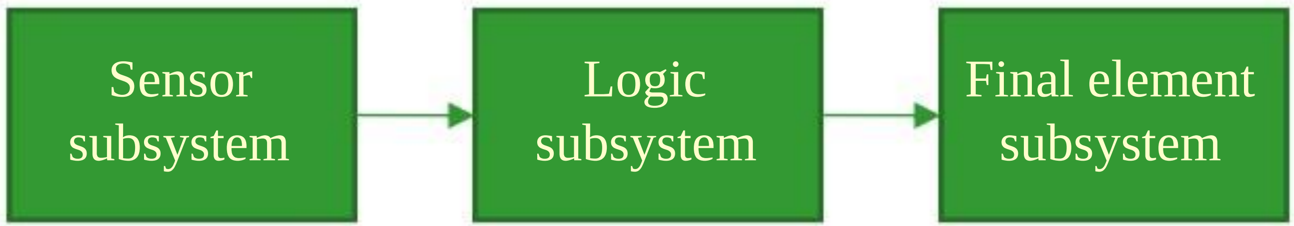
Redundancy Analysis

Alan Harding

Sub-system structure



Sensor subsystem components

- Sensors
- Barriers
- Input conditioning circuits
- etc.

Final element components

- Actuators
- Barriers
- Output conditioning circuits
- etc.

Logic subsystem components

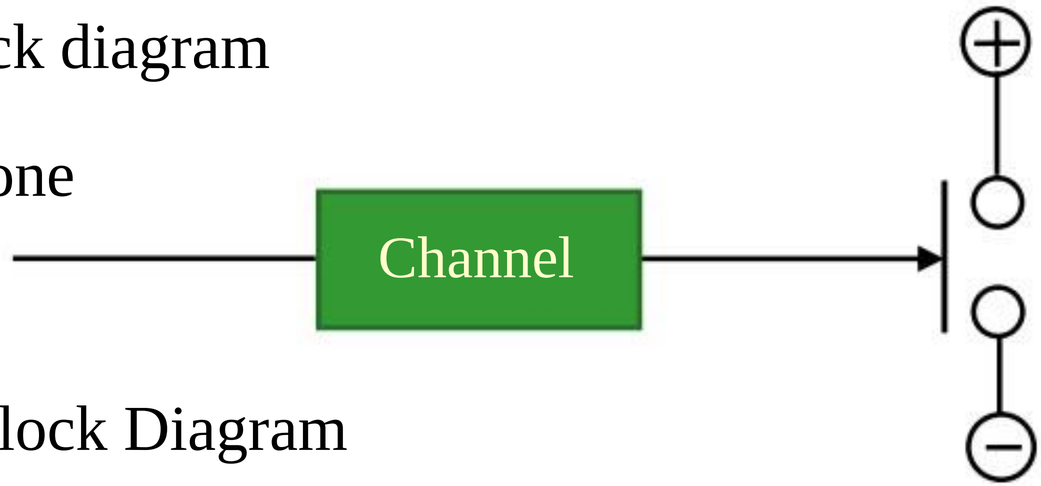
- Processors
- Computers
- Scanning devices
- etc.

1OO1 System (fault tolerance=0)

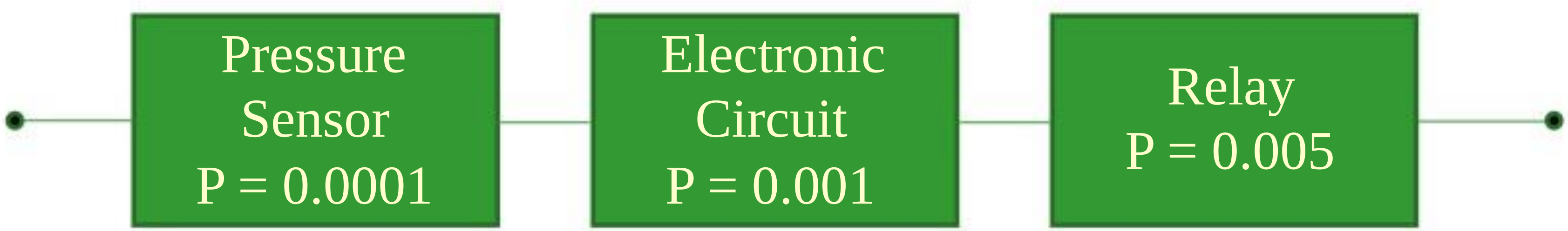
- A single channel where any dangerous failure leads to a failure of the safety function when a demand arises

- Physical block diagram

One-out-of-one



- Reliability Block Diagram

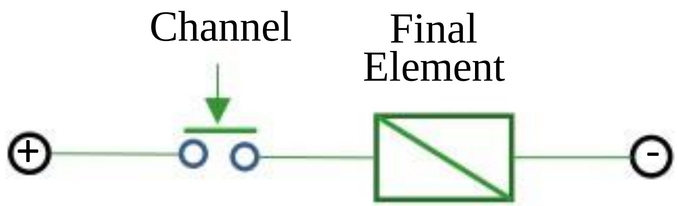


(P = Probability of dangerous failure)

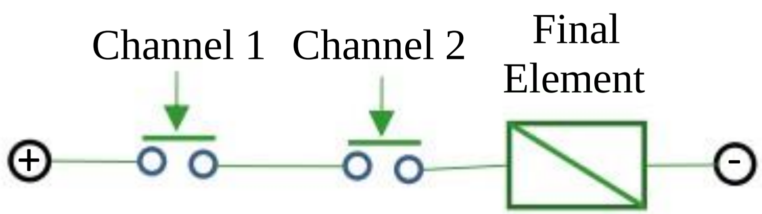
Voting Techniques

Each subsystem can be represented as one or more following voting groups

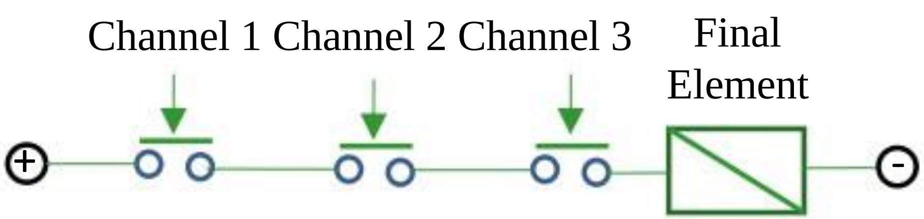
1OO1 system



1OO2 system

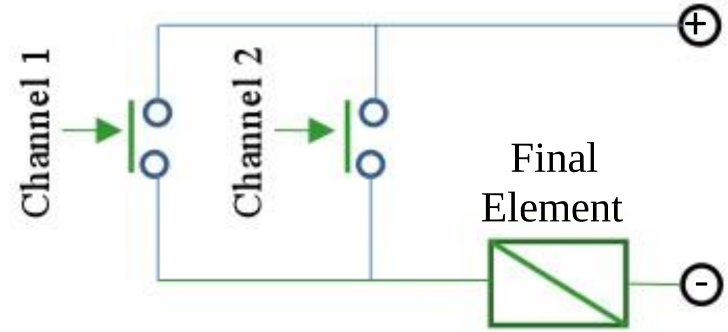


1OO3 system

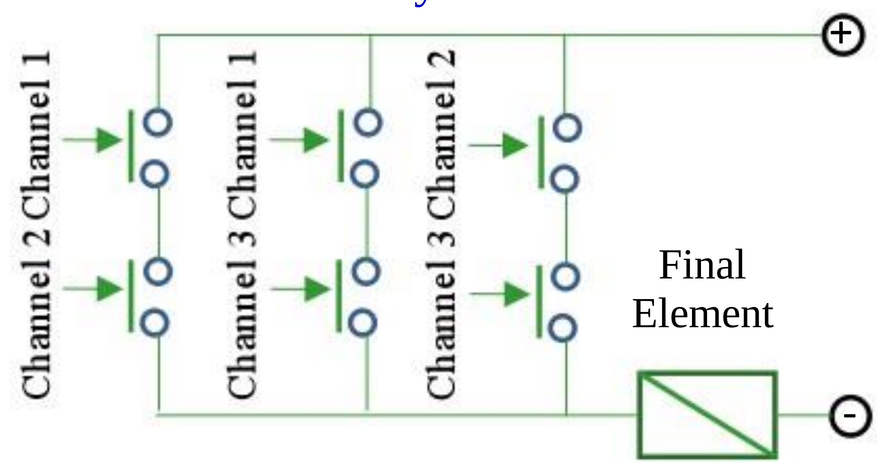


If one channel asks off → output off

2OO2 system



2OO3 system

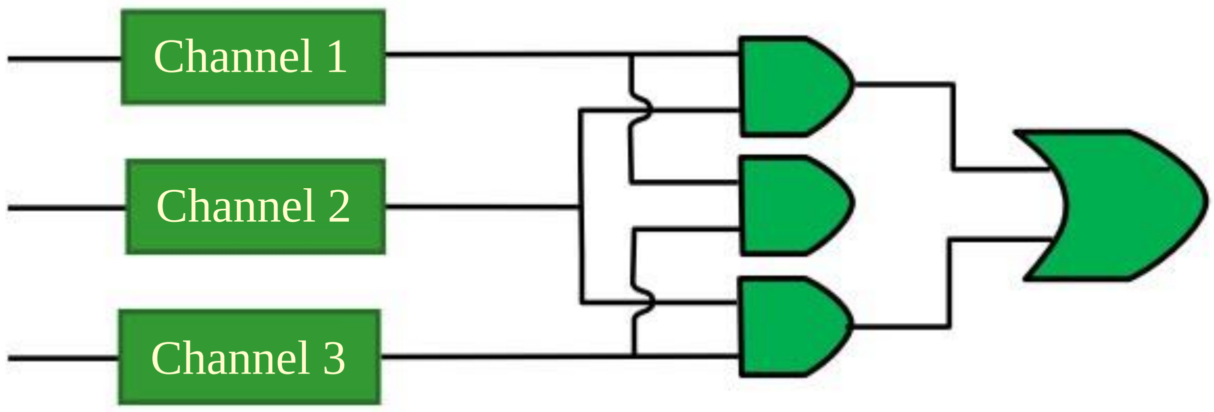


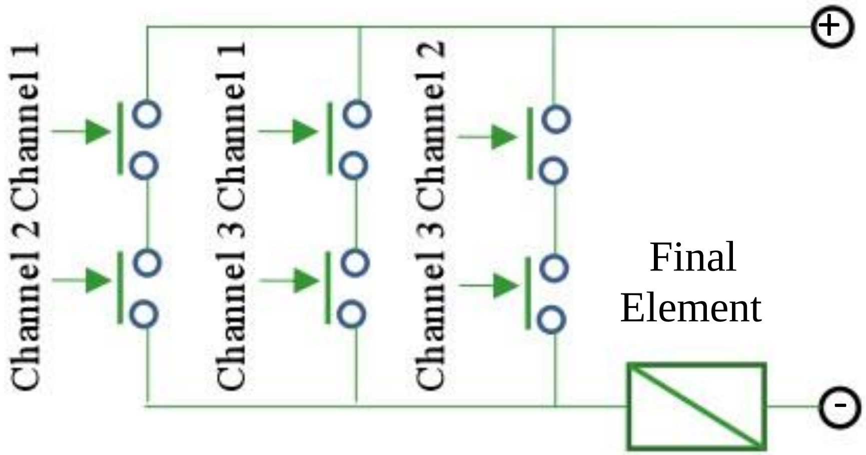
If two channels asks off → output off

2003 = two channels out of three must vote

The logic gate solution below gives one as the output for ones on two out of three channels .

It also gives zero for the output if two channels ask for zero.



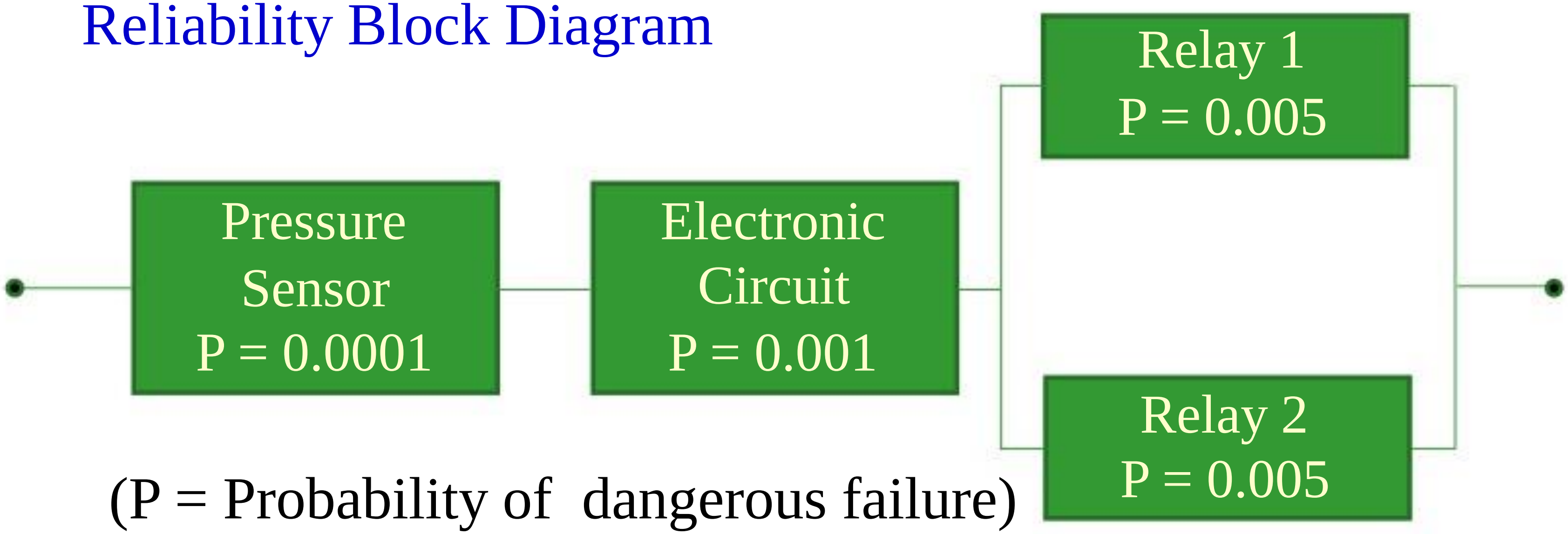


Component redundancy

Physical block diagram

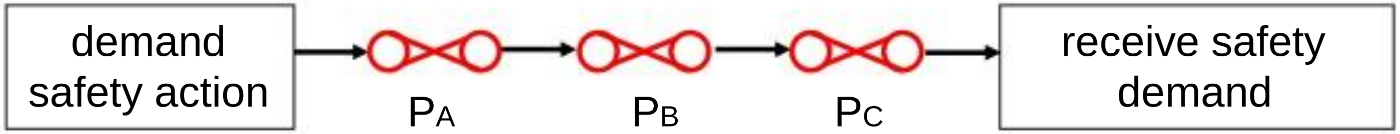
One-out-of-one

Reliability Block Diagram

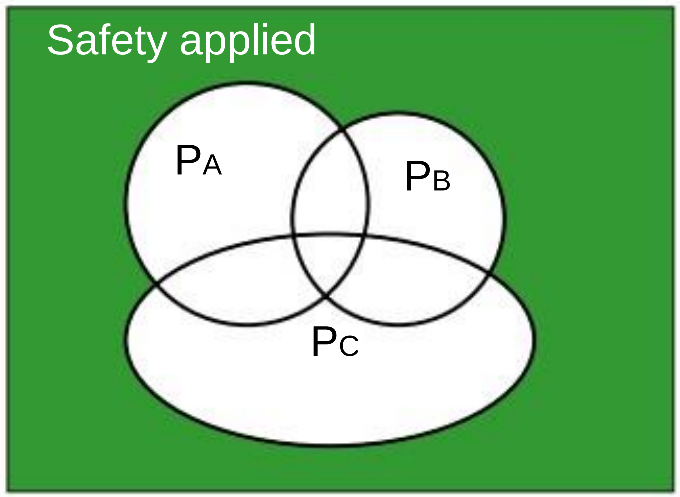


(P = Probability of dangerous failure)

Series Faults



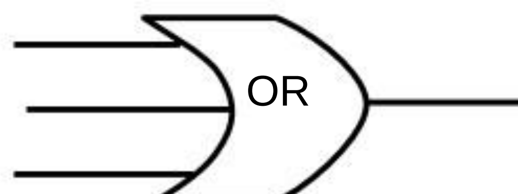
P_x represents probability of failure



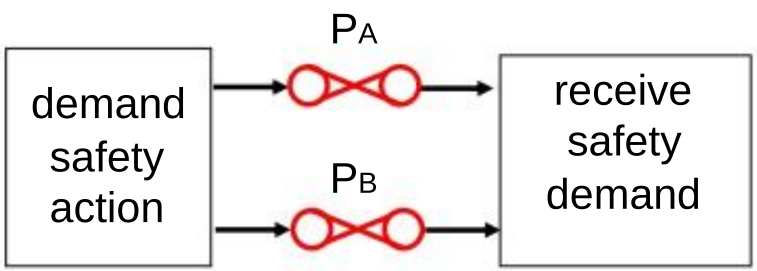
Full box represents signal sent

Probability of Failure = $P_A + P_B + P_C - P_A.P_B - P_A.P_C - P_B.P_C + 2P_A.P_B.P_C$

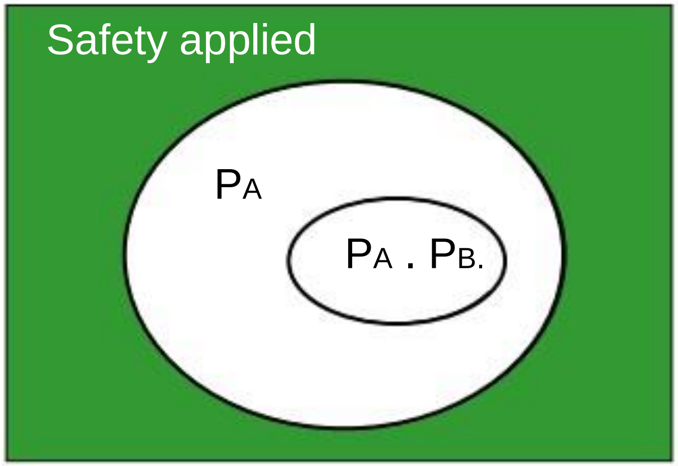
Worst Case Probability of Failure = $P_A + P_B + P_C$



Parallel Redundancy Faults



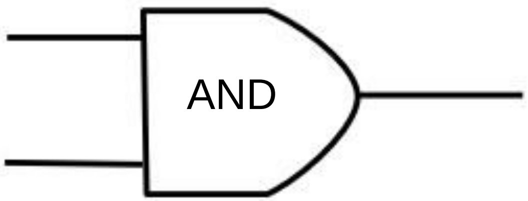
P_x represents probability of failure



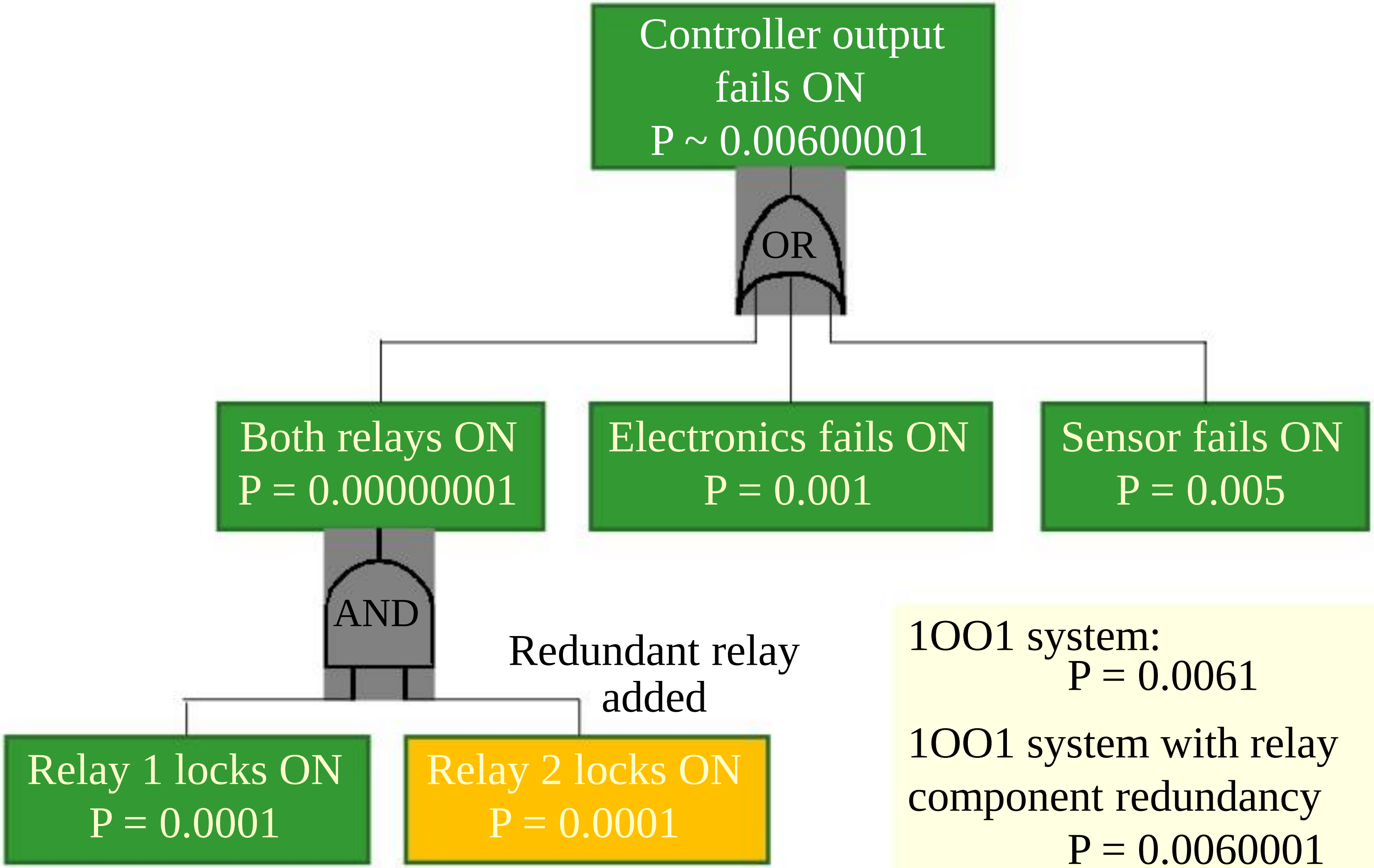
Full box represents signal sent

We now worry if B fails once A has failed

Probability of Failure = $P_A . P_B = P_B . P_A$



Fault tree analysis of 1OO1 system



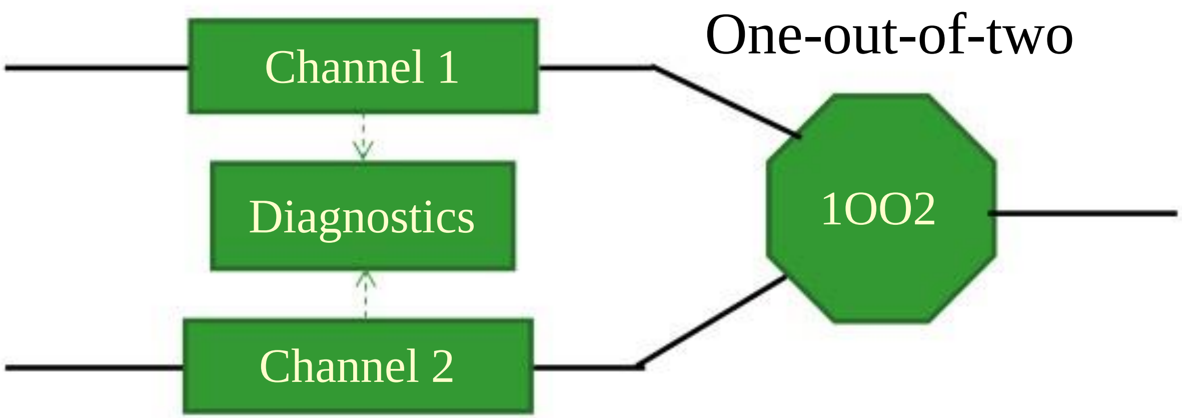
1OO1 system:
P = 0.0061

1OO1 system with relay component redundancy
P = 0.0060001

Only minor improvement

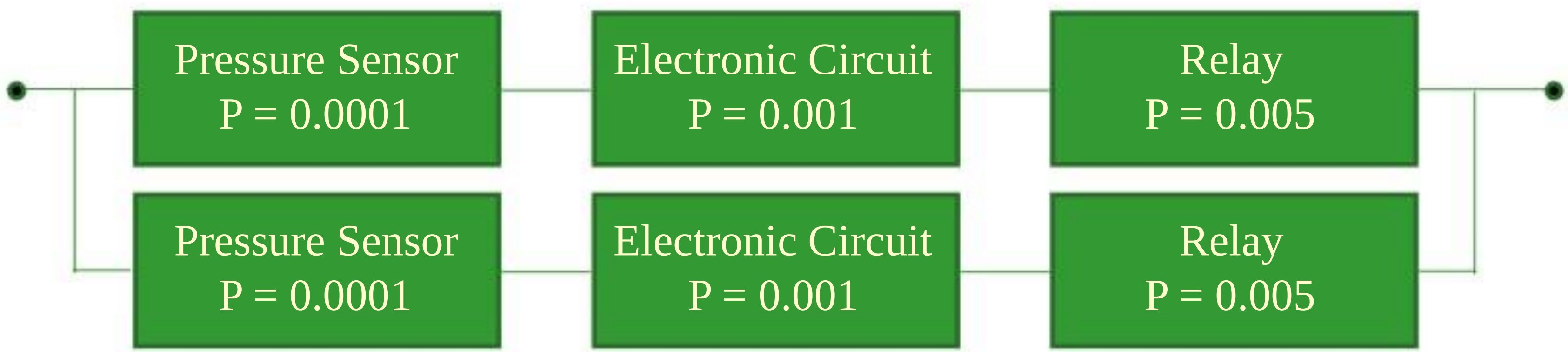
1OO2 redundant system

- Physical block diagram



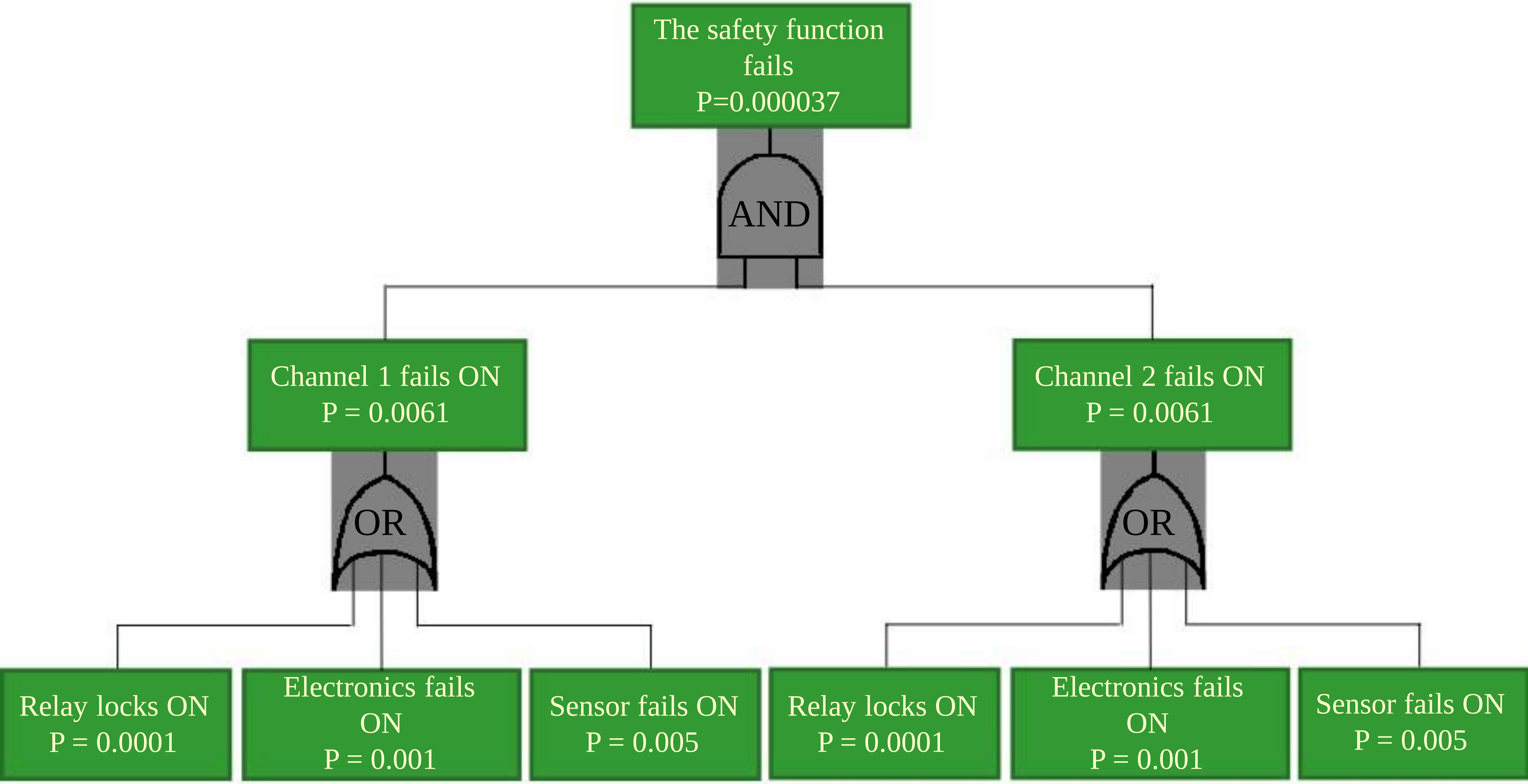
- Two channels connected in parallel
- Either channel can process the safety function
- Diagnostic testing only reports the detected faults and does not change the output voting

- Reliability Block Diagram



(P = Probability of dangerous failure)

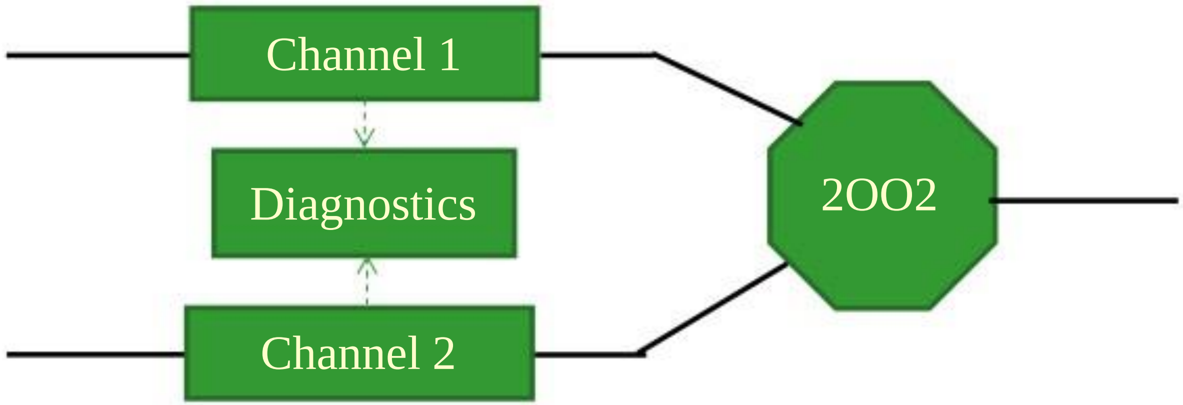
Fault tree analysis of 1OO2 redundant system



Great improvement in 1OO2 redundant control system

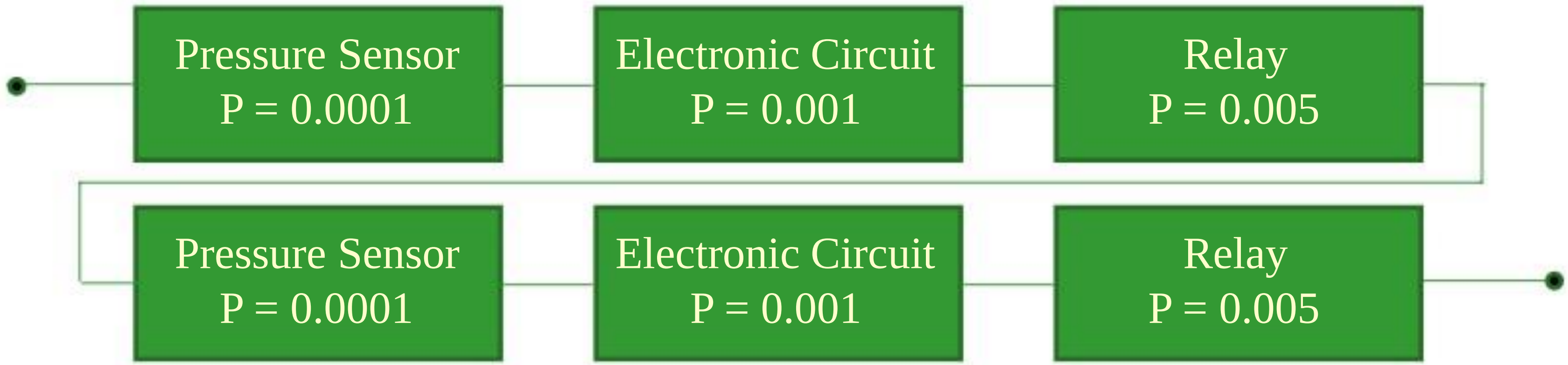
2OO2 redundant system

- Physical block diagram



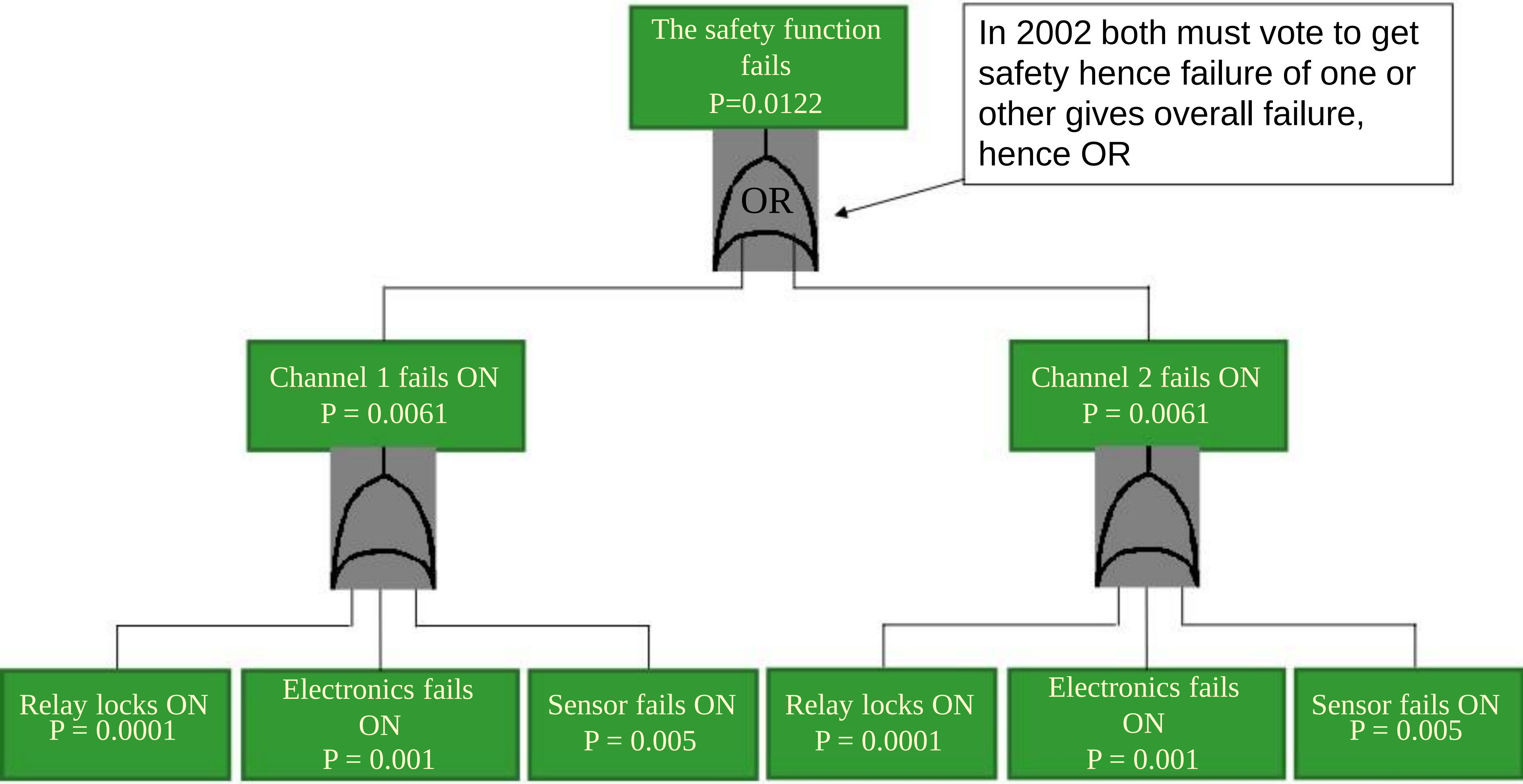
- Two channels connected in parallel
- Both channels need to demand the safety function before it can take place
- Diagnostic testing only reports the detected faults and does not change the output voting

- Reliability Block Diagram



(P = Probability of dangerous failure)

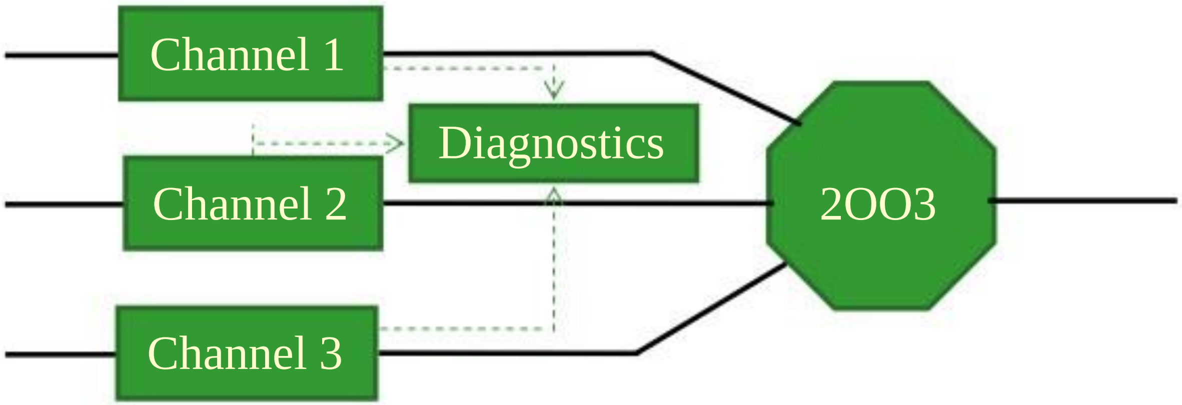
Fault tree analysis of 2OO2 redundant system



Poor safety performance in 2OO2 redundant control system

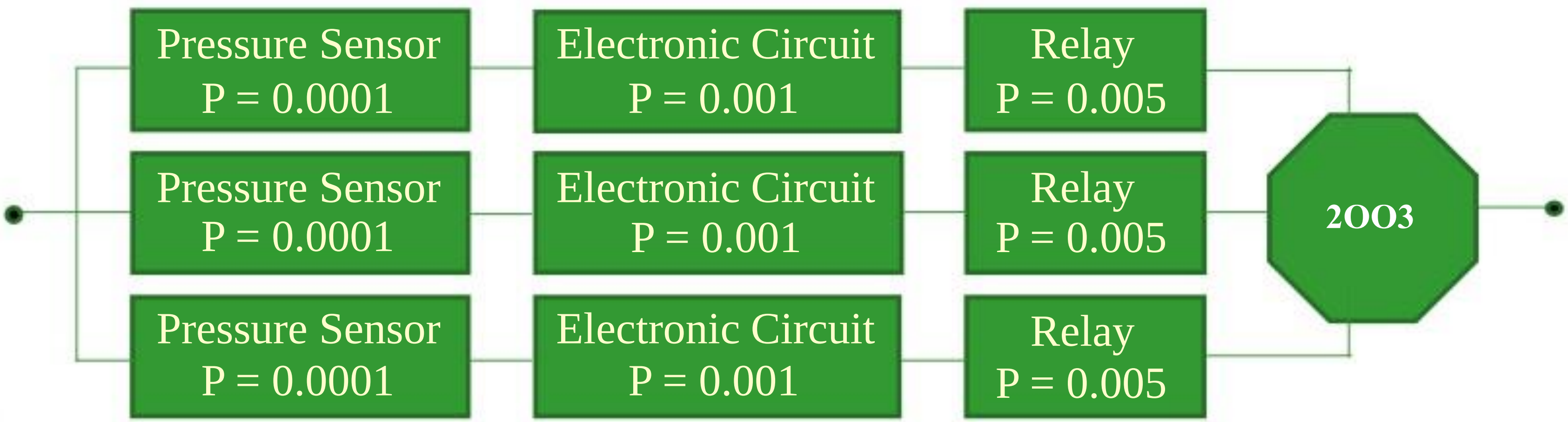
2OO3 redundant system

- Physical block diagram



- Three channels connected in parallel with a majority voting arrangement for the output signals
- The output state is not changed if only one channel gives a different result which disagrees with the other two channels

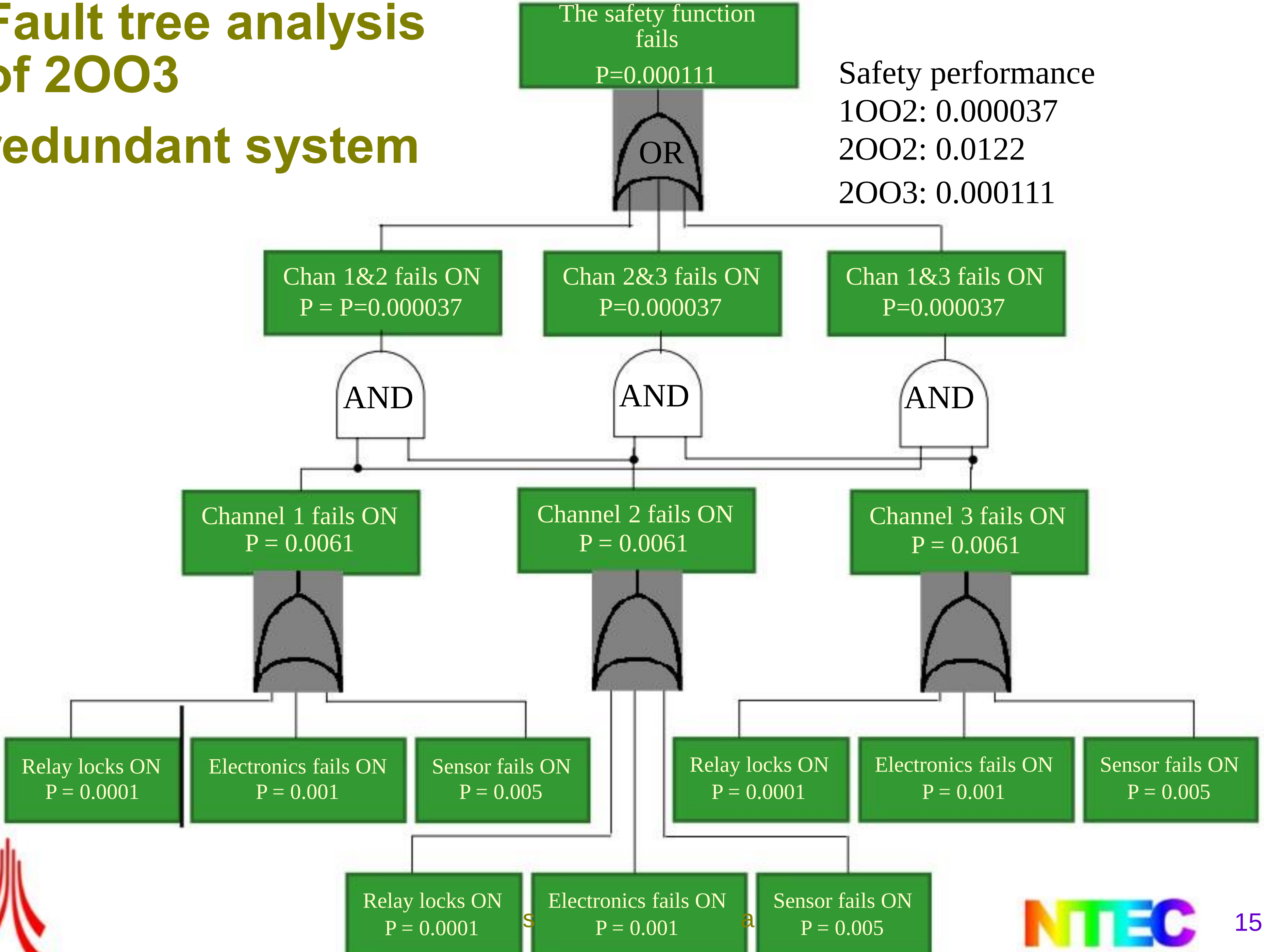
- Reliability Block Diagram



(P = Probability of dangerous failure)

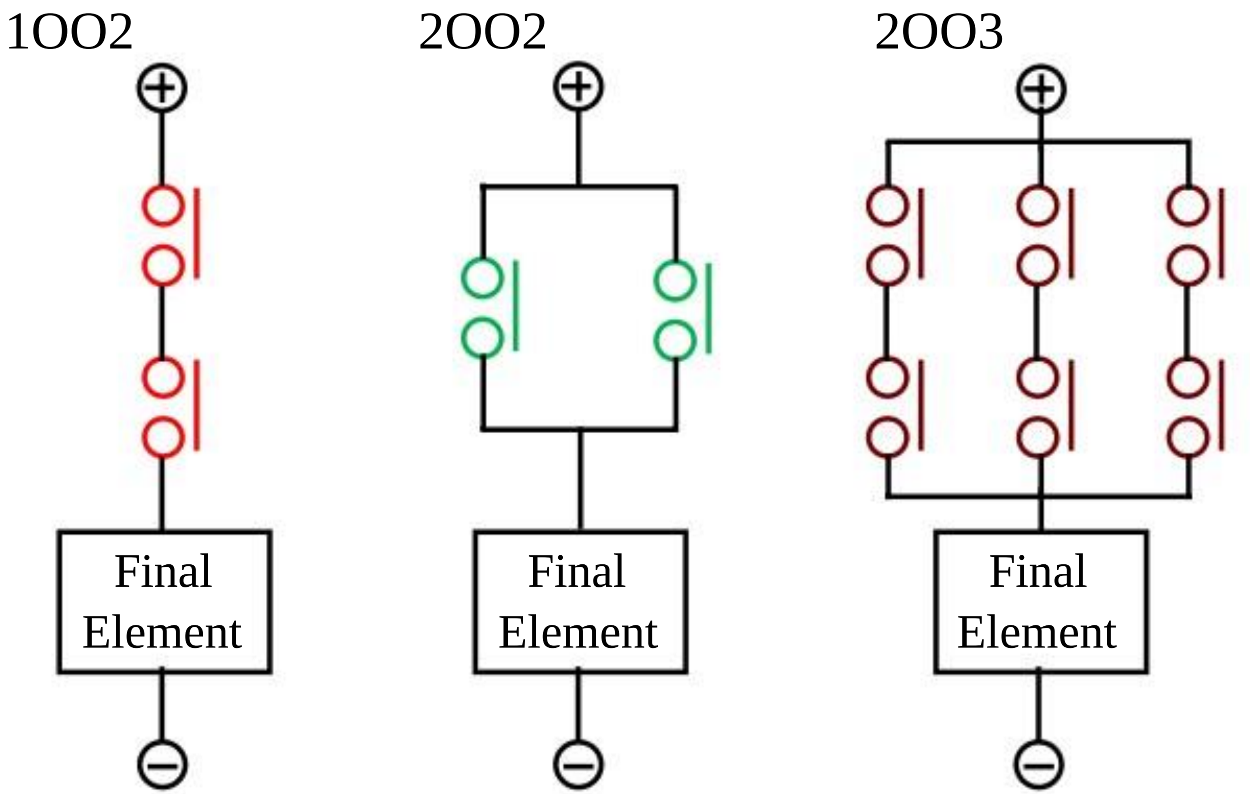
Fault tree analysis of 2OO3 redundant system

Safety performance
1OO2: 0.000037
2OO2: 0.0122
2OO3: 0.000111



Safety versus availability

A flaw with this type diagram is that it is not clear whether safe is on or off



P=0.000037 P=0.0122 P=0.000111

Safety Only	Availability Only	Safety &Availability
Either ask off	Both ask off	Two of three ask off

Assume loop normally energised, (i.e., de-energise to trip)

- Consider “stuck at 1 failures” (i.e. contacts welded)
- Consider “stuck at 0 failures” (i.e. high resistance build-up on contacts)