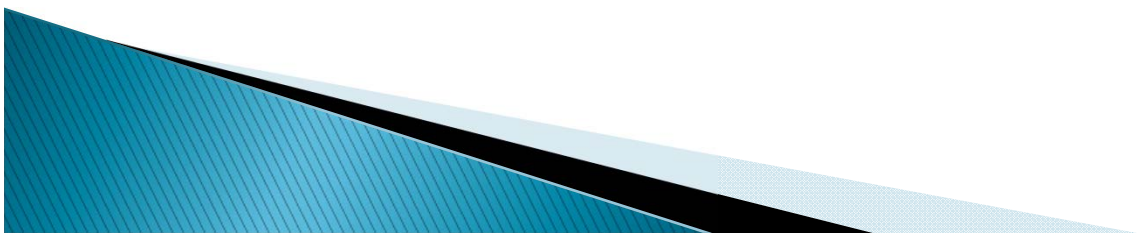
Safety Critical Computer System Design

Tolulope Kupoluyi

Computer Systems

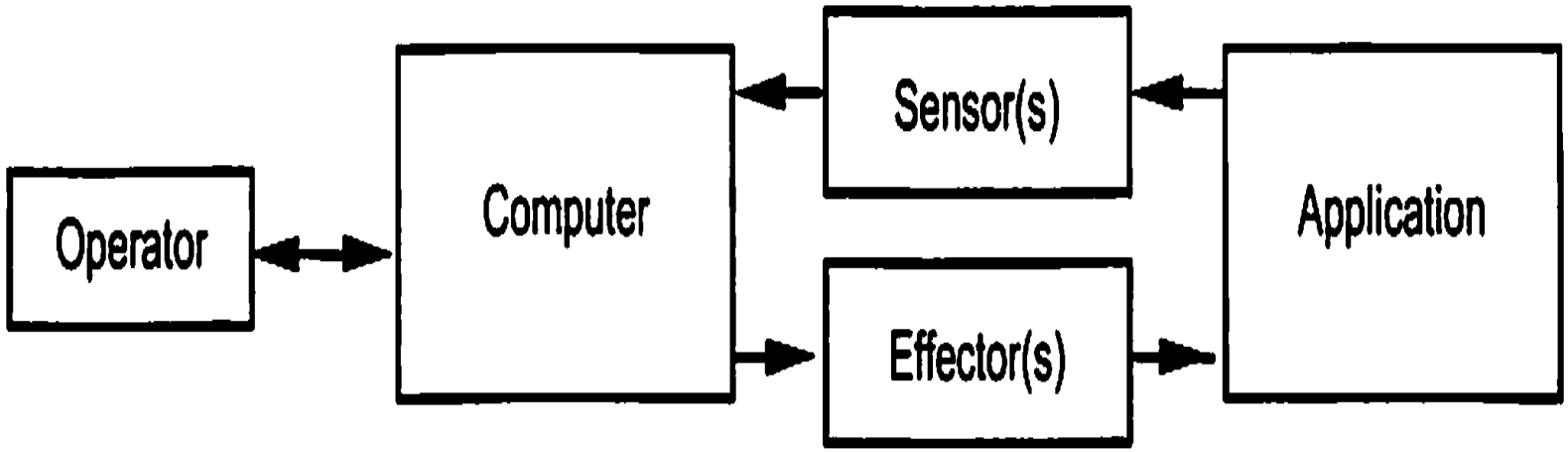
A computer system is typically made up the of a combination of the following components:

- Sensors
- Effectors
- Computer
- Operator
- Application



Computer Systems

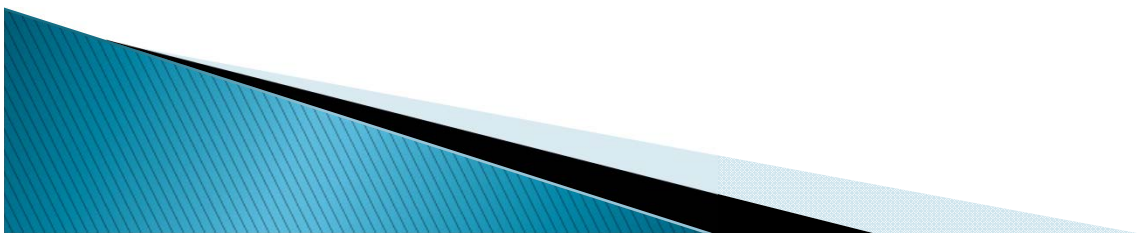
The basic structure can is represented below:



Computer Systems

- A computer control system and a computer safety system while typically the same in general structure differ in operation condition and purpose.

- While a control system is responsible for the regular operation of the application, the safety system is a passive system that is moved to action by any faults occurring at the application end.



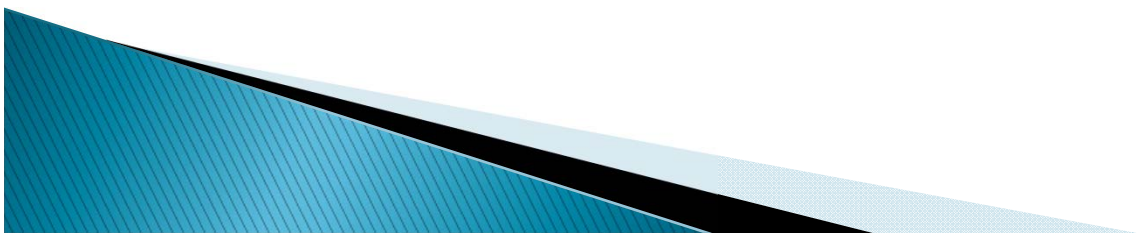
System Life Cycle

- Design
- Research
- Development
- Test & Evaluation
- Production
- Deployment
- Operations and Support
- Disposal

Mishap Risk – Definitions & Evaluation

Mishap risk can be defined as the possibility of an unplanned event or multiple events that result in death, injury, pollution, damage to equipment etc.

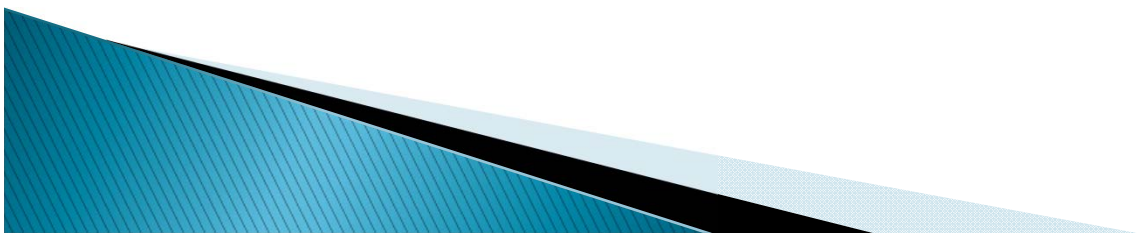
The severity of these events is determined by the resultant effects and exactly what system was involved in its occurrence.



Mishap Risk – Definitions & Evaluation

To ensure even criteria across safety critical systems development, regulatory standards exist which define minimum requirements that must be made before a system can be deployed and used.

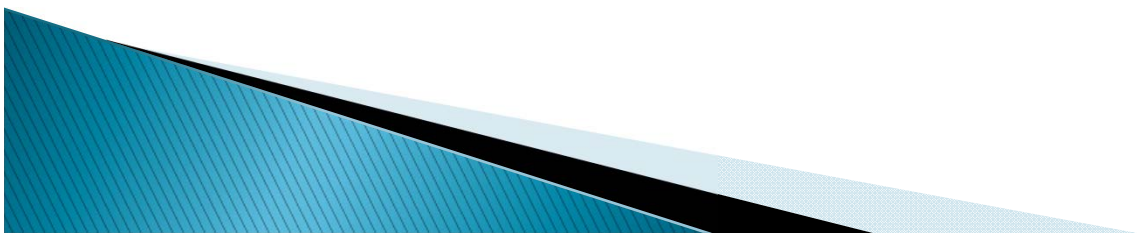
- MIL-STD-882D
- IEC 61508



Mishap Risk – Definitions & Evaluation

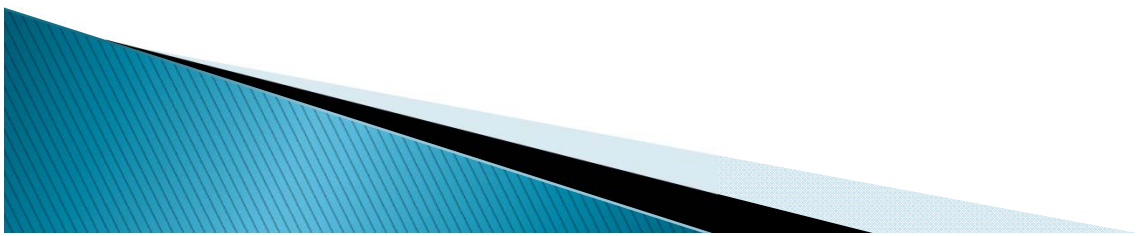
Table 1.1 Safety Integrity Levels (IEC 61508)

Safety Integrity Level	Consequence of Safety-Related System Failure
1	Minor property and production protection.
2	Minor property and production protection. Possible employee injury.
3	Employee and community protection.
4	Catastrophic community impact.



Mishap Risk – Definitions & Evaluation

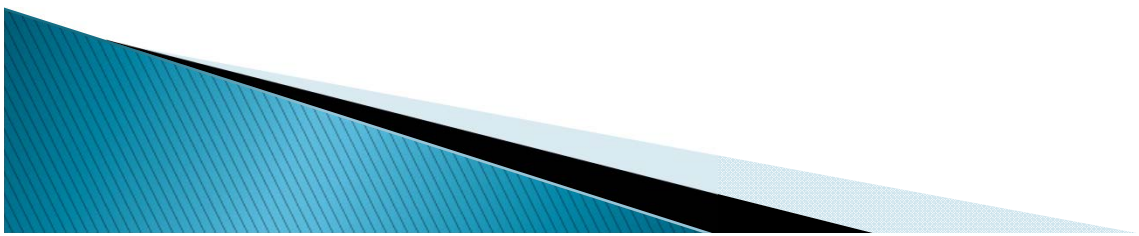
	Computer Control System	**Computer Safety System**
Safety Integrity Level	Continuous/high-demand mode of operation (probability of dangerous failure per hour)	Low demand mode of operation (probability of failure to perform its safety functions on demand)
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$



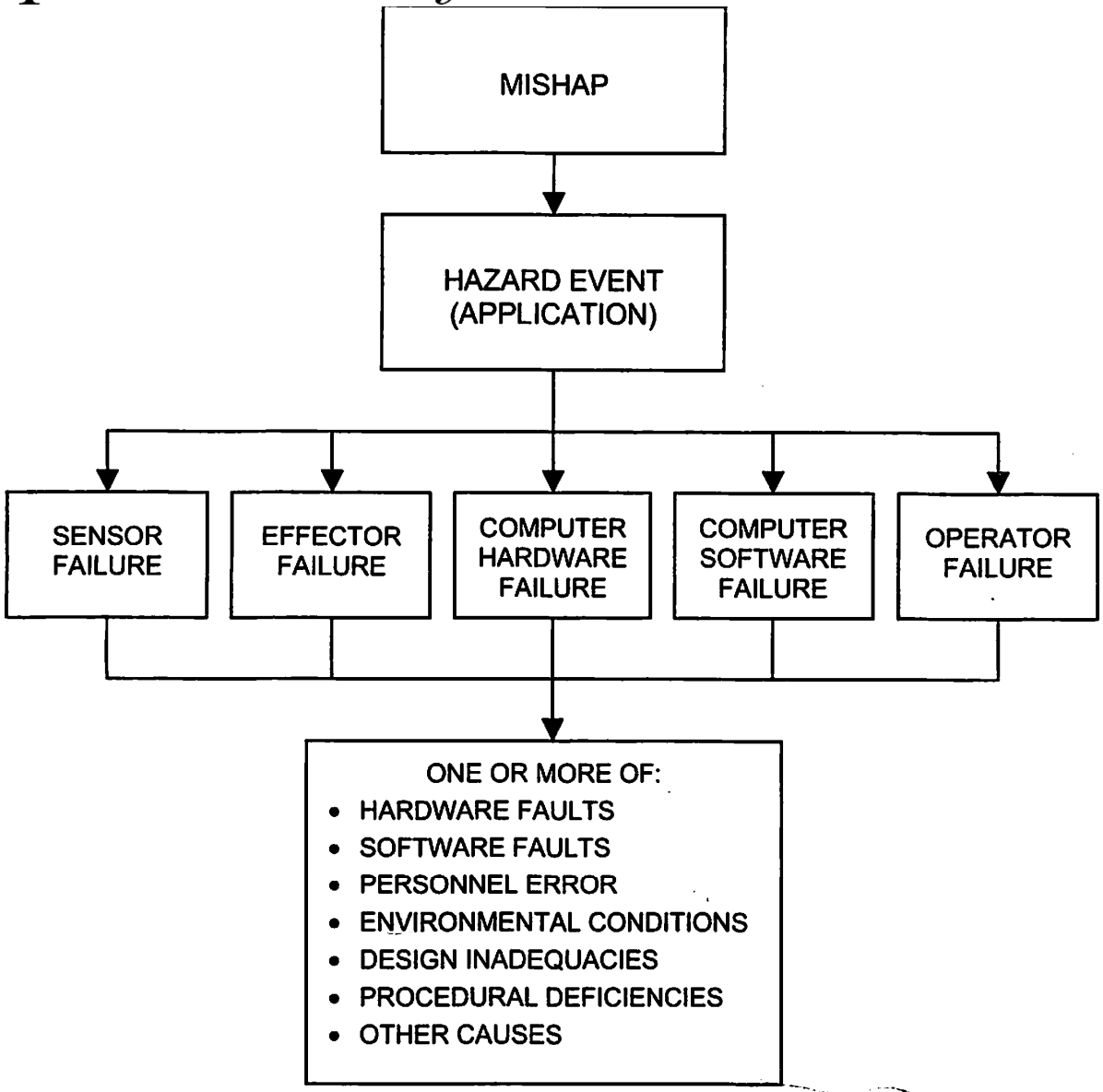
System Design Steps

Due to the outlined possibility of mishaps due to the failure of one or more components that make up either the control or safety systems, it is important to have well defined system design procedure:

- System definition
- Hazard identification and analysis
- Mishap risk mitigation
- Mishap risk and acceptance



Mishap Risk – Definitions & Evaluation



Mishap Risk Mitigation

As prescribed by the military standard MIL-STD-882D, the order of importance for identified hazard mitigation is:

- Eliminate hazards
- Incorporate safety devices
- Provide warning devices
- Develop procedures and training

As is related to the computer system itself, it also prescribes to:

- Improve component reliability and quality
- Incorporate internal safety and warning devices
- Incorporate external safety devices

Mishap Risk Mitigation