# Safety engineering SFEN

Applying appropriate methods to assure safety during all life cycle phases of safety-related systems developments.

|  |
| --- |
| **Guidance Notes:**Safety-critical systems are those in which a system failure could harm human life, other living things, physical structures, or the environment. Activities may include, but are not limited to:* safety hazard and risk analysis
* safety requirements specification
* safety-related systems architectural design
* formal method design
* safety validation and verification
* safety case preparation
* applying generic safety standards such as IEC 61508, IEC 61511 or industry-specific safety standards.

System safety is engineered and measured by safety levels based on hazard and risk analysis. |

## Level 2

Assists with safety engineering tasks under routine supervision.
Supports the documentation of hazard and risk analysis activities.
Helps collect safety assurance evidence using agreed methods and procedures.

## Level 3

Contributes to hazard and risk analysis during system development and implementation using agreed methods and procedures.
Documents the results of hazard and risk analysis activities.
Contributes to the collection of safety assurance evidence using appropriate methods and tools.
Undertakes all work in accordance with agreed safety, technical and quality standards.

## Level 4

Contributes to identifying, analysing and documenting hazards and safety risks using agreed methods and procedures.
Contributes to the specification of safety requirements.
Analyses and documents safety validation results during system development and implementation.
Contributes to developing and maintaining project safety assurance plans, and gathers safety assurance evidence for safety case preparation.

## Level 5

Identifies and analyses hazards and contributes to identifying and evaluating risk reduction measures, ensuring these are adequately documented.
Specifies safety-related systems architectures for defined safety levels.
Develops and maintains project safety assurance plans. Monitors implementation and compliance. Ensures that safety assurance evidence is gathered for safety case preparation.
Works with system architects, designers and developers to assure safety requirements implementation.

## Level 6

Takes full responsibility for hazard analysis and risk evaluation, safety-related systems architectural design and safety compliance planning.
Leads the definition and allocation of safety requirements for the system, according to the system's nature and required safety level.
Takes responsibility for the safety-related aspects of multiple complex or high safety integrity level projects.