SYSTEM SAFETY PROGRAM REQUIREMENTS

Bertold BÉKÉSI
Senior Lecturer
„Miklós Zrínyi" National Defense University
Department of Aircraft On-board Systems

The purpose of the author is to present a System Safety Program Requirements in accordance with MIL–STD 882. This article deals with the definitions of system safety, general goals for system safety, organization and responsibility, design criteria, hardware and software analysis, special analysis, accident causes, supportability, accident risk contribution budget, Prediction of maintainability parameters, verification of mean time to repair (MTTR).

INTRODUCTION

After defining main formulas of reliability theory and qualifying parameters, which help us to be able to examine the reliable work of a technical system the main activities will be determined by the author. In the article there will be presented activities and special efforts made by the aircraft constructors and manufacturers in order to create necessary conditions of safety and reliable maintenance. Since the requirements of system safety program are included in the military standard MIL–STD–882, therefore this matter is going to be introduced by me on the base of standard mentioned above. In the following the brief description of main principles, definitions and the process of realization will be outlined.

SYSTEM SAFETY

The optimum degree of safety, for the complete aircraft, equipment and support systems, within the constraints of operational effectiveness, time, and cost attained through specific application of system safety criteria, established in plan development from MIL–STD 882.

By applying these principles, hazards have been identified and risks have been minimized and will be controlled throughout all phases of the system life cycle.

GENERAL GOAL FOR SYSTEM SAFETY

The high level has been achieved through various coordinating measures such as:

- an efficient man–machine interface;
- good flight characteristics;
- high system reliability;
- safety measures;
- high availability;
- and good adaptation to service and maintenance personnel.

Due to material or system failures the low accident rate has been attained through redundancy in all systems, especially those emergency systems designed to make home-flight and landing possible in a situation with degraded system functions.

As a general goal for accident rate, the maximum mean value during service use after 100 000 flight hours (FH) must not exceed a stated number of aircraft lost per 100 000 FH. Of those not more than 50% may be caused by material or system failures.

ORGANIZATION AND RESPONSIBILITY

The general goal for a high level of system safety has been achieved primarily by those responsible for the design of the aircraft and its systems.

A program defining necessary requirements to reach the goal and according to the intentions in the plan has been carried out for each object or system.

The high level function for system safety has the overall responsibility for the requirements of the system safety program plan being followed during the whole project. This function reports directly to the project management, where system safety is concerned.

DESIGN CRITERIA

The design criteria have, in the following order of priority, guided the design of the aircraft in order to minimize potential hazards:

- The design shall eliminate hazards as much as possible.
- Hazards that cannot be eliminated through design, selection or safety devices shall be minimized as to their effect so that they can be controlled.
- When neither design nor safety devices can effectively eliminate or control an identified hazard, an adequate warning system shall be introduced to provide for an emergency procedure, that can minimize the effects.
- Where it is impossible to eliminate or control a hazard through design, safety devices or warning devices, the risks should be avoided through restrictions, special instructions etc.

HARDWARE ANALYSIS

Each system has been analyzed and reviewed to find potential hazards. Procedures used are as listed below:

- Various types of hazard analysis: preliminary hazard list (PHL), preliminary hazard analysis (PHA), fault/failure hazard analysis (FHA) etc.
- Failure mode effects analysis (FMEA) and failure mode effects criticality analysis (FMECA)
- Fault tree analysis (FTA)
- Maintenance analysis, maintenance steering group–3 (MSG–3)
- Analysis related to missions and human factor functions

SOFTWER ANALYSIS

In the aircraft there are more computers in interconnected through a data bus system. Each signal has been analyzed and its criticality determined.

I Catastrophic — critical
II Critical — essential
III Marginal — essential
IV Negligible — non-essential

Signals belonging to categories I and II are specially processed and tested.

SPECIAL ANALYSIS

Incidents affecting exposed areas of spaces in the aircraft have been analyzed by special cross-functional groups. Types of incidents examined are:

— Bird Strikes;
— Fire;
— Foreign object damage (FOD)

ACCIDENT CAUSES

As it was mentioned previously, it is planned that accident risk may not exceed 50 % of the general goal for accident rate due to technical reasons (material or system).

Accidents can be caused by the following reasons:

— Technical reasons (materiel or system failure);
— Pilot function;
— Technical personnel function;
— Other „external" reasons.

The last three are together called „OTHER REASONS".

In the following I will briefly review the concrete planning conditions and requirements and some examples concerning them.

SUPPORTABILITY

During planning process and production the main characteristics to be reached are listed below:

— High reliability – determine mean time between failures in flight hours
— Low maintenance requirements:
  - Maintenance man–hour per flight hour (O, I and D level);
  - Mean time to repair in hour.
— Excellent testability:
  - Depends on fact how many % of serviceable faults can be indicated by line replaceable unit (LRU);

- How much maintenance ground support system (MGSS) is needed to cope with the fault.

— Outstanding turn–around performance:
- fighter mission;
- ground attack.

ACCIDENT RISK CONTRIBUTION

There are about 25 material groups (MG) involved in the system safety program. Each MG has been given an accident risk contribution budget of its own. The budget states the sum of the maximum accident risk contribution of all known flight safety critical failures for the MG.

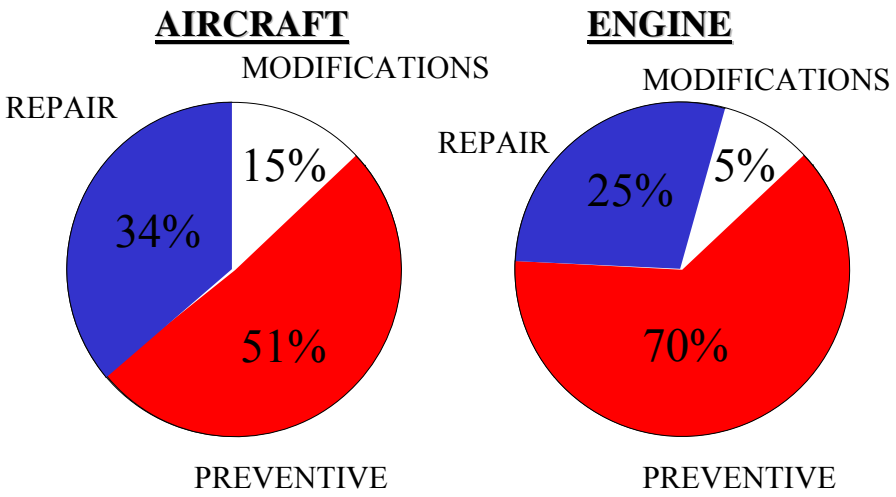
The total sum of all the accident risk contribution budgets of the material groups may not exceed:	25%
Reserve for unquantified and unanticipated failures:	25%
Technical failures total may not exceed:	50%

ACCIDENT RISK CONTRIBUTION BUDGET ADAPTED TO SWEDISH DEMANDS

The general goal for maximum Accident Rate is distributed to the MG in %.

MATERIAL GROUPS	%	MATERIAL GROUPS	%
Aerodynamics	1,0	Gun and Weapon/Ex Stores	0,5
Strength/Structure	1,0	Power Plant/Installation	1,0
Crew escape and oxygen supply	0,5	Engine	10,0
Landing gear	2,0	Avionics	0,5
Flight control	1,0	Target aquisition	0,2
Hydraulic supply	0,5	Display/Video recording	0,2
Environment control system	1,0	Reconnaissance	0,1
Fuel supply	1,0	Weapon delivery	0,5
Auxiliary power supply	0,5		
TOTAL SUM			22%
Reserve for unquantified and not anticipated failures			28%
Technical failures total:			50%

MAINTENANCE COST



DESIGN REVIEW

During the design process of the following special care must be taken of:

- possibility to perform required maintenance;
- feasibility of selected maintenance method;
- access in the aircraft;
- need of tools and other GSE (special or standard).

PREDICTION OF MAINTAINABILITY PARAMETERS

Parameters:

- Downtime per flight hour;
- Maintenance man–hours per flight hour.

DEFINITION OF DOWNTIME PER FLIGHT HOUR

Downtime per flight our includes the following elements:

— Turn around activities;
— Preventive maintenance on–aircraft;
— Corrective maintenance on–aircraft.

MAINTENANCE MAN–HOURS PER FLIGHT HOUR

Maintenance man-hours per flight hour includes the following elements:
— Turn around activities;
— Corrective maintenance on–aircraft;
— Preventive maintenance on–aircraft;
— Corrective maintenance off–aircraft;
— Preventive maintenance off–aircraft.

Preventive maintenance man–hours on–aircraft

The preventive maintenance man-hours on-aircraft includes:
— Include man–hours for minor and major inspections;
— Inspection activities are defined using maintenance need analysis according to MSG–3, adapted to military aircraft;
— Maintenance intervals are based on economic and reliability considerations besides safety requirements;
— Maintenance man–hours per inspection have been predicted by estimating the time for each task, that is included in the inspection;
— Verification of the minor inspections has been made by demonstration.

Preventive maintenance man–hours off–aircraft

The preventive maintenance man-hours off-aircraft includes:
— The preventive maintenance of units has, as for preventive maintenance on aircraft, been defined using maintenance need analysis according to MSG–3 adapted to military aircraft;
— Maintenance intervals have been based on economic and reliability considerations;
— Predictions of man–hours are based on vendor predictions, which have been revised after review and comparison with earlier experience from similar equipment in co–operation with workshop level personnel.

Corrective maintenance man–hours on–aircraft

The corrective maintenance man-hours on-aircraft includes:

— They are depending on mean time between failures (MTBF) and mean time to repair (MTTR) plus the required number of men for the different tasks;
— Have been predicted and verified in the same way as MTBF and MTTR.

Corrective maintenance man–hours off–aircraft

The corrective maintenance man-hours off-aircraft includes:
— They are depending on MTBF and direct man–hours for repair of each unit;
— Direct man–hours for repair of units have been predicted by equipment vendors;
— Vendors' predictions have been revised after review and comparison with earlier experience from similar equipment in co-operation with workshop level personnel;
— Consideration has also been taken to the depth of repair according to decisions from repair/discard analysis.

VERIFICATION OF MEAN TIME TO REPAIR

For a number of selected line replaceable units (LRU) with a significant contribution to the down time a demonstration program for replacement (including preparation work and necessary work after replacement) has been performed.

Prediction of downtime caused by corrective maintenance can be found as:

$$DT_C = MTTR/MTBF = \Sigma(MTTR_i/MTBF_i) \quad (1)$$

$$MTTR_i = R1 + R2 + R3 + R4 + R5, \quad (2)$$

where R1 through R5 represent times for
— R1 Preparation
— R2 Fault localization
— R3 Replacement
— R4 Miscellaneous
— R5 System checkout

Each of these time elements are predicted separately. For example look at the mean time between failure definitions.
The failure rate λ can be determined as follows

$$\lambda = \frac{Failures\ frequency}{Flight\ hour} \tag{3}$$

$$MTBF = \frac{1\,000\,000}{\lambda} \tag{4}$$

$$\lambda = \frac{1\,000\,000}{MTBF} \tag{5}$$

This is value for example for the 4th generation aircraft GRIPEN:

Previous Generation Aircraft

CONCLUSIONS

In this study there was made a brief introduction to system safety program requirements. The main principles, definitions and the processes of realization have been presented. Consequently, the activities during design and development should be the followings:

- Analysis of requirements;
- Formulating goals;
- Experience previous aircraft;
- Discussion Vendors;
- Prediction of reliability and maintenability;
- Impact on design;
- Design reviews;
- Collection of experience;
- Maintenance analysis;
- Definition of logistic resources;
- Establishing of assumptions (maintenance concept);

— Dimensioning of logistic resources.

It can be seen clearly, that the maintenance is accomplished with the close cooperation of the constructor and the manufacturer, where the estimated data taken in advance during planning, are finalized or even corrected with the supervising equipment built by the manufacturer.

REFERENCES

[1] BÉKÉSI BERTOLD: A repülőszerkezetek műszaki karbantartása. Repüléstudományi Közlemények, Szolnok, 1999/3, 93–104.o.

[2] DAVID Learmount: Preparing for safety. Flight International 25. 01. 2000 pp 56-59.

[3] ÓVÁRI GYULA: Nyugati és Szovjet gyártmányú légi járművek együttes üzemeltetésének, valamint repülő mérnök-műszaki biztosításának lehetőségei az MH repülőalakulatainál. Egyetemi doktori értekezés, 1994.

[4] DR. ÓVÁRI GYULA: A Magyar Honvédség repülőeszközei típusváltásának és üzemeltetésének lehetőségei gazdaságossági–hatékonysági kritériumok, valamint NATO csatlakozásunk figyelembevételével. A légierő fejlesztése tanulmánygyűjtemény, Honvédelmi Minisztérium, Budapest, 1997. pp. (9-117)

[5] DR. ÓVÁRI GYULA: Korszerű harcászati repülőgépek műszaki üzemeltetésének sajátosságai és gazdasági–hatékonysági kérdései. A harcászati repülők fejlesztésének szükségessége és lehetősége. Konferencia előadás gyűjtemény, Magyar Hadtudományi Társaság, Budapest, 1998. pp. (33–70)

[6] DR. PETÁK GYÖRGY: A repülőtechnika üzemben tartása és javítása. Főiskolai jegyzet. KGYRMF, Szolnok, 1981.

[7] ROHÁCS JÓZSEF, DR. — SIMON ISTVÁN: Repülőgépek és helikopterek üzemeltetési zsebkönyve. Műszaki könyvkiadó, Budapest, 1989.

[8] USA MIL–STD 478/778B/882 szabvány gyűjtemények.