THE CONCEPT OF DYNAMIC SAFETY

Igor Schagaev

IT-ACS LIMITED, 157 Shephall View, Stevenage SG1 1RR
info@it-acs.co.uk

Abstract

Based on analysis of Operating Cycle of airplane the model to evaluate level of safety was introduced. Steps of modernization existed system of safety was introduced and requirements to hardware and software presented. On-board hardware functions and reliability requirements have been analyzed and the structure of hardware was presented and realized. The structure of full size system to provide the Concept of Dynamic Safety was developed and presented. Economics of the Concept realization was presented, it was proved that substantial profit and higher level of safety may be achieved provided the Concept of Dynamic Safety.

Keywords

Safety Critical Systems, Dynamic Safety, Fault Tolerance, Life Cycle, Economic Effectiveness.

INTRODUCTION

Successful operation of sophisticated technical devices over provision of safe application is among most burning tasks at the today level of technological and social development. Importance of its solution is underscored by extensive application of sophisticated technical devices and systems. Their amount, especially in the economically developed countries, threatens to surpass in the future the biologically tolerable limits. Safety is an all-important factor of the span of their lifetime. Besides, the need in additional investments operational safety makes us economically dependent on technological innovations. If money investments are insufficient, we can meet with unpredictable growth of risk involved in operating the equipment. Risk grows with the amount and complexity of technical devices involved in everyday life. The available information on accidents with stationary installations (Chernobyl nuclear power plant) and vehicles such as Challenger, and several Boeing 747 crushes indicates that until now basically sound structure was not satisfactory developed for providing safety of an object and the "object-environment" system. Safety provision of vehicles such as aircraft, spacecraft, trains, ships, cars, etc., is of special importance because any serious technical failure in them could result in casualties and a lot of them. To cope with the mentioned problems A Concept of Dynamic Safety (CoDySa) has been developed during 1990-1996, working prototype of the system to realize this Concept has been developed and tested on airplane. Here this concept is presented together with short results of trial application for a real airplane.

1. OPERATION CYCLE

Consider the operation cycle of a airplane to which extremely strict safety requirements are presented. Divide the flight cycle into the following stages: take-off, flight proper, and landing. Regarding safety, successfully completed cycle is that ends with safe landing of the aircraft, crew and passengers, if any. If operation cycle completes with loss of the aircraft, crew or passengers, it is regarded as catastrophic. In terms of reliability, provision/improvement of aircraft safety, obviously, means actions for successful completion of the operation cycle as shown in Fig.1.

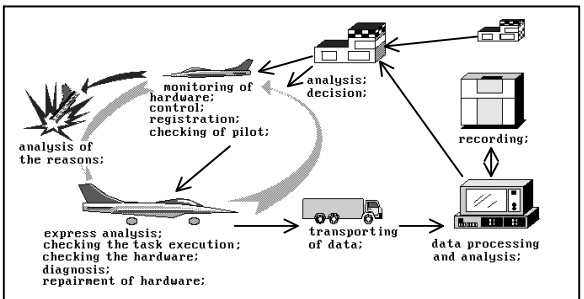

Fig.1. The model of information interaction

The existing Systems of Objective Checking (SOC) of aircraft and its related controls based on the assumption that the greater is the amount of data about safety-critical devices, the better its in-flight conditions can be evaluated and correct recommendations worked out from post-flight logistic analysis. Mentioned above accidents, however, indicate that in spite of fairly complete information on aircraft state and on-board events

such as leakage, engine troubles, pilot's errors, there was no way of avoiding them. This is mainly due to erroneous (in terms of information and, especially, hardware) organization of the safety system. Consider the well-known SOC (System of Objective Checking) structure (Figure 2). Sensors send information to the control system and also, sometimes in a processed form, to the flight recorder. Train SOC system generally organized by similar way. The main SOC functions in these and similar systems are oriented to COLLECTING, REGISTRATION and STORING of information on safety-critical devices *during* their mission.

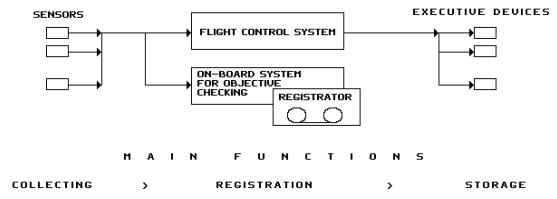

Figure2. Main structure and functions of the on-board systems for objective checking

The today trend in SOC safety is to employing flight recorders featuring greater volume of stored data, reduced size and weight, and higher environmental tolerance. It might be well to underscore that sequential data recording with mechanically translated carrier imposes on the SOC system certain functions and structure. In some extremely complicated systems such as Shuttle and test SOCs, the on-board information is sent to the ground-based part of the system where it is again tape-recorded. According to the available information on the Challenger accident, namely owing to this SOC system organization that nothing was undertaken to save the situation, although all necessary data on the state of the spacecraft and its systems were available well before the explosion (Figure 3).

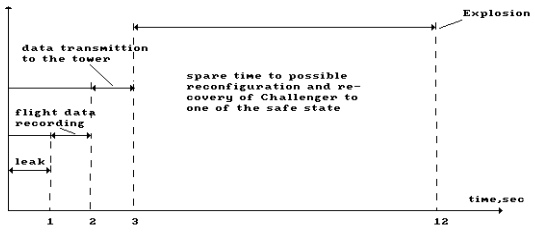

Figure 3. Challenger case

The experience gained in Russia indicates that the time required for jettisoning a fuel tank and/or a stage is 0.1 sec at most, that for cabin with crew, 0.2 sec. Therefore, one could have benefited from the 10 seconds that were left before the explosion.

The above said enables first tentative conclusions concerning the structure of future SOCs.

-The major sources of faults and accidents of vehicle are as follows: mechanical elements (body, engine, wings, fuselage, car suspensions, etc.); control system and its components: (electronic equipment; software; human operator (pilot).

-SOC informational interaction in terms of safety is basically incorrect and demands redesign. In fact, the objective checking systems as are operated by the today aviation are ensuring "safety" of the red tape of the manufacturers, of those responsible for flights, etc., instead of protecting pilots and their crews, passengers, population, and environment against flying vehicle crashes and their consequences.

- To ensure safe operation of flying vehicle, the flow of data on its state must be real-time processed so that either to eliminate the imminent accident, or to minimize its consequences. The flying vehicle itself (or any other vehicle) should be designed so that its safety checking facilities are supported by adequate facilities for elimination of the causes of undesirable effects such as blocking, equipment reconfiguration, restoration of vehicle operability.

2. MODERNISATION STAGES AND OUTLOOKS

Replace in the SOC tape-based memory to RAM-based storage (Figure 4).

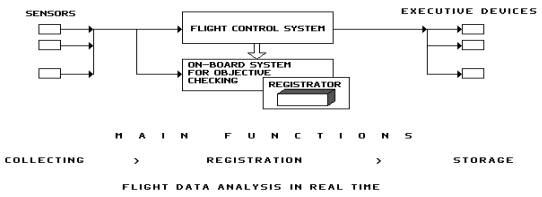

Figure 4. Modernization, first stage

For identical size, magnetic tape capacity exceeds that of RAM by the factor of 3 - 4. Nevertheless, RAM-based devices can be regarded as acceptable taking into account the fact that RAM accompanied with processor to compress and manipulate the flight information eliminate factor of capacity.

Note that RAM-based SOC devices support real-time access to the main parameters stored. Besides, the experience with handling and compressing the on-board information shows that the average compression factor varies between 9 and 12. Then, in terms of the main parameter, storage capacity, the RAM-based devices become more attractive. Another argument in favor of the RAM-based storage is that the concurrency of their recording and data analysis times allows one to check the flight control system

itself. (The arrow from the control system into the on-board objective checking system.) . Replacement of tape based SOC devices to RAM-based would enable higher sensor sampling frequency and accuracy of stored data. A powerful microprocessor core (Power PC, SPARC or ALPHA) built-in into the on-board part of SOC would enable real-time analysis of the main accident sources of flight vehicle (FV).

Consider now another phase of objective checking system modernization (Figure 5).

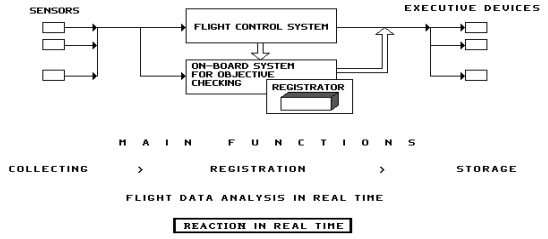

Figure 5. Modernization, second stage

As soon as a processor appears in SOC, one can, besides input compression, analyze data and forecast future trends, and also prevent possible undesirable effects, provided that there are corresponding facilities. SOC reliability, obviously, should be an order-of magnitude higher than that of the rest of FV equipment. Strictly speaking, the term SOC is obsolete for such a system. Its new functions let us call this system on-Board Active Safety System (BASS). Notably, BASS does not replace control system and pilot controls, but supports dynamically maximal flight safety.

3. BASS IMPLEMENTATION: TECHNICAL LIMITATIONS AND FEATURES

Reliability is the major concern in design and practice problem of this system. According to the estimates of Western experts, the existing tape-based on-board objective checking systems have 200 to 250 thousands hours of mean time to failure. At the same time, the similar characteristic of the today RAM-based systems and computers for the same applications is half as many. Some successful attempts have been done at the industrial level by DDC (USA). Anyway, as compared with the tape-based systems, the majorette computing systems with tripled units, first, feature comparable size and mass parameters and, second, have great edge over them in terms of power consumption. BASS prototype has been done and factory tested during 1990-1994. The major hardware designs are described in the section below. Here it is presented the technical features involved into design and production of solid-state storage (Figure 6) which must be solved to achieve a required structure of SOC.

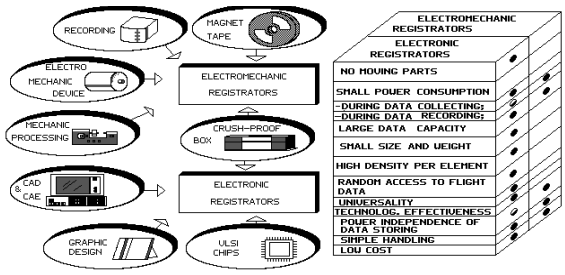

Figure 6. Technological features of on-board flight recorder design

Note here that additionally to existed advances Solid-state RAM storage would require intensive use of several CAD systems, and solution of the problem of control of *dynamic hardware redundancy* with the aim of providing high reliability. Design and/or buying of customized or semi-customized elements also involves certain financial costs.

4. BASS STRUCTURE

As any on-board unit, BASS is logically divided into two major zones (Figure7), *active* and *passive*. The former zone contains the processor and interfaces, and executes input data format in and handling. Specific features of the structures of each zone are essentially different. Today, the count of logical elements in the *active* zone is about 3 billion, the interconnections being extremely involved.

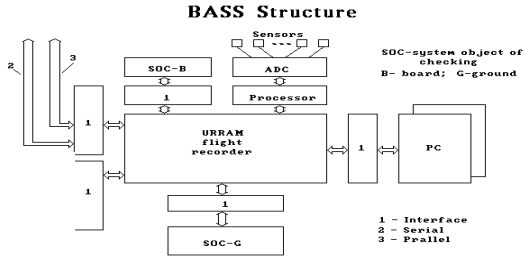

Figure7. BASS structure

The structure of the *passive* zone, on the contrary, is extremely regular, but the count of logical elements (equivalent gates) exceeds 240 million. Undoubtedly, the structural features of both zones impose certain design decisions concerning their reliability and fault-tolerance. The main principles of providing fault-tolerance in such systems are presented in (Shagaev, Stepaniants, 1987). Taking into account the current patenting procedure of the structures of both zones, mention here only that dynamic safety concept was preceded by the theory of computer system redundancy. This application of this approach

enables BASS to attain the following reliability performance of the entire system: mean time to failure 700,000 hours, dynamic availability over the whole operation circle is 0.98 at least. Reliability figures for *active zone* are about 750,000 hrs with hardware redundancy about 30%. Reliability figures for *passive zone* substructure slightly different for user and system areas - 710,000 hours for user storage part realized by sliding dropping reserve and 700,000 hours for system area of *passive* zone which realized by modified triplication. The existing BASS comprises three ARINC boards, two boards of electronics and one of universal adaptive power supply. Figure 8 depicts some of elements on the most complicated data processing hardware. The general view of the whole system to realize the CoDySa is given in Figure 9.

Figure. 8. On-board hardware for CoDySa

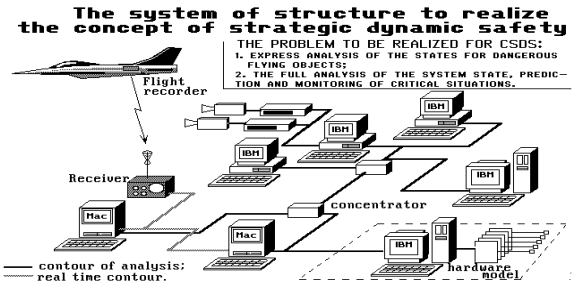

Figure. 9. The system of structure to realize the Concept of Dynamic Safety.

Modern electronic technologies use for the BASS design promise size reduction for the BASS core to a cigarette package, the reliability indices being the same or even higher. In more details the passive zone of BASS organization has been presented in (Shagaev, 1990 and 1992-1993).

5. FV DYNAMIC SAFETY SYSTEM

For provision of really safe operation of the existing, intensively operated FVs, a ground-board safety system may be realized as shown in Figure 9. It has coupled rings of two local area networks at the aerodrome enabling fast in-flight FV state analysis, automated flight preparation and servicing, and also, if using the available software and hardware simulators, profound analysis of FV state, pilot's actions, etc. Real-time tasks are executed by the local area network using advanced computers; the informational and organizational ones (including personnel training), are solved by the local area network by PC-compatible computers. This combination enables essential reduction of the total system cost at acceptable total throughput. It should be especially emphasized that the system and its functions are equally important for civil and military aircraft, aerodromes and regiments.

There exists still one specific military task that can be solved within the framework of the concept of providing dynamic strategic safety. Taking into account that the armament state defines danger of operating FV and its combat readiness, realization of the proposed ground-board BASS would guarantee safety of the military FV carrying strategic armament and make it maximum effective (Figure 10).

Importantly, within the framework of interaction with the allies, global safety of justified and timely use of the weapons is one of the major concerns. Agreements on information about deployment and state of FVs supplied with on-board BASS would contribute to international confidence, and, simultaneously, expand the application domain of the systems under consideration. Provision of maximal vector safety is another important domain requiring critical analysis within the framework of dynamic

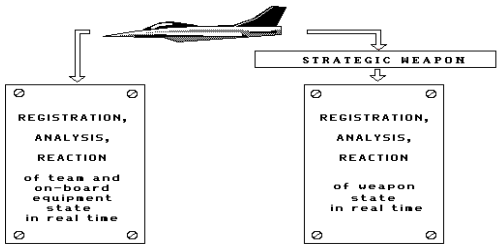

Figure 10. Concept of Dynamic Strategic Safety

safety concept. Safety vector is as follows: different exceptional situations may occur in flight for which certain actions of crew, equipment and mechanical devices are assumed. FV itself flies over areas differing in terms of safety such as towns, aerodromes, nuclear power plants, military

objectives, etc. Not all-autonomous safety measures are acceptable for any area crossed during flight. For example, fuel tank jettisoning is acceptable for emergency over open sea and absolutely unacceptable over towns, aerodromes, and other dangerous military and industrial objectives. Thus safety provision becomes a vector task.

6. PROGRAM AND PROJECT ECONOMICS

An economic effectiveness of fault-tolerant equipment for the long run applications has been analyzed. This subject has been briefly presented at the IFAC symposium (CIM) in December 19, 1992 and IAP 1995 Annual Conference. Phases of the life circle for any serious project and their relationship with negative feedback caused by errors and slips during each phase presented of Figure11. Then, to simplify simulation the aggregate states have been grouped and simulation of cost value for the whole life circle has been done.

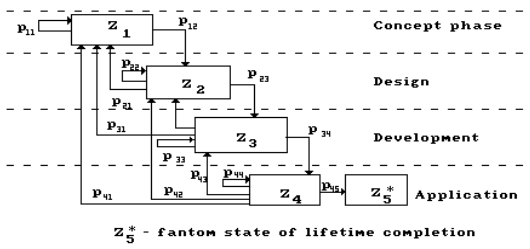

Figure11. Reduced structure of lifetime model

Comparative analysis of well known and modern project approaches such as Design For Manufacturing (DFM), Quality For Manufacturing (QFM) have been analyzed to compare with design of fault tolerant systems (DFTS). All major phases of expenditures have been taken into account: Concept, Design, Development, Production and Maintenance (Figure12). It was shown that cheaper exploitation of long lasting products one can achieve using DFTS methodology, including the safety systems of moving vehicles.

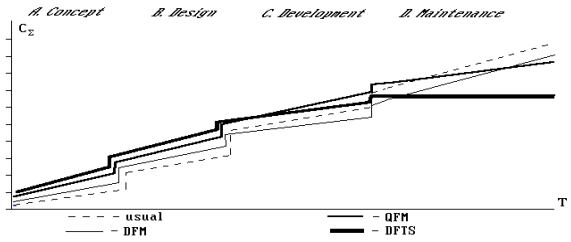

Figure 12. The comparative economic effectiveness of DFM, QFM and DFTS

CONCLUSIONS

1.Existed structure of System for Objective Checking provides only passive safety of flying vehicles.
2.The new Concept of Dynamic Safety (CoDySa), the principles and variants of its realization are proposed, and hardware reliability requirements are formulated.
3.Approaches to attaining the desired reliability are discussed, and appropriate hardware structures are proposed.
4.Fault-tolerance of avionics electronic system is shown to reduce substantially the overheads of aircraft operation.

REFERENCES

Schagaev, I., A. Stepaniants (1987). Malfunction Tolerant Ultra Reliable Processor with Reduced Instruction Set. In: *Proc. IMEKO 1987*, Prague

Schagaev, I. (1990). Yet Another Approach to Classification Of Redundancy. In: *IMEKO Congress*, pp 117-124, Helsinki, Finland.

Schagaev, I., et al. (1992). Fault Tolerant RAM With Extremely High Reliability, Part1. *Automatic and Remote Control*, **No.3,1992**

Schagaev, I., et al. (1993). Fault Tolerant RAM with Extremely High Reliability, Part2. *Automatic and Remote Control*, **No.2, 1993**

Schagaev, I. (1991) The Economic Model Of Fault Tolerant System Design And Development. In: *Proceedings of IFAC CIM Workshop*, Helsinki, 1991, December 18-19.

Schagaev, I., S. Pliaskota (1995). Economic Effectiveness Of Fault Tolerance, *Automatic and Remote Control*, **No.7, 1995**

Schagaev I., Pliaskota S. (1996) BASS: on Board Active Safety System - Active Control of Safety. *Flight Review*, **No. 7-8,1996**