N72-25968

SOME THOUGHTS ABOUT SYSTEM SAFETY ASSESSMENT AND ITS CURRENT APPLICATION IN AEROSPACE

Mr. Peter R. Allison
Design Surveyor, Responsible
for
Systems Coordination
British Air Registration Board

Presented at the

NASA Government-Industrt
System Safety Conference

May 26-28, 1971

PRECEDING PAGE BLANK NOT FILMED

SUMMARY

As the title implies this is a discussion of various issues and requirements which must be considered during the actual work of Safety Assessment, and does not deal with all the aspects of a complete programme.

The task and its objectives are considered and the importance of presentation is stressed, so that problems and their solution are displayed adequately to the many disciplines involved. The definition of areas of influence to which the requirements can be applied and for which safety objectives can be derived, is discussed. The use of rational requirements is considered in this context, as is the use of numerical methods in the exercise of judgement.

It is also emphasized in the course of this paper that the assessment is a discipline which directs the appropriate skills at the problems as required, and must never be interpreted as a means of replacing these skills.

CONTENTS

1 INTRODUCTION

Much has been said on both sides of the Atlantic on the subject of Safety Assessment, and, in fact, it is probably right to say that it has all been said. There is for example, a lot of information published by various Government Agencies, which has been written as part of their procurement activities, and this has been of immense importance with its emphasis on the orderly application of safety analysis. However, it is thought to be generally true that although all the material is there in advisory form, its application is subject to much freedom of interpretation, and assessments have been made within these frameworks at many different levels, and perhaps with varying objectives. It seems opportune, therefore, to take another look at the complex path through the safety assessment process, as simply as possible, with the object of highlighting the principles involved.

Discussion can range from the administrative structure necessary in the manufacturing company down to the specific statistical techniques required to deal with the validity of a test programme; from the type of personnel required in a safety organisation and the methods employed to make the biggest impact, or, perhaps, the influence of the computer on the safety programme. Problems of documentation and format are by no means unimportant in this subject and have been discussed in depth. Many other aspects merit separate consideration and all can have a major influence on the approach to safety. This rather daunting appreciation of the field emanates from my work in the European aircraft industry and from a recent opportunity to look at safety assessment in a variety of American Aerospace organisations and is given to emphasise the fact that the subject matter of this paper is strictly in line with its title. Consequently, I propose to touch upon various issues and requirements which must be considered during the actual work of Safety Assessment, with the intention of stimulating discussion of the basic approach which should be made.

2 SAFETY ASSESSMENT TASK

The Safety Assessment task is to ensure that the design, construction, and operation of the device being investigated is sufficiently safe for its projected use. This requires the assurance that all foreseeable faults and critical situations have been adequately taken into account. Critical situations will include any such conditions which may arise when systems are working in the fault free mode and must take account of external events.

The demands of a statement such as this are immense and, apart from the application of the engineering and other skills involved, have given rise to the creation of many procedures involving different logic and documentation in order to assist in its satisfaction.

If we endeavour to state with more precision the process necessary to carry out the task the following requirements arise:-

(a) To define the safety objectives.
(b) To display the design, construction, and operation of the vehicle in such a manner that its potential weaknesses are clearly revealed.
(c) To ensure that the best judgement in the skills relevant to the problem and its interfaces has been brought to bear.
(d) To show to the satisfaction of all concerned that the safety objectives for the complete vehicle and its operation have been met.

If the Safety Assessment satisfies these requirements the detailed procedure is not important and depending upon the technology involved, and the possible hazards, many perfectly adequate methods are available. However, because of the contributions of different technologies to aerospace vehicles, some standardization on a given project is obviously desirable. In particular a standardised approach to safety assessment should facilitate the feed back of operating and servicing data, as experience accumulates, so that the aspects can be readily up-dated.

3 DEFINITION OF SAFETY OBJECTIVES

3.1 Background

Where the overall engineering of aircraft components and systems is concerned, safety objectives have been defined in terms of good engineering practice, and this has been implemented by ensuring compliance with arbitrary design rules developed in each succeeding generation of aircraft on which experience has been obtained. Where successive designs have produced relatively small increases in weight and speed it has not been too difficult to continue safety assessment processes which require establishing that good engineering practice is being followed, and the satisfaction of certain arbitrary rules stated in the airworthiness requirements. However, when the designer is asked to produce spectacular increases in speed, weight or airfield performance, an entirely new dependence on particular systems may arise which may have considerable complexity and require a more detailed understanding of the interfaces for safety reasons. In these cases, it becomes progressively more difficult to carry out safety assessments on a subjective basis, related to arbitrary design rules. The fundamental assumptions which have been made in most approaches during the last decade are:-

(a) System engineering can be adequately assessed against the testing and experience gained with previous systems.

(b) Adequate safety criteria can be given in terms of formalised experience and arbitrary statements of good engineering practice.

(c) By complying with these criteria, and using the developing skills of the assessor the aircraft can be made to demonstrate in service a safety record expressed on a basis of fatal accidents per flight or per hour etc. which will be an improvement on previous experience.

It seems necessary to emphasise these points to demonstrate that safety has always depended upon the extrapolation of experience and the use of the designers' skills. The aim should be to provide the best framework of objectives, and techniques of assessment, so that this approach can be continued into areas where additional system dependence, interaction problems, etc., are making the task more difficult.

3.2 Rational Requirements and Major Objectives

We can now say that to give more precision to the statement of objectives and the classification of hazards we will specify a rational system of requirements which we will use in the more advanced applications, and which can be related statistically to the level of airworthiness required when the aircraft enters service.

For example we can consider the airworthiness standard TSS 1-1 which is applicable to Concorde.

The object of this sort of requirement is to erect a framework which allows a more explicit statement of the objectives, hazards and their probabilities than has been usual hitherto. This is not to say that adequate assessments have not been performed, but it is being suggested that it is advantageous to indicate more clearly than in some past assessments why the decisions affecting Safety have been taken.

An important aspect of this, to which reference has already been made, is that service experience can be more readily referred back to the basic design assessment particularly where redundancy has permitted low MTBF.

Very considerable care has been taken with the requirement to allow the various frequency levels to be defined where necessary by analogy or in broad terms, but a numerical scale of probabilities is unavoidable, at least, by implication. Some people have difficulty in accepting this numerical concept, and

I shall return to this subject later when the exercise of judgement is discussed.

4 THE ORGANISATION OF THE ASSESSMENT

4.1 General Approach

The design, construction, and operation of the vehicle should be displayed in such a manner that its potential weaknesses are clearly revealed and it is suggested that this should be dealt with in the following manner:-

(a) Consider the Significant Airworthiness Functions which are required of the complex of systems which together make up the aircraft.

(b) Designate the system boundaries which allow the best logical separation of these functions.

(c) Designate the Zones, or physical boundaries, in which systems, parts of systems, and components are installed.

NOTE: The terms 'Significant Airworthiness Function' and 'Zones' will be discussed in more detail later.

(d) Carry out a system analysis for each of these arbitrarily generated groups by piece part count, for example, or any other desirable approach, in order to validate the significant airworthiness functions.

(e) Ensure that the interfaces are adequately taken into account. This includes interfaces between System, between System and the Zones in which they are contained, aircrew and system interfaces, etc.

As stated earlier, the Certification Authorities must assist this process of logical partition for analytical reasons, by stating requirements which take account of system dependency in a rational manner without unduly restricting the design. In addition, it is necessary because of the great background of experience to retain many features of the existing requirements of BCAR and FAR where their application is practicable for the specific type under consideration. So the aircraft is subdivided into manageable parts on the basis of the significant airworthiness functions, and the zones or compartments in which systems, parts of systems and equipment are installed.

There is of course, a considerable iteration and feedback in this part of the work since many factors are involved. Significant airworthiness functions will be influenced by the impact of the airworthiness requirements on the required operational characteristics. Zones may be determined not only by the structure arrangement but also by disposition of the systems and equipment, and the hazards arising from malfunction and interaction. These aspects will be further discussed. In real cases some compromise with factors outside Safety aspects may be necessary, involving, for example, the extent of subcontract work and particular responsibilities when the project is being carried out by more than one major contractor. It may well be that ability to define and deal with the interface problems may be a powerful factor in the determination of the sub-divisions of systems and zones.

For example, if one considered a supersonic aircraft having variable intake geometry it would be difficult to disassociate the behaviour of the intake, engine and perhaps its variable exhaust nozzles. It is clearly desirable to perform safety assessment on a unit which includes each of these parts and to ensure that this is carried out by an integrated propulsion unit team.

4.2 Discussion of the Significant Airworthiness Function

In the context of this primary activity, the Significant Airworthiness Function has considerable significance when the Safety Assessment is being organised. It is important to recognise that there are many functions which do not have airworthiness significance. These could have powerful commercial implication in the way of effects on

despatch capability, achievement of desired flight profile, maintenance costs, etc., and these functions will also be submitted to exhaustive system investigation which must be separate from the analysis required for Safety reasons. For example if a feature of the aircraft to be investigated is a droop nose necessary to provide the vision required for operation in various flight phases, we could consider two of its possible functions. In one case, the system could fail in a mode which prevented the nose being raised to the supersonic position. The result might be to prohibit flight in the supersonic mode and airworthiness would only be affected by any contribution which might result from a diversion.

A significant function would be the requirement for lowering the nose during the approach, and failure to achieve this would result in an increased load on the pilot and therefore represent an airworthiness hazard. Consequently, the system ability to perform this task is included in the safety assessment and its integrity matched to the importance of this hazard (however in passing there is also an absolute requirement in the case of Concorde that it should be capable of being landed safely after malfunction of the droop nose).

This discussion emphasises the need in all safety assessment work for precision in the identification of the functions which are associated with safety. It has already been said that safety assessment should provided the best display of the weaknesses of a project and this requirement will not be satisfied by an approach which endeavours to take account of every failure when many of these do not affect safety.

4.3 Integration of the Safety Assessment

At this point we have discussed the requirements and defined the systems and zones necessary for their logical application. The systems will then be analysed on the basis of single failures and the zones on the basis of detailed checks against installation rules.

These analyses are now developed through the following stages, which are probably sufficiently self explanatory in the context of this paper:-

(a) The system single failure analysis.
(b) The system safety assessment.
(c) The aircraft safety assessment.

These stages facilitate the grouping of piece part failures, the combination of these failures as they affect systems, and the total effect of these failures and the interactions which arise, on the aircraft as a whole. In a presentation of this sort it is difficult to describe the complete procedure with greater depth but it is not difficult to see a direct parallel with the Failure Mode and Effects Analysis combined with Criticality Analyses which are performed in the US industry.

In a previous paper on the subject of safety assessment dealing specifically with Concorde (Ref: 1) the way in which these middle level assessments are combined was discussed. Essentially, we have designated a basic system element (Figure 1) which has an input of system control signals, stimuli from other systems, system internal failures and, of course, the system output functions. Within this concept it is endeavoured to have discrete analysis but the output of the analysis will be grouped in so far as their effects on the whole aircraft are concerned. A feature of each of these analyses is the use of dependence diagrams which make very important contributions to the achievement of total visualisation of system vulnerability.

The problem of display and total comprehension of the safety assessment introduces us to the question of choice between fault tree, logic tree, success path, dependence diagram, etc. I have had many discussions in the American and European industries where this has arisen and it is clear that there are applications and objectives which are suited to each approach. Bearing in mind the need to ensure that every section of the design/manufacturing/operating team should have the widest

understanding of the safety problem, it is suggested that some care should be taken over this choice. If the fault tree is considered it is thought that some variant, such as the logic tree, is very suitable as a high level linking discipline. It could link, for example, the outputs from the discrete system analysis referred to above and its use should be limited to the integration of these effects at the total aircraft level. It is suggested therefore that the roots of the fault tree should culminate in events which are described in dependence diagrams.

It is undeniable that pure fault tree analyses carried out with a view to automation are ideally suited to projects where development and operational time in a fully assembled mode is minimal. The fault tree programme in this case has some relationship to the flight development programme on aircraft but it is thought that from the point of view of original safety assessment on aircraft projects it is extremely difficult to highlight the safety problem, when a fault tree perhaps of many thousand events may be needed to go from a part failure to, for example, a minimum safe pitch capability over a limited Mach range. It is realised that statistical analysis will produce dominant paths, critical modes, etc. but it is possible that the complexity of the process could swamp the safety effort.

The dependence diagram is ideally suited to the examination of failure modes at system level and draws particular attention to the need for redundancy and the weight which must be put on the assessment. Attention is particularly drawn to systems which are unduly sensitive to series effects.

4.4 The Zonal Analysis

This is an analysis which is required to cover proximity, environmental and other associated effects which together constitute a considerable problem in most aerospace applications. A zone for the purposes of this paper is considered to be a volume or compartment of the aircraft which is structurally or even arbitrarily bounded and in which equipment and systems are installed. Convenient means of identification could be by the use of the ATA 100 coding suitably modified according to the specific structural requirements of the aircraft.

Zonal analysis could be considered to be primarily concerned with problems which arise as a function of position whereas the system analysis discussed elsewhere in this paper is primarily directed at failure to achieve Significant Airworthiness Functions. 'Primarily' is a key word in this context since there is an essential overlap and the dual approach is important. Zonal analysis would therefore be primarily directed at problems of containment, jamming, fire, leakage, radio interference, etc. These are essentially areas which require an adherence to design rules in respect of environment and segregation which can often be enshrined in arbitrary airworthiness requirements, and which have been developed with continuing experience over the years.

A systematic approach is required when the assessment is being made in the context of the rational requirement but the task of quantifying segregation for example is clearly a difficult one. The following method has been proposed for the use on current projects. The chosen zone must be identified in relation to the aircraft and its contents indicated by drawing or list. Installation rules are developed for each zone based on general experience, consideration of the particular equipment present, and its failure modes. The objective is to ensure compliance with the installation rules with reference to the hazard classification of the general requirement. If there is a case where the assessed hazard probability is not favourably matched to its effects then this will appear as an output of the Zonal Analysis. Apart from the direct environmental effect which would require local design action this hazard

would appear as an input to the safety analyses of the functional systems which are present in the zone insofar as the achievement of the associated Significant Airworthiness Functions are concerned.

It is worth repeating the primary features of this analysis which are to achieve a logical arrangement of the zones, clear identification of the contents of these zones, and the presentation of comprehensive installation rules. These installation rules must take account not only of the best engineering practice but also consider the specific failure modes and their local effects. Finally the zones must be comprehensively checked against these rules and positive conclusions reached.

5 THE EXERCISE OF JUDGEMENT IN SAFETY ASSESSMENT

Assessed probabilities are the essential tools of safety analysis and it is important that this statement is fully understood. In many cases it is possible to assemble an ideal structure of numerical probabilities on the basis of component failure rates. Particularly this is so in the case of avionics which are specially suited to statistical analysis on this basis and where substantiated failure rates for most of the parts and techniques involved are available. However, when safety assessment is being performed in this manner utilising component failure rates, weighting factors must be applied, to take account of particular usage, environmental conditions, etc. Therefore, even in what could be postulated as an ideal application of safety assessment where substantiated failure rates under known conditions are available, it becomes necessary to introduce general, if not subjective, experience into this numerical analysis when the required operating conditions are different from those under which the reliabilities were determined. The apparent derogation of a potentially 'pure' numerical analysis has been emphasised because the weighted analysis represents a point on the scale between 'numerical approach' on the one hand and 'engineering experience' on the other. Where the range of systems concerned extend from the purely electronic, through auto-throttles with, for example, sensors and clutch mechanisms, to flying controls where linkages, actuators, structural parts, etc. should also be included then it is obvious that the mixture has progressively become less 'pure'.

The 'pure' approach would be severely compromised when the interface between electronic parts and mechanical parts occurs, where one element has been assessed by proved reliability techniques and the other, such as a linkage or hydraulic component, may have been assessed on engineering experience associated with a limited but fully understood test programme. In cases of this sort, the failure of a mechanical locking device and a soldered joint in a circuit may have similar results.

So how should the task be approached? It must be emphasised that, as was said earlier, we are discussing only the tools of the trade; the designers and specialists have the desired input and it is the management of this input that is being discussed. Where computer techniques are required then the skills appropriate to these techniques must be available but only to ensure that the best use is being made of engineering judgement or the other relevant skills.

It is thought that a numerical approach is an excellent method of recording the exercise of judgement and it is emphasised that this should not be unnecessarily inhibited by the limitations of the data. The designer makes his numerical assessment implicitly by presenting his design and it can only do good to display how his thought processes have distributed the probabilities. The application of experience becomes more credible if directed at the component parts rather than at the assembly as a whole, and the design can be assessed by the extent of this dependence on unduly favourable assumptions. However it must be said that even here judgement must be exercised.

Unimaginative use of the numerical approach has tended to bring it into disrepute in some quarters and single faults estimated at 10^{-6} or less which produce dangerous hazards cannot be treated as the cornerstones of safety assessment. To avoid this

pitfall, rational requirements need to be backed by some safeguards stated in arbitrary form, as in TSS 1-1.

6 CONCLUSIONS

It is important to say before concluding, that there are major omissions in this paper, considered necessary because of possible effects on emphasis, within the limited time available. For example, safety assessments require major inputs from consideration of Crew Procedures; flight handling is closely linked with system analysis and rational requirements have been developed to take account of this; also no mention has been made of the importance attached to the use of the flight simulator and the importance of the continuing maintenance effort has only been mentioned indirectly. More specifically the analysis of digital systems (including their software) if employed where sufficient authority exists to create serious hazards is also relevant to the discussion of the fundamentals of Safety Assessment.

I think these examples suggest the extent of the field from which my particular observations could have been drawn. However I have chosen to bring out some of the essential features of Safety Assessment in more fundamental terms, which could have been obscured by these other considerations.

I have endeavoured to discuss Safety Assessment under four headings chosen at the beginning of this paper. I have talked about the definition of Safety Objectives, the organisation and display of the Assessment, and the exercise of judgement. I find that I have not specifically discussed the final point which was to show to the satisfaction of all concerned that the safety objectives have been met, and although it is largely implicit in the other headings, I will return to it later.

I think that the broad conclusion which emerges from this discussion is that Safety Assessment continues to require a disciplined approach, which, although it cannot displace the specialist design functions, is necessary as a means of directing these efforts at the right problems with a lower probability of subjective error.

In more detail, I have emphasised the need to determine and set out safety objectives with precision so that the analysis is not complicated, with occurrences which are not relevant to safety. Also it is important that the Safety Assessment can be readily understood by all concerned, and visual techniques such as the variants of the fault tree, dependence diagrams, should be used.

The exercise of judgement should be assisted where possible by a reasonable use of numerical methods, but these should not be allowed to obscure the objectives or saturate the Safety Effort. In addition, the particular importance of a methodical analysis of Zonal, or environmental problems, cannot be over-emphasised.

To return to the final point in my introduction which required the assessment to show to the satisfaction of all concerned that the safety objectives have been met, this is of course a problem of data display and management. If judgement has been applied in the manner discussed so that simulator, development flying, and service experience can rapidly and effectively update the assessment, then I believe that we are some way along the line towards ensuring that the Safety Objectives will be achieved in service.

7 ACKNOWLEDGEMENT

I would like to express my thanks to the Air Regulation Board for permission to present this paper and to point out that the opinions expressed are entirely my own.

8 REFERENCE

1. HAAS, J. (Aerospatiale), 'An Application of Modern Maintenance Concepts and Safety Analysis to the Multinational Certification of a Supersonic Aircraft.' Presentation to the 6th Annual International Maintenance Symposium.

APPENDIX

NOTE ON TSS 1-1 AIRWORTHINESS OBJECTIVES AND SYSTEM ANALYSIS

TSS 1-1 introduces a probability approach to the Safety Assessment of aircraft systems, together with a framework of defined terms. To fit the requirements into a consistent framework, a number of terms needed to be defined.

At root there are the things which happen, described as Occurrences. These include Failures of parts of the aeroplane, Events arising from outside the aeroplane (e.g. gusts) and Errors arising from the actions, or failures to act, of flight or ground personnel.

An Occurrence has various potential Effects. These can be classified according to the associated level of danger, into Minor, Major, Hazardous or Catastrophic.

The requirements must state the acceptable frequency of Occurrences, and according to the magnitude of the Effect, various frequencies can be ascribed - Frequent, Reasonably Probable, Remote, Extremely Remote, etc. To give technical significance to these words some idea of the numerical probability needs to be quoted (e.g. Reasonably Probable, of the order of 10^{-3} to 10^{-5}).

The constructor's task is then to assess the frequency of Occurrences, singly and in combinations, and the Effects of these Occurrences. These results are then to be matched against the acceptable probability of the various levels of Effect.

One clearly defined difficulty with this approach is that of proving compliance with the requirements, particularly in cases where a failure or combination of failures would result in catastrophe. In such cases it is necessary to impose some additional arbitrary criteria in addition to, or instead of the numerical criteria (e.g. a double failure may only be acceptable as an Extremely Improbable failure when (a) both failures are assessed to be not more probable than Remote, or (b) at least one is assessed to be Extremely Remote).

The requirement then states broadly that the Occurrence of failures or errors must not produce an accident risk greater than prescribed levels, and that systems or combinations of systems operating normally without failures or errors must not be able to able to prejudice the safe operation of the aircraft.

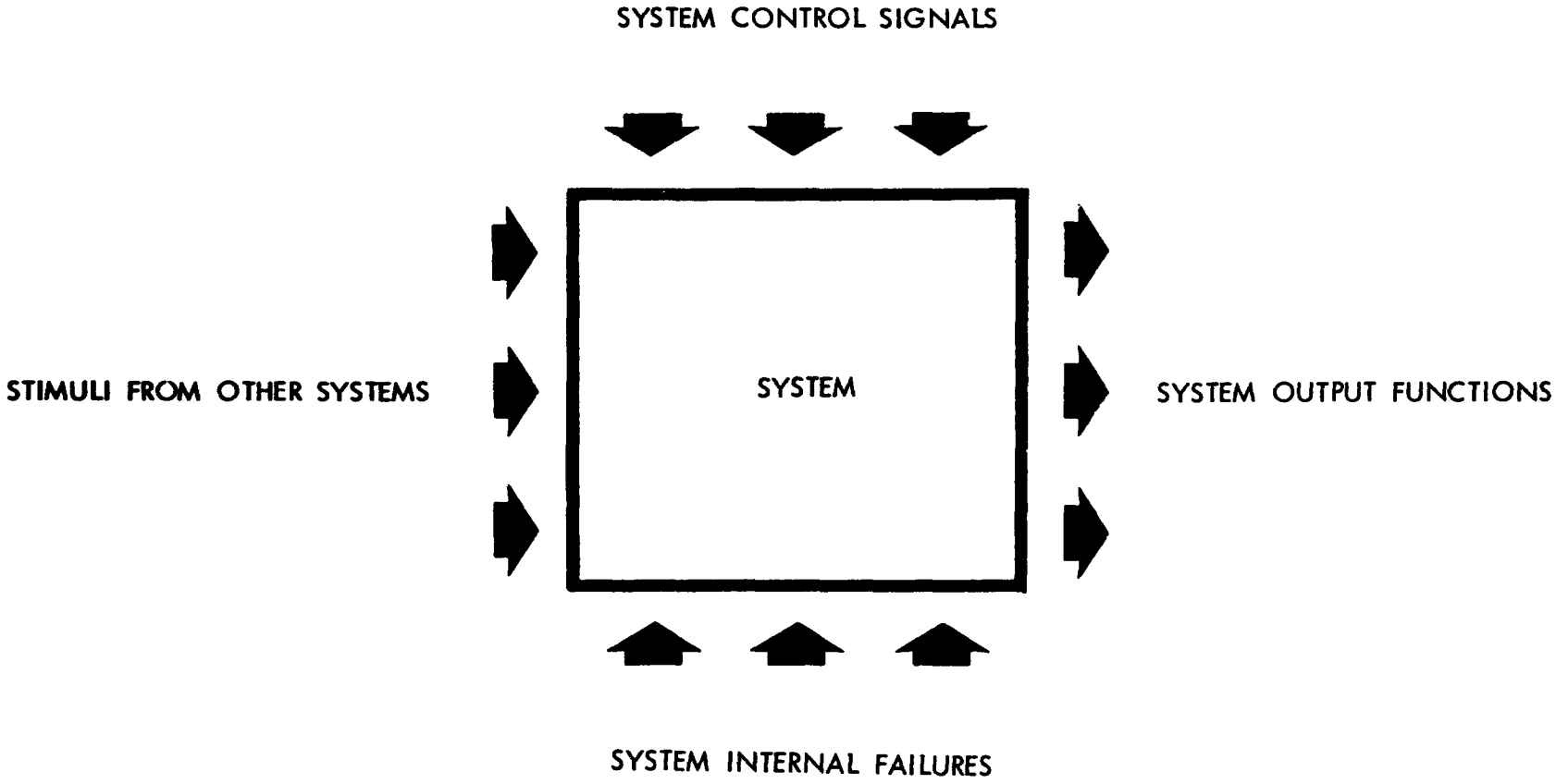

FIGURE 1 BASIC SYSTEM ELEMENT