Safety Corner

What are fault-tolerant designs and fail-safe designs?

A fault-tolerant system is designed to avoid total service failure caused by faults at any single point. Typically, a fault-tolerant design applies redundancy or multiple safety barriers to enable the system to continue its intended mission, possibly with reduced performance or increased response time in the event of some partial failure, rather than to fail completely. An example of a fault-tolerant design is an aircraft with multiple engines, so that it will keep flying even if one of the engines failed.

A fail-safe system is designed to fail in a safe and controlled manner, so that the failure will not endanger lives or properties, or at least be no less safe than when it is operating correctly. For example, the brakes on a train are designed to apply when the brake control system fails, to ensure safety by stopping the train. It must be noted that a fail-safe system can also suffer 'wrong-side failure', as when, for example, a malfunctioning traffic light shows green rather than flashing red or goes dark; but is to have a very low probability of this occurring.

In some cases, it may not be acceptable for one or even more failures to cause a system to cease functioning. Unlike a fail-safe system that puts safety ahead of function or mission objective, a 'fail-operational' system will continue to operate in spite of control systems failure. An example is the thermostats in home air-conditioners.

The Safety Corner is contributed by Ir Dr Vincent Ho, who can be contacted at vsho@UCLA.edu