Safety Corner

What is a failure and what is a fault?

Let’s say a system consists of a set of hardware and software components, and is designed to provide a specified function, so what is the difference between a system failure and a system fault? The terms, failure and fault, are often used interchangeably. If we were to ask 100 engineers to define failure and fault, we would probably get 100 different definitions.

In general, a failure is the inability of a system or a system component to perform a required function within specified limits. A fault can be seen as a defect or an abnormal situation that may cause a reduction in, or a loss of, the capability of a functional unit to perform a required function. One can say that failure is a “user-oriented concept” in a sense that a failure is a departure of system behaviour in execution from user needs; it is a problem that users or customers see. A fault, on the other hand, is a “developer-oriented concept”; it represents problems that developers see. A fault doesn't necessarily result in a failure, but a failure can only occur if a fault exists. Thus, a fault is a state, and a failure is an event.

A fault, if encountered, may cause or can potentially cause a failure. To resolve a failure you must find the faults that are capable of causing failures. This is the reason why safety engineers apply Fault Tree Analysis to identify logical combinations of faults, conditions and errors in causing an event to failure, which, we call it a “Top Event” in a Fault Tree Analysis.

==

The Safety Corner is contributed by Ir Dr. Vincent Ho, who can be contacted at vsho.hkarms@gmail.com