Safety Corner

What is System Safety?

System Safety is the application of engineering and management principles, criteria, and techniques to achieve acceptable hazard risk, within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle.

The concept of *System Safety* was developed in the late 1950s to manage the risks and avert the failures of the American space and rocket programmes, and was later applied in the 1960s to ensure the safety of the U.S. nuclear weapon programmes where system engineering sought to understand the integrated *whole* rather than merely the component parts of a system, with an aim toward optimising the system in meeting multiple objectives.

Safety should not be considered an "add-on" to engineering systems. For almost any engineering system, the most effective means to ensure inherently safety with minimal operational requirements or restrictions and to reduce total system cost is to incorporate health and safety requirements early on and to manage their risks throughout development, fabrication, testing, production, commissioning, operation, maintenance, and, ultimately, decommissioning and disposal of the system. This drive of integrating safety into engineering processes created a new stream in engineering called the *System Safety Engineering*.

System Safety Engineering concerns with achieving and assuring safety of systems, including their hardware, software and human elements, through the application of engineering approach. It encompasses, but is broader than, Functional Safety, as it concerns with hazards arising from operations and physical causes; e.g., toxic materials or uncontrolled energy sources, as well as functional failures.

Experienced *System Safety Engineers* have been in high demand worldwide. To date, many major corporations in Hong Kong employ *System Safety Engineers* to apply the *System Safety* concept in safeguarding their assets by proactively identifying all foreseeable hazards during the design process and system lifetime, reviewing system operations systematically for possible faults and failures, and providing a system engineering approach to control safety risks by either eliminating them or engineering them to reduce the likelihood or the consequence of accidents.

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