

NUCLEAR TECHNOLOGY EDUCATION CONSORTIUM

N30

THE DESIGN OF SAFETY-CRITICAL SYSTEMS

Summary

This module provides students with knowledge of the design issues relevant to safety-critical systems. Topics included cover safety standards relevant to the design of engineering systems, and the IEC 61508 Safety Lifecycle and the implementation of the various steps of the process. Hazard identification and analysis techniques such as FMEA, HAZOP, and fault trees are also addressed.

On completion of this module students should:

- Have an awareness of the IEC61508 Safety Lifecycle, functional safety, ALARP, and other standards;
- Understand the various hazard analysis techniques, including Failure Modes and Effects Criticality Analysis (FMECA), Fault Trees, Hazard and Operability Studies HAZOP including both quantitative and qualitative approaches
- Have an appreciation of the difference between random and systematic faults. and the overlap of this with software issues.
- Have an appreciation of the synergy between safety, reliability and quality.

Syllabus

- Safety standards relevant to the design of engineering systems.
- The IEC 61508 Safety Lifecycle and the implementation of the various steps of the process.
- Hazard identification and analysis techniques such as FMEA, HAZOP, Fault Trees etc. including the use of appropriate software tools.
- Qualitative and quantitative approaches. The hazard log.
- The assessment of risk and establishing safety criteria.
- Assigning SIL values. Random and systematic faults and the achievement of appropriate SIL values.
- The interplay between safety, reliability and quality.