NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Report No. 32-960

System Engineering Considerations in Spacecraft Design

A. G. Conrad

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

June 15, 1966

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Report No. 32-960

System Engineering Considerations in Spacecraft Design

A. G. Conrad

J. H. Gerpheide, *Manager*
System Design and Integration

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

June 15, 1966

Prepared Under Contract No NAS 7-100
National Aeronautics & Space Administration

CONTENTS

ABSTRACT

Consideration of the Spacecraft System as an entity is the most significant aspect of system engineering as applied to the design of planetary spacecraft The system design activity discussed in this Report is limited to those considerations involved with the establishment of the required Spacecraft System capability, the development of the design concept, and the generation of the subsystem functional capability requirements.

I. INTRODUCTION

System engineering can be described as an engineering approach to a problem whose solution requires consideration of multiple technical disciplines This is immediately recognized as a description that typifies most engineering design activities To limit the term *system engineering* it is necessary to first define what is meant by *system* Some reflection reveals that a defined system is very likely a subsystem of a larger system Thus, in discussions involving the term *system engineering* one acknowledges that he is dealing with a specialized definition of the term *system*

This Report emphasizes the design activities of definition and coordination of the interaction between elements (subsystems) of the total spacecraft system The key words here are *total spacecraft*, and the key concept of system engineering as it pertains to spacecraft design is the consideration of the design of the total spacecraft Spacecraft System engineering demands an understanding and appreciation of each subsystem's interaction with other elements of the system, and also the system's interaction with other elements of the project, namely the Launch Vehicle and Mission Operations Systems In summary, system engineering is the coordination of the activities of specialists in subsystem areas to achieve an optimum total design

The system engineering concept of viewing the entire design as an entity to perform certain functions in an integrated fashion is a vital consideration in the design of spacecraft systems To achieve a reasonable, workable system it is mandatory to utilize this system engineering approach at the earliest possible time—as soon after project inception as is practical, because many complexities of a spacecraft design become evident only when the necessity arises to identify subsystem interactions that are needed to achieve a specific result Spacecraft System engineering was an integral part of the *Mariner* Mars 1964 Project from its inception, and the success of this effort is history History also shows that the lack of system engineering considerations in spacecraft design has resulted in unsuccessful projects

It is popular to speak of the principle of maximizing the expected value when discussing the optimization of a system In Spacecraft System engineering activities this principle is essentially rewritten *minimization of the undesired quantity, mission failure* This distinction is important because at the present time the data available are inadequate to permit any realistic quantitative assessment of the probability of mission success The numerical values associated with each quantitative analysis are not of primary interest to the system engineer, his goal is to

know that, within the myriad of constraints he must consider, he has pursued every means of minimizing failure At this point the term *mission* must be defined Throughout this Report *mission* means all spacecraft with the same assignment which are launched in a given planetary opportunity

Considerable emphasis is placed on applying good engineering judgment in determining how best to increase system reliability A means of achieving this is through a technique called *failure mode effect analysis,* described by Casani in Ref 1 This technique permits examination of critical functions in a spacecraft design and develops appropriate system logic and redundancy to provide a reasonable level of reliability

This Report will discuss some considerations of concern to the system engineer in his effort to achieve a flightworthy spacecraft design No attempt is made to identify those techniques used in defining, coordinating, and verifying the design The *Mariner* Mars 1964 spacecraft design activity provides the basis for those examples given

II. SYSTEM ENGINEERING AS APPLIED TO THE SPACECRAFT DESIGN

The most significant aspect of system engineering as applied to the design of planetary spacecraft is the consideration of the spacecraft as a whole—an entity—which involves the interactions between the subsystems of the spacecraft and those between the Spacecraft System and some comparable system such as the Launch Vehicle or the Mission Operations Systems A key consideration, the common denominator in many of the Spacecraft System and subsystem interactions, is the flight path followed from Earth to the distant planet This mission parameter constrains and is constrained by the spacecraft design Because system engineering involves various mission trade-offs, the system engineer—who in this case is the system designer—must necessarily examine all the spacecraft interactions to be in an advantageous position for making the requisite decisions

Again, the system designer's responsibilities dictate that he examine the *total* spacecraft—there is no other way he can fulfill his assignment In addition to the trade-off decision just mentioned, he must help determine the requirements which the design must satisfy to achieve mission success, evolve the design concept and philosophy, define required subsystem functional capabilities, review and control interactions between subsystems, establish the degree of complexity for each subsystem, generate design restraints to guide spacecraft design activities, determine functional and block redundancy requirements, provide alternative operating mode capability for use in mission operations, assure capability of spacecraft testing in anticipated environments, and verify that the design is capable of performing the mission

A. Required Spacecraft System Capability

Before any design activity can be initiated, the spacecraft requirements must be understood It is the system designer's responsibility to determine what these requirements are, on the basis of the mission objectives outlined in the Project Office Faced with the problem of designing a spacecraft to go to Mars, the system designer is forced to consider all reasonable means of achieving the optimum design He identifies the primary tasks which must be accomplished and limits the design to that which is necessary for successfully satisfying the mission objectives

One feature of the required system capabilities is that these are not evolved in series with the mission objectives In theory, the mission objectives precede the system requirements, but, in practice, to establish achievable mission objectives, the system designer must conduct studies to determine what mission possibilities exist This form of feedback is typical of much of the design activity the various phases may be shown in sequential fashion on paper but the actual practice is to review later phases of the project and provide feedback to permit reasonable accomplishment of the preceding sequential steps (Fig 1)

In judging what needs to be achieved by the spacecraft, the system designer must be certain that his understanding of the requirements of the mission objectives is consistent with the wishes of the Project Management As the possible design approaches are considered, the situation will arise where one design aproach might achieve the required objectives, but at the expense of some other

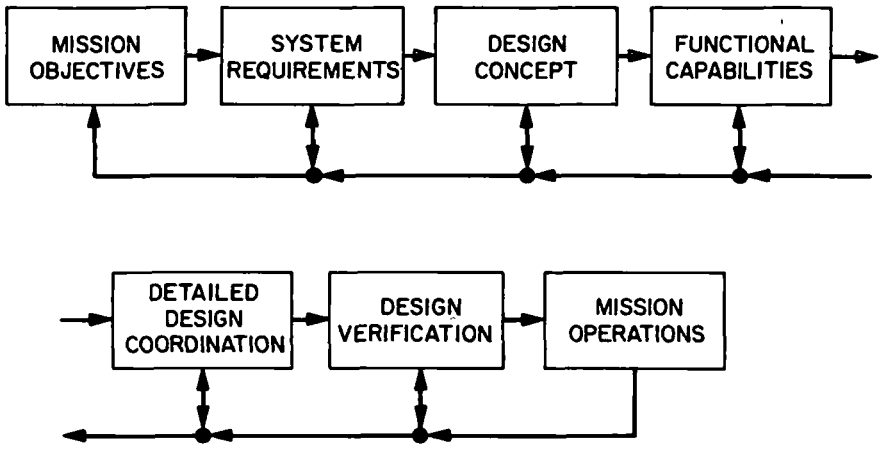

Fig. 1. System design activities

objective. The question may then arise about which objective is most important and on what basis this decision (and subsequent decisions) should be made To facilitate this decision-making process, the Project Office publishes the list of mission objectives on a priority basis, and a list of competitive design characteristics. Armed with these two priority lists, the system designer is better able to make the inevitable design decisions and compromises To illustrate the difference between the lists, the *Mariner* 1964 mission objectives and competing characteristics are shown below

1. *Mariner* Mars 1964 Mission Objectives

1. The primary objective of the *Mariner* Mars project is to conduct close-up (flyby) scientific observations of the planet Mars during the 1964–1965 opportunity and to transmit the results of these observations back to Earth

2 A secondary objective is to provide experience in and knowledge of the performance of the basic engineering equipment of an attitude-stabilized flyby spacecraft during a long-duration flight in space farther away from the Sun than the Earth

3 An additional secondary objective is to perform certain field or particle measurements, or both, in interplanetary space during the trip to and in the vicinity of Mars

4 A tertiary objective is to provide a design compatible with a repetition of the flyby mission to Mars, or provision of a mission with minimum modifications, for the 1966–1967 Mars opportunity

2. *Mariner* Mars 1964 Competing Characteristics

1. Arrival at the planet within the prescribed accuracy and capability to communicate telemetry during the encounter period and for one week thereafter This total function requires the following specific functions
   a Continuous proper Sun-line attitude orientation
   b Continuous proper temperature control
   c. Proper functioning of the solar power equipment
   d Proper roll attitude control during and for one week after encounter
   e Proper operation of the communication equipment during and for one week after encounter
   f Proper operation of the midcourse maneuver
2 Proper operations of the planetary instruments and the capability of these instruments to observe the planet during the encounter mode
3 Proper operation of the science data storage and handling equipment
4 Telemetry communication capability during the transit phase, this function requires roll attitude control when the high gain antenna is required
5 Adequate operation of the interplanetary science equipment
6 Operation of the planetary scan in the desired fashion
7. Compatibility of the design with later mission requirements

Another valuable contribution of the Project Office to this decision-making process of the design effort is the

publication of mission worth statements in which quantitative values are placed on a variety of achievements that provide some mission return These values permit a quantitative analysis of the mission from the standpoint of reliability and mission return They also provide an additional basis for future design decision

Other factors in the decision-making process are budget, schedule, reliability, and state-of-the-art.

From the initial stages of the design process, the system designer must consider the entire spacecraft design and make decisions concerning the achievement of the mission objectives Such early consideration of the spacecraft design concept is required to permit the Project Office to publish the design criteria that will be followed during the spacecraft design activity These criteria establish the design approach to be taken, the reliability considerations to be observed, and the schedule and weight constraints to be met Here again is an example of feedback in which a later phase of the design process affects the spacecraft design requirements

B. Development of the Design Concept

The development of the design concept is an intermediate step in the design process between the definition of the mission objectives and design criteria by the Project Office, and the establishment of requirements on the respective spacecraft subsystems by the system designer The objective is to identify what must be accomplished and establish the means of satisfying these requirements The establishing of the design concept for optimal achievement of mission objectives is one of the prime functions of the system designer He chooses, from all the alternatives, the specific design approach which best fits the mission objectives

Design concepts must be chosen which allow primary mission objective achievement with the least risk to the mission, and at the same time consider budget and probability of schedule accomplishment, by limiting the design to necessary functions and implementing them in the least complicated manner The primary spacecraft capability required is that of communicating scientific data to Earth In support of this requirement there must be a radio, a telemetry system, a power system, and some scientific instruments At JPL we augmented this complement with an attitude control system, an on-board sequencer, a command receiving system and a propulsion system It is readily recognized that these functions and their basic relationships are generally repetitions from mission to mission This concept of a standard spacecraft often permits the use of existing designs and hardware, and tends to diminish the risk to the mission. This concept also has the advantage of some saving in cost.

The implementation of specific mission objectives requires that special functions be integrated with the standard functions These special functions are often dictated by the nature of the experiments during the transit phase and those in the vicinity of the planet Successful design concept development depends upon the ability of the system designer to establish the requirements for special functional capabilities This can be done only after the spacecraft is examined as a whole to assure that all functional interactions are recognized and carefully considered against the mission objectives, design criteria, and competing characteristics, as published by the Project Office

As was mentioned, the development of mission objectives depends upon the feedback provided by looking at the design concept under consideration to see what looks feasible. When we state that the functional interactions must be considered against the mission objectives, we acknowledge that the Spacecraft System design functions as a continuing, iterative procedure Only where the iterations do not uncover any additional design conflicts can the system design approach be established To achieve this status of no unresolved design conflicts, even at this gross level, some reasonably detailed examinations of the respective interface areas must be accomplished These examinations are really part of a later design phase, note that feedback plays a critical role here in the development of the design concept

The first philosophy basic to the concepts chosen at JPL for planetary spacecraft is that a spacecraft must be capable of operating entirely without assistance from Earth, except in the case of a postinjection propulsive trajectory correction To allow the entire mission to be accomplished without ground commands, a sequence must be preprogrammed into the spacecraft The trajectory correction is an exception because there is no way to preprogram this maneuver This automatic spacecraft concept does require that there be sufficient spacecraft operating modes to accommodate those conditions which are expected during the mission Since the data requirements differ during various mission phases, the spacecraft must be capable of altering its mode of operation

A second design philosophy influencing the ultimate design concept is that of providing at least two independent means of initiating critical, discrete functions The

interrelationships chosen between subsystems must reflect this philosophy Although the use of radio commands is the primary means of providing the second of the discrete events should the automatic sequencing fail, other techniques are used effectively. A complete description of the *Mariner IV* design features implementing this philosophy is given in Ref. 2.

A third design philosophy recognized as being critical to planetary spacecraft design is that all critical continuous functions be supported by redundant or alternate modes An example of this is the redundant analog-to-digital converter that was incorporated in the engineering telemetry subsystem of *Mariner IV* This redundant capability was attainable by ground command

C. Required Functional Capabilities

The completed spacecraft design must reflect certain functional capabilities Thus specific functional capabilities are required from each spacecraft subsystem to provide this overall system capability Subsystems are identified on the basis of unique functional capabilities grouped under the cognizance of a single organization The identification of these functional capabilities on the subsystem and system levels represents the intermediate step between the development of the design concept and the detailed hardware design phases of the system design activity

Successful translation of the design concept into specific functional requirements to guide hardware design requires that the spacecraft be examined as an entity to assure that recognized problems will be considered from all aspects and that the greatest likelihood exists of uncovering new problems Also associated with this overall examination is the fact that later mission phases must be considered at this time when specific requirements of these phases can be accommodated by the spacecraft design. Decisions must be made about what will be implemented as automatic recovery capabilities, what will be initiated by on-board logic, and what will be initiated by ground command if nonstandard or failure mode conditions exist on the spacecraft The use of ground commands is a recognized means of activating redundant elements when a delay in the transmission of the command can be tolerated without danger to the life of the spacecraft Ground command reaction to spacecraft anomalies is not instantly available during the mission operations phase for a variety of reasons, not the least of which is the two-way communication time delay Mars missions have approximately 25-min round-trip delays, on the basis of 140,000,000-mi communication ranges. Of primary importance is whether the spacecraft will cease to operate before the ground command can be transmitted to the spacecraft. On-board logic must therefore be employed to activate redundant elements when command delays could endanger the life of the spacecraft

The design of the spacecraft is also influenced by the requirement to perform certain test and assembly operations on the spacecraft Although functional capabilities of subsystem designs usually consist of statements describing what the subsystem should do in flight, there must also be capabilities to tolerate certain conditions on the ground Examples of the latter are:

1 No operations requiring physical access to the spacecraft are permitted while in the launch complex This indicates that sensors whose field-of-view requirements vary with date of launch must be designed to be operable with a fixed field of view over the entire launch period

2 No services of liquid or gaseous umbilicals will be available to the propulsion subsystem This dictates that the propulsion subsystem must be fueled and pressurized before going to the launch complex For spacecraft safety considerations, the propulsion subsystem must be removable for the fueling and pressurizing operation

Automatic unmanned planetary spacecraft designs must incorporate capabilities which permit mission objective achievement, even under some degraded modes of operation Identification of the minimum functional capabilities to achieve the mission objectives is accomplished assuming no failures aboard the spacecraft Subsequently, failure modes and degraded operational modes are examined to identify capabilities which should exist to permit survival and mission accomplishment despite these nonstandard conditions. Sufficient capability should exist to permit at least two independent means of initiating critical, discrete functions and to provide redundant, or alternate, modes of operation for all critical continuous functions Reference 1 discusses a technique, failure mode effect analysis, for assuring that these conditions are satisfied

A consideration in this effort of defining the required functional capabilities is the necessity for design tradeoffs As more and more becomes known of the system design there is increased recognition that all desired capabilities or functions cannot be implemented, and that design compromises must be accepted The role of the system designer in this activity is to precipitate the various arguments involved with recognized problems and decide which functions should be implemented

III. EXAMPLE: SYSTEM DESIGN ACTIVITY

The encounter phase of the 1964 *Mariner* Mars spacecraft flight sequence is a good example of the system design activity necessary to define the required functional capabilities This example illustrates the need to examine a multitude of interactions to ensure total spacecraft capability for fulfilling the primary mission objective

A consideration of the mission objectives and Project Office definition of mission value clearly showed that every effort had to be expended to achieve successful television pictures of the planet. The design concept which resulted can be summarized in several statements

1 A vidicon sensor with appropriate optics takes the television pictures

2 A magnetic tape recorder stores the data readout from the television subsystem

3 A scanning mechanism orients the television subsystem toward the planet

4 A specialized sequencer controls the acquisition and recording of the television picture data

5 All encounter-oriented equipment is de-energized during the transit from Earth to Mars

This basic concept had to be translated into specific requirements for functional capabilities affecting nearly every spacecraft subsystem

A question which arises when one considers an automatic spacecraft, is how and when the encounter sequence should be initiated An acknowledgment of the philosophy which requires two independent means of initiating critical events (one of which is on-board to permit the spacecraft to be automatic) led to the selection of a central computer and sequencer (CC&S) signal and a ground command to initiate the encounter sequence This sequence was to activate the planetary (planet-related) equipment, cause the television subsystem to be oriented toward the planet, initiate and control the recording of data, and turn off the planetary equipment

The time of the encounter sequence start was bounded by the desire not to energize the planetary equipment after passing the planet and by the desire not to energize this equipment so early that television shutter mechanism failure or scan platform actuator failure would occur before the television subsystem observed the planet A time was selected for this sequence which placed the spacecraft as close to the planet as possible, consistent with the uncertainties which existed about when the closest approach to the plant would occur Because the CC&S has event times with only a 3⅓-hr resolution from its master timer, the ability to select the time of the CC&S sequence initiation is limited to ± 1⅔ hr The 3-sigma trajectory dispersions contribute about a 2¼-hr uncertainty. An additional 36-min uncertainty exists due to the 0.01% allowable drift in the CC&S clock This total uncertainty of when the CC&S would initiate the sequence, relative to closest approach is 4½ hr Acknowledging that the television pictures could be taken 25 min before closest approach on some trajectories, the initiation of the sequence should be at least 5 hr before nominal closest approach to the planet Consideration must also be given to the fact that the scan subsystem must orient the platform toward the planet, and this too requires time. Some allowance must be made also for sending backup commands in case of failure of the automatic features. The nominal time selected for initiating the encounter sequence was 6⅔ hr before closest approach

The time for automatically de-energizing the planetary equipment had to be long enough after closest approach that worst-case early tolerances would not cause initiation and cessation of the encounter sequence before the acquisition of the encounter sequence Owing to the 3⅓-hr CC&S timing resolution, 13⅓ hr was selected as the interval between starting and stopping the encounter sequence

The magnitude of these uncertainties in spacecraft timing and trajectory dispersions illustrates why television picture recording cannot be initiated by a preprogrammed clock The recording sequence can only be about 25 min to allow pictures to be taken across a major diameter of the planet, therefore, a recording sequence of excessive length would complicate the design and increase the playback time

The sequence was to be initiated only when the television was looking at some portion of the planet Since preprogramming was not effective in providing an on-board recording sequence initiation capability, other means of achieving this result had to be found Thus two, on-board, independent, redundant means of initiating the sequence were provided

The television itself provided one means of sensing the planet The design of the television subsystem was such

that it took pictures whenever it was on, not knowing when the data were being recorded Internal logic examined the intensity of the signals being sensed and, when a preset threshold level was surpassed, the television subsystem would indicate to the data automation subsystem that the recording should commence The backup for initiating the recording sequence was a cadmium sulfide detector with a narrow field of view pointed parallel to the TV Whenever the planet entered the field of view of this detector the recording sequence would be initiated This rather simple device replaced a more complicated sensing circuit intially incorporated into the ultraviolet (UV) photometer instrument The realization that the desired redundancy was being provided by two non-simple logic circuits that were not required by the UV instrument in its mechanism resulted in the design change to employ the cadmium sulfide detector In this manner the required functional capability of the UV instrument was reduced In addition to the initiation of the recording by the above techniques, a ground command backup was employed because of the criticality of the function

An important aspect of the system designer's activity is to protect the system against failure modes The effort to prevent a loss of data already recorded on the tape represented an area of major concern A two-track endless-loop tape recorder, started and stopped for each picture, was employed for recording the television data Should the recorder not be stopped when the two tracks were filled with data, the first data recorded would be obliterated The acquisition of a limb picture was very desirable Since this would be the first picture, special precautions were taken to ensure that these data would not be lost The tape recorder design was required to provide a counting circuit which sensed the number of tracks of data recorded and stopped recording when the record track had been filled Backups to this circuit were two signals generated internally to the data automation system (DAS) which inhibited further "start record" commands to the tape recorder

The examples given of the system designer's problems are comparable to many other problems which must be solved to generate an optimum spacecraft design Only through the process of answering questions similar to What is being done to prevent the loss of previously recorded data? is the design adequately reviewed and the necessary requirements for subsystem and system functional capability recognized

IV. SUMMARY

The system design aspect of Spacecraft System engineering is chiefly a technical discipline concerned with the spacecraft as an entity composed of many interacting elements (subsystems) Only when the design is viewed as a whole is there sufficient opportunity to identify the interfaces to permit an optimal design to be fabricated A significant amount of feedback in the system design process is required to permit the various phases of the design to be concluded Since consideration of the entire spacecraft is the most significant aspect of the systems design function, the more complex spacecraft of the future will be an increasingly difficult and challenging problem for the system designer This increased complexity may necessitate computerizing the design process.

REFERENCES

1 Casani, J R , "Use of Failure-Mode Effect Analysis for Improving Spacecraft Reliability," AIAA Meeting, March 28, 1966, Baltimore, Maryland

2 Casani, J R , Conrad, A G., and Neilson, R A , "*Mariner 4*—A Point of Departure," *Astronautics and Aeronautics*, August 1965.