# A SYSTEMS ENGINEERING APPROACH TO RELIABILITY

Alexander W. Boldyreff

November 1961

P-2476

# A SYSTEMS ENGINEERING APPROACH TO RELIABILITY

Alexander W. Boldyreff*

Consultant to The RAND Corporation, Santa Monica, California

Professor of Engineering and Production Management, UCLA

Systems engineering may be defined as an activity aiming at optimum operation of existing complex integrated systems or optimum design and development of future systems.

This activity must necessarily start with a good understanding of the customer's mission, of the state of the art as a function of the time, and of the budgetary and time constraints.

System optimization can then be reduced essentially to seeking the best balance between performance, reliability, and cost.

Here the cost must be measured both in time and in dollars, and the latter must include not only the development and manufacturing costs, but also the cost of handling and transportation, storage and surveillance, support equipment, maintenance, replacement, logistics, and personnel and their training.

The old definition of reliability as the probability of failure-free operation, for a specified length of time, and in a specified environment, is both incomplete and inadequate.

---

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

This paper was prepared for presentation at the 11th National Conference of the Aircraft and Missile Division of American Society for Quality Control, Los Angeles, California, November 9, 1961.

Likewise the computation of reliability of a complex system from the reliabilities of its components is often of questionable utility.

Reliability must be approached as primarily a problem of design, not a mere exercise in elementary statistics. The primary goal should be achievement of reliability; reliability measurement and prediction, while important, are merely secondary.

As an example, let us assume a series system of n components, such that the failure of any one component results in system failure. It is usual to estimate the reliability of such a system in terms of the (geometric) mean component reliability.

Consider then a system of no more than 500 components. For systems reliabilities of 0.70 and 0.95, the mean component reliabilities are 0.99929 and 0.99995, respectively. Thus, it may be argued that the reliability of the system can be increased from 0.70 to 0.95 by an improvement in mean component reliability of only 0.07 per cent. But of course this reasoning is misleading. Component improvement means decreasing the probability of failure. In this example, to improve system reliability from 0.70 to 0.95, requires decreasing the probability of component failure from 0.00071 to 0.00005, and this means elimination of more than 90 per cent of failures of components which are already highly reliable. This can only be done through extensive and expensive testing to determine the assignable causes of failure, the actual physical mechanisms of failure, and subsequent redesign, followed by more testing. To carry out such a program for each of the very large number of different components of many complex systems now in the process of development is patently impossible, even at a prohibitive cost in time and money.

While I do not underestimate the importance of component reliability improvement programs, I do feel that such programs alone are not enough.

Furthermore, the whole concept of component reliability is hard to define. Unlike such physical constants as mass, volume, density, etc., component reliability cannot as a rule be described by a single number. Thus, the same vacuum tube may have a mean life to failure of 10,000 hrs in ground equipment, 2500 hrs in aircraft, and only 13 minutes in a missile.

It is for the above reasons, and because of a general lack of faith in numerology, that I have been concerned during the past twelve years with a systematic study of the problem of reliable system design using existing and therefore none too reliable components.

This is then the main theme of my present paper. The central point, of course, is that reliability must be sought as an integral, and perhaps the most important part, of the over-all system design.

I shall begin with a listing of what I believe should be the principal areas of concern to a reliability engineering organization:

1. Conceptual design. This is where reliability improvements can be gained in big chunks, instead of infinitesimals, through relaxation in unnecessarily stringent performance requirements, with the resulting reduction in system complexity.

2. Malfunction reporting in test and field.

3. Environmental tests in laboratory and field.

4. Reliability analysis and prediction.

5. Determination of assignable causes of failure, and of the actual physical mechanism of failure.

6. Recommendations of redesign.

7. Shop follow-up and project coordination.

8. Recommendations of optimum maintenance and logistics.

9. Education:

a) of reliability engineers

b) of management

c) of the customer

d) of the designers.

10. Standards, vendor evaluation, and receiving inspection.

11. Manufacturing inspection and quality control.

12. Handling and transportation.

13. Storage and surveillance.

14. Procedures for sound operational use.

I shall next give a short list of some general methods of increasing system reliability which I believe to be basic in designing for reliability.

These are as follows:

1. Critical examination of systems objectives in the light of customer's mission, the state of the arts, and the costs involved.

a) Avoidance of excessive performance requirements and consequent reduction in complexity.

b) Avoidance of multifunction systems, whenever these functions can be separated.

2. Designing for realistic environment.

3. Designing for producibility and maintainability.

4. Designing with a clear understanding of the conditions of operational use.

5. Using tested (proven) components whenever possible.

6. Using standard mechanisms and circuitry whenever possible.

7. Maximum standardization.

8. Optimum use of modular design.

9. Development of reliable failure detecting equipment.

10. Optimum use of redundancy.

11. Widest possible use of fail-safe design.

12. Provisions for adequate customer training.

13. Provision of adequate support equipment.

14. Intelligent use of approximate solutions as a means of simplifying mechanization.

15. In manned systems, provisions for maintenance without interruption of operation.

Time will not permit a detailed discussion of each of these subjects.

Instead I would like to concentrate on just one of these—that of the uses of redundancy.

It has been generally recognized that in the case of aircraft, after a half-century of experience, acceptable reliability was attained only through redundant design, so that if one component failed another could assume its function. It is because of this that while some kind of failure (calling for emergency service outside of normal maintenance routine) may occur in aircraft every seven and a half hours of flying, the ratio of such failures to disasters is ten thousand to one. Not so for those systems that are strictly serial in nature. In such systems every component must function properly for successfuly system operation, so that the failure of a single component fails the system. The guided missiles and many other weapon systems are examples of systems that are almost entirely serial in nature in this sense. Here the ratio of failures to disasters is one to one.

It is customary to express the reliability of a series system by the product of the reliabilities of the components. The realism of this

assumption is open to serious doubt, except for those cases where the individual components have reliabilities of the same magnitude, and component failures may be treated as independent events.

Nevertheless, with this assumption, we can readily see the dramatic way in which complexity decreases reliability. Thus 100 components with mean reliability of 0.90, when operating in series have a system reliability of only 0.000026, or practically zero.

However, if it were possible to replace each component of this hypothetical system by three components in parallel, the new system would have a reliability of 0.90.

Why is it then that paralleling or redundancy is not used more widely? There are several good reasons:

1. In many cases redundancy is either impossible or impractical.

2. In all cases the use of redundancy implies penalties—of added volume, weight, power, environment control, increased frequency of component failure and corresponding increase in maintenance, spares, etc. Likewise, uncritical use of redundancy may seriously affect performance. For example, the increase in weight will decrease the range.

Nevertheless, redundancy is used extensively in the design of manned aircraft and is standard practice in the design of more critical subsystems of special weapons.

Simple paralleling of components is not the only type of redundancy, and I shall now describe several other, less familiar, types.

1st Example

In a certain subsystem successful operation required simultaneous proper functioning of some thirty-five identical components.

With a mean component reliability of 0.99, the subsystem reliability was 0.70—unacceptably low.

The solution of the difficulty was found in the subsystem redesign such that successful operation required that any thirty-four components worked, tolerating the failure of any one (but not more than one) of them.

This simple expedient raised the reliability to 0.94.

2nd Example

Many types of components are characterized by being, at any given time, in either one of two mutually exclusive states:

open or closed

off or on

non-conducting or conducting

0 or 1

Proper operation of such devices consists in the transition from the first state to the second at a specified time.

Switches or valves are simple examples of such devices

Let us use a single throw switch as an illustration.

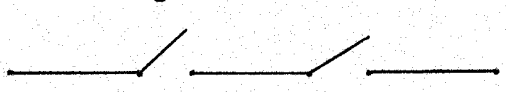
There are clearly two modes of failure possible:

a) the premature failure, when the switch closes before it should, and

b) the dud failure, when it fails to close at the specified time.

Let the probabilities of these two modes of failure be denoted by $f_c$ and $f_o$ respectively.

Suppose instead of a single switch we use two switches in series:



Now the probability of premature failure will be given by

$$F_c = f_c^2$$

and the probability of dud failure by

$$F_o = 1 - (1 - f_o)^2 = 2f_o - f_o^2$$

For a concrete example, let $f_c = f_o = 0.001$. Then

$$F_c = 0.000001 \quad \text{and}$$

$$F_o = 0.002,$$

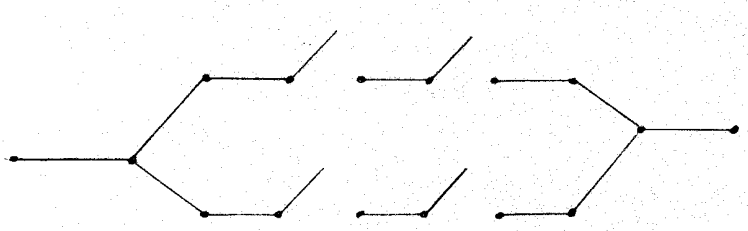
so that the series arrangement, while very greatly decreasing the probability of premature failure, doubles the probability of dud failure.

When the two switches are arranged in parallel the situation is reversed. Now

$$F_c = 2f_c - f_c^2$$

$$F_o = f_o^2 .$$

This suggests a series-parallel arrangement of four switches as shown below:



For this network the premature and the dud failure probabilities are given by:

$$F_c = 1 - (1 - f_c^2)^2 = 2f_c^2 - f_c^4 , \quad \text{and}$$

$$F_o = [1 - (1 - f_o)^2]^2 = 4f_o^2 - 4f_o^3 + f_o^4 .$$

Again let us assume $f_c = f_o = 0.001$.

Then, for a single switch the total probability of failure is

$$f = f_c + f_o = 0.002 ,$$

while for the series–parallel arrangement of four switches

$$F = F_c + F_o = 0.000006 ,$$

a tremendous improvement.

Such reliability net works have been comprehensively studied at Sandia, but unfortunately this work is virtually unknown, and very little use is being made of these ideas in actual design.

Example 3

Perhaps the most striking example of the use of redundant design may be illustrated by the following hypothetical case.

Assume in a transport airplane a communication system composed of two identical VHF sets, two identical UHF sets, and two identical LF sets.

The operational conditions are such that only one communication channel is to be used at any one time.

Each of the six sets is a complete, self–contained system. The equipment inside each box may be theoretically divided into three parts: the power package, the amplifier section, and the oscillator section.

Suppose the sets were redesigned so that the power supplies, amplifiers, and oscillators would be built as modules.

With proper switching there would be now eight different ways of operating on each of the three frequency bands, instead of only two.

Considering the extremely high state of the switching art, the addition of switching should have a negligible effect on the over–all system reliability.

Now, let us take the next logical step.

It is certainly an easy matter to design a general purpose power supply capable of operating any of the sets.

Although, more of a problem, the design of general purpose amplifiers is also technically feasible with a sufficient R and D effort.

We now could replace the old communication system by one composed of two general purpose power sources, two general purpose amplifier sections, six oscillator sections, and proper switching.

Let us now take inventory.

In the present system we have an equivalent of eighteen pieces of equipment, nine different equipment types, and only six ways of getting through.

In the proposed system there are only ten pieces of equipment, only five different equipment types, and twenty-four possible channels of communication.

A comprehensive use of the above design philosophy would not only increase reliability, but would also decrease equipment weight and volume, reduce frequency of failure, decrease maintenance, decrease spares inventories, simplify logistics, reduce procurement requirements, and generally lead to tremendous savings.

Successful implementation of a reliability program involves not only technical problems, but similarly important organizational and management problems.

Time will not permit me to go into a discussion of the latter.