

## **Vital – What does it really mean?**

Bill Petit

[www.billpetit.com](http://www.billpetit.com)

*This article was originally published in the September 2005 issue of Railway Systems and Controls.*

With the FRA's recent entry into regulations for processor-based systems, questions have been raised regarding the meaning of vital and if it differs from safety-critical. Vital has become an emotionally charged word and is frequently misunderstood or used out of context. When first looking at a safety system, a preliminary identification of all the hazards that could be created by that system is done (and continually expanded as more is learned about the system). For example, an interlocking displaying a Proceed aspect inappropriately is a hazard. Hazards are then classified according to their overall risk in a range from "Unacceptable" to "Acceptable without Review" (determined by a matrix of the severity of the hazard and its frequency of happening). The AREMA Manual for Communications and Signaling ([www.arema.org](http://www.arema.org)) Section 17.3.5 identifies 3 classes of systems. A safety-critical system is defined when at least one of the identified hazards can lead directly to a mishap (accident). A safety-related system is defined as one where the hazards do not lead directly to a mishap but may significantly increase the overall risk of a mishap. Finally, a non-safety-related system has no safety implications. IEEE Standard 1483 (<http://shop.ieee.org/ieeestore/>) defines a safety-critical system as one where the correct performance of the system is critical to the safety, and the incorrect

performance (or failure to perform the function) may result in an unacceptable hazard.

This standard also provides an interesting appendix on types of systems used to achieve safety.

According to most standards, hazards that have risk ratings of “Unacceptable” or “Undesirable” must be mitigated (i.e. reduce the risk, which is generally done by decreasing the frequency of occurrence) through system and equipment design. In order to do this, you have to identify all of the functions that are necessary to implement the system (down to a very low level). Functions that have to be implemented so that they are both performed and performed correctly are implemented fail-safely and are identified as vital functions. The fail-safely implementation means that you look at all the credible failures that could occur and make sure that occurrence of any one of them (or combination of failures in the event that the first failure is not self-evident) maintains the system in a safe state, either by forcing the system to a stop (or other safe state such as a less permissive signal) or by transferring control to a secondary system (e.g. redundant computer).

This is where we get into trouble with the word “vital”. All it really implies is that a function must be done correctly, or the failure to do so must result in a safe state. In relay systems, we fell into the habit of calling components vital relays when what we really were looking at were relays that did vital functions (allowed the front contacts to be made only when voltage was present on the relay coil, even in the presence of all credible failures). Relays performing these vital functions are just one part of an overall safety-

critical system design, which is based on signaling principles. People talk about vital computers but there really is no such thing. Instead, there are computers that perform vital functions and their operation must be comprehensively analyzed to verify that any failure maintains the safety of the system.

In summary, there is no difference between a safety-critical system and a vital system. In both cases, you have to analyze the functions and make sure that any credible failures maintain a safe state. In railways, we've had the economic advantage of a safe state being to stop the train, while designing reliable equipment so that doesn't happen very often. Other industries, such as aircraft, go through the same analysis but are forced to support multiple redundant or backup systems because they don't have a single safe state available to them like the railways do. (They also have additional mitigations available to them since the pilot has multiple degrees of freedom available such as up, down or sideways.)