



Risk, Safety and Security

An Introduction to Risk, Safety and Security that will draw upon many domains to provide the basis of what different engineering perspective is needed to grow from functional engineering (making it work) to functional safety (making it cope with component faults) to security (making it cope with malicious intent).

Duration: 3 days

Course Overview and Modules

The course covers the progress of Safety for development (with an emphasis on product solutions that are significantly electronic/software) from planning through concept and systems engineering through electronic hardware and software engineering and their subsequent integration, verification and validation.

This course brings about a cultural change to engineers to extend their thinking from just 'making it work' (i.e. the intended functionality) to consider:

- how things might fail (including understanding what might fail and how it might fail)
- how faults are detected and the possible propagation of failures from faults
- how the design accommodates those failures (fail safe, or fail operational for example)
- how the design manages the disruption to operation caused by the failures (reduced capabilities as a strategy say)
- how the design alerts the user to malfunctions
- how the design diagnostic mechanisms identify what has failed/needs to be fixed
- how the design enables the system to recover from failures and/or faults (automatically, through maintenance etc)
- how the design avoids common cause, common mode and cascade failures
- ... and many more

Delegates will learn to understand the development of safety requirements to mitigate the hazards identified and defined in the safety goals. The techniques for analysing and designing solutions for these vary significantly between electronic hardware and software, so are useful to address as knowledge for 'systems engineers' to enable an understanding of the implications of selecting these technologies as part of a safety solution.

They will also learn the parallels between Safety Hazards and Security Threats and analogous process needs, with different methods.



SCARECROW CONSULTANTS

Risk (1 day)

- Learn what a Risk is, where Risks arise and who manages them
- Learn about the Risk process, Risk models and terminology

Safety (1 day)

- Understand Product and Functional Safety
- Understand the Functional Safety Process for Systems Engineering and the Safety implications for the whole Systems Engineering life cycle
- Learn how Hazards are Analysed to form Safety objectives (goals) and developed into technical safety requirements
- Understand what Integrity or Assurance level means

Security (1 day)

- Security standards and relevance to cyber-physical systems
- Learn how and where Security is addressed in the System Engineering life cycle
- Learn how Threats are Analysed to form Security objectives and developed into technical security requirements
- Get an overview of the implications and techniques for Security in Electronic and Software development, implementation and integration and the fundamentals of trust and authentication.



SCARECROW CONSULTANTS

Target Audience

This course is intended for Systems Engineers advancing beyond functional engineering, to considering what the system should do when it has faults (component faults), is used in an unintended environment (out-of-spec or performance limit), or abused maliciously to cause disruption or failure.

Benefits

The benefits of this course are as follows:

- Understand why a fault doesn't necessarily mean failure if you design a system to accommodate it
- Understand the techniques of accommodating faults by design of system response, when necessary
- Understand when and why you need to manage risks in cyber-physical systems
- Understand why a Hazard to Safety is somewhat analogous to a Threat in Security
- Understand Risk, Safety and Security relationships

Prerequisites

Although it would be useful to have some prior SysML knowledge, this is not essential.

Material

Delegates receive annotated PDF copies of the course notes.

More Information

For more information on this course, or any of our other offerings, please contact Scarecrow Consultants Limited using the details above.