RECEIVED BY TIC SEP 27 1972

QUALITY ASSURANCE FOR RISK CONTROL AND ENGINEERING VERIFICATION

M. Bender

Oak Ridge National Laboratory*
Oak Ridge, Tennessee

Most of us are not concerned with the final engineering of space vehicles or military aircraft although we may contribute materials or components to their assembly. Normally, we are content with a successfully engineered product that can be repetitively marketed to a satisfied customer. But even if we are not directly concerned with the final application of exotic hardware, we are still strongly influenced by the practices that make these new engineering ventures successful. The term that is most frequently cited as the key to success is "quality assurance". One might almost think that quality assurance was the invention of the space age, but we all know this to be a fallacy. From the day when Damascus steel became the symbol of quality weaponry, we have been conscious of quality assurance. The master sword maker was one who established his reputation by maintaining sufficient control over his product to assure a reliable quality expectancy. This attitude of the Middle Ages is not greatly different from the modern one; it is just applied in a more complicated engineering framework today.

Be it the Middle Ages or the Space Age, the intent of quality assurance is to attain a successful end result for the user at an acceptable cost for the engineering result with a reasonable risk to the engineering sponsor. This accomplishment might mean different things to different engineering organizations. For a producer of materials, an acceptable cost might be the cost at which he could market 100% of his production capacity. But a user who needed only a small amount of that material might be willing to pay severalfold the prevailing market price to assure its successful use in his application. The engineering sponsor's

*Oak Ridge National Laboratory is operated by Union Carbide Corporation, Nuclear Division, under contract with the United States Atomic Energy Commission.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

GA

prime interest in quality assurance stems from his need to control the level of risk that accompanies his capital venture. The implication is that among the participants in an engineering enterprise, different terms of quality evaluation may prevail. The relationship between quality assurance and the engineering sponsor's management practice is discussed here. The intent is to show how the effectiveness of a quality assurance system is influenced by engineering management actions.

The methods used by an engineering sponsor to implement quality assurance usually involve several types of arrangements. The most common element used by the sponsor is probably a quality control and assurance department which is limited in responsibility to the product quality requirements as defined by sales-service agreements for customer or market needs. Such a quality assurance system is a service provided to the engineering sponsor by his suppliers, and in many cases, the sponsor has no control over its functions. As a counterbalance, the sponsor will often provide an inspection and test organization to serve as an acceptance group for the sponsor for determining whether contractual agreements with suppliers and constructors are being satisfied. Additionally, an engineering review function is sometimes used by the engineering sponsor as a part of his quality assurance system to provide an overview of specific areas where engineering practice and performance considerations must be correlated. An operational-use group, supplemented by engineering consultants, often serves this purpose. For very complex applications, the sponsor may establish a separate engineering control group oriented to the selection of engineering standards, analysis methods, and safety evaluation techniques. This group will function under the direction of upper-level engineering management to provide an independent check on design as well as construction. Occasionally, a top-level-management review group functioning under the sponsor's direction will be set up to determine whether the engineering execution is consistent with sponsor risk philosophy.

Each of these quality assurance arrangements has its own disciplinary requirements and deserves special consideration with respect to the interests of the engineering sponsor. The subject is so broad that complete coverage here would be impossible. This discussion will be limited to

treatment of a few of the more important characteristics of the above-mentioned quality assurance elements. Attention will be confined to the engineering management philosophy in dealing with risk evaluation and performance verification.

Quality Assurance and Engineering Interface

Decision implementation is generally considered to be the principal function of engineering. Given a set of objectives by a sponsor, the engineering responsibility is to decide how these objectives can best be accomplished, beginning with conceptual ideas and finishing with an operating result suited to the sponsor's purpose. Quality assurance is a tool used by the sponsor to establish whether the engineering decisions are well founded and properly implemented. Thus, the quality assurance function is the policing of engineering decisions. The only decision making involved in this function is the determination of whether engineering decisions are well founded. Typical decision matters are

1. whether the engineering is based on suitable resources,
2. whether the engineering technology is properly understood,
3. whether there are suitable quality control arrangements to guide implementation of the engineering, and
4. whether the decision-making apparatus is able to make timely engineering decisions.

These considerations may seem strange to those used to identifying quality assurance with surveys of record controls in manufacturing and construction operations. What most people consider as current quality assurance practice is really only the audit system used to monitor quality assurance effectiveness. The quality assurance approach with which we are dealing begins long before the conventional audit system is put into action. It spans the entire engineering program and calls for knowledgeable evaluation and control of engineering decisions at a point in time when engineering action is controllable with a reasonable cost and risk to the sponsor.

In this comprehensive approach to quality assurance, the decision actions are evaluated by responsible representatives of the engineering sponsor. Regardless of whether the evaluation is performed by a high-level management panel or a lower-level quality control group, the purpose is to make certain that each important decision is separately examined by an individual or group who understands the engineering sponsor's viewpoint and has a suitable risk aversion attitude concerning the pitfalls resulting from a faulty decision. This examination provides the engineering sponsor with a means of attaining a clear perspective of the engineering risk considerations, thereby permitting him to exercise control over the risk he is willing to accept.

The quality assurance action usually interfaces with the engineering management actions through direct contact between engineering participants. This often means head-to-head discussion in which all of the interrelated decision factors are laid on the table for consideration by both the quality assurance and engineering management participants. The attention of the quality assurance participants is directed toward determining whether the criteria for judgment are valid and whether they have been properly considered. It is the responsibility of the quality assurance participants to recommend against decisions when the judgment criteria are improperly evaluated. But engineering management and the engineering sponsor must jointly decide whether to accept the quality assurance recommendations since the basic judgment consideration involves the acceptability of risk by the sponsor. The importance of this joint decision cannot be overemphasized. An overly rash or overly conservative decision by the sponsor could leave engineering management without sufficient latitude to effectively implement the decision.

Adversary Relationships

The number of participants involved in any large engineering operation and the variety of their interests guarantees that the motivation of some participants will not be totally consistent with the quality assurance goals of the project in question. A customer satisfaction

motivation based on the premise that "the customer is always right" is traditional in a buyer's market, but it does not suit the modern engineering environment. Consider, for example, the base metal manufacturing business. The bulk producer of steel plate or the quantity supplier of forgings can hardly concentrate his engineering attention on the meticulous needs of one customer who is attempting to use the extreme capabilities of the material. The supplier tailors the quality assurance requirements of his product to satisfy the less severe demands of the average customer. It is normal to expect that the material supplier will resist attempts to impose the most severe requirements of the special user because it interferes with this normal mode of operation. Often the special user cannot provide sufficient profit incentive to motivate the bulk supplier to alter his mode of operation.

When the goals of two or more engineering participants fail to mesh, their diverse interests may lead to an adversary relationship. Such a situation sometimes arises because risk-sensitive engineering managers are prone to shift the risk burden away from their sponsors. But those who are being asked to assume the risk are not likely to do so without commensurate profit potential. The concern of engineering management is the establishment of an effective balance between the risk-taking and risk-averting positions of the participants. In a marketing sense, this balance is often dependent upon whether the engineering action is being executed in a seller's market or a buyer's market. The compatibility of the marketing situation with the realities of the engineering risk is the governing factor. Since time and circumstances usually influence market agreements, all aspects of engineering risk are seldom covered in marketing contracts. Even liquidated damage arrangements provide only limited risk insurance. The aim of the quality assurance approach is toward fair apportionment of the risk and profit potential among participants regardless of market conditions.

The arrangement under which heavy steel plate is provided to fabricators of nuclear vessels is illustrative of this approach. The steel plate supplier is asked to provide a product with a very low defect frequency and to affirm the quality of his material with suitable nondestructive tests. The vessel fabricator adds certain additional

quality requirements to the plate for which he has no economic recourse to the supplier. Each accepts some risk and some profit opportunity from the successful use of the end product. Both are motivated to attain success for the engineering sponsor, who is buying the services of both the base metal supplier and the vessel fabricator.

If the engineering sponsor should choose to require that the plate supplier accept all responsibility for the quality of the product, which he now shares with the fabricator, without adding any further profit opportunity; the plate supplier is certain to resist such an arrangement. Even when marketing circumstances provide sufficient leverage to override this resistance, experience has shown that the supplier who ultimately must incur an unusually large share of the loss potential will find a way to avoid this risk. Hence, the risk reduction from marketing situations is often illusory, and the precept of fair apportionment of risk and profit opportunity is essential in motivating all participants toward engineering success.

Controlling the Level of Quality Assurance Interdiction

The criticism most often directed toward quality assurance is that it hampers engineering efficiency. Whether this is so is debatable. For the most part, acceptable efficiency is more a matter of what is tolerable than what is optimum for effective engineering. One could hardly argue against the extensive checking and rechecking involved in the engineering of a space vehicle. The cost has been deemed reasonable, and the fantastic reliability speaks for the success of the quality assurance approach. While adequate success might have been attained at less cost, the fractional cost reduction could have no meaningful value in this instance.

However, the circumstances in the space program are not typical. Most engineering actions are governed from the beginning by some closely controlled cost level assigned to the task by an engineering sponsor. Once the assignment of cost and the resources which it represents has been made, the level of engineering effort is defined. The effort must

then be distributed to attain the most effective results, and the type of quality assurance program that will best exercise effective control over the effort must be selected.

We know that it is impractical to review every engineering decision in detail. The engineering effort would become cumbersome and the participants would lose that sense of responsibility which is an all-important motivational force. Those assigned the responsibility for quality assurance must therefore be highly selective in choosing the review times and the nature of the evaluation to be made. Significant stages of the engineering activity can be preselected for comprehensive evaluation of the engineering status, or the current status at the time of review can be used as a guide to the need for future review actions. Systematic program plans and reporting systems in which decision actions and their implementation are defined in written form can also be used as a guide. Ad hoc examinations of engineering subjects which have been shown to need evaluation by current events can also be called for. Some portion of this approach can be systematized and prearranged with the engineering participants. A large portion is contingent upon the interpretation of day-to-day signals, some of which may be recognized by experienced engineers as warning flags suggesting the need to take stock of the current situation.

The nature of the control measures to be applied is best indicated by previous experience. In most repetitious engineering programs, we know what is customary. For example, shop drawings for pieces of specialized hardware must be reviewed before fabrication is started. The test reports for shop-tested equipment will be examined before the equipment can be shipped from the supplier's plant. The qualification records for craftsmen must be reviewed and evaluated before the men are assigned critical work. These are customary quality assurance measures, and they form a part of the basic quality assurance program which most engineers consider standard practice.

Those concerned with quality assurance must decide whether such customary engineering practices are suitable and sufficient for the application in question. The really critical determination is whether further action should be taken to alter the customary engineering practice,

as was done for the space program and is now being done for nuclear power installations. The need for such action is determined by first studying previous engineering experience and then considering new circumstances that might change the nature of the quality assurance requirements.

The judgment made in the space exploration program was that customary engineering practices would not be adequate for the application. As a result, an elaborate set of new quality assurance practices was introduced for the space program. Generally speaking, the new practices were built around the successful procedures already developed for the aircraft industry. The difference was the introduction of more extensive engineering analysis, more comprehensive control of materials and fabrication practices, and most importantly, a more critical examination of failure contingencies and failure defense arrangements. The judgment to institute the new quality assurance practices undoubtedly resulted from reconsideration of the risk factors involved in this new application and an appraisal of the engineering problems associated with the risk considerations used in the aircraft industry.

The same type of shift in quality assurance practices is now taking place in the nuclear power industry. This is reflected in the recently published ANSI Standard N-45.2-1971, "Quality Assurance Program Requirements for Nuclear Power Plants". These new quality assurance requirements are founded on previous experience with fossil-fueled power systems, the use of these older practices in more recent fossil-fueled power plants, and the results of early application of these practices to nuclear power installations. The quality assurance practices of the aerospace industry have been introduced through interchange between personnel of the nuclear and aerospace industries, resulting in an intermix of the techniques of both industries. The nuclear engineering procedures commonly used in the nuclear navy have also contributed heavily to these new quality assurance practices. Thus, the new requirements of ANSI Standard N-45.2-1971 represent a consolidation of conventional power plant, modern aerospace, and nuclear navy practices best suited to the nuclear goals of public safety and performance reliability. However, the new practices would not have been instituted in the nuclear power industry if the engineering

sponsors had not seen the need to reconsider their quality assurance practices because of an increased emphasis on public safety and system reliability.

But new risk factors need not be the only impetus for changes in quality assurance systems. Consider, for example, the recent developments in the use of tape-controlled machining operations. The quality assurance methods applied to metal machining in the past involved frequent dimensional checks against reference drawings that were made with gauges and measuring fixtures. Now that tape-controlled automated systems are in general use, the older quality assurance practice is cumbersome and would make the new manufacturing techniques inefficient. Quality assurance in the automated system is established by manufacturing a prototype production unit or making practice runs to determine how the automated operation fits the requirements at critical dimensional checkpoints. Once this determination has been made and the tape control confirmed, there is no reason to worry about the operational errors that were common in human-controlled machining operations. Thus, much of the older quality assurance practice, which was directed mainly toward controlling human error, can be eliminated. Some elements of the older quality assurance system must be retained because wear and tear of the tooling and possible malfunction of the controls must still be accounted for. But the focus of attention is now on machine malfunction, whereas previous attention was directed toward human error. In this case, technological developments have caused a new quality assurance approach to displace much of the older one.

Although the current vogue is to update all engineering activities by instituting new quality assurance systems, each engineering organization has to decide whether existing methods are satisfactory and appropriate to its end purpose. The presumption that the most modern method is the best method of exercising engineering control is not always true. For example, many engineering organizations now require full radiographic examination of all high-vacuum welded connections, but the results are often no better than those attained by using low-pressure soap-bubble testing methods. The result sometimes is only a more costly end product;

thus, the new inspection requirement has doubtful value. The point is that if the quality assurance approach in current use yields satisfactory results, a change in the approach must be justified by improved engineering effectiveness or a valuable reduction in engineering risk.

Value of Standards to Quality Assurance

The emphasis on customary practice and balanced engineering effort in the quality assurance function demands the identification of reference experience as a means of defining customary practice and weighing the engineering balance. Engineering standards are recognized to be the most usable devices for this purpose. Every organization that engages in repetitive engineering actions tries to perform its engineering in a manner that will make the work reusable. Every new engineering job is begun by trying to take advantage of what others have done before. The net result is that knowledgeable engineering managers start their efforts by demanding a definition of the reference standards that will be used as an engineering basis.

These standards are really only documented descriptions of successful engineering methods, but the quality assurance controls and the risk evaluations that engineering sponsors rely on to determine success probability are built into them. Most engineering sponsors are unaware of the risk control considerations included in standards, but discussion and common gossip in the business community direct the sponsor to the use of standards even though he may not comprehend their risk significance. The same approach applies even to public regulatory bodies who find that the only practical way to exercise risk control in the public interest is through engineering standards. Thus, both engineering sponsors and regulatory groups have a common interest in this quality assurance tool.

However, the use of standards cannot be an effective quality assurance measure unless the risk evaluation implications of the standards are understood. For example, the engineering standards associated with "improved risk" fire protection for industrial installations are

directed toward limiting property damage loss to less than \$1 million for any fire incident. But this limitation is not a 100% certainty. It represents a judgment of the insurance risk evaluation community that the imposed engineering standards will be consistent with the risk utility on which the capital use is premised. To extend the fire protection standards from conventional industrial installations to a unique technological facility, such as a space vehicle launching stand, would undoubtedly be stretching the use of these standards beyond the risk premises upon which they were founded. But the standards are still very useful as a frame of reference for this purpose if they are used as a comparison basis in determining whether the new technological factors influence the risk considerations. The standards can then be applied with suitable modification to account for the new risk factors.

Within the quality assurance framework, there must be differentiation between the use of the term "standards" as a mark of achievement and its use in a risk control context. What most of us mentally strive to attain are perfect engineering results the first time, and the standards we set for ourselves are often unattainable goals. We measure our success by how closely we approach the goals. But in the quality assurance context, we set standards which have a probability of attainment that is correlated with risk acceptability which is implied if not explicitly defined. To this end, those associated with engineering applications of quality assurance must deal with standards pragmatically. They are used when they fit the application, they are modified when circumstances warrant, and they are wholly restructured if the risk considerations require a different engineering approach.

Failure as a Quality Assurance Consideration

Inevitably, in some portions of a complex engineering installation, allowance must be made for unforeseen failures. The purpose of the quality assurance function is often deemed to be an evaluation of actions affecting failure frequency. Under such conditions, the measure of quality assurance effectiveness is how often failures occur in spite of

the quality assurance actions. Reliability analysis is sometimes used in very complex engineering applications (e.g., the design of air transport systems) as a gauge of quality assurance practice. Such reliability studies can be useful in almost any type of engineering execution. The relationship between failure frequency and engineering methods can show whether the selected engineering methods are appropriate to the application.

The quality assurance approach taken in considering the risk of failure is to analyze engineering reliability by examining the consequences of historical failure modes. A quantitative analytical statistics approach can sometimes be applied to engineering decisions to determine the value of such things as dual braking systems for automobiles, a redundant power supply for a control system, or even the replacement frequency for oil filters. In principle, the same approach could be used to establish fatigue crack limits for aircraft wing structures, heat treatment requirements for weldments, or the application of cast iron fittings to fire sprinkler piping. The only difference between the two categories is that in the first instance, there may be statistical data for mathematical evaluation, while in the second instance, the data may be useful only for highly uncertain statistical extrapolation. But regardless of whether actual or extrapolated failure statistics are used, the failure considerations are dealt with by reviewing historical failure incidents. The tolerance for the consequences of such failures is balanced against the vulnerability of the failure defenses to determine whether the quality assurance actions will satisfy the failure control requirements.

Frequently, however, there is no experience basis for failure evaluation. This is generally the case for an entirely new engineering concept. The use of failure analysis as an element of quality assurance in such cases is not ruled out, but the approach is through a speculative type of analysis sometimes called "what if" engineering. It is basically a systematic examination of the potential areas of failure, the modes of failure propagation, the ultimate failure consequences, and an examination of whether the consequences are tolerable. From this type of analysis, the backup protection to resolve quality assurance uncertainty is indicated.

For example, a fuel tank farm is usually laid out to assure that a tank failure and concurrent fire will not spread to adjacent tanks.

Special retaining walls are often provided around each tank to act as a sump for leaking oil as a secondary containing provision. To many people, this would not be classed as a quality assurance provision, but quality assurance is implicit in this engineering notion. The available engineering practices cannot guarantee that there will be no leaking tanks in the tank farm or that fire will not have the potential to spread from a leaking tank to other property. The retaining walls are a quality assurance backup provided to account for an engineering weakness arising from failure uncertainties.

Quality Assurance Documentation

So much emphasis is placed on documentation requirements for quality assurance purposes that their place in the quality assurance function should be understood. At best, documentation is only a written statement of quality needs and affirmative measurements. In most cases, it serves only to verify that certain quality control actions have occurred. But this documentation has a value in the quality assurance policing action of the same type that is attained by the individual who keeps track of his banking transactions through his monthly bank statement. Its usefulness to the engineering function develops when something goes awry during engineering execution. The record system often provides a clue to the solution of the engineering problem.

A quality assurance system might require the producer of alloy plate to keep track of certain process controls and to correlate these with the physical properties of the production run of material. When the physical properties do not meet the requirements, the process records might suggest the cause. The primary interest of the user is the final physical property data, but if he wanted to be certain that the producer would be able to sort out difficulties affecting production, it would not be unreasonable for process controls and their documentation to be made a part of his quality assurance requirements.

Generally, a material user examines the supplier's records only to determine whether the supplier is conscientiously controlling his product.

Documentation is needed to show what controls are being exercised and how the quality of the product is being monitored. The same logic is applicable to fabricators, constructors, and installers. The requirements for documentation may range from the simplest test records to elaborate detailed procedures, but basically the engineering purpose is to make certain that the executing agent knows what he needs to do, how to do it, and is taking the actions required to meet those needs.

Performance Proof Through Testing and Analysis

In spite of careful review of decision bases and close control of engineering execution by a quality assurance system, verification of engineering success still is heavily dependent upon performance proof of capability. The detailed engineering execution for more than one installation has been painstakingly controlled only to find that the composite result is inadequate for the intended purpose. Regardless of whether the engineering sponsor is protected by performance warranties or even liquidated damage clauses, he stands to lose at least as much as the supplier. Most often, he stands to lose more. Thus, verification of performance capability is a necessary ingredient of any quality assurance program.

The final proof of performance is, of course, in the actual operational use of the engineered result. But the tendency to place too much reliance on one final overall test is one of the great fallacies of many quality assurance programs. While the final test can verify performance, it does little to minimize the risk of engineering error. Corrective action, at the very least, costs valuable time for beneficial use. The essence of effective quality assurance practice is therefore the verification of performance at the earliest opportunity. The engineering sponsor must make this a cornerstone of his quality assurance approach.

The quality assurance system must deal with what, when, and how to verify performance as a means of reducing risk. Timely testing and acceptance methods must be selected. In many cases, the selection of an acceptable supplier is contingent upon his ability to demonstrate the

performance capability of his product. Suppliers of pumps for use in nuclear power plants have established facilities for verifying the capability of their product prior to shipment. Manufacturers of large motors are expected to demonstrate the load characteristics of their product by shop testing as a part of the manufacturing program. A quality assurance program that is well founded will gain maximum risk protection from requirements for such shop testing of engineered hardware. Such requirements will be omitted only when the test cost is disproportionate to the risk protection or when the nature of the project is such that routine manufacturing practice has established a high probability for suitable performance.

However, all performance uncertainties cannot be resolved by shop testing, especially when system compatibility is in question. The shop test data can be used as a performance basis for analytical evaluation of system characteristics, and such analyses can do much to reduce risks prior to final acceptance. Performance uncertainties in the system are often exposed by such analyses, and the need for change or improvement in equipment performance is sometimes suggested. The timeliness of such performance analysis must be defined by the quality assurance program, and the determination of whether the analysis is to be based on actual equipment data or typical performance characteristics must be made. Multiphase analyses may sometimes be required so that test data can be considered promptly.

Summary

The aim of quality assurance is to make certain that engineering actions are controlled in accord with the objectives of the sponsor. The controls must have meaningful engineering purpose to have quality assurance value, and they must be geared to meet suitable engineering risk criteria. These controls are normally based on experience and custom, and they make maximum use of standards. The quality assurance system itself serves a policing function, but it must be balanced in such a way that all participants share in its benefits as well as its

disciplines. Documentation is used as a tool for auditing the engineering controls and for identifying problem areas. When the quality assurance system has the confidence of the engineering organization responsible for the work and has commensurate value for all participants, it will be an effective tool for attaining the objectives of the engineering sponsor.