Introduction to Safety Terminology

Nicholas Mc Guire
Distributed & Embedded Systems Lab
Lanzhou, China

Types of Safety

- Mechanical
- Elektrical
- Functional

Why use computers for functional safety ?

- Limits of mechanical systems
- Growing complexity
- Adaptability issues
- Monitoring
- Cause detection

Missing costs-reduction ?

General Terms Discussion:

- Safety vs Security
- Availability vs Safety
- Fault/Error/Failure
- Fault Tolerance and Robustness

I'm not the authorative source for these definitions - but lets not start this seminar with a specification error!

Failures of Safe Systems:

Safe systems need not be fault free.

- Fail Safe
- Fail Operational
- Degenerated modes of operation
- Safety related failures
- Non-safety failures

The basic model of functional safety: Fault detection -> Fault reaction

Types of Failures

- Systematic Failures
  - Common Cause Failures
- Stochastic Failures
- Concurrency related failures
- Aging related failures
  - Software Aging
- True stochastic errors
  - Transient errors
  - Accumulated errors (stuck at)

HighLevel errors

- Requirements Errors
- Specification Errors
- Design Errors

Errors in these early life-cycle stages are not only the most safety critical they are also the hardest to detect in the running system.

Determinism vs Non-determinism

- Sources of non-determinism
- Divergence of systems
- Limitations of resynchronizing systems

Modes of Opperation

- Continuous mode
- Low demand mode

Low demand mode is disputed, atleast for safety related systems.

Modeling

- Limiting Complexity
- Limitations of Abstraction
- Hirarchical models of systems
- All development procedures are essentially hirarchical models

Modeling at different levels is our primary method for managing ever increasing complexity of systems.

Systematic problems of high-complexity systematic Safety it self

- It's absence can introduce hazards
- Abstraction limits the scope of human response
- Acceptance of risk rising due to safety
- Order of consequences increasing

Functional safety is a resonable response to the increased safety eeds - but the first option should stay to design simple and clean systems from the start.

Key qualities driving Safety

- Simplicity
- Clarity
- Reproducibility
- Experience