* $T_{PM}(i)$. *Here* $T_{PM}(i)$ *is a variable, actually a function of* i, R_0, α_c, α_m, λ *and* T_{PC}, *where* α_c, α_m *stand for coverage of checking and maintenance respectively.*

The reliability function for the aircraft is then calculated according to:

$$R(t) = R_I \alpha_C^{(n-1)} e^{-\lambda(t-nT_{PC})}, \quad nT_{PC} \le t < (n+1)T_{PC}. \quad (2)$$

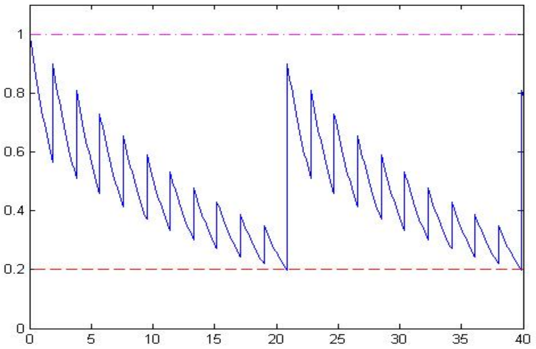


Fig. 4. Reliability with preventive maintenance

The improved efficiency of the preventive over conditional maintenance can be assessed by:

$$y(T_1, T_2) = \frac{V_{PM}(T_2) - V_{CM}(T_1)}{V_{CM}(T_1)} \quad (3)$$

where

$V_{CM}(T_1) = \int_0^{T_1} R_{CM}(t)dt$, $V_{PM}(T_2) = \int_0^{T_2} R_{PM}(t)dt$.

In typical cases the efficiency of preventive maintenance twice outperforms the efficiency of conditional maintenance. Above all, using the active safety approach with real time monitoring of a safety level becomes possible.

5. Active safety implementation

To implement the active safety approach additionally to ICT fault tolerance and extreme reliability new models of an aircraft as mentioned previously are required to embrace analyzed and monitored features in terms of safety.

When there are symptoms that system is faulty (with differences or deviations from a scheduled scheme, behaviour or rules) it is required to determine “guilty” element(s). Well-developed analytic solutions [7] for the localization problem are based on very strong assumptions about an analyzed system and fault model information, including “simple”, i.e. single faults. In turn, practice vote for multiple fault assumptions.

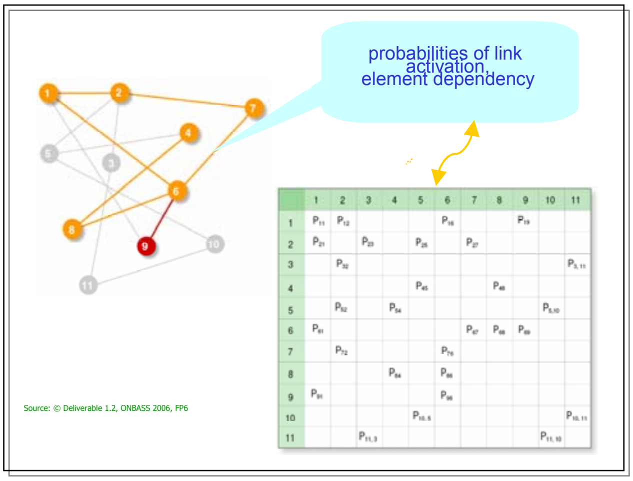
Above all, probabilistic models using for *location* of a faulty element for real time systems are not always adequate. Recovery and/or graceful degradation needs fault monitoring, thus… new models of an aircraft in terms of system safety are required. Fault tree analysis (FTA) does not fit the goal of active safety as it assumes an existence of predefined scenarios. Also, there must be Markovian property of the fault propagation over the analyzed system in advanced FTA scheme.

6. Dependency and recovery matrices

To avoid FTA drawbacks an aircraft for the purpose of safety monitoring was described as a dependency matrix (DM). DM consists of three main areas DM_{fd}, DM_{fm}, DM_{ae} that reflect dependencies of flight data, flight modes and aircraft elements (devices, sensors, actuators etc.) The last area (DM_{ae}) affiliates also to recovery actions arranged as a sub-matrix that mirrored in structure of element dependencies in terms of recovery actions that may require. Clear that the elements and reasons of a fault combined *define* recovery or controlled degradation actions. A recovery matrix is defined as RM_{ae}.

An example of DM_{ae} and its “probabilistic” mirror of DM is presented on Fig. 5. Note that weighted dependencies are affiliated to graph edges and not vertices. Note also that Markovian property of DM_{ae} does not hold for the probabilities of possible transitions between the *i*-th and *j*-th elements from DM_{ae}.

The probabilistic dependence of, say elements the *i*-th and *j*-th elements, in terms of fault dependence, i.e. a fault of one element probably causes (induces) a fault of another. It is also assumed that there are possible inequalities of conditional probabilistic dependencies in opposite directions: to and from elements.



	1	2	3	4	5	6	7	8	9	10	11
1	P_{11}	P_{12}				P_{16}			P_{19}		
2	P_{21}		P_{23}		P_{25}		P_{27}				
3		P_{32}									$P_{3,11}$
4					P_{45}			P_{48}			
5		P_{52}		P_{54}						$P_{5,10}$	
6	P_{61}						P_{67}	P_{68}	P_{69}		
7		P_{72}				P_{76}					
8				P_{84}		P_{86}					
9	P_{91}					P_{96}					
10					$P_{10,5}$						$P_{10,11}$
11			$P_{11,3}$							$P_{11,10}$	

Source: © Deliverable 1.2, ONBASS 2006, FP6

Fig. 5. Dependencies of aircraft elements

In other words, for the *i*-th and *j*-th elements, two probabilities P_{ji} and P_{ij} are defined and generally $P_{ij} \neq P_{ji}$. The probability matrix for the graph on Fig. 5 defines diagnostic features of DM_{ae} for each particular implementation. It generalises the well-known fault tree scheme and introduces a flexible ordering using informational, structural or time redundancy [8].

Evaluating a set of processes defined on DM_{ae} provides a powerful tool to analyse possible consequences of faults that appear in the aircraft. Three processes are defined on the matrix presented above: detection of possible consequences of a fault determination of “the locus or loci”, and preparation and performing of recovery actions.

The first process is about making a prognosis about a possible flow of events. It is initiated by information derived from flight data analysis regarding existing systematic discrepancies, such as approaching of flight data margins for current flight mode, speed of data decline or growth etc. The processes are developed as an algorithm of diagnosis and prognosis.

The second process implements the evaluation of a possible reason, or reasons, for the manifestation of the discrepancy. The method and the apparatus for active system safety are patented [9]. Recovery process is based on backward search over DM_{ae} and includes signals for a pilot, automatic switch off or reconfiguration of aircraft equipment, etc.

A DM complete structure is presented on Fig.6. Note that complexity of a DM structure grows linear to flight information (flight data dependency quadrant) and aircraft structure (element dependency quadrant).

	Flight data	Flight mode	Aircraft elements
Flight data	Flight data self-dependencies	Flight data margins per flight mode	Flight data affiliation to aircraft elements
Flight mode		Flight mode self-dependencies	Dependencies aircraft elements upon flight mode
Aircraft elements			Element dependencies such as Fig. 5

Fig. 6. Structure of dependency matrix

7. Future of active safety: ABBA and MESSA

Principle of active system safety with challenges and implementation aspect was discussed. The project ONBASS proved active system safety possibility for GA and CA.

Results have high IPR potential and, if implemented, will restore EU leadership in aviation and aerospace safety domains.

Further development of active safety implementation is two-fold. At the aircraft level this is an Active Black Box for Aviation (ABBA) as a new device that performs active safety monitoring as well as provides existing functions typical for accidental data recorders. At European level it is a Monitor of European System Safety for Aviation (MESSA). More above ABBA and MESSA see [10].

The last one will provide real time monitoring of aircraft health during flight and maintenance over Europe as a whole. The whole picture of European ATC therefore might be updated with safety status for every aircraft over Europe.

There is no doubt that maximize aviation safety using the proposed active safety approach a widening of cooperation/collaboration among research EU and Russian leading centres, regulatory bodies (Eurocontrol, EASA) and manufacturers EADS, Airbus, Galileo JU are required. Taking into account that active safety for aviation involves flight operators, regulatory bodies, aircraft manufacturers as well as avian companies and user coordination of this research is required at EC level.

8. References

[1] I. Schagaev, *Concept of Dynamic Safety*, ISSC, Proc. of the 16th Int. System Safety Conference, 444-452 (1998)

[2] I. Schagaev, S. Plyaskota, *The Concept of Dynamic Safety for Aeroplanes*, Air Fleet Herald, 7 (1996)

[3] I. Schagaev, L. Overtoon, *Active Safety System for General Aviation*, Proc. of the 17th Int. System Safety Conf., Orlando, Florida (1999)

[4] www.istc.ru/istc/sc.nsf/html/projects.htm=1553

[5] www.onbass.org

[6] S. Birolini, *Reliability Engineering*, Springer (2006)

[7] V.N. Bukov, A.P. Bazanov etc. *Theoretical foundations and mean of automatic testing*, Moscow, Zhukovsky Air Force Engineering Academy (1997)

[8] J. Zalewsky I. Schagaev, *Redundancy Classification and its Applications for Fault Tolerant Computer Design*, IEEE TESADI-01, Arizona, Tucson (2001)

[9] *Method and apparatus for active system safety*, Patent GB 0707057.6

[10] www.itacsltd.com/projects.html