Controlling Risks
Safety System Architectures

Architectures

- High level implementation of system
- Takes in to account:
  - Fault Tolerance
  - Final control devices
  - Physical Environment
  - Constraints on physical design
  - R-M-D (Redundancy Multiplicity Diversity)

RMD – Redundancy Multiplicity Diversity

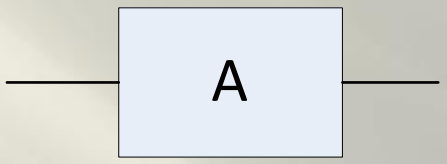
- Three elements of the architecture are used to achieve the required safety integrity level
  - Redundancy – is the use of identical safety instrumented functions to achieve a high safety reliability
  - Multiplicity - is the use of multiple shutdown paths or protection devices
  - Diversity – is the use if different types of devices to reduce the probability that multiple or redundant devices can be affected by common failure modes.

Architectures

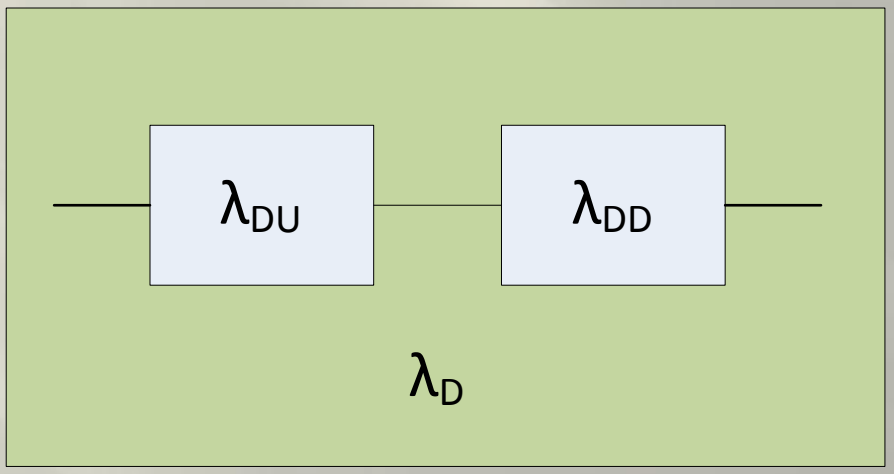
Architecture	Number of Units	Output Switches	Safety Fault Tolerance	Availability Fault Tolerance	Objectives
1oo1	1	1	0	0	Base Unit
1oo2	2	2	1	0	High Safety
2oo2	2	2	0	1	High Availability
1oo1D	1	2	0 – fail not detected 1 – fail detected	0	High Safety
2oo3	3	6 (4*)	1	1	Safety and Avilability
2oo2D	2	4	0 – fail not detected 1 – fail detected	1	Safety and Avilability Bias toward availability
1oo2D	2	4	1	0 – fail not detected 1 – fail detected	Safety and Avilability Bias toward safety

* Some implementations of 2oo3 use 4 output switches.

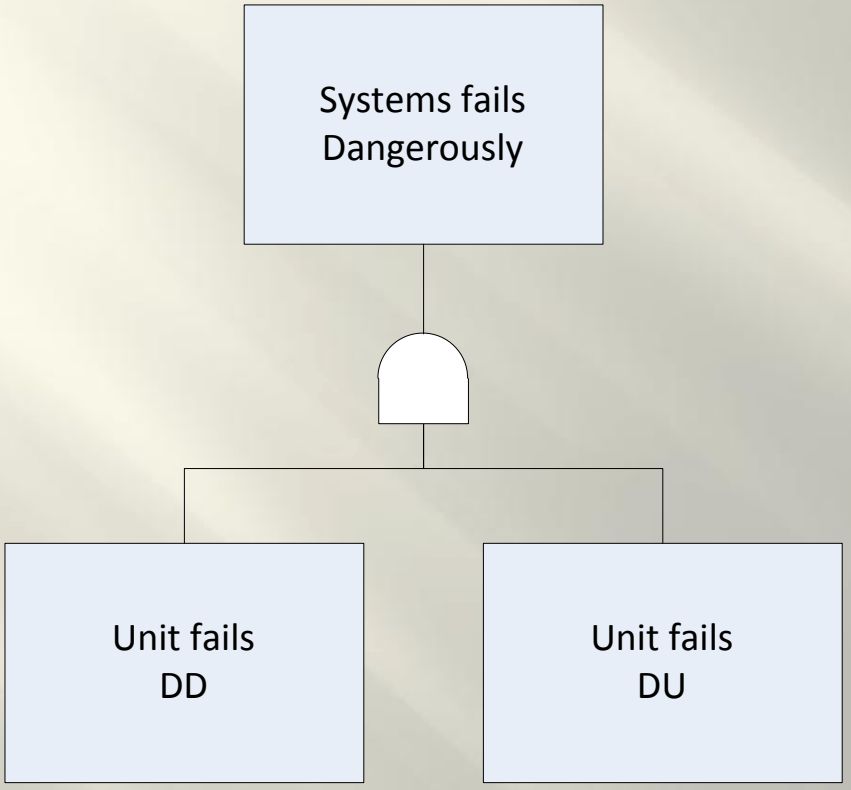
1oo1



$PFD \approx \lambda_D * TI$



PFD for 1oo1



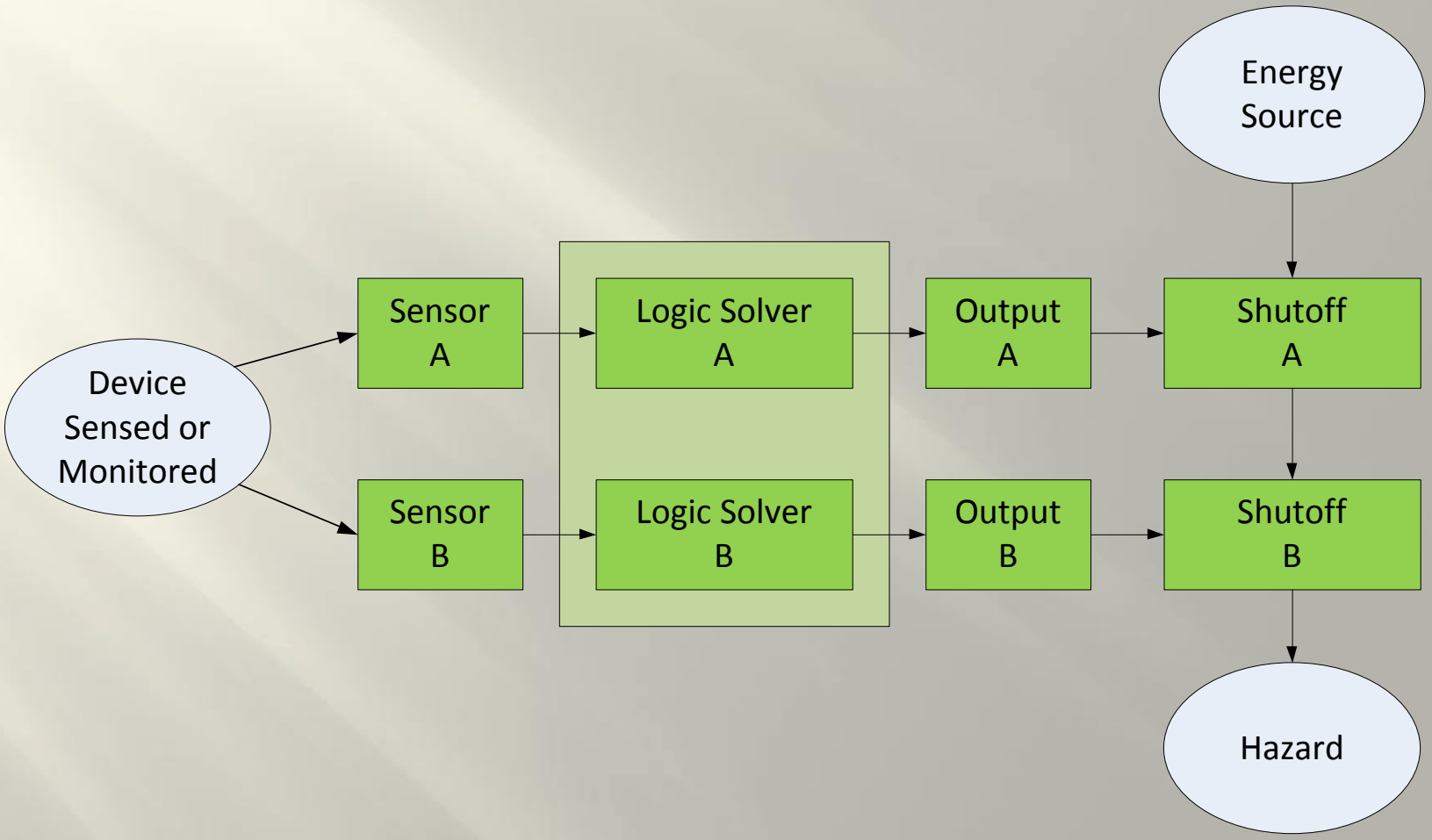
$$PFD_{1oo1} = \lambda^{DD} * RT * \lambda^{DU} * MT$$

Where detected failures are repaired and undetected failures remain until end of life or revealed by test.

Integrating over mission time

$$PFD_{avg} = \lambda^{DD} * RT * \lambda^{DU} * \frac{MT}{2}$$

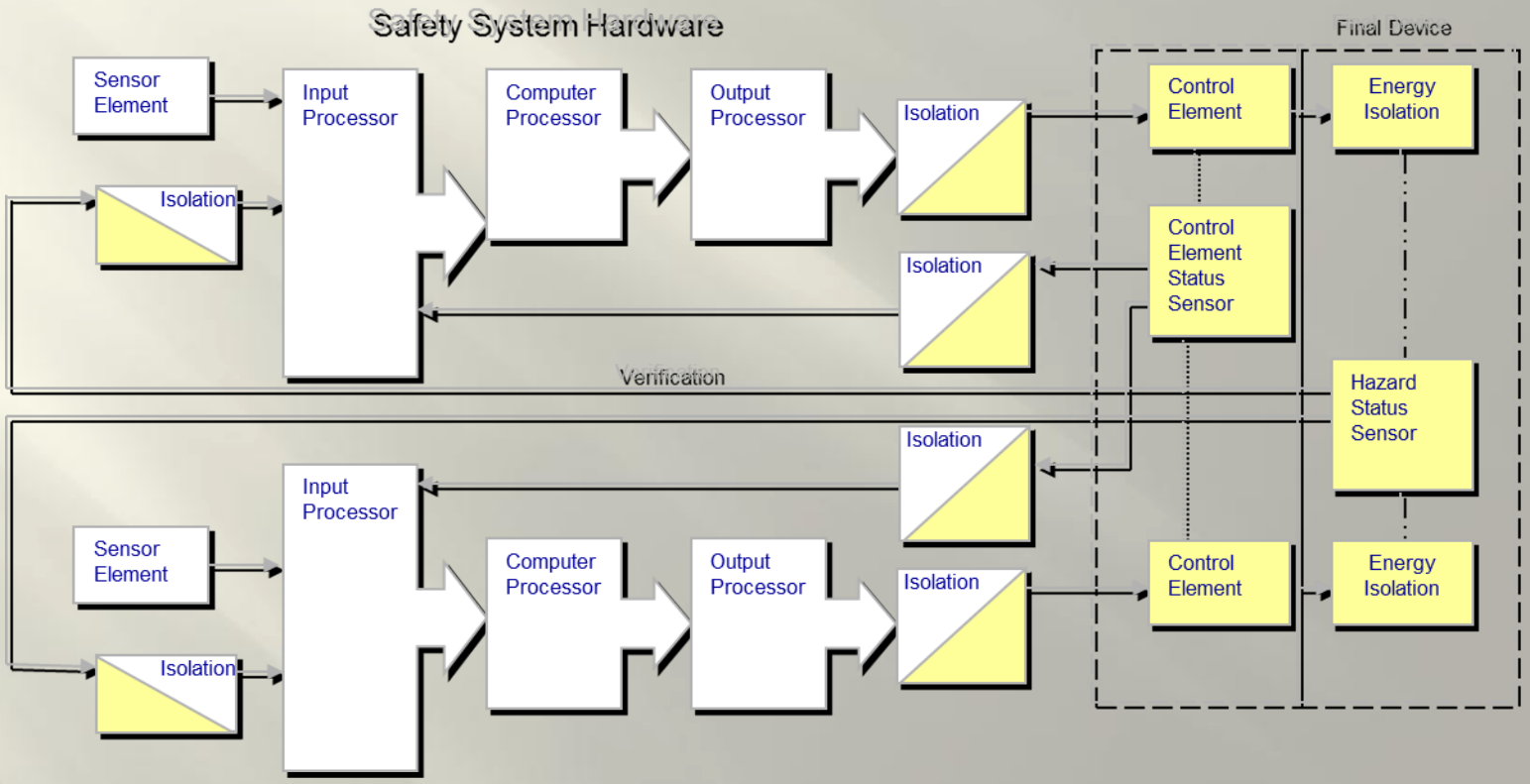
1oo2 Block Diagram



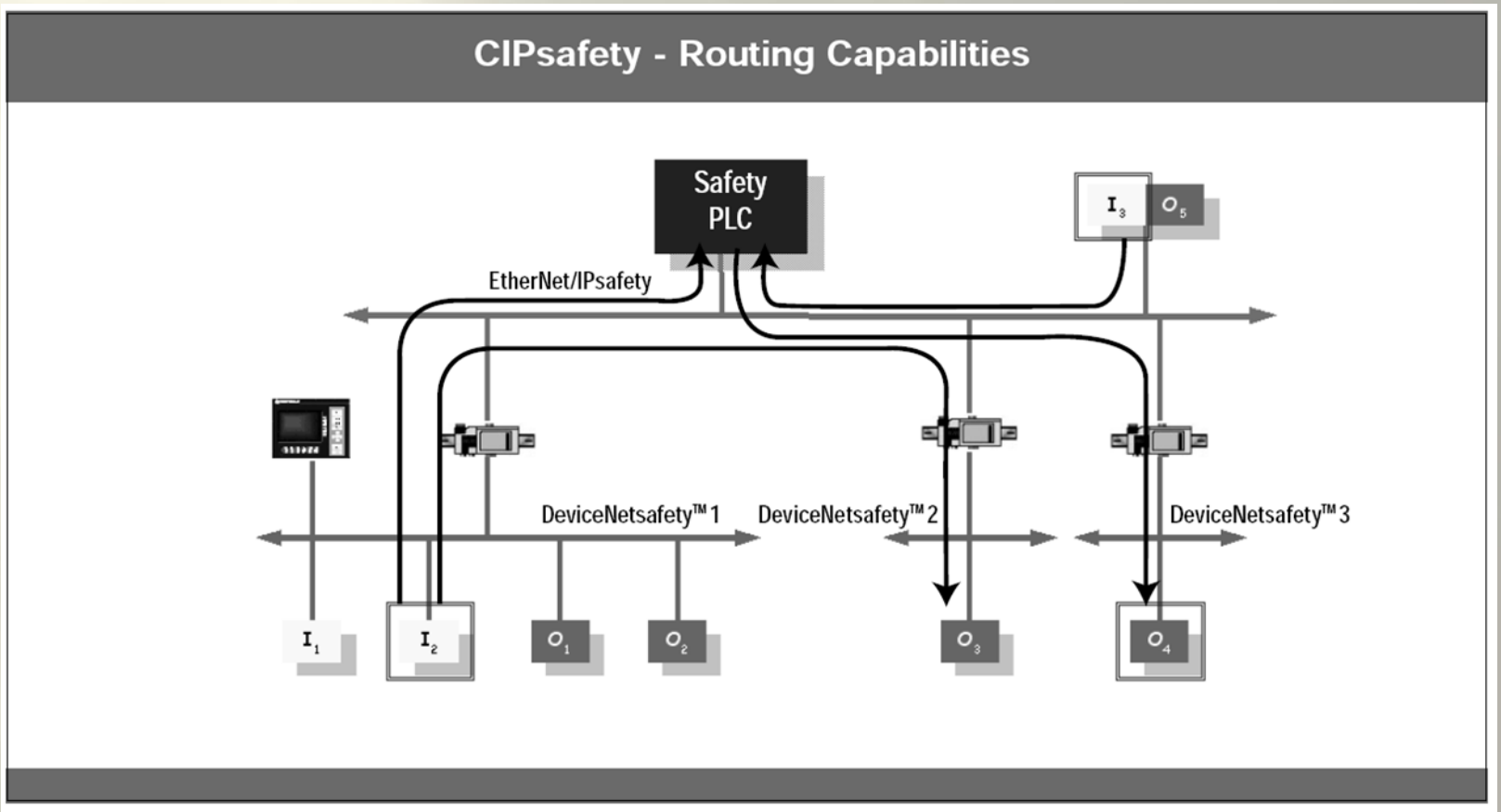
1oo2 Features

- Two circuits are wired to minimize the effect of dangerous unit failures
  - Input shorted
  - Output shorted
  - Logic error (hardwired)
- For de-energize to trip systems a series connection of two output circuits both need to fail dangerously for the system to fail dangerous
- A PLC implemented 1oo2 architecture may have one physical controller with redundancy implemented internally

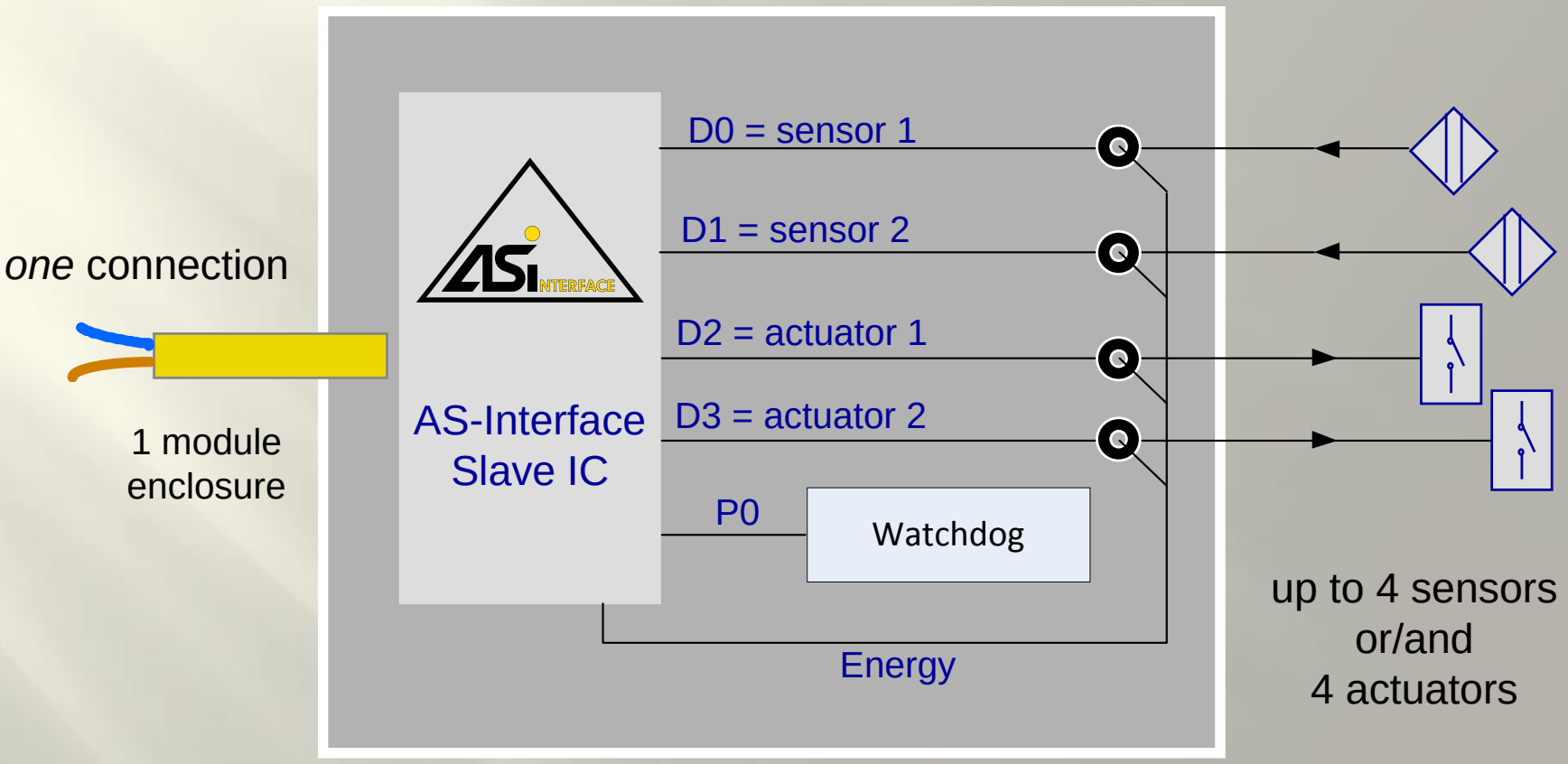
PLC Implemented 1oo2



CIP=Common Industrial Protocol

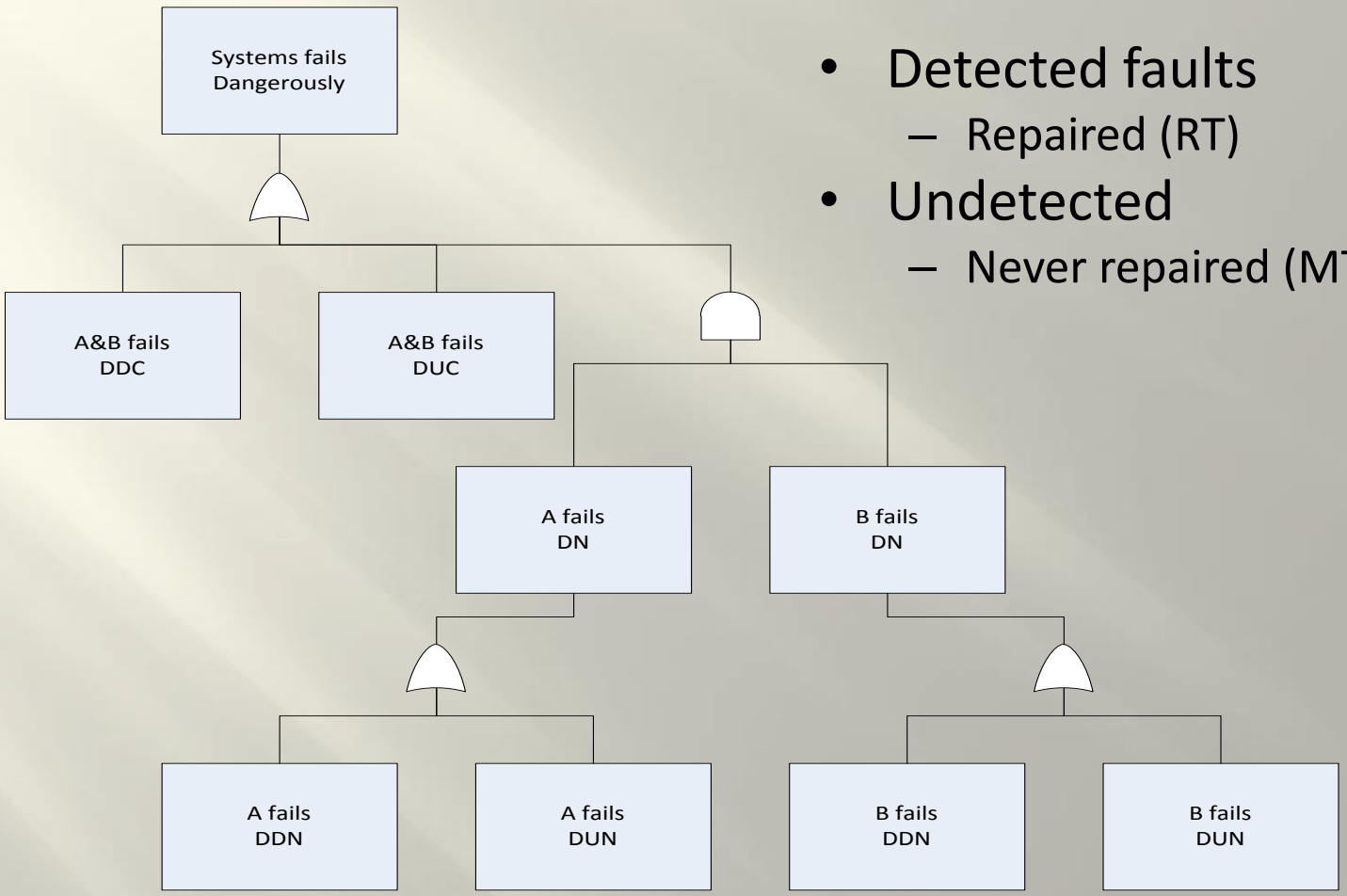


Actuator Sensor Interface



Courtesy of ASI International Foundation

Fault Tree 1oo2



- Detected faults
  - Repaired (RT)
- Undetected
  - Never repaired (MT)

Story Time

- Subject
  - Site Architectures
  - Hardware Implementation