APPROACH TO RELIABILITY WHEN APPLYING NEW TECHNOLOGIES

John C. Bear, General Dynamics Corporation
(Pomona Division), Pomona, California

ABSTRACT

General principles derived from experience in achieving high reliability in tactical weapon systems are selectively summarized for application to new technologies in unusual environments

INTRODUCTION

The General Chairman of this meeting, in suggesting some topics for this paper, observed that much of the technology which is important in precise time and time interval applications is new and immature in the sense that it has not been fully qualified for the most demanding field applications. Tactical weapon systems, while different in many respects from PTTI applications, probably face similar risks in achieving reliability in development. A supersonic guided missile, for example, must cope with continuing modernization of its state-of-the art sensors, oscillators, and other special-purpose devices, and it must operate reliably in severe environments including high and low temperature, shock, and vibration. Perhaps some of the lessons learned in the development of tactical weapons can therefore be of value in PTTI applications.

PRINCIPLE NO. 1: START EARLY

During development the reliability of a design grows as the sources of failure are unearthed and eliminated. In this context reliability is more or less synonymous with maturity, whereas state-of-the-art technology is by definition infantile. It follows that any successful approach to the problem will require an early start and an acceleration of the normal processes for avoiding or removing the root causes of failure (Figure 1).

But many factors inhibit an early start. Cautious program managers are reluctant to transfer funds allocated to the downstream "curative" engineering into the category of upstream "preventive" engineering. After all, testing is certain to produce failures, whereas an analysis has only a probability of payoff. Then too, managers who have grown up under the heavy influence of Murphy's Law do not necessarily believe that the really big failures are preventable. Furthermore, state-of-the-art designs deal with arcane concepts that do not easily yield to analysis nor readily reveal their weaknesses. Also, the reliability experts do not come from an ancient and universally admired discipline, and their ministrations are not always trusted.

For these reasons, it is necessary to adopt a high-level, deliberate, well-focused management determination to attack unreliability at the beginning, to muster up a lot of interest and excitement in specific approaches, and to reward creative planning and successful effort. A good way to converge quickly on a plan of action is to prepare a list of the devices or design elements that are immature, and identify for each item on the list a series of tasks that will reduce the risk. What follows is a discussion of some of the more useful tasks.

PRINCIPLE NO.2: KEEP IT SIMPLE

Complexity and sophistication, obviously, are the primary obstacles to the achievement of reliability in the initial design. On the other hand, a simple design (Figure 2) is straightforward, well-balanced in its accomplishment of the essential requirements, and free of frills--one might say it is elegant in concept. But how can simplicity be achieved while striving for some new and difficult level of performance?

An effective (but often neglected) procedure for achieving a balanced design is the design trade study (Figure 3). Its value lies in forcing alternative design solutions to the surface, in clarifying the relative importance of requirements (indeed providing the basis for deleting requirements that are "costly" in one way or another), and in suggesting back-up designs in case the primary selection fails to prove out. The trade study technique adapts well to the simulataneous analysis of multiple parameters (reliability, weight, power consumption, cost, etc.) and is an excellent mechanism for bringing design features and weaknesses out of the hallowed shadows of the expert mind.

Another method for promoting simplicity, especially on larger systems, is component standardization. The benefit, of course, is reduced variability and thus fewer sources of failure. But where a design applies redundancy as a way of compensating for low reliability, one must beware of standardization in the parallel components, for under severe stress they will tend to suffer the same failure modes, thus negating the assumed independence in the probabilistic model that justifies the redundancy.

Another technique for achieving design simplicity is the FMEA (Failure Modes and Effects Analysis). There are many different ways to do an FMEA, and the scope of the analysis can be adapted to designs of different sizes. In essence, the object of the FMEA is to examine the dark side of the design. The bright side, of course, is how it works or is supposed to work, whereas the dark side is how it can fail and what will be the consequences of failure. A good way to perform the FMEA is with a team composed of the design engineer, the systems engineer, and the reliability engineer. Pooling their different viewpoints can often lead to a simplified design if they do the analysis early in the development process when changes are still relatively easy to incorporate.

PRINCIPLE NO. 3: MAKE IT STRONG

Assume now that an attempt has been made to simplify the design, with a concentration of effort on the state-of-the-art technologies that will dominate the failure rate of the operating system. The final step is to take the resulting, optimized design concept and make it strong enough to withstand its usage environment.

The general concept of conservative design (Figure 4) takes the view point that environmental stress is the ultimate cause of failure, so that failure prevention is a matter of assuring adequate separation between expected strength and expected stress.

To begin with, it is necessary to define the environments with full respect for their lethality, with regard for not only their average values, but also for their natural variability and worst-case values. The design specification must reflect these worst-case expectations.

Then the strength objective is established, either in the same specification or in formalized design guidelines. Ideally the strength requirement will take the form of a safety margin, which sets strength as a function of both its average and its variance. Or, when the variance is not known or is not a problem, the objective will take the form of a safety factor (for mechanical designs) or a derating factor (for electronic designs).

Finally, the strength-minus-stress difference is controlled by analysis. That is, a stress analysis is performed on the design before it is released so as to assure that the specifications and guidelines have been followed. Even though safety factors are as old as engineering itself, they suffer de-emphasis whenever there is pressure to squeeze extra performance out of a state-of-the-art device. The stress analysis is essential, therefore, to enforce the guidelines, to surface the risks, and to assure time for pursuing alternatives.

WHEN ALL THIS FAILS

If the foregoing approaches to preventive analysis do not materialize for one reason or another, what then? The standard fall-back position is to rely on testing, followed by diagnosis and fixing of test failures so that they can't recur. A very good technique for flushing out problems early in the test program is the overstress screen (Figure 5)). In applying this test, the high-risk devices are exposed to one or more important environments to assure that they individually exhibit an adequate strength-stress safety margin. The stress level should exceed the worst-case expected stress in actual usage. The type of environment(s) should be tailored to the suspected weaknesses of the device. The test should be performed as early as possible, ideally by the designer or supplier. Proposals for this kind of testing can evoke outspoken (and usually unwarranted) fear of damage and wearout, which can be dispelled by exploratory step-stress testing of dedicated or spare hardware.

SUMMARY

The key to achieving reliability in new technologies is to really want it--that is, to align the development team toward the essentiality of reliability right at the beginning. Given that significant attention will be devoted to

reliability early in the design phase, there are a number of analytic tools such as trade studies and failure modes analysis that will help keep the design simple, and others such as derating and stress analysis that will help make it strong. Further down stream, when hardware is available, an environmental overstress screen in selected environments will help expose remaining problems. In applying these techniques success will be directly proportional to the care with which they are tailored to fit the specific design program.

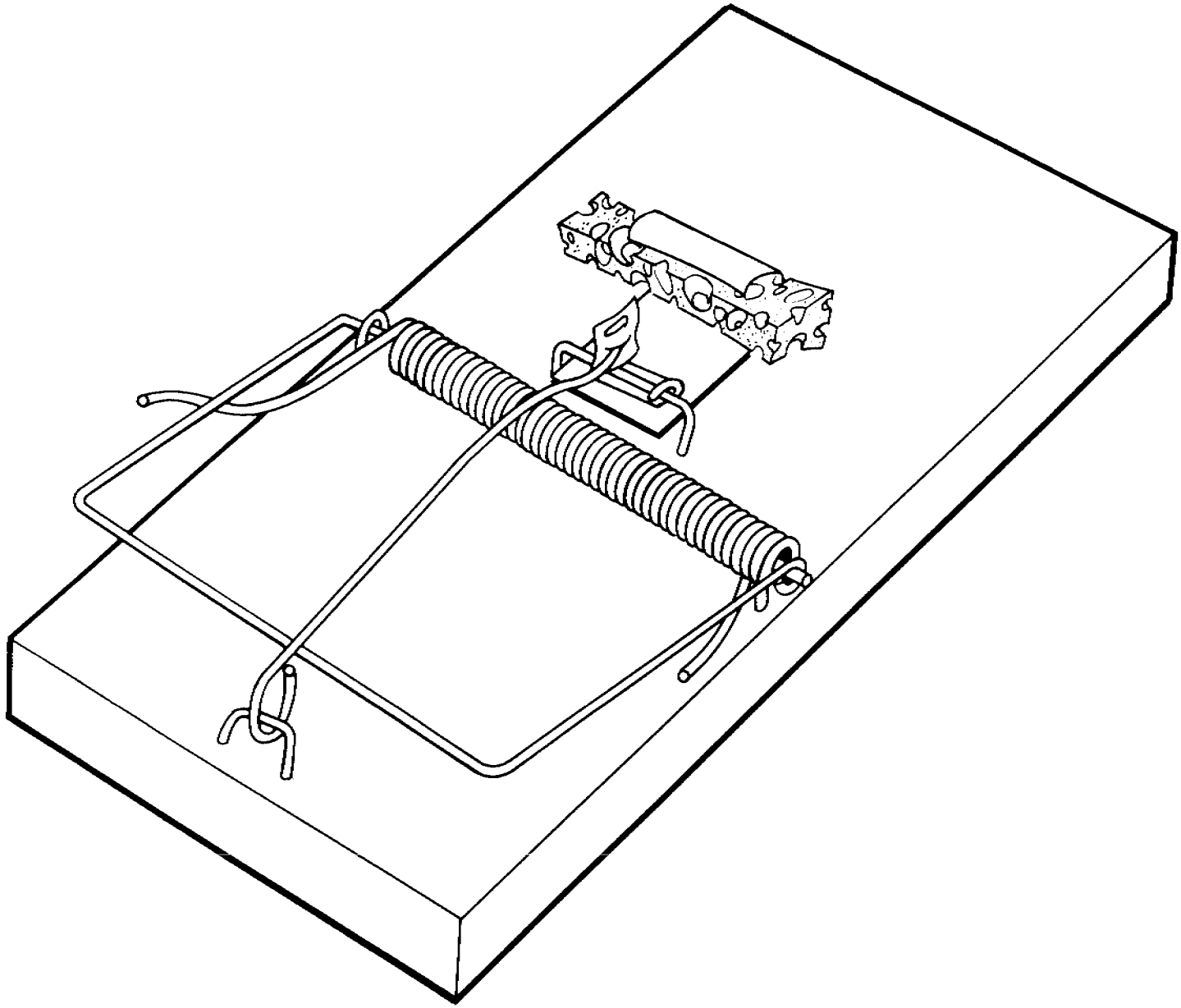
FIGURE 1
START EARLY

- STATE-OF-THE-ART MEANS RISK

- CURATIVE ENGINEERING IS TOO LATE
  - BUT PREVENTIVE ENGINEERING CAN BE HARD TO SELL (DOESN'T GUARANTEE TO FIND ALL THE FAILURES)

- THEREFORE THE BOSS HAS TO GET INVOLVED AT THE START
  - ESTABLISH RELIABILITY AND PERFORMANCE CO-EQUAL
  - IDENTIFY A LIST OF RISK ELEMENTS
  - FUND SPECIFIC TASKS TO REDUCE RISK

KEEP IT SIMPLE



F269083 8110

FIGURE 3
DESIGN TRADE STUDIES

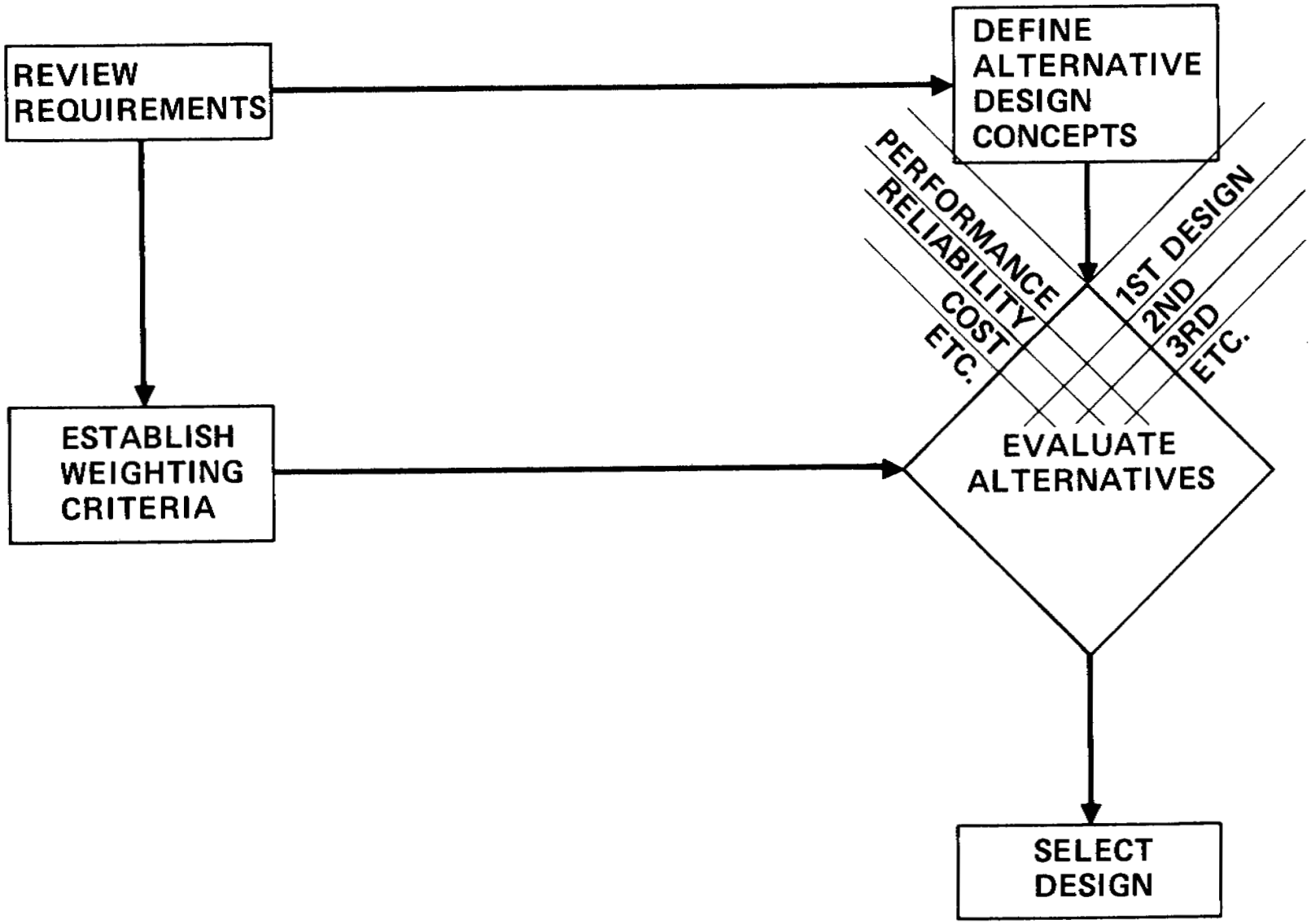
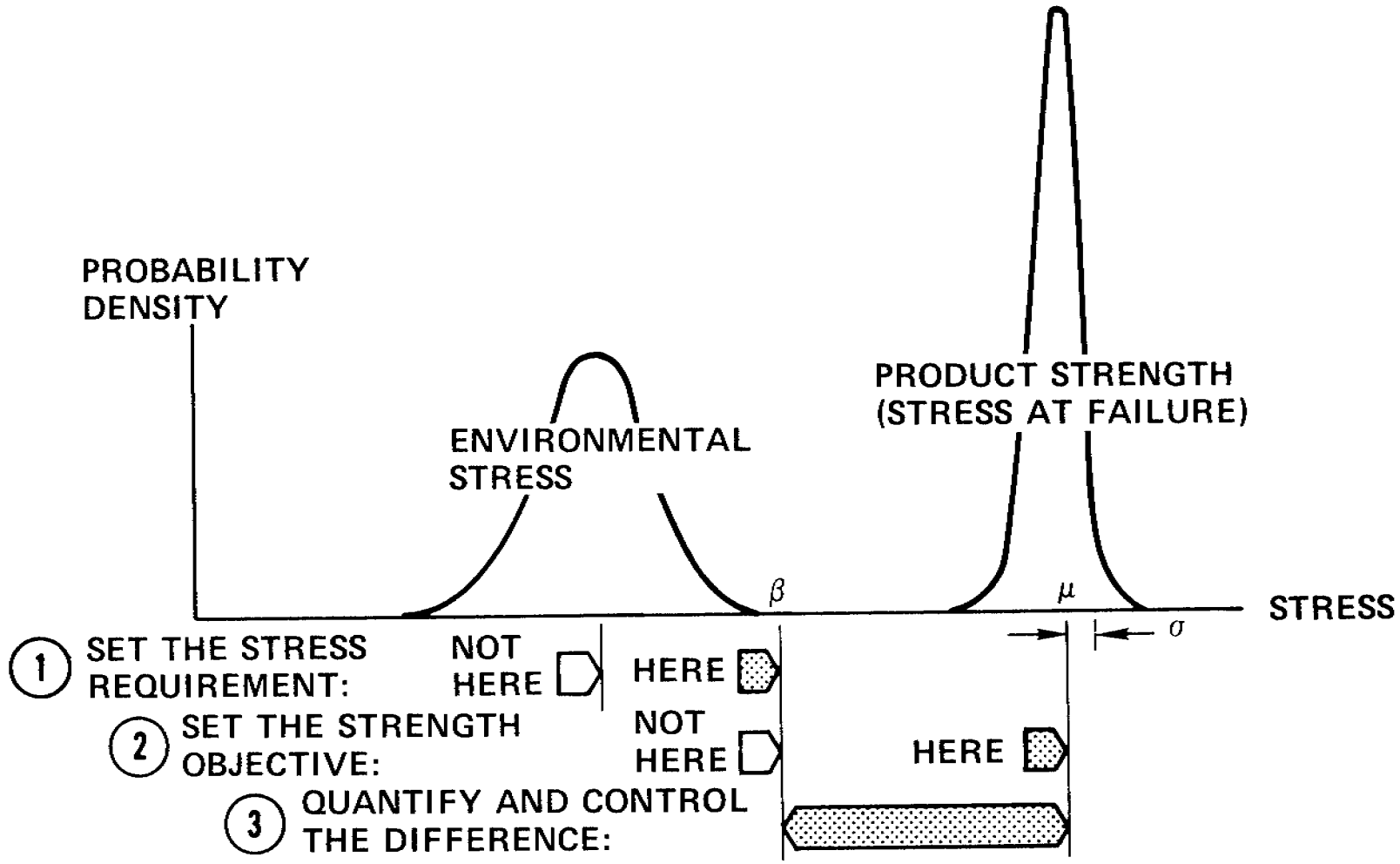


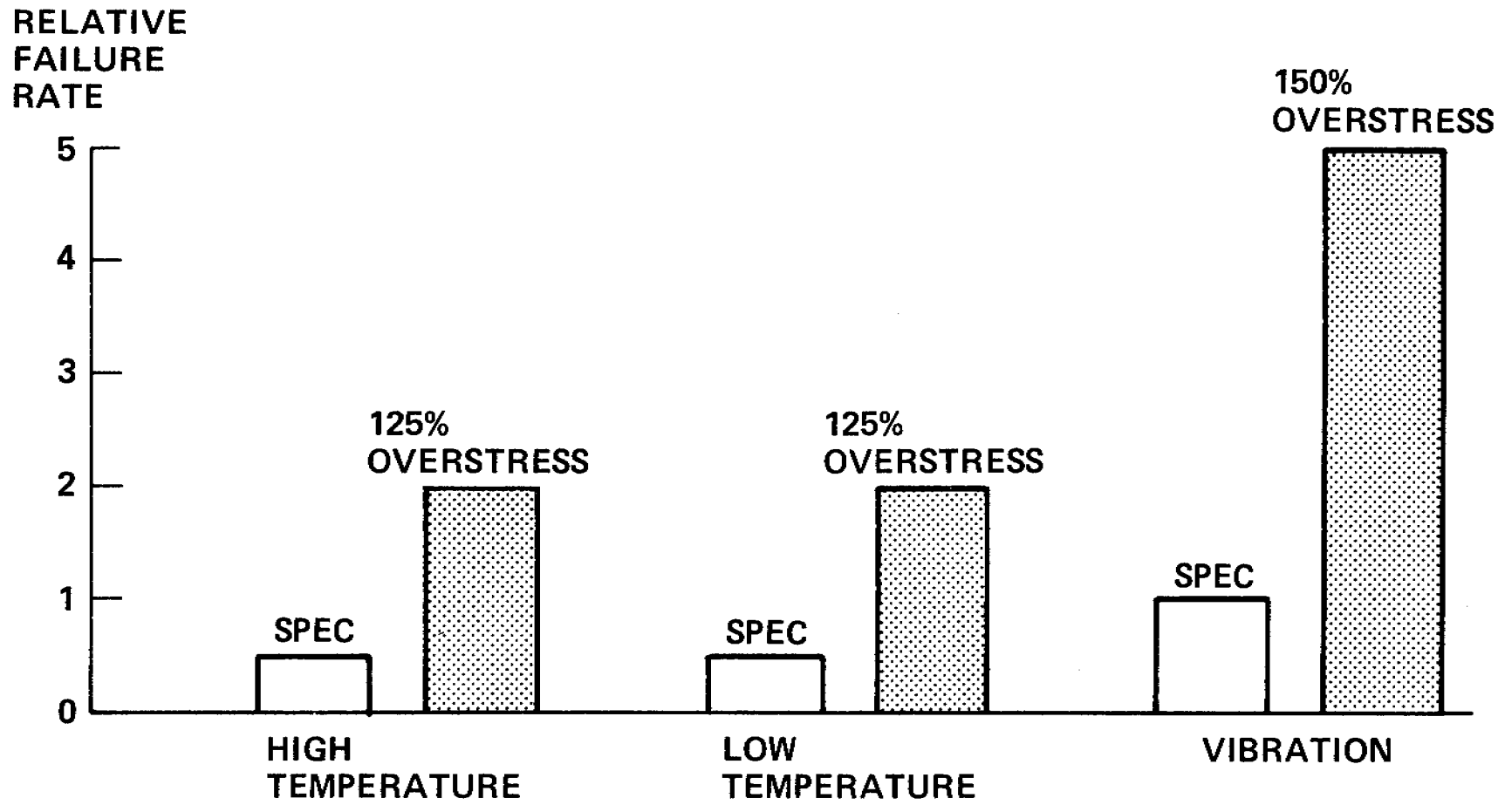
FIGURE 4
CONSERVATIVE DESIGN



- SAFETY MARGIN: $(\mu-\beta)/\sigma$
- SAFETY FACTOR: μ/β
- DERATING FACTOR: β/μ

F269805 8110

FIGURE 5
OVERSTRESS SCREENING
(DEVELOPMENT MISSILE ASSEMBLIES)



F269086 8110

QUESTIONS AND ANSWERS

DR. STOVER:

I would like to question you about the simplest design because it seems to me that one of the most complex devices we do is the micro processing. I am convinced that using it gives us more reliable equipment then if you use the less complex method of achieving the same result that it achieves. Yet that must be by far the most complex device that we ever use in electronics.

The little tiny chip has so many parts on it, it can't be looked at as the simplest approach. But gives us the smallest, simplest project, the least soldering, the fewest connectors, they are reliable products. They are appearing in our automobiles now. I am sure the reason they are there is because they can't achieve the same result as reliably by other methods.

MR. BEAR:

I think that is a simple development.

DR. STOVER:

You do?

MR. BEAR:

Yes, I do. I think that solid state, the programs of solid state technology is moving toward simpler devices even though you count the gates, it seems more complex. Yet the reliability is going up. And the reason it is going up is that the more things are being done mechanically without human intervention and that is primarily the reason. We are doing more things in a systematic way and every-time we go to a new grade of micro processors, you are not only achieving a much higher performance, but we are also improving reliability. So I consider that to be simple.

DR. STOVER:

Well, I guess that your definition of simple needs to get around through the industry because I am sure that the desgin engineer who comes up with a circuit diagram that includes the circuits that are on that micro chip and then comes up with all the firms that don't use this micro chip, it is a much smaller circuit diagram, much less on it and he gives that to his manager and which one is the manager going to tell him is the least complex.

MR. BEAR:

I guess my definition would be that simplicity is eliminating sources of variability.

DR. STOVER:

How can you get the definition across to the rest of the world?

MR. BEAR:

I don't know. That is a good challenge.

DR. STOVER:

Thank you.

DR. WINKLER:

Thank you. I think we have some time to think about that and maybe return to that question of simplicity. I think it is a very interesting one since it appears to me that reliability engineering or prevention of failure has very much to do with our ability to rationalize things, to think ahead your idea of putting the best brains together into a review group and design group as early as possible. I think that would be the best way to attack that failure to be able to foresee.