THE SYSTEM SAFETY DISCIPLINE SIMPLIFIED
By Myron Papadakis

The system safety discipline provides the engineer with several standardized studies to perform. They are known as:

1. Hazards analysis
2. Failure modes studies
3. Failure Modes and Effects studies (Cause and Effect)
4. Fault Tree Analysis
5. Lessons learned studies
6. Field tracking studies (a variety of names)
7. Sneak Circuit Analysis for electric designs.
8. Common cause failure studies

Once the engineer has determined the potential hazards, the severity of the hazard and the probability of the hazard occurring, he is in a position to advise as to what the acceptable risk is and what the loss rate will be.

Probably the most important aspect is the early determination of the severity of the hazard study. In aviation, the standard approach required by the military and carried over in some analogous form to the civilian field is to quantify hazard Severity into 4 categories: THEY ARE:

CAT l. Hazard, results in the potential for loss of the aircraft and loss of life.

CAT ll. Causes the immediate loss of a mission, immediate abort and divert.

CAT lll. Causes the loss of a essential system. Fix on landing.

CAT lV. Routine loss, fix on schedule

From this categorization, it is easy to see that if such a study has been accomplished and there are CAT l. hazards in the design, then the company has opted to allow an acceptable loss rate
or acceptable risk rate to be associated with an identified hazard.
This is far different from a company first discovering a defect as the result of an accident.

The reason for doing these studies in the first place was to aid the manufacturer in designing a product as hazard free as possible. Most manufacturers of aircraft attempt to design a failsafe airplane.

In general, this means that no single point failure is allowed to exist that will cause the loss of life or loss of the aircraft. While not a requirement, most prudent manufacturer will expand this to include no common because failure will cause the loss of life or of an airplane.

With respect to a single point failure causing a CAT l loss it is standard engineering preference to eliminate such hazard in that:

1. Such a failure should be designed out
2. A redundant system should be included
3. Warning system should be designed to warn of impending failure.
4. Maintenance, inspection and replacement should be scheduled to replace part before failure.
5. If allowed to be present in the design its chance of occurrence should be extremely remote

The order of preference in correcting for an identified hazard is.

1. It should be corrected in the design phase
2. It should be corrected in the production phase
3. It should be retrofitted through field kits.
4. If it can't be fixed remedial measures should be taken from recall to stringent warnings issued.

One can see that a enlightened manufacturer was already using a discipline, that if accomplished appropriately would have the effect of lessening the chances of producing a defective product. The natural goal of the manufacturer's system safety department is precisely the same as the expectation and duty the law holds them to as a standard. It is the failure of the manufacturer to meet the goals that expose them to legal liability, be it in Strict Products Liability.