Controlling Risks
SIS and SIL Evaluation

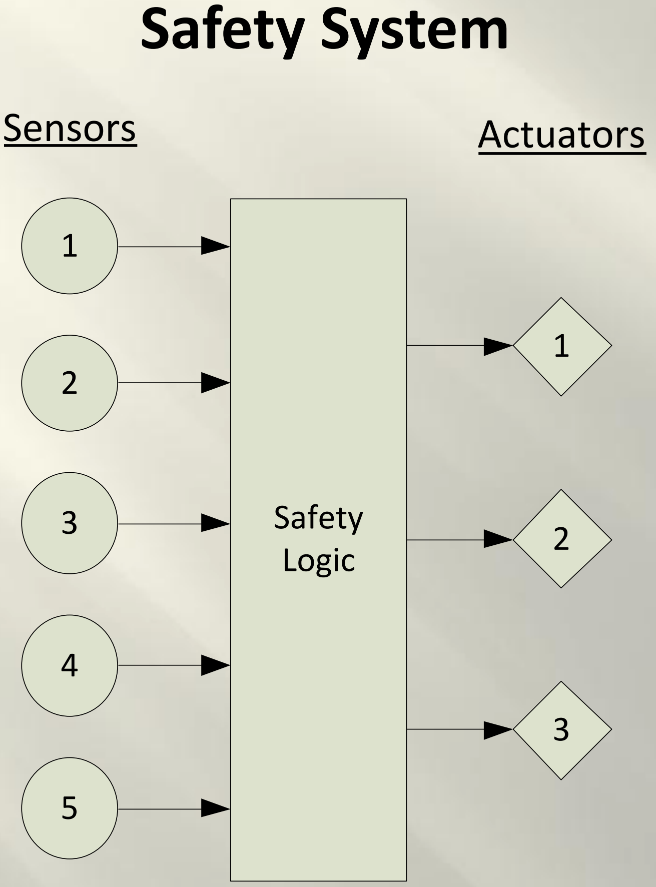
Risk Analysis

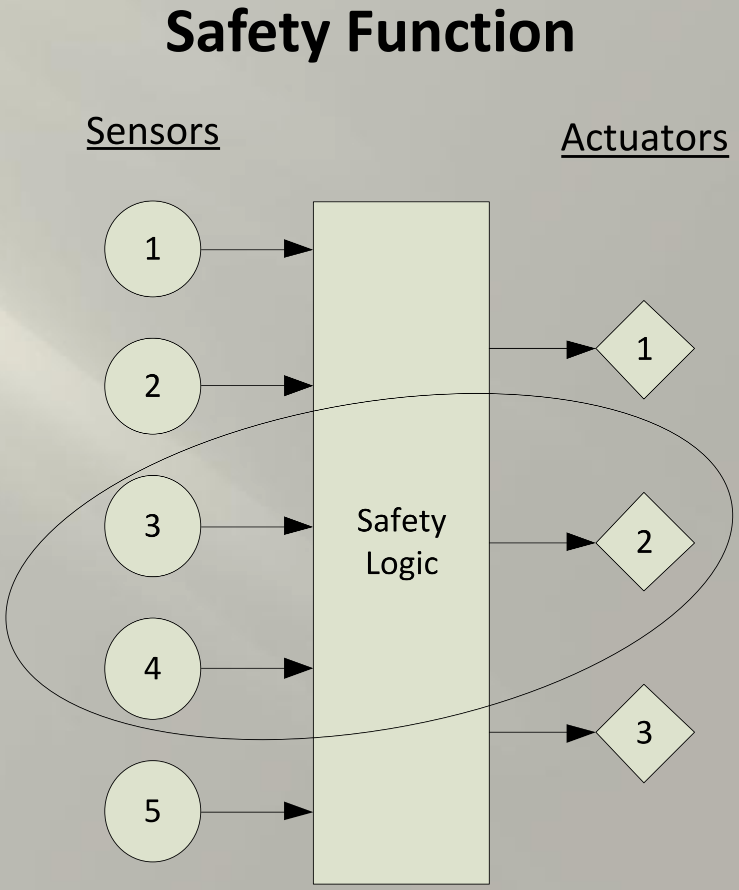
- the International Telecommunication Union (ITU) is meeting in Geneva, and one of the items on its agenda is the abolition of the leap second. If the assembled delegates vote in favor, then the next leap second (which will be added one second before midnight on June 30th, causing clocks set to UTC to display 23:59:59 for two seconds instead of one)
- America's Global Positioning System satellites, for instance, do not add leap seconds to their internal clocks, and are therefore out of step with UTC. Receivers on the ground can correct for that discrepancy. But the satellite-navigation systems being launched by China, Europe and Russia use still other definitions of time, so exceptions to UTC are proliferating. That has led to worries that mismatched time signals could cause navigation problems, since even small errors in a time signal would mean positions being off by tens of meters.

Interlock Circuits

- Interlock circuits are sometimes complicated
  - Many devices in circuit
  - Multiple circuits acting on multiple hazards
  - Combination of control system and safety interlocks
- Therefore the SIS is not evaluated
  - Due to misconceptions about what is being calculated

SIS and SIF

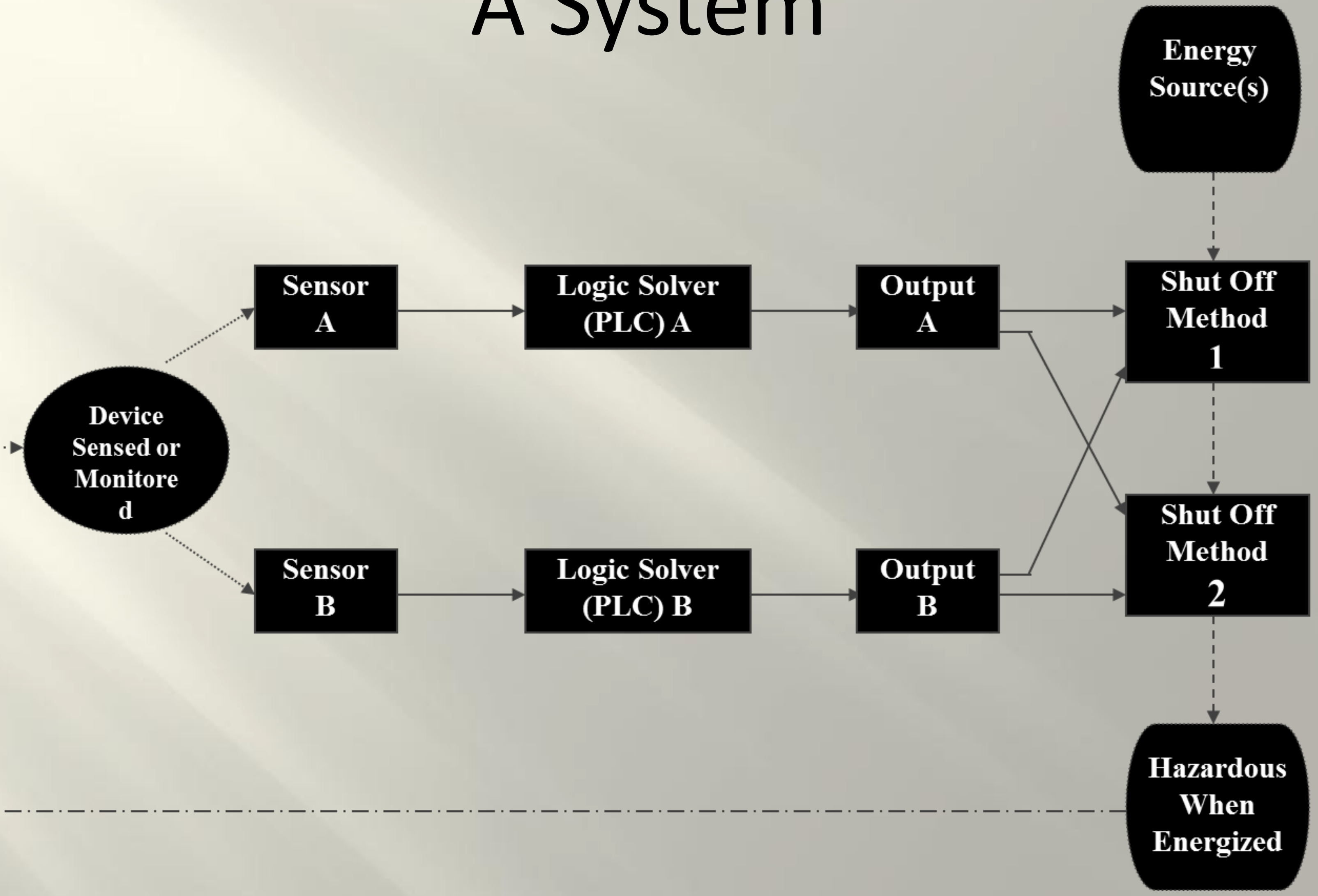

Safety System
Sensors
Actuators
1
2
3
4
5
Safety Logic
1
2
3


Safety Function
Sensors
Actuators
1
2
3
4
5
Safety Logic
1
2
3

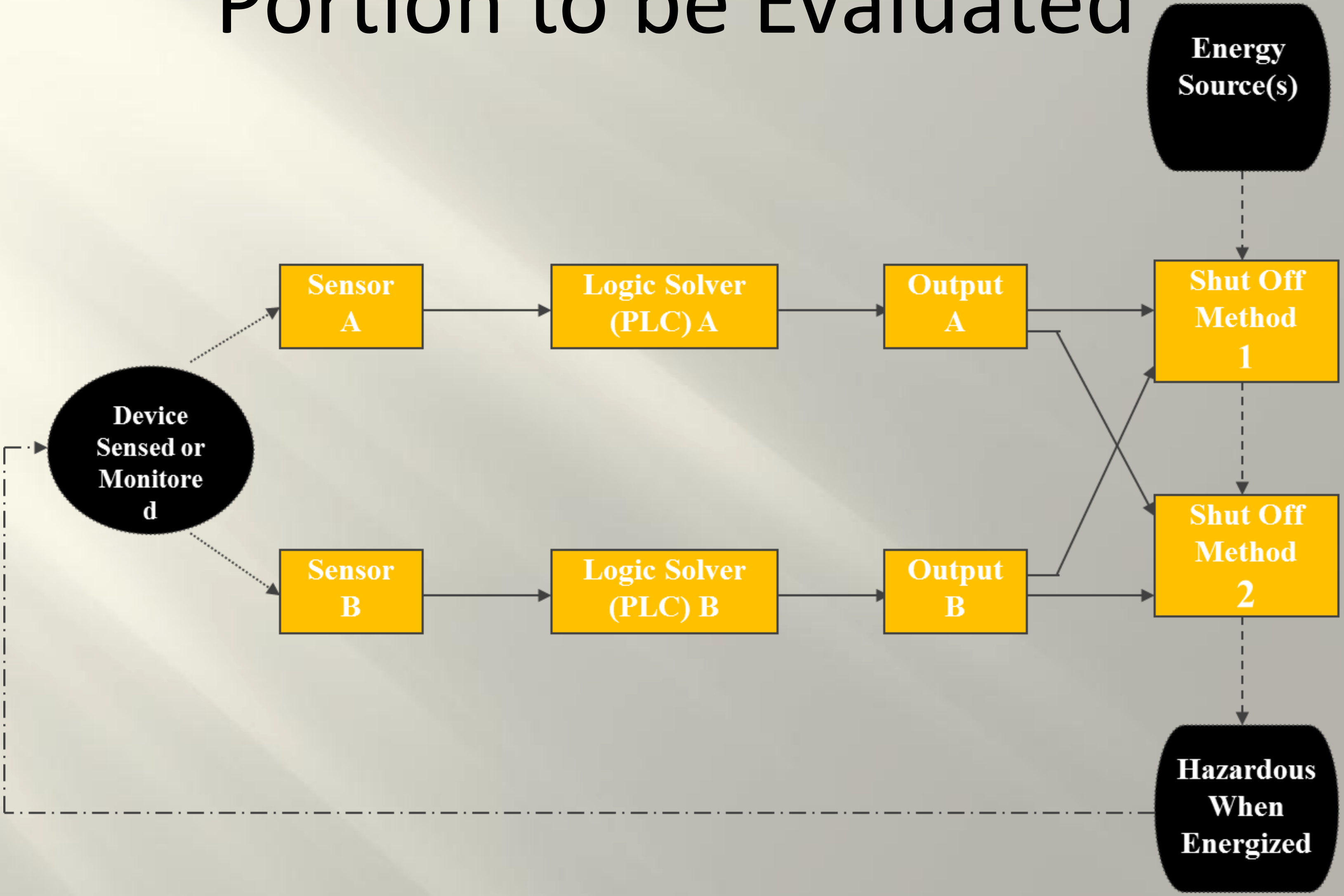
Evaluation

- SIS Evaluation
  - Is evaluated by hazard not the entire circuit at once
  - Is calculated for each individual SIF
  - Relies on the weakest SIF calculated

A System

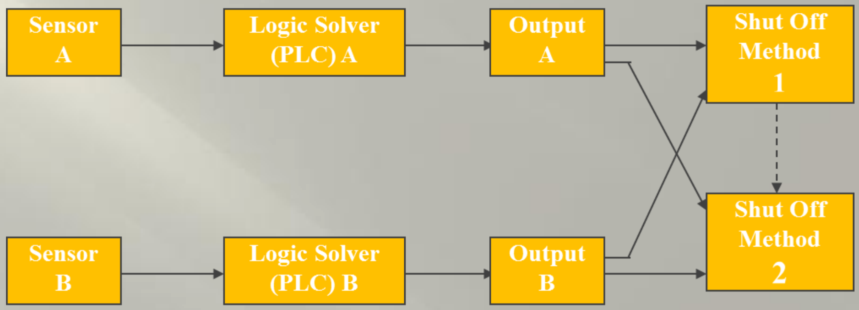

Energy Source(s)
Sensor A
Logic Solver (PLC) A
Output A
Shut Off Method 1
Device Sensed or Monitore d
Sensor B
Logic Solver (PLC) B
Output B
Shut Off Method 2
Hazardous When Energized

Portion to be Evaluated

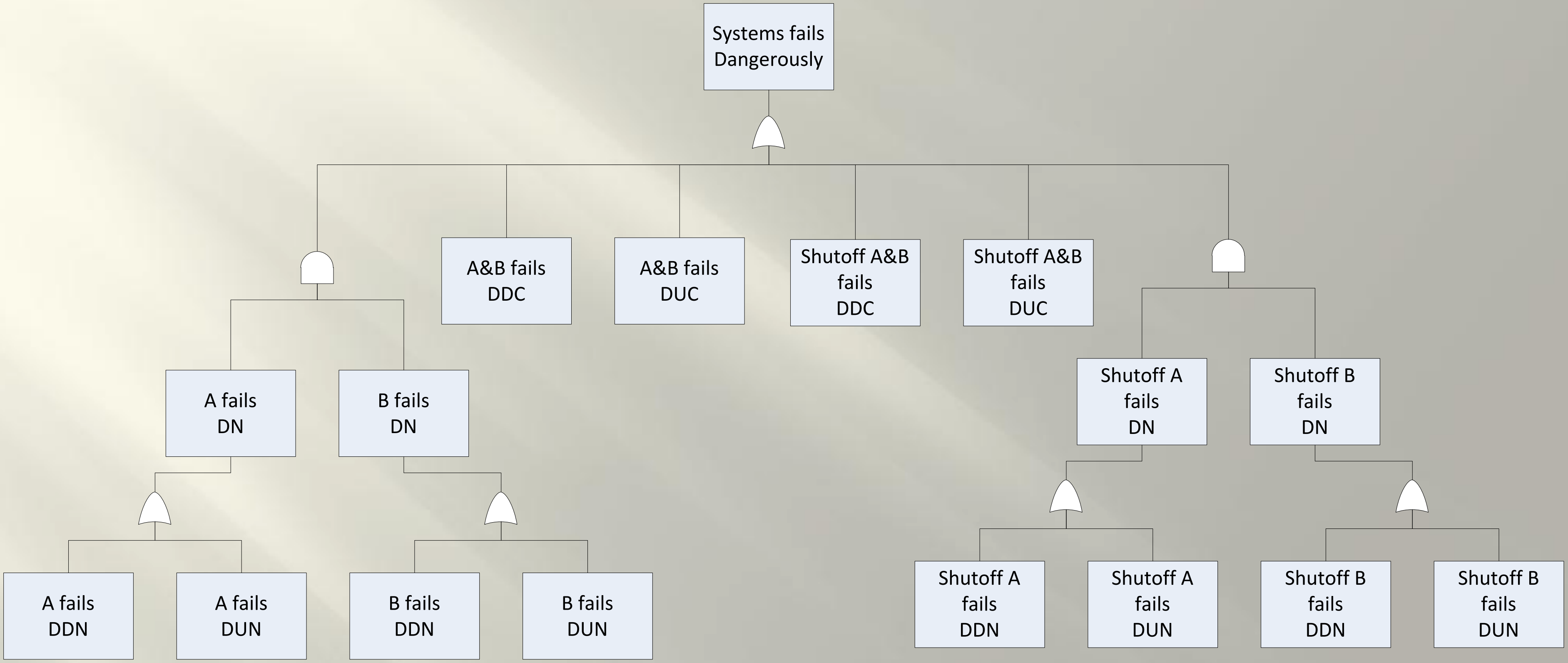


Evaluation

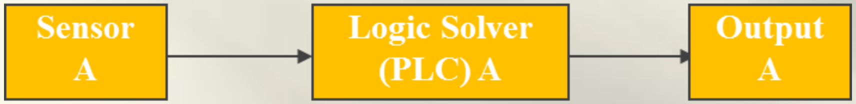
- A failure of sensor A or B trigger the shutoff method
- A failure of Logic Solver A or B trigger the shutoff method
- A failure of Output A or B trigger the shutoff method
- A dangerous failure occurs only with a failure of
  - system A and system B
  - or
  - Shutoff Method A and Shutoff Method B



Fault Tree


Systems fails Dangerously
A&B fails DDC
A&B fails DUC
Shutoff A&B fails DDC
Shutoff A&B fails DUC
A fails DN
B fails DN
Shutoff A fails DN
Shutoff B fails DN
A fails DDN
A fails DUN
B fails DDN
B fails DUN
Shutoff A fails DDN
Shutoff A fails DUN
Shutoff B fails DDN
Shutoff B fails DUN

System A



- The probability of system A failing is the sum of MTBF for
  - Sensor A
  - Logic Solver A
  - Output A
- If components are identical then $\lambda_B = \lambda_A$

Dangerous Failure Rate

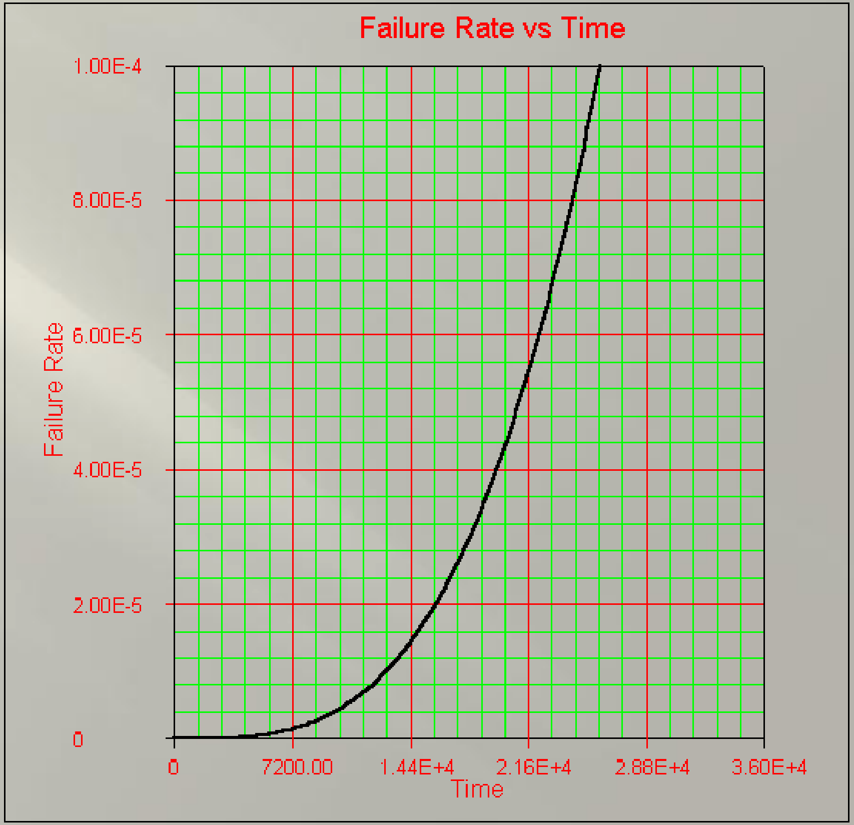
- A probability of fail-dangerous calculation for safety verification purposes requires more than just the failure rate
- The failure modes and diagnostic coverage should also be taken into consideration

Conservative Estimates

- Safe failure percentage
  - Most electronic hardware = 50%
  - Relays = 70% - 80%
  - Solenoids = 40%
- Diagnostic Coverage
  - Mechanical devices = 0%
  - Normal microprocessor = 50%

Failure Rate Data

- Offshore Reliability Data
  - OREDA handbook
  - Can be found on Amazon
  - Few copies are available
- Create your own
  - You may have enough data from operational experience to determine the failure rate of components



"That's all Folks!"