Safety Corner

What are the Key Characteristics of Component Failure?

One key element of Quantitative Risk Assessment (QRA) is the use of fault-tree analysis to assess the unavailability of a safety system. The faults and failures of components or subsystems that can contribute to the occurrence of the top event of the fault tree are called basic events. To quantify a basic event, its failure modes must be clearly defined and they must be realistic, consistent and compatible with the context of system operational requirements, environmental factors and system configurations. In general, component fault events can be described by one of the following three failure characteristics:

1. Failure on Demand. Some components are required to start, change state, or perform a particular function when required. Failure to respond as needed is referred to as failure on demand. Numerically, failure on demand or per demand is typically modeled by a fraction or a probability.

2. Standby Failure. Some components, especially those that are safety-related, can be put on hot standby and cold standby, and are required to operate on demand when needed. Failure could occur during this non-operational standby period, preventing operation when required. Unlike failure on demand, standby failure requires the knowledge of the component during the full duration of the standby. Furthermore, the reliability of the switch that connects the standby system to the mainline should also be considered.

3. Operational Failure. A given component may be normally operating or may start successfully but can then fail to continue to operate for the required period of time. This failure characteristic is an operational failure, which is time-dependent because we expect the performance of a system or component will change over time. This failure characteristic is the most commonly modeled among the three.

Depending on the specific context of a specific system operation, we should evaluate each component in terms of the above failure characteristics. Certain components may involve all three failure characteristics. As an example, an emergency fire water pump is required to start from a standby state on demand, and then run for a specific period after starting successfully. The unavailability for the pump must then include the consideration of all three failure characteristics.

==========

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