Safety Corner

What is functional safety?

Functional safety looks at aspects of safety that relate to the function of a device or system and ensures that it works correctly in response to commands it receives. Applying originally on electronics and related software, functional safety is a concept applicable across all industry sectors. It is fundamental to the enabling of complex technology used for safety-related systems. It provides the assurance that safety-related systems will offer the necessary risk reduction required.

Functional safety covers the complete safety life cycle and treats the function of a component or subsystem as part of the function of the whole system. This means that whilst functional safety standards focus on electrical, electronic, and programmable systems (E/E/PS), the end-to-end scope means that in practice functional safety methods have to extend to the non-E/E/PS parts of the system that the E/E/PS actuates, controls or monitors.

Functional safety is achieved when every specified safety function is carried out and the level of performance required for each safety function is met. This is normally achieved by a process that includes the following steps as a minimum:

1. Identifying hazardous events, which include potentially dangerous environments, situations, or incidents that could cause harm to personnel or property
2. Assess the risk-reduction required by the safety function
3. Ensure the safety function performs to the design intent, including under conditions of incorrect operator input and failure modes
4. Verify that the system meets the assigned risk level
5. Conduct functional safety audits to examine and assess the evidence that the appropriate safety lifecycle management techniques have been applied consistently and thoroughly in the relevant lifecycle stages of the product.

Safety achieved by passive systems is not functional safety. Functional safety typically relies on active systems; for example, the detection of smoke by sensors and the ensuing intelligent activation of a fire suppression system; or the activation of a level switch in a tank containing a flammable liquid, when a potentially dangerous level has been reached, which causes a valve to be closed to prevent further liquid entering the tank, thereby preventing overflow.

==========

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