Industrial Embedded Systems
- Design for Harsh Environment -

Dr. Alexander Walsch
alexander.walsch@ge.com

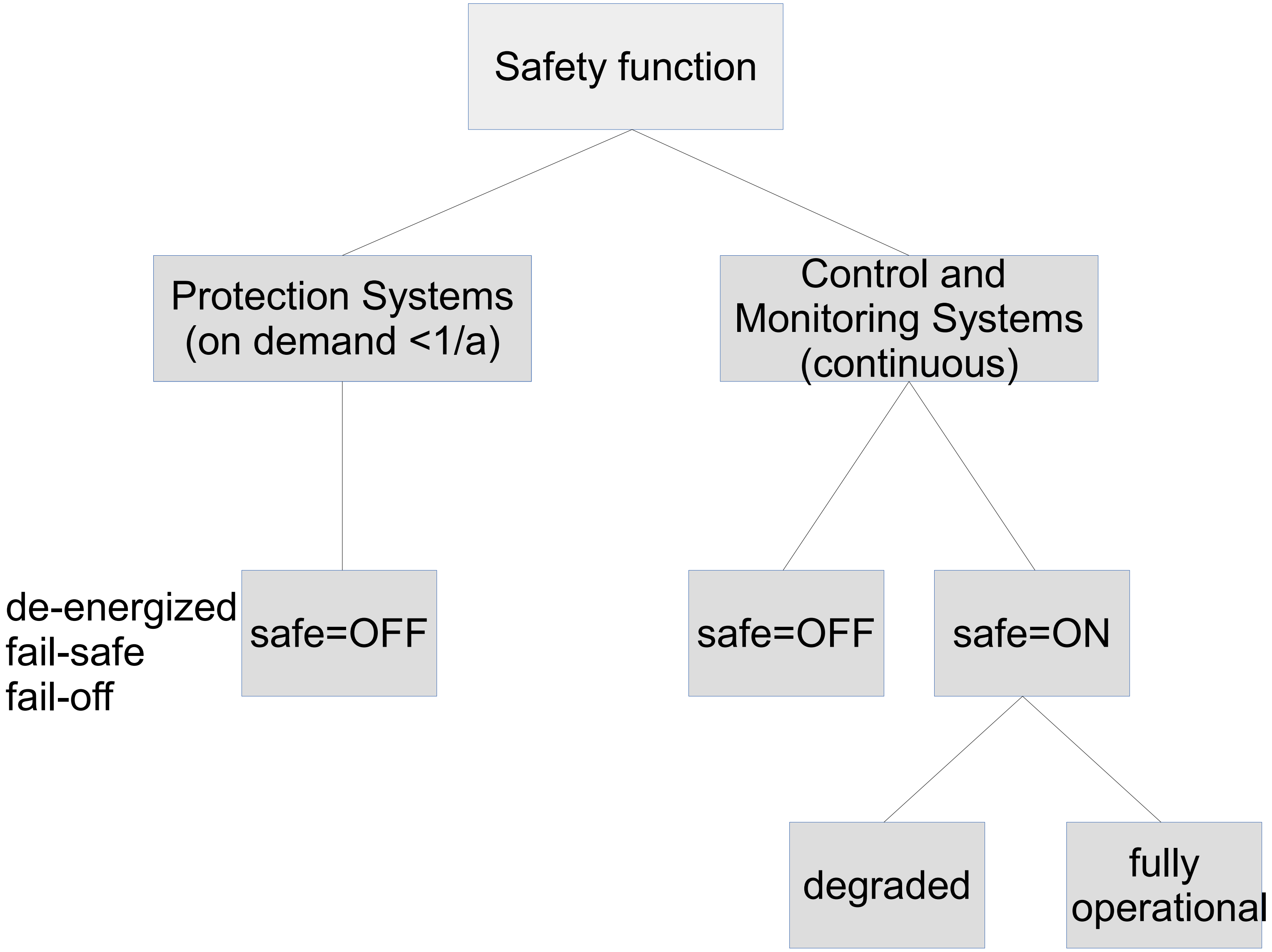
IN2244

Part VI – Safety Architectures

WS 2015/16

Technische Universität München

Fail-safe and Fail-operational Systems



Safety function

Protection Systems (on demand <1/a)

Control and Monitoring Systems (continuous)

de-energized
fail-safe
fail-off

safe=OFF

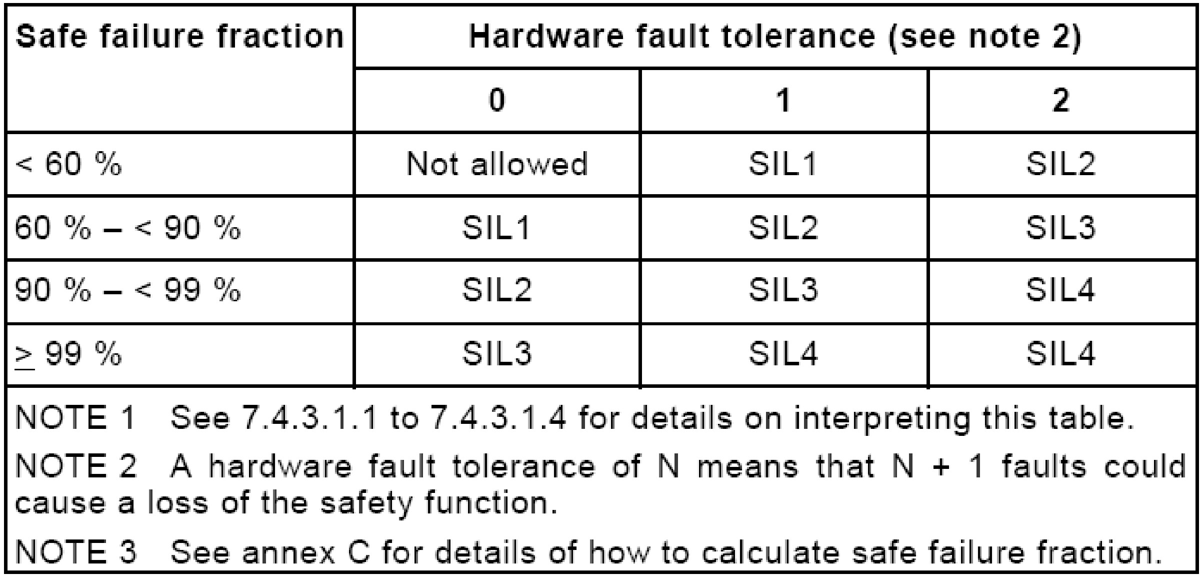
safe=OFF

safe=ON

degraded

fully operational

Architecture Constraints



Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.

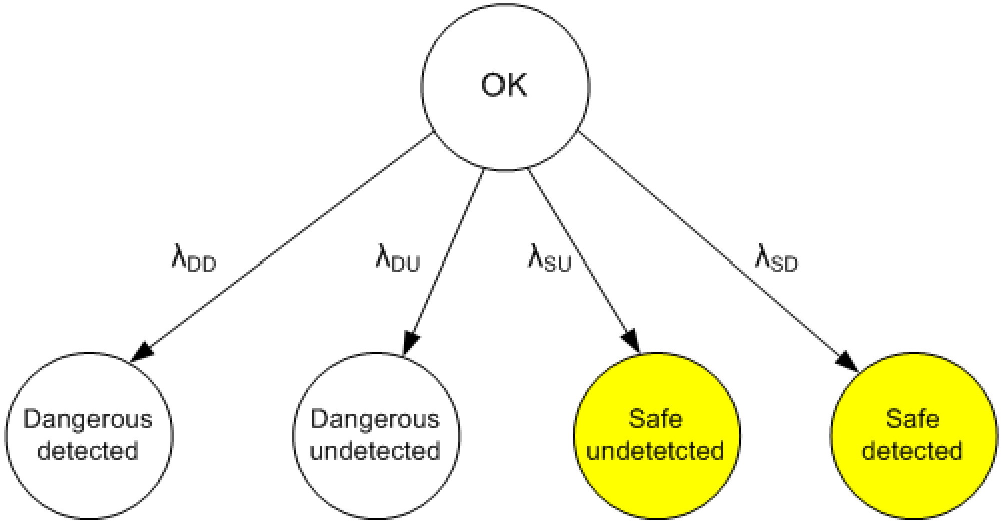
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.

NOTE 3 See annex C for details of how to calculate safe failure fraction.

Source: IEC61508

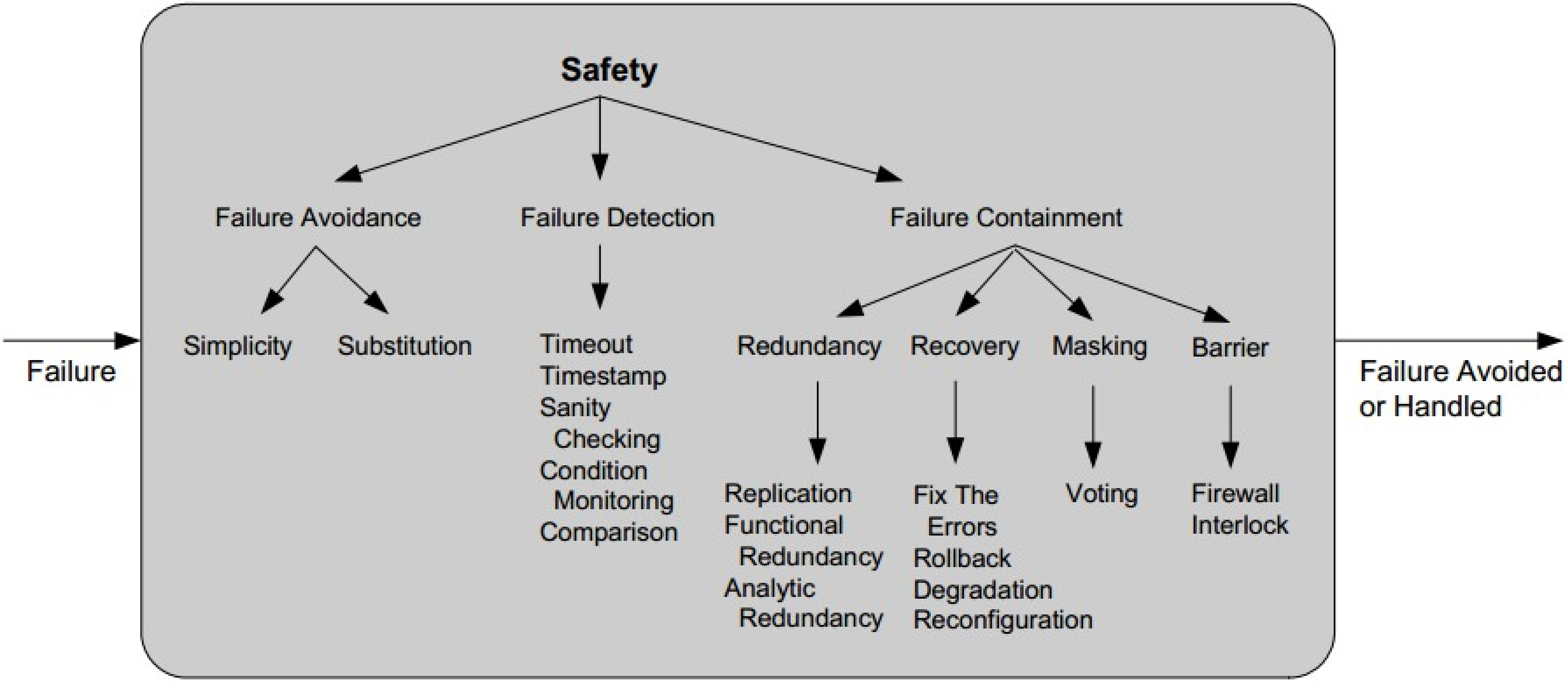
- Besides providing a specific quality (failure rate) a safety function must be hosted by a specific architecture in context of IEC 61508
- Besides architecture constraints also specific fault detection mechanisms must be realized by the final design. This is expressed by the safe failure fraction (SFF)

Safe Failure Fraction (SFF)



- Failure (this is the same failure rate as in the reliability lecture) can happen in a safe or dangerous way.
- $SFF = 1 - \frac{\lambda_{du}}{\lambda_{total}}; \lambda_{total} = \lambda_{du} + \lambda_{dd} \lambda_{su} + \lambda_{sd}$

Failure Mitigation



Failure

Safety

Failure Avoidance

Simplicity

Substitution

Failure Detection

Timeout
Timestamp
Sanity Checking
Condition Monitoring
Comparison

Failure Containment

Redundancy

Replication
Functional Redundancy
Analytic Redundancy

Recovery

Fix The Errors
Rollback
Degradation
Reconfiguration

Masking

Voting

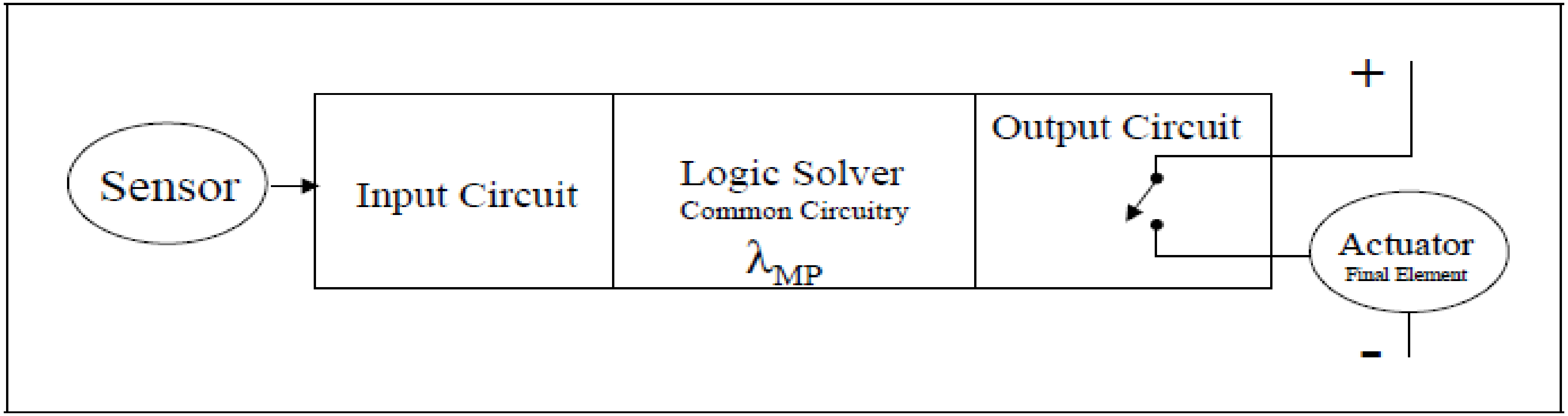
Barrier

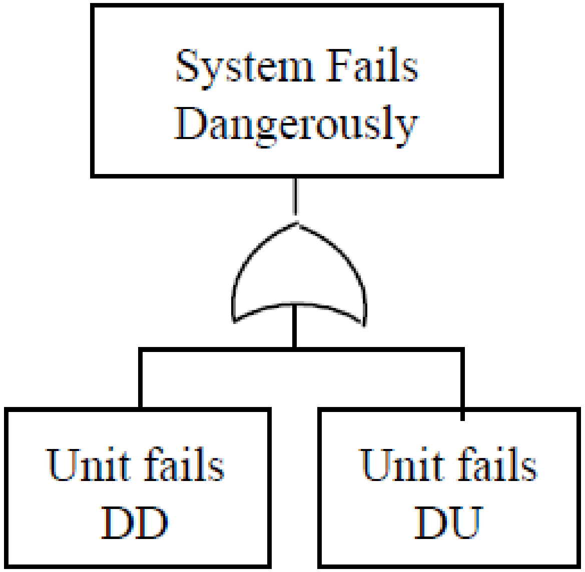
Firewall
Interlock

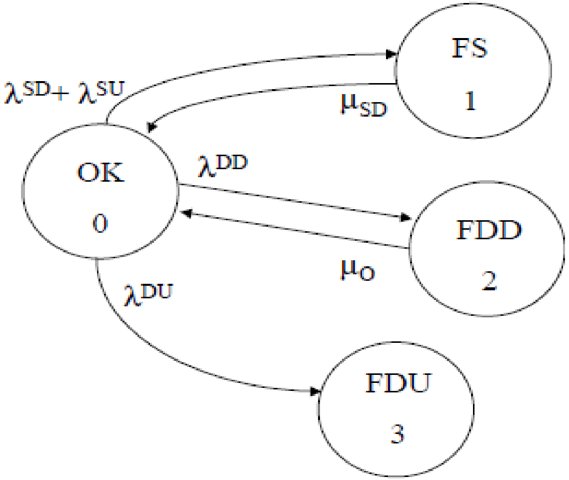
Failure Avoided or Handled

Source:
Wu, Kelly: Safety Tactics for Software Architecture Design

One Channel - 1oo1 System

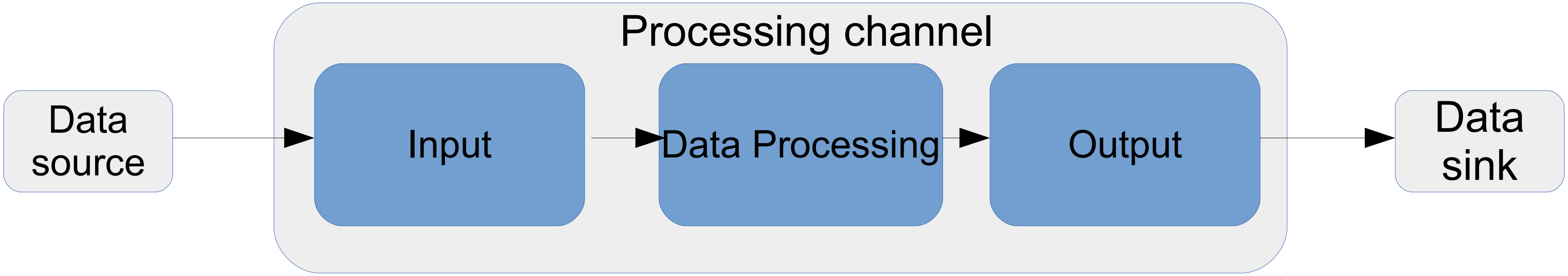






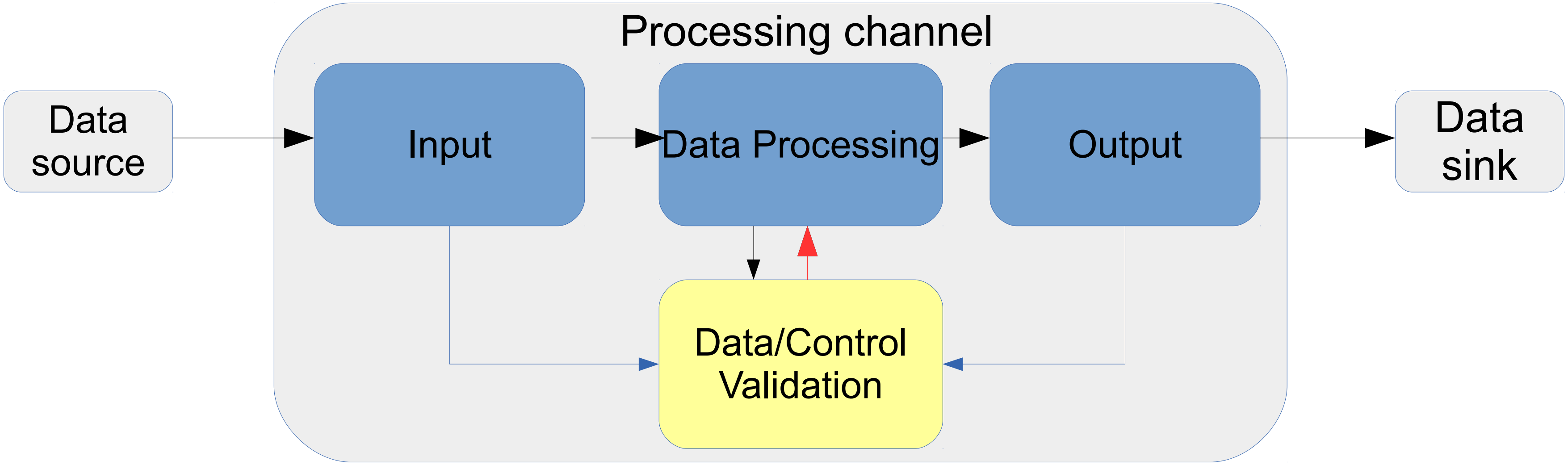
Source:
Goble, Safety instrumented systems verification: practical probabilistic calculation

1oo1
- Basic -



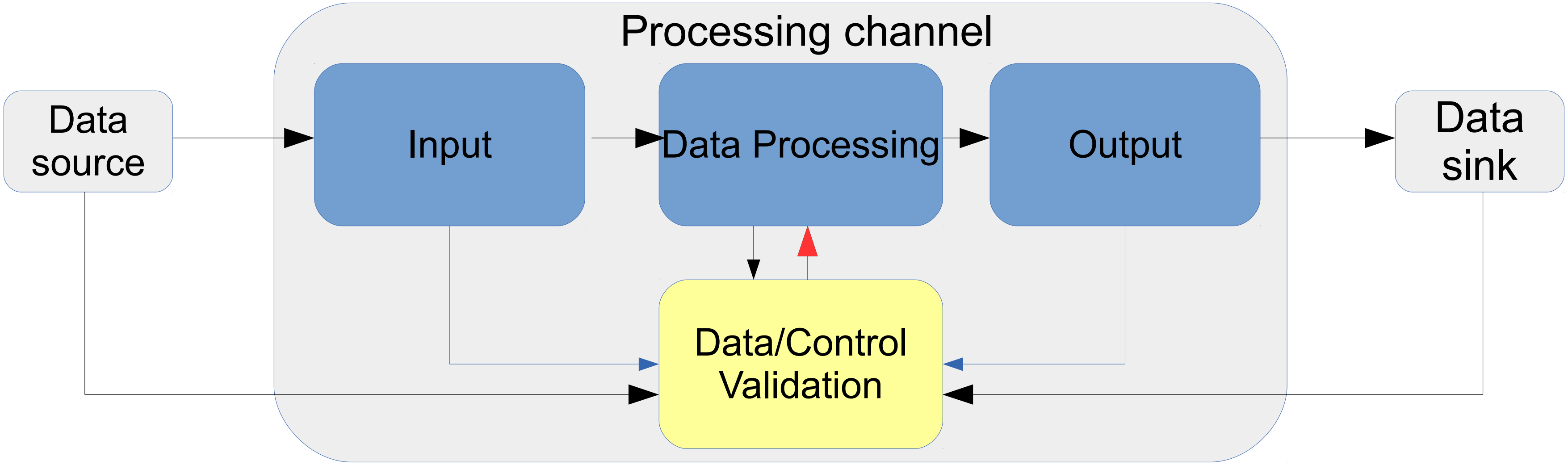
- Reliability (random faults): see previous calculations
- Reliability (systematic faults): highly affected
- Safety: 1oo1 architecture, not used

1oo1
- self-monitoring -



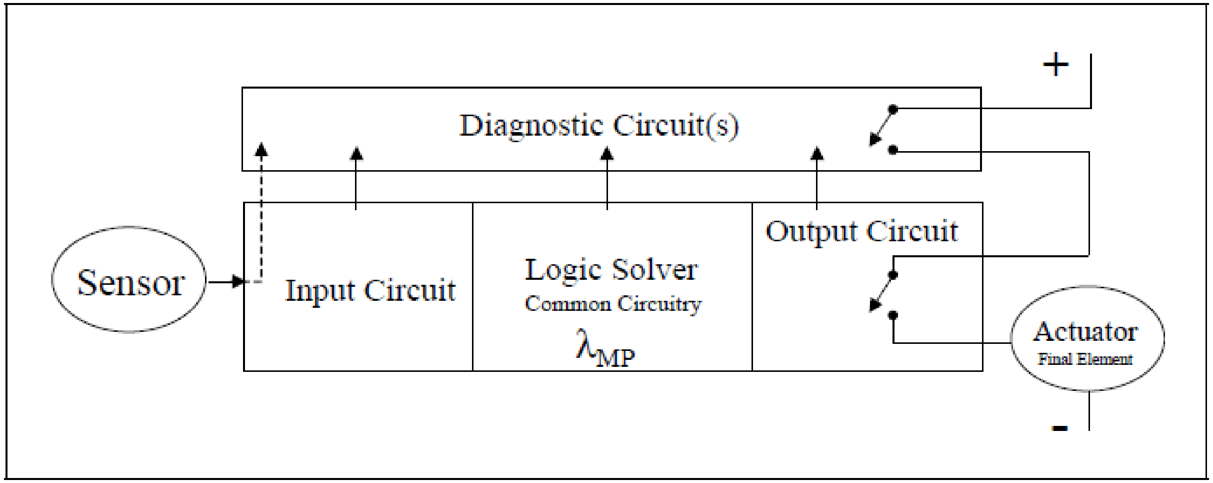
- Provides data and control flow checks (sanity checks)
  - Internal watchdog, acceptance tests by limits, etc.
- Use: not used in safety-related applications, reliability increase (depends on application)

1oo1
- condition-monitoring -

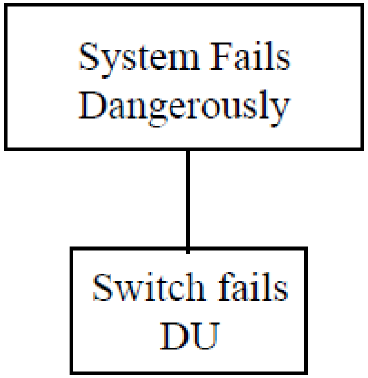


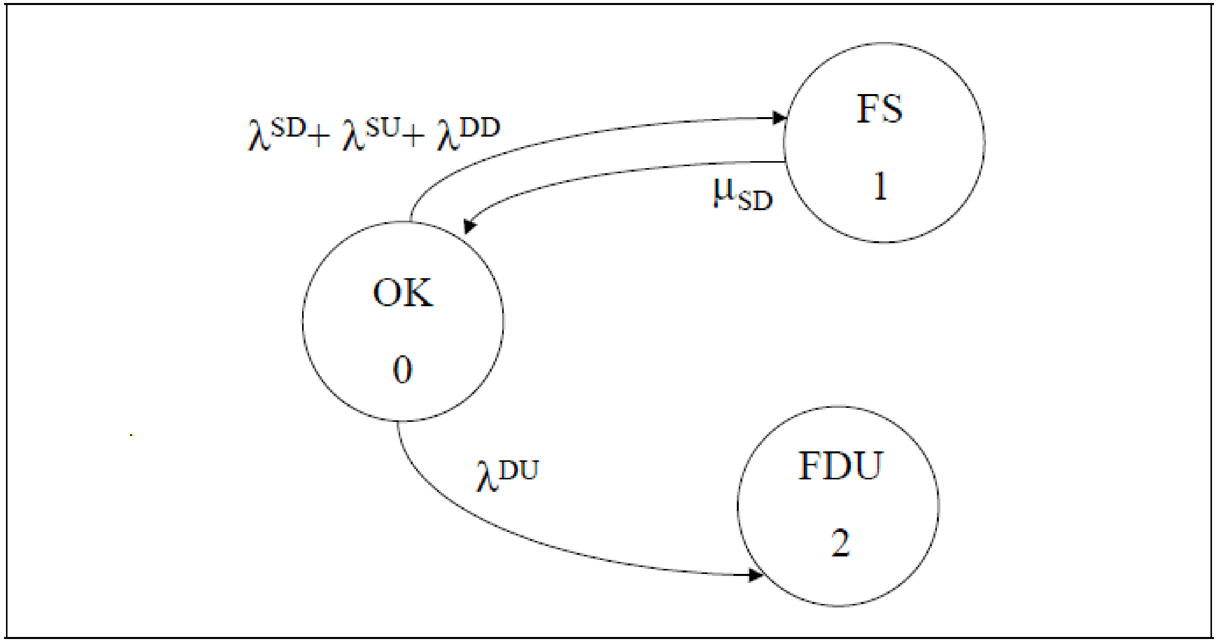
- Provides additional checks on input and/or output
- Use: not used in safety-related applications, reliability increase (depends on application)
- More expensive since additional hardware needed

One Channel - 1oo1D System

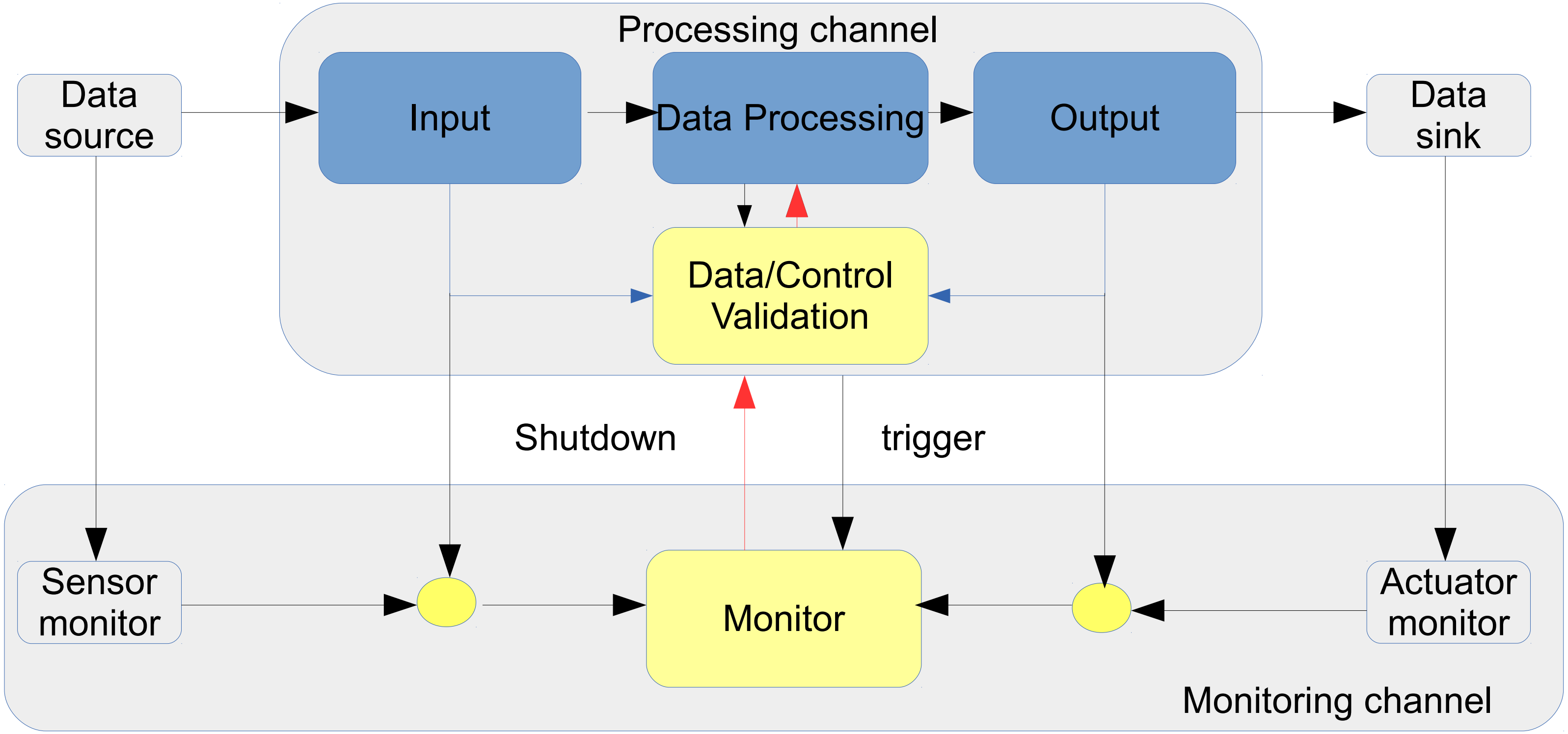


Source:
Goble, Safety instrumented systems verification: practical probabilistic calculation



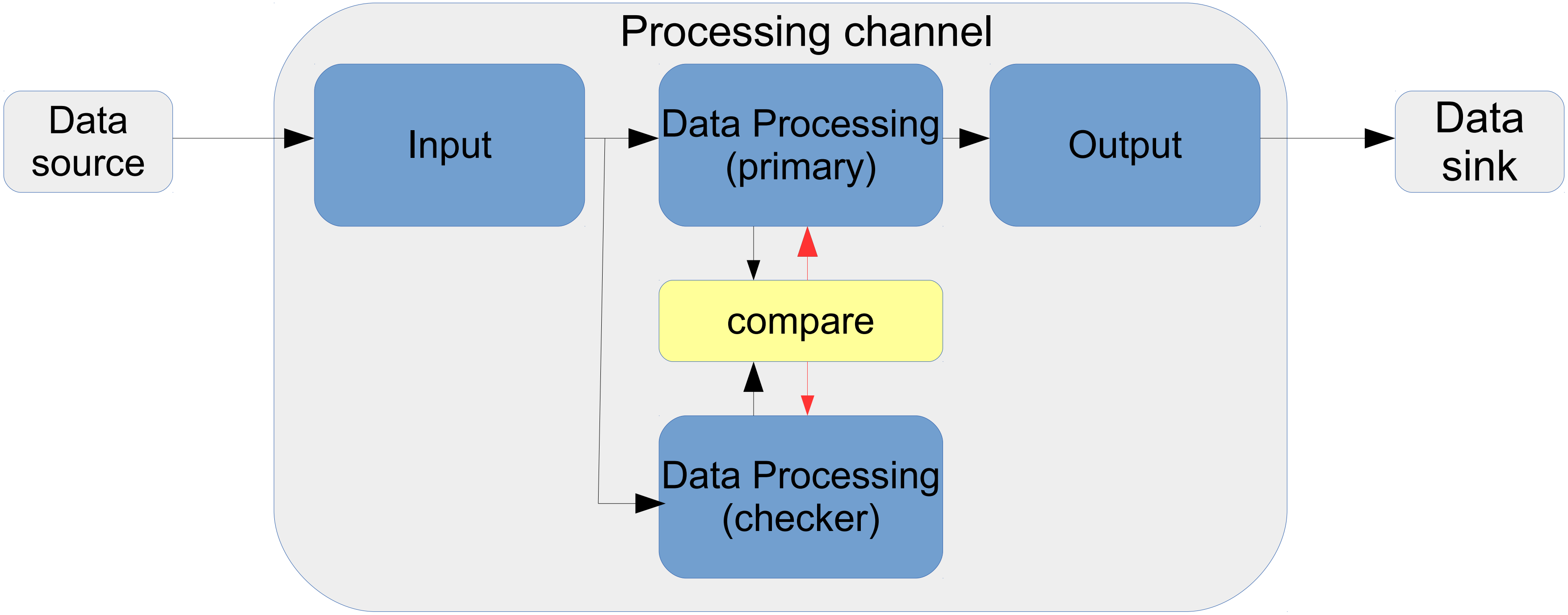


1oo1D
- external monitor -



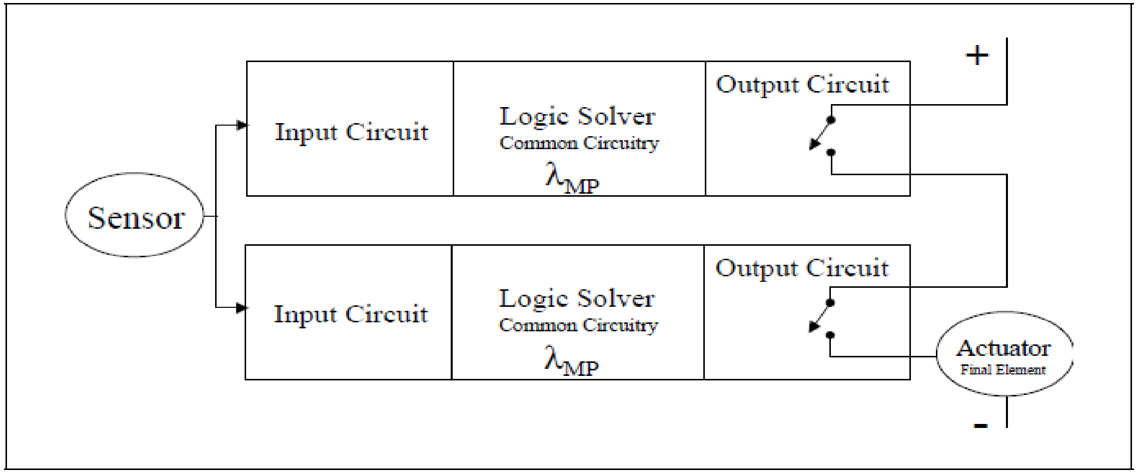
- Provides data and control flow checks (sanity checks and/or condition monitoring)
  - External watchdog, acceptance tests by limits, etc.
- Use: up to SIL2

1oo1D
- lock-step -

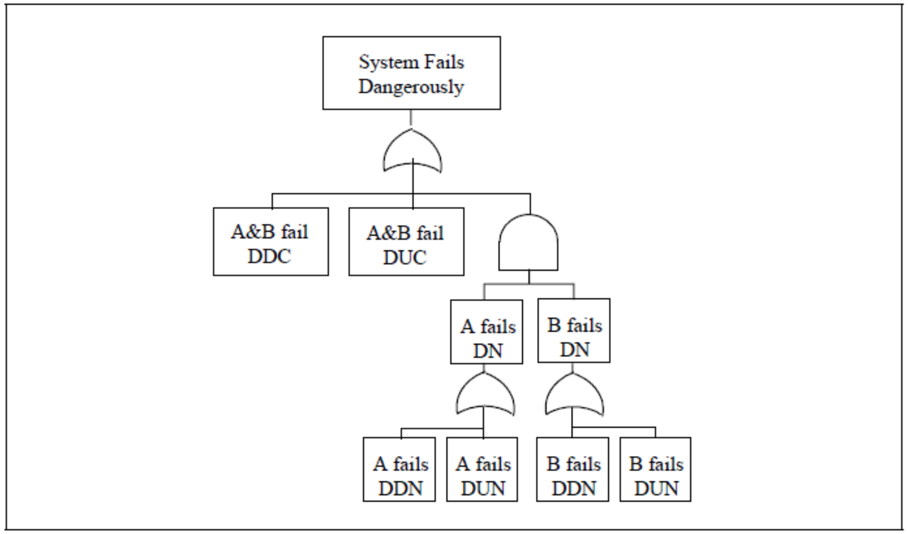


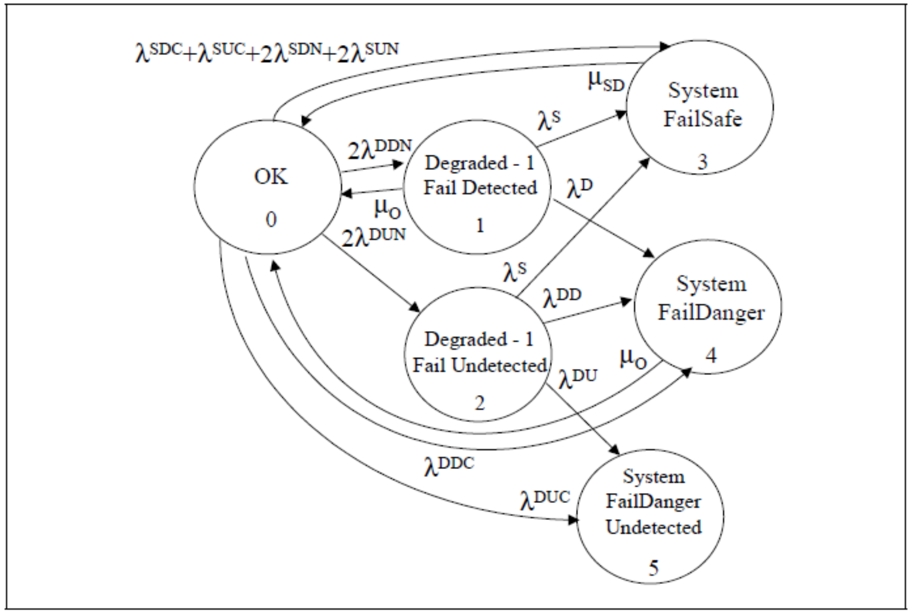
- Provides data and control flow checks in hardware (parallel execution with time shift, layout diversity)
- Use: up to SIL3

Dual Channel - 1oo2 System

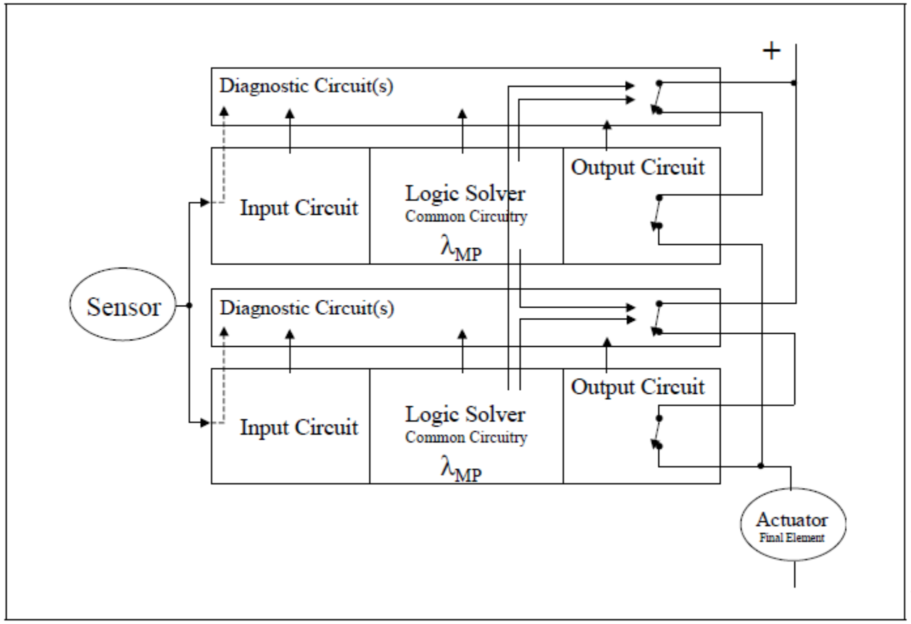


Source:
Goble, Safety instrumented systems verification: practical probabilistic calculation

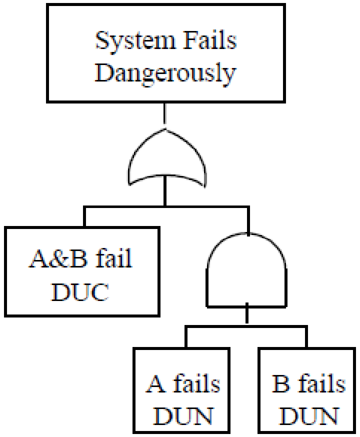


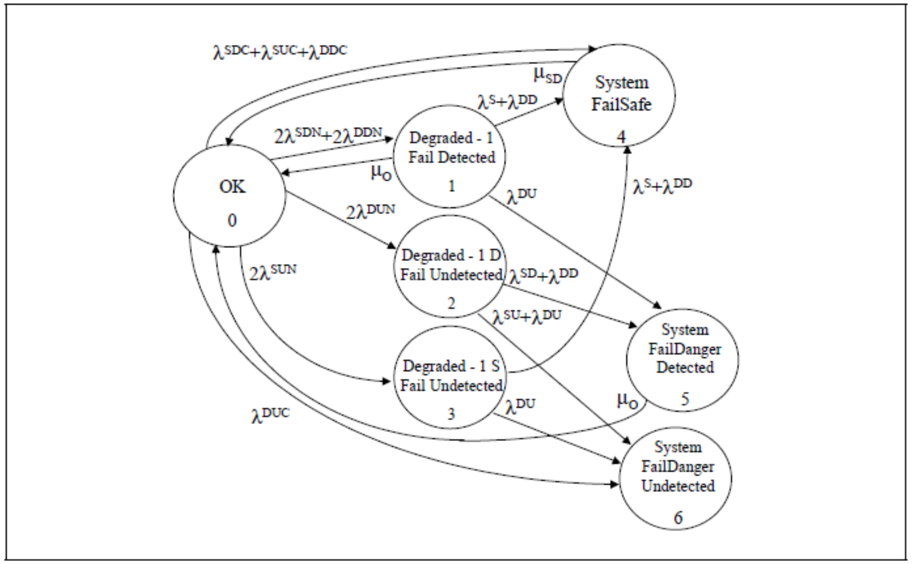


Dual Channel - 1oo2D System



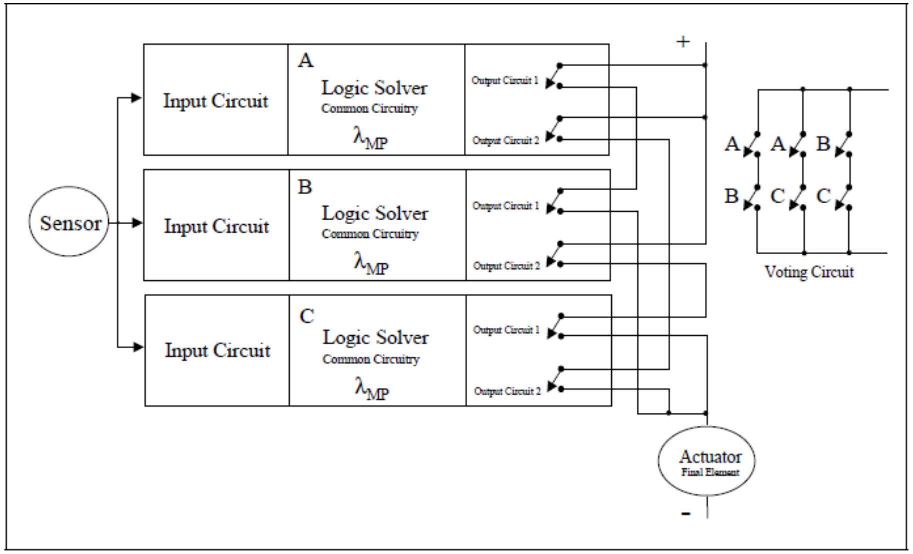
Source:
Goble, Safety instrumented systems verification: practical probabilistic calculation



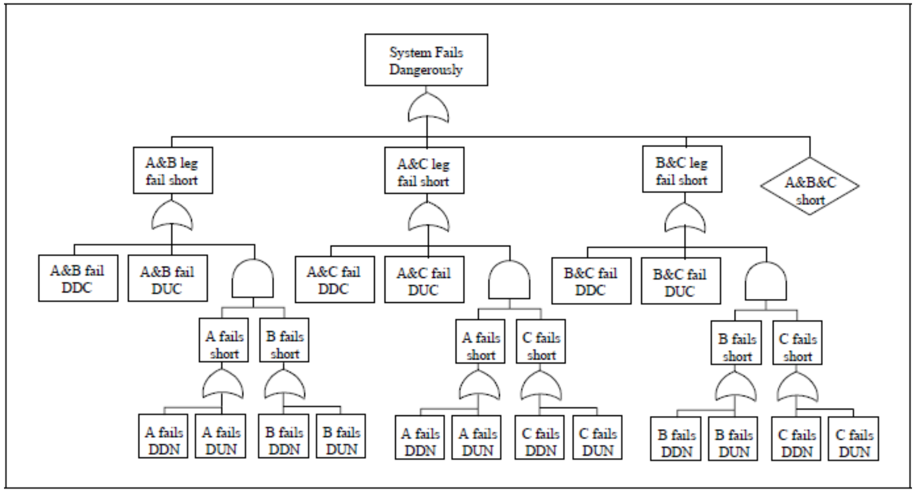


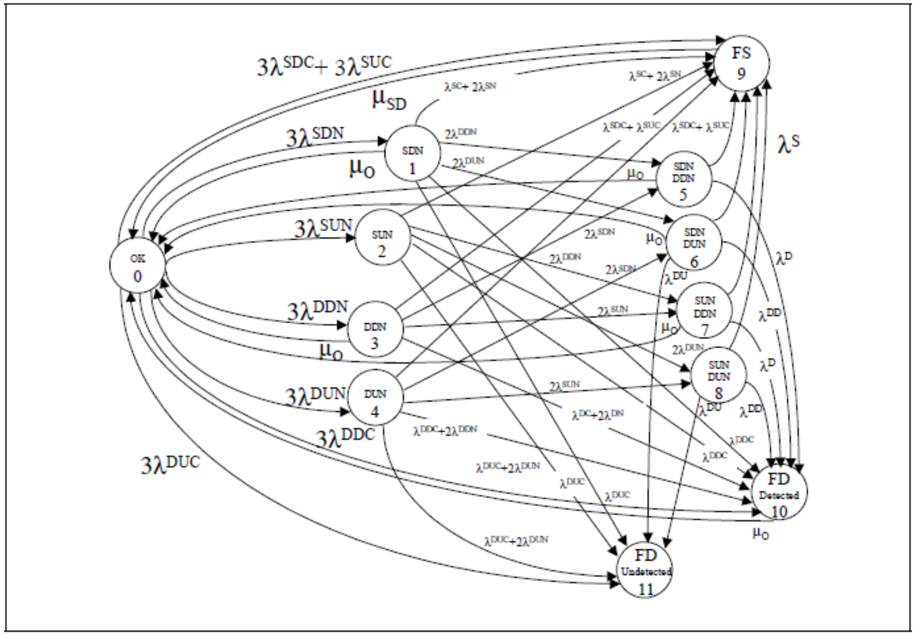
$\lambda^{SDC}+\lambda^{SUC}+\lambda^{DDC}$
μ_{SD}
System FailSafe
4
$\lambda^{S}+\lambda^{DD}$
$2\lambda^{SDN}+2\lambda^{DDN}$
Degraded - 1 Fail Detected
1
μ_{O}
OK
0
λ^{DU}
$\lambda^{S}+\lambda^{DD}$
$2\lambda^{DUN}$
Degraded - 1 D Fail Undetected
2
$\lambda^{SD}+\lambda^{DD}$
$2\lambda^{SUN}$
$\lambda^{SU}+\lambda^{DU}$
System FailDanger Detected
5
Degraded - 1 S Fail Undetected
3
λ^{DU}
μ_{O}
λ^{DUC}
System FailDanger Undetected
6

2oo3 System

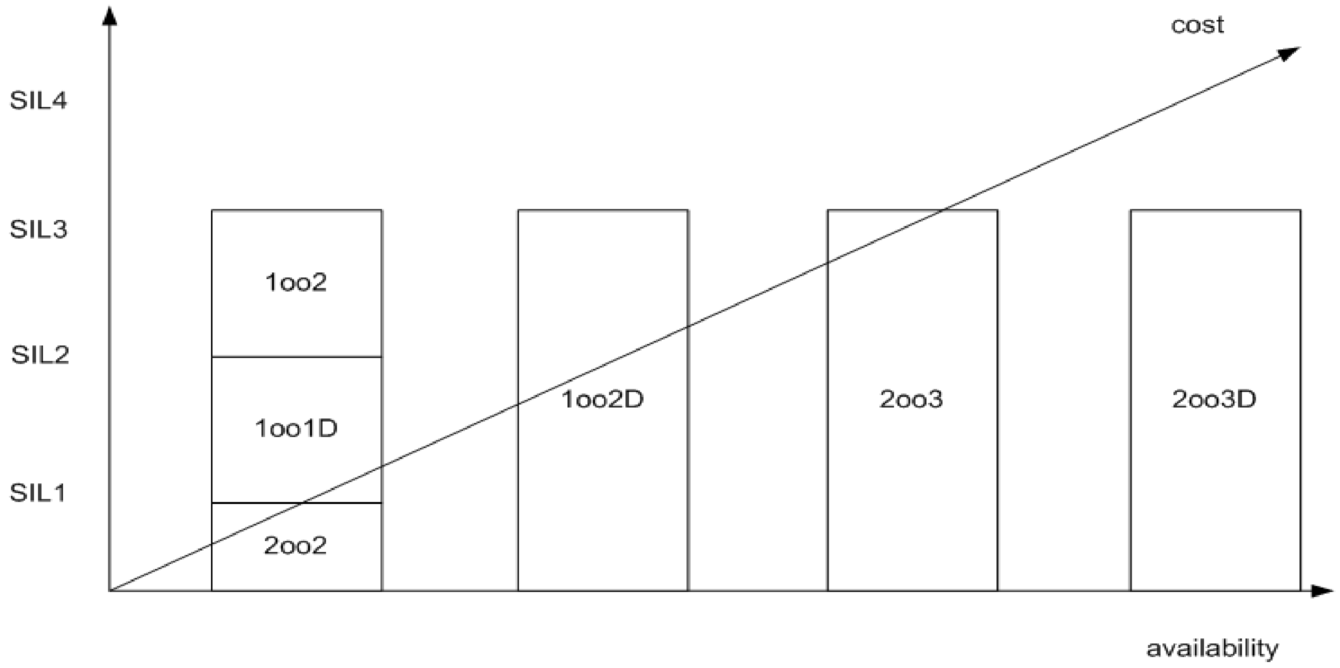


Source:
Goble, Safety instrumented systems verification: practical probabilistic calculation

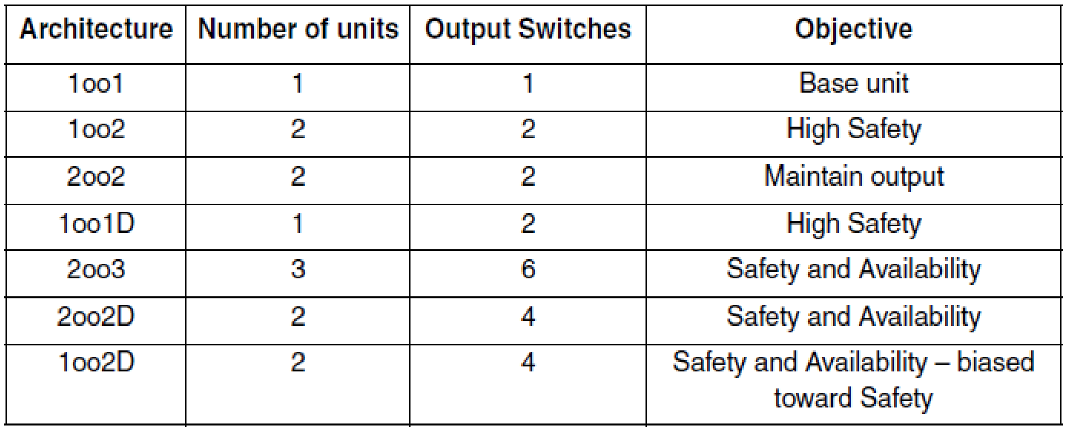




Architectures and Cost



Source:
Goble, Safety instrumented systems verification: practical probabilistic calculation



Architecture	Number of units	Output Switches	Objective
1oo1	1	1	Base unit
1oo2	2	2	High Safety
2oo2	2	2	Maintain output
1oo1D	1	2	High Safety
2oo3	3	6	Safety and Availability
2oo2D	2	4	Safety and Availability
1oo2D	2	4	Safety and Availability – biased toward Safety

Systematic Failures

- Architecture: common cause failures, dependency failures
  - Freedom from interference
  - Look at common cause failures in previous Markov diagrams
- Software: SIL for software renamed to systematic capability (SC) in IEC61508 Edition 2.0
  - SC N supports a safety function of SIL N