System Design and Assessment Notes
Note 33
12 January 1994

THE RELATION OF COST TO EVALUATION AND MONITORING OF ELECTROMAGNETIC PROTECTION

Edward F. Vance
6885 Highway 1187
Fort Worth, TX 76140

ABSTRACT

The means of evaluating electromagnetic protection are discussed. When failure of the protection is affordable, operating experience can be used for evaluating the protection. When the consequences of failure are dire, simulated environments are used to evaluate the protection initially and throughout the life of the system. The amount of protection required depends on the cost of failure; when the cost of protection less than the cost of failure, the protection is a good buy.

I. Electromagnetic Protection

A. Protection of Concern

As used here, electromagnetic protection encompasses all measures taken to prevent interference sources from producing unwanted responses in a circuit. We are concerned primarily with sources outside the system and protection in or on the system. The protected circuit may be part of a subsystem or system. The unwanted response may be poor signal-to-noise ratio, errors in data transmission, circuit upset, or damage to components of the circuit (or the system it controls).

We attempt to define practical rules for establishing the amount of protection needed and for establishing that the needed protection exists. The protection may be tested by exposing it to the environment in which it must operate, or it may be tested in a simulated environment. Which is used depends on the availability of the working environment and on the cost of a failure. Generally, protection against environments that are rarely available is tested in simulated environments. Evaluation of the in-service protection may also require testing in simulated environments if the cost of an in-service failure is high.

B. Value of Protection

The value of electromagnetic protection is determined by the consequences of system failure due to lack of protection. No protection is justified if the cost of failure is nil. When the cost of protection is less than the cost of the failure that it prevents, the protection is a good buy. When the cost of the protection is greater than the cost of the failure, it is not a good buy. Hence the economics of protection dictates that protection may be increased until the cost of the next increment of protection exceeds the cost that would be incurred if we didn't have that protection.

The cost expectation is the product of the overall probability of failure and the cost C of the failure if it occurs. The overall probility of failure will be written as the probility of failure P_f, given an encounter, times the number of encounters E. Then the cost expectation C_e is

$$C_e = EP_fC$$

Both the probability of failure P_f and the cost of the failure C are may depend on the amount of protection applied. That is, adding protection may change the probability of failure and the cost of the failure that occurs (in the best case, both P_f and C are reduced!). The protection is sufficient when the incremental cost of protection, ΔC_p, is equal to the incremental reduction in expected cost ΔC_e:

$$\Delta C_p = \Delta C_e$$

Unfortunately, the probability of failure P_f, and the cost of failure C, are most accurately evaluated by observing the system operation and failure characteristics for long periods of time; we can have the best estimates of P_f and C, and their dependence on level of protection, for old (sometimes obsolete) systems. Hence we resort to qualitative measures of the cost expectation. Intolerable costs are those that entail loss of human life or large sums of money. The cost expectation can be intolerably large either because the probability of failure P_f is too large (reliability too low) or because the cost of a failure C is too large.

If the cost of preventing the failure is perceived to exceed the cost expectation of the failure, the cost expectation is usually judged tolerable. Tolerable cost expectations imply that either the probability of failure is small, the probability of encounter is small, or the cost of a failure (given that it occurs) is small, such that their product is equal to or less than the acceptable cost. That is, even a very costly failure may be tolerable if its probability of occuring is sufficiently low. While the probability of failure Pf may be small because the system is well-protected, adding protection against a very unlikely, but costly, failure is not warranted if the cost expectation is tolerable.

II. Evaluating Protection

A. Operating Experience

Operating experience is usually used to evaluate the elements of the cost equation. The probability of failure, the cost of a failure, and the encounter rate are all determined ultimately from operating experience. When a failure of the protected system can be tolerated, operating experience is often the most economical way of evaluating the effectiveness of the protection.

In lightning protection of power and telecommunications systems, for example, a complement of protection measures is installed as the utilty's "standard practice." The installation is not tested with simulated lightning to evaluate its effectiveness or adequacy; instead, operating experience is used. If losses due to lightning are found to be excessive, additional protection may be applied. When lightning losses are acceptable, no protection will be added.

The utilities' lightning protection is a classical example of the economics of protection in which feedback from operating experience is used to evaluate both the effectiveness of the protection and its adequacy. Years of experience have been used to adapt and improve the "standard practice" so that in most applications it provides adequate and economical protection. In those cases where it is found wanting, the damage is local and contained; the damage from a single thunderstorm rarely has a significant effect on the utility's finances. Thus perfecting the protection by trial and error (feedback from operating experience) is practical (economical) when failure is affordable.

A second factor affecting the use of feedback from operating experience to evaluate electromagnetic protection is the frequency of exposure to the electromagnetic threat. If the threat is encountered frequently (or always), the protection is tested early and often in its operating life. In this case, feedback clearly indicates the adequacy of the protection initially and at any time after it is placed in service. However, if the threat occurs rarely (severe lightning) or never (superbolt?) the use of feedback from operating experience becomes difficult or impossible. If protection is installed, it may, in fact, be adequate, but it will take a long time to evaluate it using operating experience.

In any case, the expected cost of failure must be acceptable if operating experience is to be used as the means of evaluating the protection. But as noted above, the expected cost may be tolerable because EP_f is small, whether this is because the protection is good or because the threat is rare. The effect on the expected cost is the same. (The perception that the cost expectation is small, may change when a failure occurs, e.g., the solid rocket booster problem after the space shuttle Challenger disaster.)

B. Artificially Generated "Experience"

Even when the encounter rate E is small, the cost of a failure C may be so large that the cost expectation C_e is unacceptable. When the cost expectation C_e is unacceptable because the consequences of failure are dire, feedback from operating experience alone is not an acceptable means of evaluating the adequacy of the protection. Instead, the feedback must be generated artificially by applying a simulated threat and observing the system response. The need for tests with simulated environments and artificial feedback is illustrated in Figure 1 as a function of the encounter rate. Tests with simulated threats can be performed under controlled conditions such that failure (if it occurs) does not entail unacceptable loss.

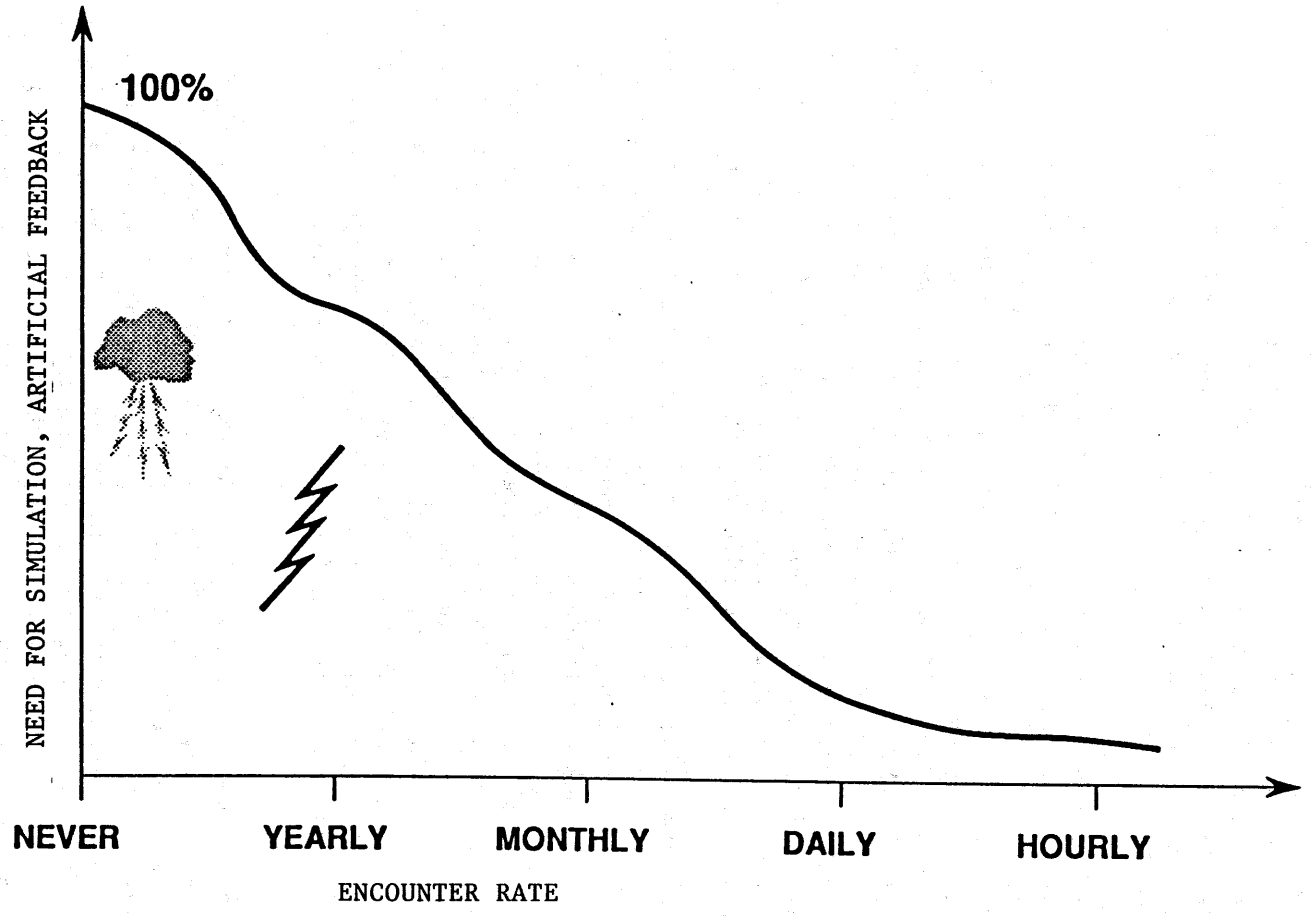

FIGURE 1. Illustrating the increasing need for testing in simulated environments with decreasing frequency of encountering the threat

In addition, when the cost of a failure is unacceptable, the continued effectiveness of the protection must also be evaluated by means other than operating experience. Testing may be necessary to determine when the protection has degraded and requires maintenance. Periodically repeating the design-evaluation test (or some portions of it) can generate feedback on the adequacy of the protection. This artificial feedback can be used to tell whether the protection has degraded to marginal levels and needs repair or replacement (i.e., before a disastrous in-service failure occurs). Such testing may also be necessary following maintenance actions that can affect the electromagnetic protection (e.g., shielded cable disconnects, grounding and bonding changes).

An exemplary use of artificial feedback to evaluate electromagnetic protection was found in military systems designed during the cold war to survive the nuclear electromagnetic pulse (EMP). For strategic systems, the cost of failure was perceived to be enormous; national survival was believed to be at stake. But the EMP was not available after 1962 when the test ban treaty was signed; all evaluation of the EMP protection had to be done with simulated EMP. Great effort was expended to develop protection methods, test methods, and simulators to facilitate the evaluation of the HEMP protection. Since operational systems were not exposed to the EMP environment, no feedback on the performance of the protection could be obtained except by artificial means (i.e., periodic retesting of the protection).

Another example is found in aircraft lightning protection (see appendix). The effectiveness of the lightning protection design is always evaluated with tests using simulated lightning. Although airliners are struck by lightning about once per year, the probability of a strike being a severe strike is only about 1:100. Because the severe lightning is rare and the consequence of failure could be dire, the adequacy of the protection design is evaluated with artificial lightning. The protection against the physical effects of lightning is sufficient that the remaining failures are almost always "affordable." Feedback from operating experience is sufficient to evaluate the effectiveness of the protection. Punctured radomes, burn-holes in skin, and damaged fuel vents are easily detected visually.

With the advent of flight-critical avionics, however, protection against the electromagnetic effects of lightning has become important. As with mechanical protection, the evaluation of the effectiveness of the electromagnetic protection is best done with simulated lightning. However, visual inspections may not be sufficient to evaluate the integrity of the electromagnetic protection. It is nearly impossible, for example, to determine the quality of cable shields, connectors, electrical bonds, etc., by visual inspection. Nevertheless, when the performance of flight critical systems depends on these (and other) interference control measures, it is imperative

that their initial and continuing effectiveness be assured without operational failures. Some kind of test is required to evaluate such components.

C. Conditions for Artificial Feedback

The use of artificial means of evaluating the electromagnetic protection presumes that the threat can be simulated, and that the effectiveness of the protection can be evaluated with the simulated threat. These seemingly trivial stipulations are crucial to the successful application of artificial feedback. This is because the simulated threat always differs from the actual environment in some respects. To use this simulated, but different environment to evaluate the effectiveness of the protection, one must understand what the differences are and how they affect the responses of the system.

However, if the responses of the system are to be understood, the possible (or likely) responses must be fairly simple. For example, the coupling between an external transient source and a digital circuit deep inside an aircraft is much too complex to permit accurate analysis or thorough understanding. (It may involve field penetration at dozens of points, such as cockpit and cabin windows; exposed wiring near wing slats and flaps, wheelwells, vertical fin; VHF/VOR and many other antennas. Very complex interior interactions with plumbing, wiring, and structural materials are also involved. If it is necessary to understand these complex interactions in order to establish the effectiveness of the protection, it will indeed be very difficult.) The evaluation of the system protection will be facilitated if the protection uses a few elements, places simple bounds on the interaction, and the bounds are well below the failure levels.

Alternatively, one may use a high-fidelity simulation and test often enough that, statistically, all system states, points of entry, coupling paths, angles of incidence, polarizations, etc., will be tested and any weaknesses in the protection will be found and corrected before a catastrophic failure occurs. If the simulation is good enough and the system is tested often enough, and the fault detection is accurate, artificial feedback can be obtained on any kind of protection design. However, developing a test system that meets these criteria may be quite challenging.

III. Controlling the expected cost of failure

The expected cost of failure C_e depends on the probability of failure P_f and on the encounter rate E and the failure cost C. Reducing any of these will reduce the expected cost. It is certainly good policy to use avoidance schemes that reduce the encounter rate (or to eliminate the source) when practical. It is also good policy to use damage control (as is done in airframe lightning protection) to

reduce the cost of some failures that occur. However, it will be assumed that avoidance and damage control are being used to the extent practical, so that the principal means of controlling cost expectation is through the probablility of failure.

The probability of failure can be reduced by

* Improving the degree of protection

* Improving the durability of the protection

* Using redundancy or proliferation

Improving the degree of protection reduces the likelihood that an stress event will cause a failure. Improving the durability of the protection reduces the likelihood that that the degree of protection will degrade with time to a susceptible level. The durability can be increased by using rugged, change-resistant protection elements and by monitoring and maintaining the protection elements.

A. Redundancy

Redundancy is a fault-tolerance scheme in which a critical function can be performed (or controlled) by two or more means, so that failure of one does not cause loss of the function. In effect, redundancy allows the system to continue to function even after it has suffered damage. It is a very effective way of increasing reliability, because the probability of failure of both of two independent functions, each of which has a probability of failure P_f, is P_f^2. This is true, if the redundant controls are truly independent so that damage to one does not cause damage to the others or prevent the others from operating.

Whether this technique is effective against electromagnetic overstress is not clear. It is clear that if both redundant control systems are overstressed, both may fail. This was demonstrated in the Brown's Ferry nuclear plant incident in which the redundant safety circuits were all routed through the same conduits and destroyed by the same fire. The designers of the safety system evidently did not consider the fire threat when designing high-reliability safety circuits. Likewise, avionics designers do not always consider electromagnetic overstress when designing high-reliability flight systems. External sources (lightning, HF transmitters, and other ground-based emmiters) may stress all systems simultaneously. Therefore, identical circuits with identical protection may all be overstressed by the same external source.

B. Margin

Increasing the degree of protection is equivalent to increasing the margin between the protection level and the system susceptibility level. This is, of course, a very effective way of decreasing the probability of failure. The cost of providing a large margin may be high because of the greater engineering effort required and the added cost of the protection components. Maintaining a degree of protection is deemed more important than having a large margin, since it is this durability that gives confidence in the protection in the operating system.

C. Durability

Achieving reliability in systems exposed to abnormal stresses is often a matter of assuring the durability of the protection. Adequate protection can be designed, installed, and tested, but there is uncertainty about its effectiveness at some later time. The concern is particularly great when the encounter rate is low and the cost of failure is high. Under these conditions, it is not desirable to let operating experience be the indicator of excessive degradation of the protection.

Other options include performing periodic tests to obtain artificial feedback on the protection effectiveness, and using built-in test equipment to monitor the protection and indicate when service is needed. Built-in test systems to monitor protection against external electromagnetic threats are difficult to design and not very effective unless a very-high-quality shield is the principal protection. In addition to the initial cost, these systems also add weight and require operating energy. At present, built-in test systems for monitoring protection against external threats are not available for aircraft.

Periodic testing using ground-based simulators is feasible, but also quite expensive unless it can be integrated into the normal maintenance schedule. Combining the surveillance testing with the scheduled maintenance is also desirable because most electromagnetic protection malfunctions are man-made and arise from maintenance operations (connectors removed and not reseated properly, filters shorted and bypassed, RFI gaskets left out, bonding surfaces painted, etc.). Therefore a post-maintenance check would identify these flaws before the system is returned to service.

For the surveillance testing to be combined with the scheduled maintenance operations, the mean-time-before-failure (MTBF) of the protection must be greater than the period T between maintenance operations. In fact, regardless of when the surveillance testing is done, the criterion for the frequency of testing is

$$T \ll MTBF$$

Unless this condition holds, the surveillance testing cannot assure a high-reliability protection system.

IV. Conclusions

The amount of electromagnetic protection required is determined by economics. When the cost of protection is less than the cost of the damage it prevents, buying the protection is sound. If the cost of the protection is greater than the cost of the damage, the protection is not a bargain. This simple rule for determining the optimum amount of protection applies to those cases where failure due to lack of protection is not disastrous. Operating experience is often used to evaluate the adequacy of the protection.

When failure is disastrous because of loss of life or other great calamity, the amount of protection required is that necessary to reduce the loss expectation to a tolerable level. This may be interpreted as making the expected loss caused by any one threat, such as lightning, small compared to the overall loss expectation from all causes. We have shown that a maximum allowable probability of failure can be deduced from such reasoning.

When failure is disastrous, it is also necessary to provide some means of evaluating the protection, and of assuring that it endures and is maintained. Feedback from operating experience cannot be used if the first indication of degradation is disastrous failure. Testing in a controlled simulated environment is usually required to determine the adequacy of the protection initially and periodically during the service life of the system.

APPENDIX

Aircraft Lightning Protection Example

An example of the use of cost expectation to estimate the protection required is found in aircraft lightning protection. Although airliners are struck by lightning about once per year, the probability of a strike being a severe strike (over 100 kA) is only about 1:100. Since the world-wide fleet of passenger aircraft is about 9000, the expected severe strike rate E is about 90 encounters per year. Let us assume that the consequence of failure of the lightning protection is a fatal crash with an average loss of 200 lives and the aircraft. We will also assume that only severe lightning is of concern, and that there are no partial failures always; either 200 lives, or none, are lost.

Our cost expectation C_e is thus

$$C_e = ECP_f$$

where E = 90 encounters per year, C = 200 lives per failure, and P_f is the probability of failure, given an encounter.

If we will stipulate C_e, the "tolerable" cost expectation, we can evaluate the maximum probability of failure P_f that can be allowed. To estimate the "tolerable" cost expectation, let N be the overall fatality rate from all airliner accidents from all causes (in lives lost per year). Let us then postulate that the losses due to severe lightning will be tolerable if they are small compared to overall loss rate (say, less than 0.1N). Then the tolerable cost expectation is

$$C_e = EP_fC < 0.1N$$

or the maximum acceptable value of the probability of failure P_f is

$$P_f < 0.1N/EC$$

If the actual airliner fatality rate is of the order of 100/year, the probability of failure due to severe lightning must be less than 10/18000 or 1/1800. That is, with 90 severe lightning encounters per year, on the average we would expect less than one loss due to severe lightning every 20 years.

Acknowledgement

This note was prepared for Mission Research Corporation under Contract f29601-87-C-0054, Subtask 02-15.