Introductory Remarks

EDWARD P. COLEMAN†

WHAT does reliability mean? It is not strange to find that the term "reliability" means many things to many people. However, we hope to illuminate a number of these meanings which relate to the art, science, and industry of computing. Typical of many definitions in use today is the following:

> "*Reliability* is the *probability* of a *system* performing its purpose *adequately* for the *period of time* intended under the *environmental conditions* encountered."

In introducing the subject, one should speak briefly of some of the past and present trends in reliability. First, we mention the concept of improvement of reliability by the detection of unreliability. In order to isolate, examine, and improve reliability of a system, the reliability engineer puts his best efforts on the unreliability problem. He studies the failures in the system for it is only through corrective action on failed elements in a given system that significant improvement can be made. This technique is an old problem to quality control engineers, who have worked out many standard procedures for detecting unreliability based upon the Shewhart Control Chart and other fundamental contributions of the last quarter of a century.

A second concept, which is almost an economic derivative of the first, is that of improvement of reliability by the prevention of unreliability. Significant advances in reliability procedures are being made today, many of which have as their underlying principle the prevention of unreliability before hardware is put into production.

The placement of emphasis on unreliability appears to be a negative approach, which is standard practice in quality control organizations and which uses this so-called negative approach. In the quality control division of manufacturing industries, parts may be classified as "defective" or "nondefective." At the end of any such inspection, the number of defective parts are counted. If the number of defective parts exceeds a predetermined allowable number, the production process is halted, and it may not be resumed until the assignable cause for defective products is found and removed. Thus, the tradition in quality control of "detecting defects" and "preventing defects" seems to have a continued longevity in modern reliability techniques.

This point suggests what might appear to be a paradox. As an organization approaches its objective of the total prevention defects, it would appear to have less and less work to do in the future and ultimately none at all. This kind of thinking has manifested itself in industrial organizations in many forms. It has caused some quality administrators to not proceed first directly to the most important reliability problems. Moreover, it has caused some to attempt to build beautiful and permanent procedures for processing unreliability information. One moment of reasoning will show that reliability engineers are needed most where the going is most difficult and where reliability is least predictable. It goes against better nature to leave a beautiful, consistent, and predictable process with little or no unreliability and proceed to one which is ugly, inconsistent, and unpredictable; but this is the lot of the modern reliability engineer.

There are many terms being used today in reliability considerations. Let us list a few of these:

Physical Terms—Part, item, subassembly, assembly, and system.

Merit Terms—The term reliability itself as applied to general effectiveness of system. Reliability in supporting equipment and in operations. Minimum acceptable reliability and mean-time to failure.

Mathematical Terms—Risk, hypothesis, test, random variable, probability, population parameter, sample, and statistic.

Acceptance and Control Terms—Quality characteristic, rational subgroup, attributes, variables, process average quality, sampling plan, sample size, and operating characteristics function.

We first turn our attention to the fundamental concepts of reliability and then to the various details of the problem.

† Univ. of Calif., Los Angeles, Calif.

Keynote Address—Techniques for Reliability in Computers for Weapon Control

JAMES M. BRIDGES†

THE RAPID advances made in computer developments during the past few years have had a profound effect upon the security and economy of the country and upon all our lives. Today, the influence of the high-speed, high-capacity computing machine is being felt throughout our total society: in industry, commerce, science, education, medicine, and in many other areas of human existence and progress. The most significant use of the computer, however, in this era of international instability, is its vital role in maintaining our national security.

Because of my association with the Department of Defense, I am naturally most interested in those computer applications which are of the greatest importance to our defense. I wish I could discuss in detail all the different ways in which various kinds of computing machines are being used throughout the military organization. Since that would not be appropriate here, I am going to limit my remarks to the types of computers used for the dynamic control of weapons and weapons systems.

Since the computer is now essential to the effective performance of all modern weapons and weapons systems, it is obvious that a very high level of reliability is essential. I can assure you that we in the Department of Defense consider that the theme "Techniques for Reliability" is completely appropriate for this Joint Computer Conference.

I shall begin my discussion by presenting a little more detail on the widespread usage of computers in weapon control, together with a few highlights of their developmental history. Perhaps I should make it clear at this point that I use the expression "weapons and weapons system control" to include all computers involved in direct control of weapons such as guns, missiles, torpedoes, rockets, bombs, or aircraft and those involved in such functions as tracking, threat evaluation, and weapon assignment.

Although computing machines have received much publicity over the past few years, I seriously doubt that the vital role they have played in the development of military weapons is generally appreciated.

It is probably not widely known that the fire of naval and army artillery was being controlled with computing devices even before World War I started. I doubt if many appreciate the fact that the precision and capabilities of these weapon control computers have advanced steadily since Hannibal Ford started development of his first computer for naval fire control in 1915, until today practically every offensive or defensive weapon depends for its effective operation upon one or more of these computing devices, some very simple and others even more complex than the largest machines in commercial use today.

On one end of the size-complexity scale is the tiny computer that is packed into the nose of a medium-caliber bullet to compute the point in space with respect to an air target at which detonation should occur. On the other end of this scale are the huge digital computers in the ground environment of the air defense system, which employ tens of thousands of electron tubes and occupy thousands of square feet of floor space. Between these two extremes of size and complexity are scores of different kinds and sizes of computers, each performing a specific function in the dynamic control of some weapon or weapons system. Although the performance, complexity, and packaging requirements of these many types of control computers differ widely, the need for a high degree of precision and operating reliability is common to all.

Until very recently, all these diversified weapon control computers were of the analog type. Although much development work has been done on digital weapon control computers, to my knowledge there is no digital weapon control computer in actual military service operation.

Because the history of weapon control is truly the history of analog computer development, it may be of interest to review very briefly some of the development highlights. As I mentioned before, the history of the fire-control computer in this country started in 1915 when Hannibal Ford began to develop the first computer to control naval surface-to-surface guns. His early computers, known as "rangekeepers," represented the first application of precision analog techniques to the solution of the gun fire-control problem.

At the conclusion of World War I, the need for control of surface guns against aircraft became apparent, and Ford again pioneered with the development of the first antiaircraft-gun fire-control system. This system, completed in 1926, was designed to handle aircraft having a maximum speed of 95 knots.

The computation in these early analog computers was performed entirely with mechanical cams, differentials, multipliers, component solvers, and integrators. With the exception of the electrical contact-type servos, the reliability of these mechanical analog computers was controlled almost entirely by the mechanical designer

† Office of the Assistant Secretary of Defense, Washington, D. C.