N72-25973

CONTRACTING

FOR

SYSTEM SAFETY

Dr. Leslie W. Ball
Director of Safety

NASA

Marshall Space Flight Center

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

This paper is concerned with those requirements for safety that are, or should be, part of the hierarchy of contractual relationships between government and prime contractors, prime and subcontractors, and subcontractors and vendors.

Each of these interfaces involves the contractual sequence of

1. Request for proposal (RFP's)
2. Proposal documents
3. Contractor selection
4. Contractor performance measurement
5. Fee adjudication

Safety requirements are, or should be, a significant factor in all five of these aspects of the buyer-seller relationship.

The National Aeronautics and Space Agency, the Department of Defense, and most aerospace prime contractors have already a surfeit of policy statements and general specifications that require that safety should be a significant factor in their contracting practices. The purpose of this paper is neither to add to nor to summarize these policy and specification requirements. Rather, our purpose is to invite attention to some of the ways in which traditional contracting methods fail to give confidence in the achievement of safety and then to show how modern system engineering and system management techniques have provided us with the means to overcome these shortcomings in our traditional contracting practices.

OUTPUT CONTRACTING

Let us start our discussion by recognizing two very popular sayings. These sayings have typified supplier attitudes ever since the birth of aerospace industry. They are "Tell me what you want, don't tell me what to do" and "Once the contract is signed, leave me alone until I am ready to deliver the product." Government documents use the term "disengagement policy" to describe this seller attitude to the buyer-seller relationship. Figure 1 "Conditions For Output Contracting" sets forth four conditions that must exist if this type of relationship is to be acceptable to the buyer.

The term "Tangible Characteristics" will be used for those product characteristics that meet the first two conditions shown in Figure 1. For example, in the case of an automobile, top speed, miles per gallon, turning radius, and trunk capacity are tangible characteristics because they can be specified quantitatively and they can be demonstrated by quantitative test.

The term "Intangible Characteristics" will be used for those product characteristics that either cannot be specified quantitatively or, if specified, cannot be measured within acceptable cost and schedule constraints. In the case of an automobile, the intangible characteristics include safety and to some extent the characteristics of operational reliability and quality. In the case of a complex aerospace system, the intangible characteristics may include many other characteristics, such as electromagnetic compatibility or storage reliability.

When all the essential characteristics of a product are tangible, output contracting is the prefered method of contracting from the point of view of both the buyer and the seller. Obviously this is so, because it minimizes the time and effort required by both parties to negotiate and to monitor the fulfillment of the contract. However, even when all essential characteristics are tangible, development risks may make the seller unwilling to forego payment until he has developed the new product and demonstrated that it meets all the specified characteristic requirements. For example, in the case of most missile and space systems, United States aerospace companies are neither willing nor able to forego payment until they have developed a new system, even if all the essential characteristics can be specified and demonstrated by test.

Quite often in the aerospace industry, the customer is unable to meet the fourth condition shown in Figure 1. For example, in the case of the atomic bomb, the intercontinental ballistic missiles, or the Apollo space program, failure to meet all the essential product characteristics within the defined development time would have meant a national disaster.

In summary, we may say that pure output contracting often is unacceptable either because certain characteristics of a product are intangible or because either the seller or the buyer cannot tolerate some of the risks that are inherent in developing a complex new product.

INPUT CONTRACTING

Let us ask, if it is not possible for a buyer and a seller to contract solely on the basis of defining and demonstrating the characteristics of the product, what then can be done. The only choice is for the buyer and the seller to supplement output contracting by defining the work that the seller will do and paying for the accomplishment of this work. We will call this type of arrangement "input contracting."

A precedent for input contracting was established long ago when the government contracted with universities for research. It is inherent in the nature of research that the product cannot be defined and certainly cannot be guaranteed. Consequently, the agreement between the buyer and the seller is for a defined effort which the seller will make in fulfillment of the contract.

An oversimplification of input contracting would be to say that it consisted of negotiating program plans and monitoring the compliance with the execution of these plans as a condition for payment of the contract costs.

CONTRACTING FOR SAFETY IN THE 1960'S

During the 1960's, several relatively intangible characteristics became of vital importance to the customer. Some of the most important of these characteristics were reliability, maintainability, safety, electromagnetic compatibility, and security.

For each of these characteristics, an effort was made to apply the principles of output contracting. For example, several of us were involved in helping develop the first Department of Defense policy on reliability. This policy oversimplified the problem of contracting for reliability by stating bluntly that quantitative values would be specified in all procurement contracts and that they would be demonstrated before the product was accepted by the government. By the time that contracting for the intercontinental ballistic missiles came along, it was recognized that output contracting was inadequate because condition three in Figure 1 was unacceptable to aerospace industry and that condition four was utterly unacceptable to the government agencies. Consequently, input contracting in the form of requirements for the negotiation, execution, and auditing of reliability program plans developed as a supplement to specification and demonstration of quantitative reliability values.

In the case of safety, there were some initial efforts to apply output contracting by specifying accident probabilities and requiring demonstration of these probabilities by quantitative analysis. However, the limitations of this approach soon were recognized and during the 1960's, contracting for safety was dominated by requirements for safety program plans. These requirements did lead to the growth of a substantial system safety engineering profession. In this author's opinion, many of the members of this profession together with the program plans that they wrote and executed did achieve substantial good. However, a realistic assessment of the current situation must include the criticisms set forth in Figure 2 "Criticisms of Specialist Program Plans."

In general, safety program plans are written by system safety specialist engineers in the contractor's organization to satisfy their professional colleagues in the government agency's organization. In the opinion of many designers, the writing and execution of these program plans has no real impact on their design decisions, and in the opinion of many program managers, these plans have no real impact on their program management decisions.

In the present atmosphere of severe cost reduction throughout the aerospace industry, all specialist engineering staffs are vulnerable. In particular, system safety staffs are being and must be reduced from the levels that existed in the late 1960's.

A relatively new factor has been brought out within the National Aeronautics and Space Agency by the deliberations of the McCurdy Committee on procurement practices. Some members of this committee have pointed out that government specialist engineers, such as system safety engineers, tend to tell the competing contractors so exactly what they require in a program plan that the resulting proposal documents are essentially identical. Consequently, a source evaluation board is not able to establish discriminators between competing contractors on the basis of their safety or other specialist engineering program plans.

CONTRACTING FOR SAFETY IN THE 1970.

During the first sixteen months of the 1970's, there has been a marked trend away from a multiplicity of specialist engineering program plans and toward the five basic function program plans shown in Figure 3. Continuance of this trend will result in contracting for safety and other intangible characteristics being performed in a manner represented by Figure 4 "Safety Inputs To Contracting." Let us now use Figure 4 as a basis for discussing safety inputs into the five steps in contracting shown in the left hand column.

STEP 1 - REQUEST FOR PROPOSAL

From the point of view of the system safety engineer, the essential elements of even the most voluminous request for proposal are as follows:

1. Product Specifications which define quantitative requirements for the tangible characteristics and qualitative requirements for the intangible characteristics of the product which is to be developed.
2. A Statement of Work delineating the development activities that the buyer considers must be performed by the seller to give confidence in the achievement of both the required tangibles and the required intangible characteristics.
3. Proposal Data List delineating the development program planning data that all the sellers must submit to support the source evaluation and contractor selection processes.
4. Performance Measurement Data List delineating the development program control data that the successful contractor must submit during the execution of the contract.

Item 1 in this list corresponds with the Product Specification column in Figure 4. Items 2, 3, and 4 correspond with the five Basic Program Plans columns shown in Figure 4.

Safety inputs to the product specification inevitably include a motherhood type statement that safety must be a primary consideration in design. However, these inputs can include quite specific requirements such as control of materials flammability, or the use of redundancy to control single point failures for catastrophic hazards. Design practices criteria, in the form of checklists based on experience retention, are applicable to assuring the adequacy of safety engineering inputs into the Product Specification segment of the request for proposal.

The Program Management Plan should be written by the contractor's program manager. It should be a first person description of how he will use his authority and his program management techniques to assure achievement of all the product characteristics set forth in the Product Specification. Specifically, it should describe how he will make use of specialist engineers to help assure that design decisions are right the first time and also to assure that design errors are detected and corrected at the earliest possible time. For example, it should discuss the role of safety analysis in guiding design decisions and participation of safety engineers in design review and development failure analyses.

The Manufacturing Plan should be written by the contractor's manufacturing manager. It should include descriptions of how he will assure achievement of operational safety in the factory and how he will use people such as manufacturing planners and quality engineers to support hazard identification and hazard control.

The Support and Use Plan should be similar to the Manufacturing Plan in that it also should describe how the support manager will assure operational safety and how his quality assurance engineers will contribute to hazard control.

The Integrated Test Plan should bring together in one document an account of development testing, design verification testing, receiving inspection testing, manufacturing check testing, quality acceptance testing, and so on through operational checkout testing.

It should include descriptions of how appropriate supervisors will assure both the safety of the personnel conducting the test and protection of the operation equipment from the stresses that may be imposed during testing.

STEP 2 - PROPOSAL DOCUMENTS

The same safety criteria, set forth in checklist form, which the buyer requires for writing the request for proposal, are needed by the seller for responding to these requirements with his Proposal Documents. The specification segments of his proposal should show how the design that he intends to develop will be capable of achieving all the requirements including the safety requirements.

The program plan segments of the seller's proposal should first describe the resources that he has available for performance of those critical activities that are either set forth in the request for proposal or proposed by the seller himself. In this context, the term "resources" includes the procedures, such as safety analysis procedures, the supporting data, and the available qualified people, such as professional safety engineers. The seller's Program Management Plan should show how his development program organization will facilitate communication between specialist engineers, such as safety engineers, and the design and program decision makers. Each of the other program plans should deal with hazard identification and control activities that are appropriate to the basic function covered by the plan.

STEP 3 - CONTRACTOR SELECTION

Let us distinguish between two extreme cases. In the first case, the buyer has told the seller in the request for proposal precisely what he wants done in each area, such as the system safety area. This means that the buyer has identified all the critical activities that he wants to be performed during the development program. In this case, the only basis for contractor selection is to evaluate the potential effectiveness of the resources that the seller is offering relative to each critical activity. This type of request for proposal has been a major cause of the fifth criticism shown in Figure 2.

In the other extreme case, the buyer has not told the seller what critical activities he wants to be performed; however, he has asked the seller to propose such activities. For example, he may ask the seller to propose such activities. For example, he may ask the seller "What has been your experience in regard to the achievement of system safety? What activities do you propose to perform?" In this case, the source evaluation process must give credit to the seller's identification of appropriate critical activities as well as to the resources that he proposes to put to work to accomplish these activities.

STEP 4 - PERFORMANCE MEASUREMENT

For the tangible characteristics, performance measurement is dominated by qualification testing and system testing. These tests demonstrate that the quantitative values required by the product specification have been achieved by the seller's design.

In the case of safety and other intangible characteristics, quantitative performance measurement is almost meaningless. Consequently, criteria must be established for evaluating the performance of the critical activities set forth in the five basic program plans. The key to accomplishing this objective is illustrated by Figure 5. Modern system management requires that all the work to be accomplished during a development contract be related to a single Work Breakdown Structure. Cost Accounts are formed by matrixing the work breakdown structure with the contractor's organization units. Work Packages may be formed in several logical manners. This chart illustrates the formation of work packages by dividing the work to be done by a particular organization on a particular work breakdown structure item into short duration packages.

The vital management requirement illustrated by Figure 5 is that critical activities, such as safety analyses, must be specifically required and scheduled and funded by their inclusion in the Work Package Work Description. Also, satisfactory completion of the critical activities must be provided for by inclusion of tangile criteria in the Work Package Closeout Criteria. For example, such criteria must be

2-5

established for the accomplishment of each type of hazard identification analysis and for each type of hazard control activity.

STEP 5 - FEE ADJUDICATION

From the point of view of the customer's system safety manager, the award fee type of contract is by far the most attractive. This type of contract provides incentive for the buyer and the seller to agree on what should be done during each award fee period of, say, six months. If the total award fee is to be in the range from two to fifteen percent, it is reasonable to assign, say, one-half of one percent to the accomplishment of the safety program. It is this tie-in between the performance of safety activities and award fees that provides the best hope for full exploitation of the skills, knowledge, and techniques of the professional system safety engineering during the 1970 decade.

SUMMARY

In summary, the safety contracting methodology of the 1960's was dominated by individual safety program plans together with a need for large and expensive system safety staffs to prepare, execute, and audit the execution of these plans. During the 1970's, there is a rapid trend toward the absorption of system safety disciplines into the five basic function program plans. The contracting practices of both the buyer and the seller should reflect and encourage this trend. In particular, the award fee principle should be used to provide confidence that system safety technology will be fully exploited during the 1970's.

BASIC FUNCTION PROGRAM PLANS

- PROGRAM MANAGEMENT PROGRAM PLAN (PHASE A, B OR C/D)
- SYSTEM ENGINEERING PLAN (MIL-STD-499 SEMP)
- MANUFACTURING PLAN (INCLUDES FACILITIES AND QC)
- SUPPORT AND USE PLAN (INTEGRATED LOGISTICS SUPPORT)
- INTEGRATED TEST PLAN

SPECIALIST ENGINEERING CRITICAL ACTIVITIES MAY BE DELINIATED IN SEPARATE PLANS BUT THEY MUST ALSO BE INTEGRATED INTO THE ABOVE.

FIGURE 3

SAFETY INPUTS TO CONTRACTING

- CRITERIA REQUIRED EITHER TO HELP WRITE OR TO HELP EVALUATE THESE ITEMS

	BASIC PROGRAM PLANS: PRODUCT SPECIFICATIONS	PROGRAM MANAGEMENT	SYSTEM ENGINEERING	MANUFACTURING	SUPPORT AND USE	INTEGRATED TEST
REQUEST FOR PROPOSAL	•	•	•	•	•	•
PROPOSAL DOCUMENTS	•	•	•	•	•	•
CONTRACTOR SELECTION	DECISION BASED ON EVALUATIONS					
PERFORMANCE MEASUREMENT	•	•	•	•	•	•
FEE ADJUDICATION	DECISION BASED ON EVALUATIONS					

FIGURE 4

CONDITIONS FOR OUTPUT CONTRACTING

- ALL ESSENTIAL PRODUCT CHARACTERISTICS CAN BE SPECIFIED QUANTITATIVELY.
- ACHIEVEMENT OF ALL CHARACTERISTIC CAN BE PROVED WITHIN ACCEPTABLE COST AND SCHEDULES.
- SELLER IS WILLING TO FOREGO PAYMENT UNTIL ACHIEVEMENT OF ALL CHARACTERISTICS HAS BEEN DEMONSTRATED.
- BUYER CAN TOLERATE THE SCHEDULE AND COST IMPACT OF CANCELLING THE CONTRACT FOR NON-PERFORMANCE AND STARTING AGAIN WITH A NEW SUPPLIER.

CRITICISM OF SPECIALIST PROGRAM PLANS

- WRITTEN BY SELLER SPECIALISTS TO SATISFY BUYER SPECIALISTS
- NO REAL IMPACT ON DESIGN DECISIONS
- NO REAL IMPACT ON PROGRAM DECISIONS
- REQUIRE LARGE STAFFS TO WRITE, EXECUTE AND AUDIT
- NO DISCRIMINATION BETWEEN COMPETING SELLERS

FIGURE 2

TECHNICAL ASSURANCE THROUGH CSTCS

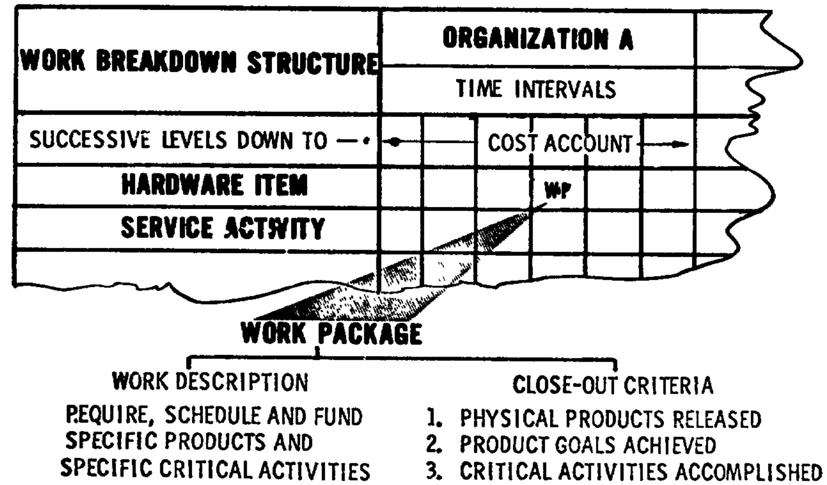

FIGURE 5