Basic Process Control System (BPCS) Reliability in Risk Analysis

Florin Omota, CFSE

FLUOR®

AIChE NL/B Lecture Dinner Meeting
Zoetermeer, 29-Feb-2024

About Presenter

Florin Omota

- 12 years experience in chemical industry
- 6 years research at UvA, PhD Chem. Eng.

Process Engineering Manager at Fluor B.V.

- 18 years experience in process design, control, safety & optimization
- Fluor Fellow in Process Control & Functional Safety
- Subject Matter Expert – Process Control – FLUOR
- Certified Functional Safety Expert – EXIDA

E-mail: Florin.Omota@Fluor.com

SAFER TOGETHER

CFSE

CFSE 181206 007

FLUOR®

About Fluor

One of the World's Largest Publicly-Traded EPCM Companies
Engineering Solutions to Meet the Most Complex Challenges


Ma'aden Umm Wu'al Phosphate Project - Saudi Arabia

- Technology consultation
- Design incubation
- Conceptual engineering studies
- Independent design reviews
- Front-end engineering & design (FEED)
- $\boxed{\text{Energy transition licensed technology}}$
- Advanced process modeling
- Advanced modularization
- Value engineering
- Engineering management
- Construction-driven execution

FLUOR®

Lecture Content

Why?

Accidents
Safety Layers
SIS vs. BPCS
Process Safety Time

How?

Reliability modeling
HAZOP vs. LOPA
BPCS reliability assumptions
Case studies results

- 2oo3/Moo3 voting
- 2oo2/1oo2 voting

HAZOP = Hazard and Operability
LOPA = Layers of Protection Analysis
SIS = Safety Instrumented System
BPCS = Basic Process Control System

FLUOR®

Accidents Happened (<2000)

Flixborough, UK, 1974

- major explosion and subsequent fire
- 28 fatalities
- over 100 injured

Seveso, Italy, 1976

- release of chemical cloud containing dioxin
- 600 persons evacuated
- 2000 persons treated

Bhopal, India, 1984

- release of toxic cloud
- over 2500 fatalities
- over 100.000 persons affected

FLUOR®

Accidents Still Happen (>2000)

AZF (Azote de France) fertilizer factory (Sept 2001)

- Explosion of ammonium nitrate
- 31 death
- Total loss of plant

BP Texas City Refinery (March 2005)

- Explosions and fire in isomerization unit
- 15 death
- 170 injured

BP Deepwater Horizon (April 2010)

- Explosion and well blowout with fire
- 11 death
- Total loss of platform
- Largest ever oil spill in American waters

FLUOR®

Accident Causes

Human error

- Design
- Operation
- Maintenance

Failure of

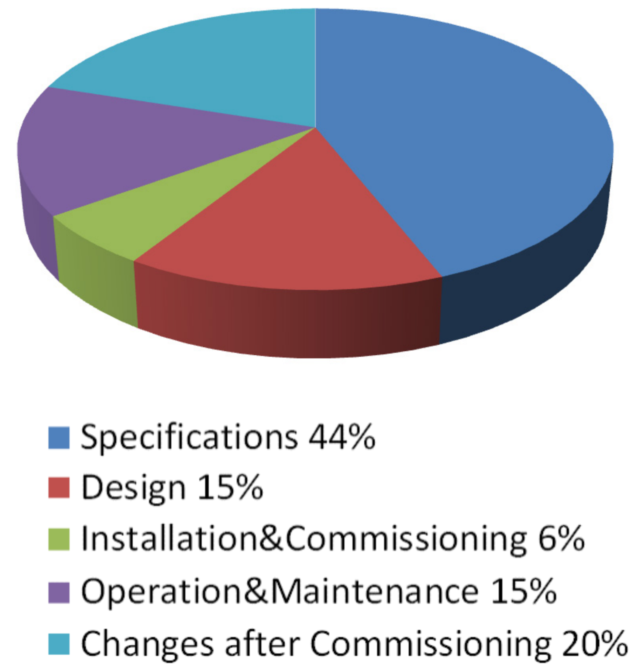
- Utility system
  - power supply, instrument air, cooling water, steam
- Mechanical equipment
  - pump, compressor, reactor mixer, heat exchanger tube rupture
- Piping and auxiliaries
  - corrosion, blockage, check valve or manual valve failure
- Instrumentation & Control system
  - sensors, control loops, alarms, system hardware or software

Combination of factors, in most of the cases

Safety System Failure Analysis

Health and Safety Executive (U.K.)

- Analysis of 34 accidents
  - resulted from control or safety system failure
- Causes grouped by phase
- Major contribution: Specifications
  - Incorrect or incomplete



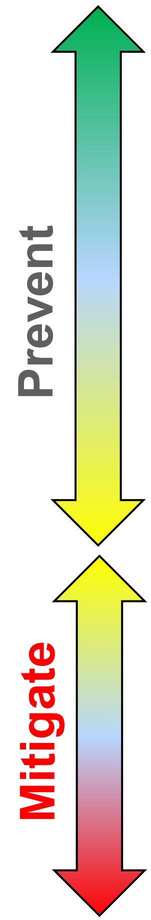
Specifications

- Functional specification (i.e., what the system should do) SIF
- Integrity specification (i.e., how well should do it) SIL

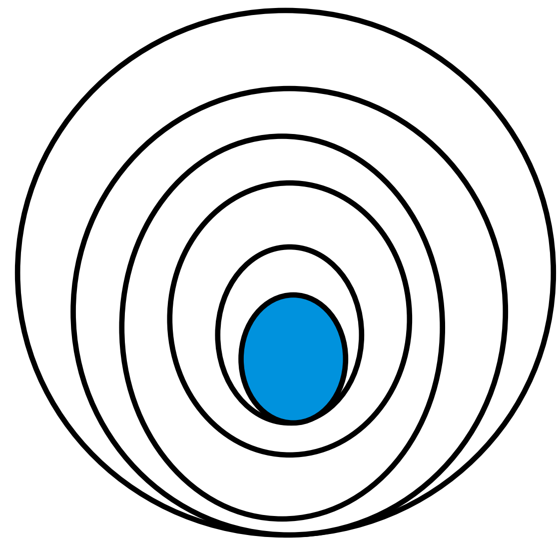
SIF = Safety Instrumented Function
SIL = Safety Integrity Level

Safety Layers

- Process Design (core)
- Process Control — BPCS
- Protective Process Control
- Alarm System
- Safety Instrumented System (SIS)
- HIPPS
- Mechanical protection
- Fire & Gas System (FGS)
- Bunds, dikes, walls
- Plant and emergency response
- Community emergency response

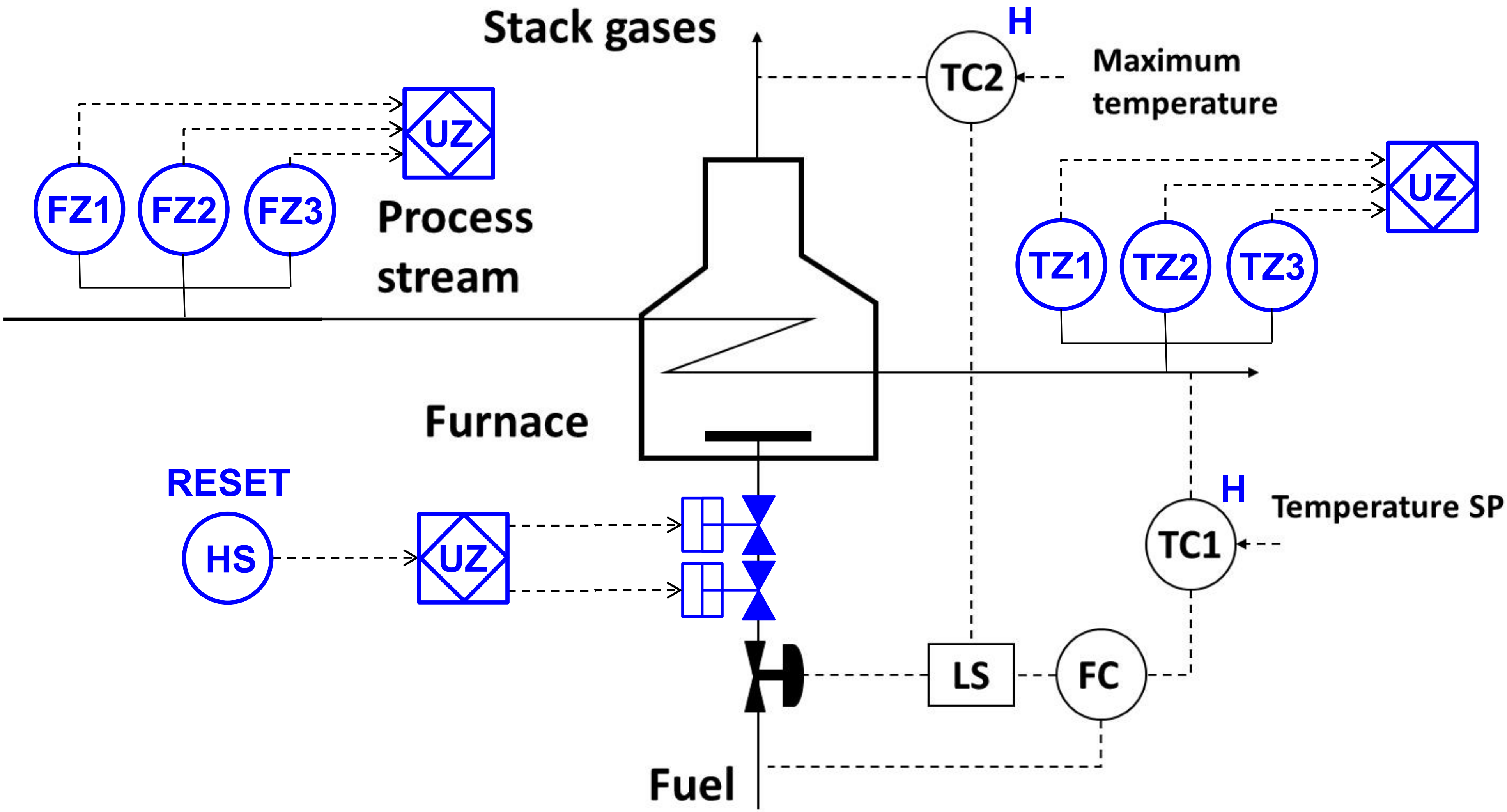


ONION model



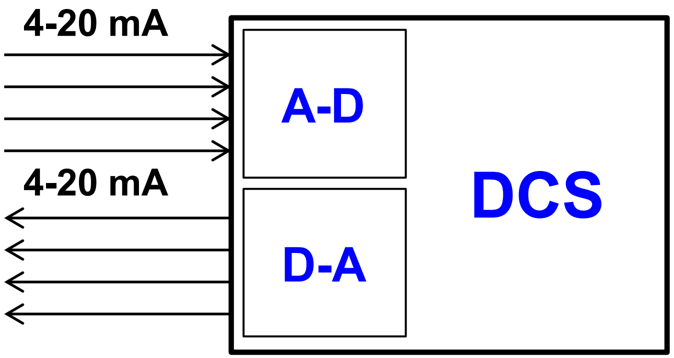
HIPPS = High Integrity Pressure Protection System

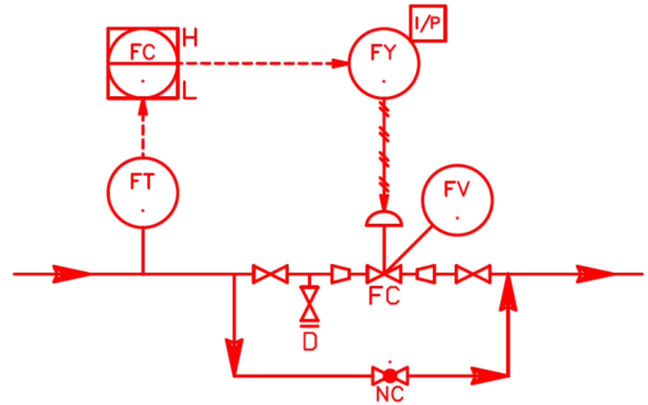
Safety Layers - Example

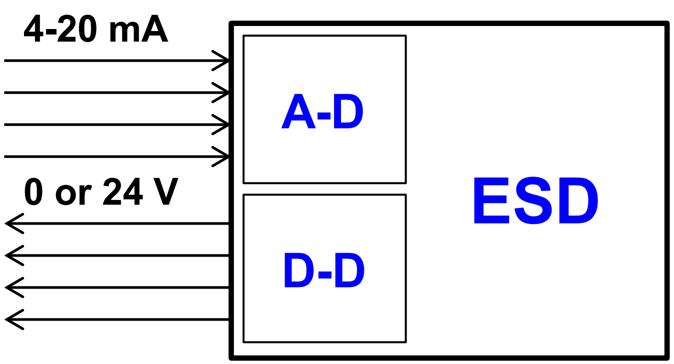


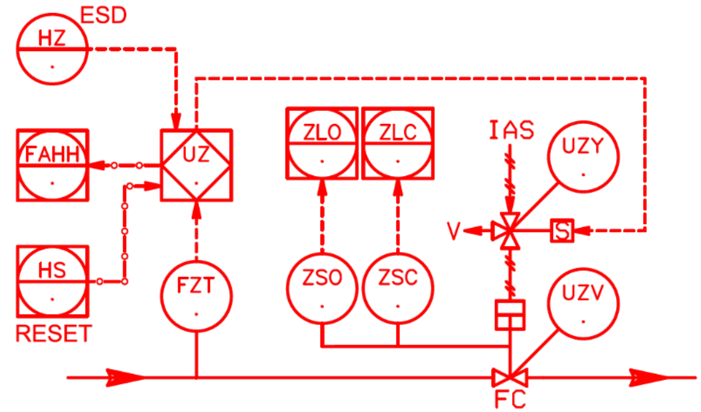
SIF = Safety Instrumented Function

BPCS vs. SIS









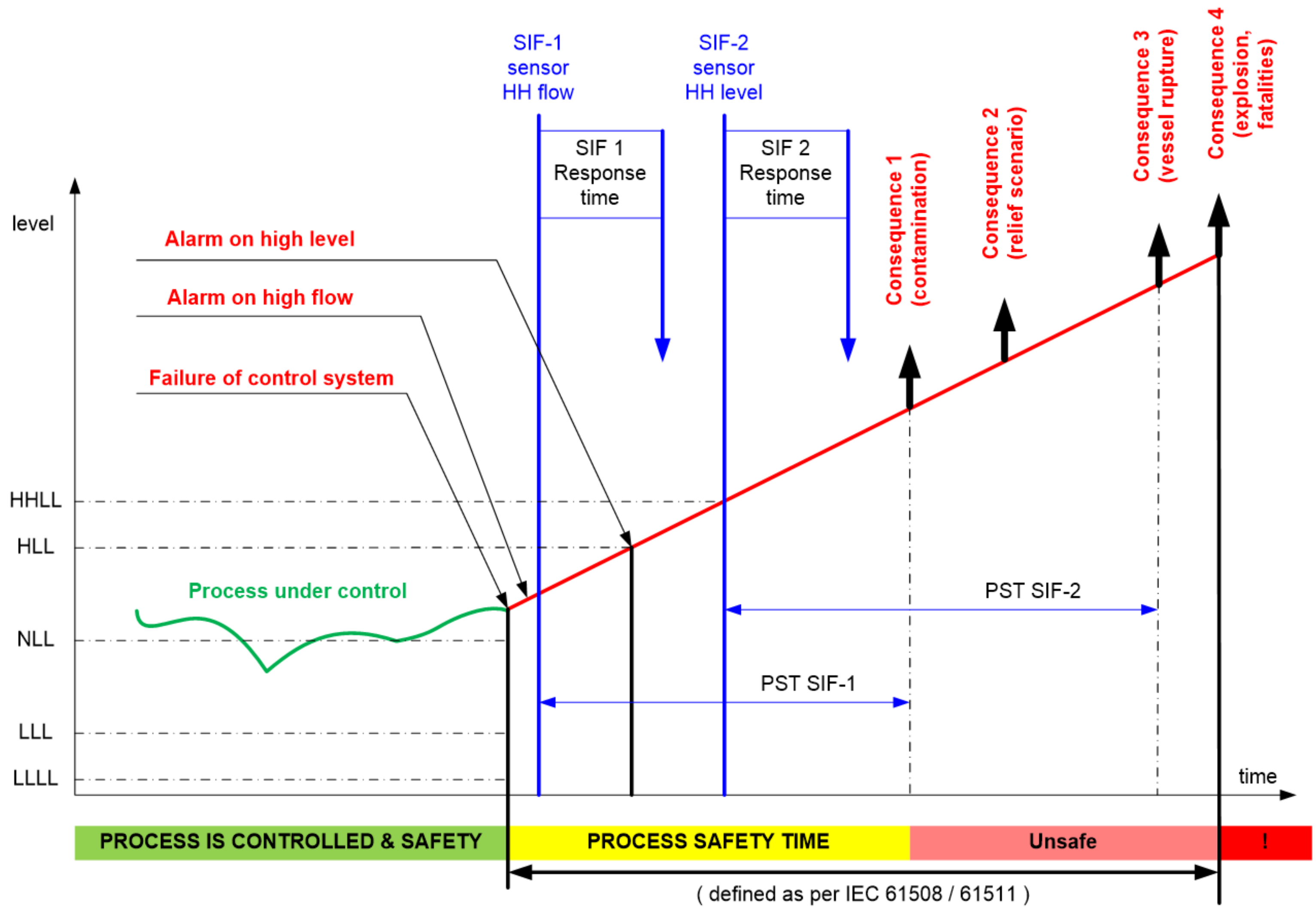
DCS = Distributed Control System / BPCS

BPCS = Basic Process Control System

ESD = Emergency Shut Down

SIS = Safety Instrumented System / ESD

Process Safety Time

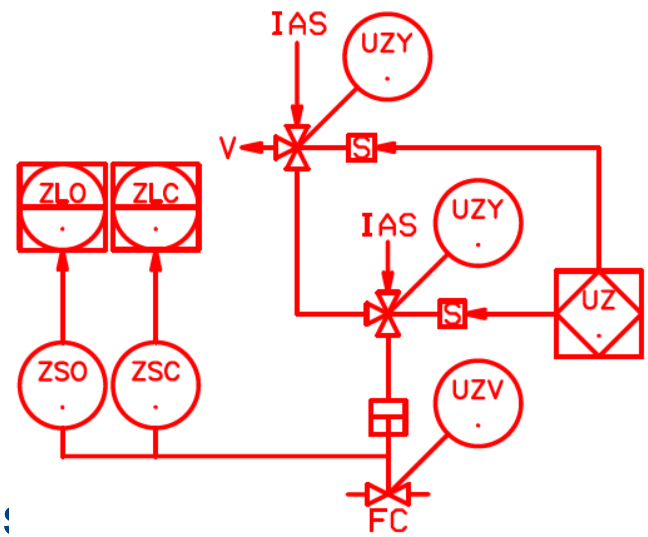


FLUOR®

PST = Process Safety Time

Redundancy

- Why multiple instruments?
  - Apparently not needed
  - Single instrument is sufficient
- Increased reliability (1oo2)
  - Two shut-off valves in series
  - One valve fails
  - The other will stop the flow
- Increased availability (2oo2)
  - Two solenoid valves
  - One solenoid fails
  - The other will supply IA
  - UZV remains open, no disturbance to proce



1oo2 = One out of two voting system
2oo2 = Two out of two voting system

Reliability Modeling

- Example 1
  - Failure rate, λ=500 FIT
  - Availability after 10 years

$$A_{(t)} = A_0 \cdot e^{-\lambda t} \qquad A_{(10y)} = 95.7\%$$

- Example 2
  - 2 devices, $\lambda_A = \lambda_B$
  - 1oo2 voting
  - 2oo2 voting

$$U_{(1oo2,t)} = U_{A(t)} \cdot U_{B(t)} \qquad A_{(1oo2,10y)} = 99.8\%$$

$$A_{(2oo2,t)} = A_{A(t)} \cdot A_{B(t)} \qquad A_{(2oo2,10y)} = 91.6\%$$

- Example 3
  - MooN voting
  - HFT can fail
  - HFT=N-M

$$P(MooN) = \sum_{k=0}^{N-M} \frac{N!}{k! * (N-k)!} A^k (1-A)^{N-k}$$

FIT = Failures in time (1 billion hours)
MooN = M out of N voting system
HFT = Hardware Fault Tolerance

FLUOR®

Availability

- Availability due to failure & repair
  - Mean Time Between Failures (MTBF)
  - Mean Time of Repair (MTR)
  - Mean Time To Restore (MTTR)
    - Repair
    - Testing
    - Installing
    - Restarting process

$$MTBF = \frac{1}{\lambda}$$

$$Availability(\%) = \frac{MTBF \cdot 100\%}{MTBF + MTTR}$$

- Spurious trips
  - Failure in safe position
  - Requires process restart
  - Mean Time To Fail Spurious (MTTFS)
- Safety system failures:

Safe	Detected
Dangerous	Undetected

FLUOR®

HAZOP Features

- Qualitative technique
- Identifies both safety and operability problems
- Assume no problems if process is operated as intended
  - Process controlled within design limits

- BPCS is frequently the cause
- BPCS can be listed as safeguard
- BPCS alarms are frequently safeguards or recommended

FLUOR®

Risk tolerability

- Risk of fatality from a car accident in US is about one in 800 years
- Most companies accept as tolerable risk 1 fatality in 10.000 years
- Risk Matrix is a measure of tolerability for a given company
  - indicates consequence severities
  - at different frequencies

- **Tolerable**: - accepted by company and employee
- **ALARP**
  - cost involved in reducing the risk further would be grossly disproportionate to the benefit
- **Inacceptable**

FLUOR®

ALARP = As Low As Reasonably Practicable

Risk matrix

LIKELIHOOD

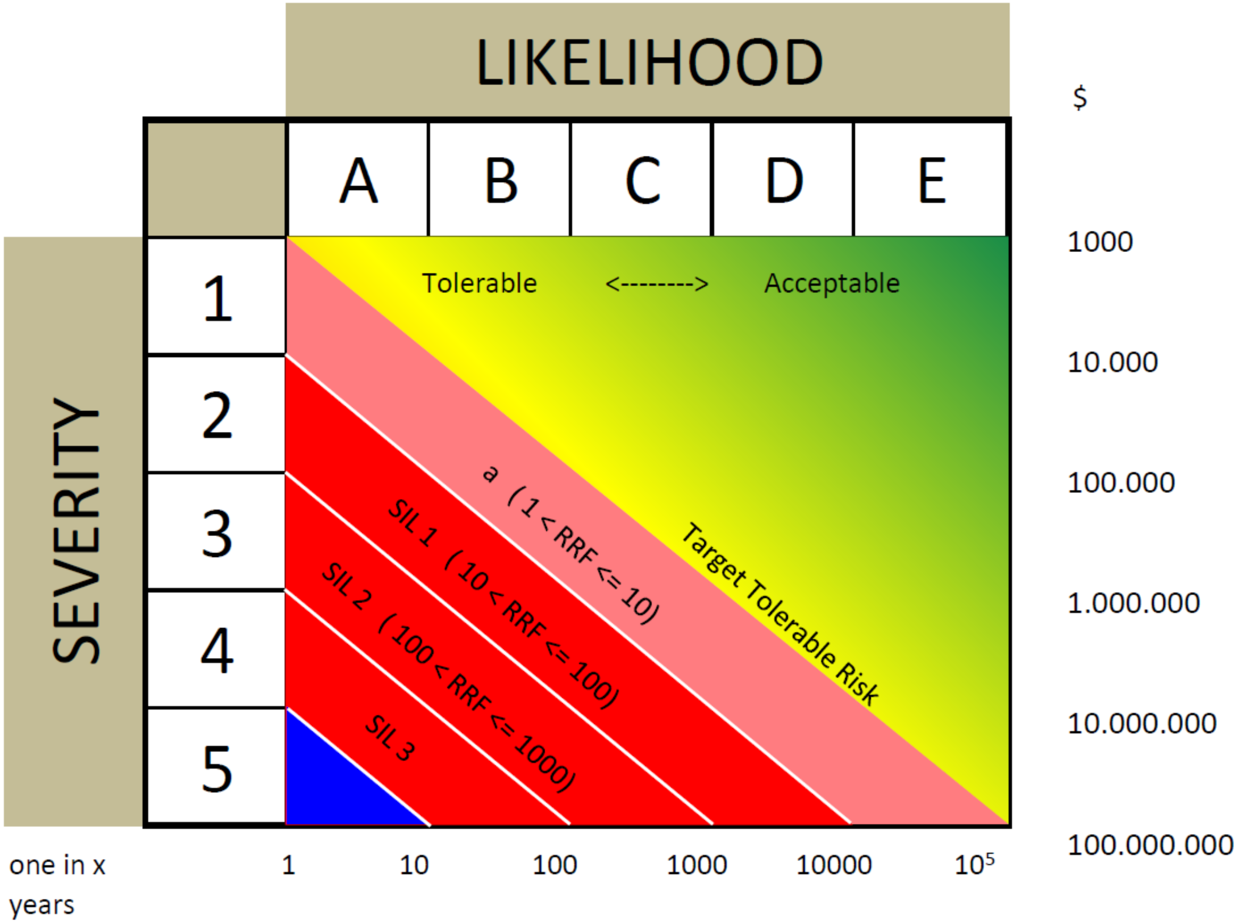
SEVERITY	A	B	C	D	E
1	10	1	1	1	1
2	100	10	1	1	1
3	1000	100	10	1	1
4	10000	1000	100	10	1
5	100000	10000	1000	100	10

one in x years: 1, 10, 100, 1000, 10000, 10^5

$: 1000, 10.000, 100.000, 1.000.000, 10.000.000, 100.000.000

Note: Likelihood A is >=1 and <10 and E is >=10000
Consequence severity 1 is <=10000$ and 5 is >10.000.000$

Quantitative risk



Note: Likelihood A is >=1 and <10 and E is >=10000
Consequence severity 1 is <=10000$ and 5 is >10.000.000$

SIL = Safety Integrity Level
RRF = Risk Reduction Factor

LOPA study

- Multi-discipline team; facilitator, scribe and specialists
- Focus on quantifying the risk identified in HAZOP
- Evaluate the gap between risk without SIS and tolerable risk
- Might recommend additional layers of protection
- Remaining residual risk to be reduced by SIS expressed as:
  - tolerable PFD_{avg} of SIF
  - Risk Reduction Factor

$$\mathbf{RRF = 1 / PFD_{avg}}$$

FLUOR®

PFD_{avg} = Probability of Failure on Demand, average
SIF = Safety Instrumented Function
RRF = Risk Reduction Factor

Independent Protection Layer

Requirements

- Specificity
  - IPL prevents or mitigates the consequences of one hazardous event
  - Multiple causes may initiate action of one IPL
- Independence
  - IPL is independent of the other protection layers associated with the identified danger
- Dependability
  - It can be counted on to do what it was designed to do
- Auditability
  - It is designed to facilitate regular validation

Notes

- An IPL shall meet all four requirements, without exception
- IPL design for that specific scenario (e.g. relief valves have more design cases)

FLUOR®

SIL Assessment

- Qualitative methods provide SIL as an integer number (e.g. SIL 1, SIL 2, SIL 3)
  - Simple, easy to apply but more conservative (e.g. if RRF=100 then **SIL 2**)
- Quantitative methods provides both SIL and RRF (e.g. **SIL 2 with RRF=300**)

LOW DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	PFD_{avg}	Required risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

CONTINUOUS MODE OR HIGH DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	Average frequency of dangerous failures (failures per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

FLUOR®

PFH = Probability of Failure per Hour
PFD_{avg} = Probability of Failure on Demand, average

Sharing BPCS/SIS instruments

It is attractive

- Reduced cost when using less instrumentation
- Better control based on redundant instrumentation
- When covered by client standards or agreed

Not recommended

- Avoid BPCS failure impact on SIS reliability
- Past accidents when a single instrument was shared by BPCS and SIS
- Common**HAZOP vs. LOPA**
- cause of failure (e.g. different instruments but same vendor)
- No reliability calculation tools

FLUOR®

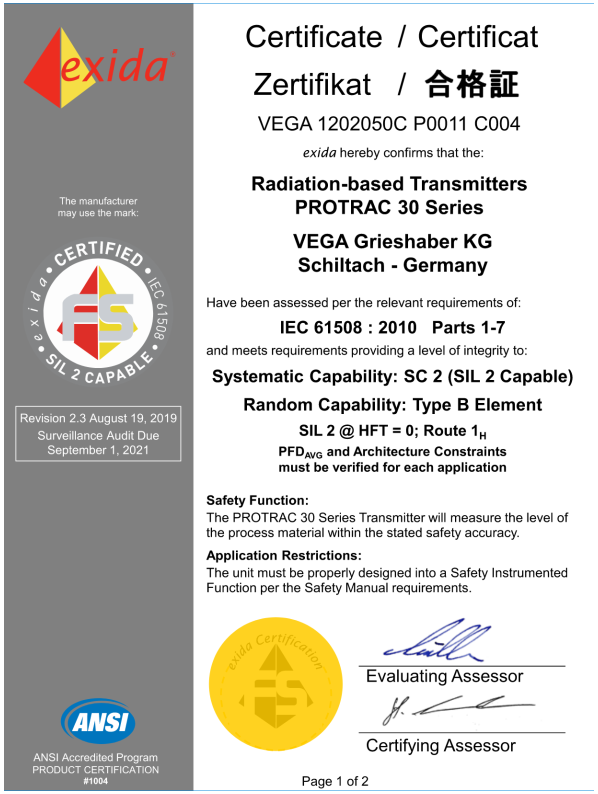
BPCS vs. SIS

SIS

- Highly reliable – typically redundant systems
- Certified for SIL 1 up to SIL 4 applications
- SIS failure rates and calculation well documented
- SIL Verification tool – exSILentia software
- Spurious trip rate calculation (MTTFS)

BPCS

- Redundancy is not a requirement
- Certification for safety reliability not required
- Failure rates and modes not available
- Availability based on MTTR and MTTF
- Assumption of an arbitrary RRF=10


exida

The manufacturer may use the mark:

CERTIFIED exida IEC 61508 SIL 2 CAPABLE

Revision 2.3 August 19, 2019
Surveillance Audit Due
September 1, 2021

ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証
VEGA 1202050C P0011 C004

exida hereby confirms that the:

Radiation-based Transmitters
PROTRAC 30 Series

VEGA Grieshaber KG
Schiltach - Germany

Have been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; Route 1_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The PROTRAC 30 Series Transmitter will measure the level of the process material within the stated safety accuracy.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

exida Certification

Evaluating Assessor

Certifying Assessor

Page 1 of 2

FLUOR®

BPCS vs. SIS – IEC 61511:2016

- Limitations of two layers of protection
  - One or two independent SIF's in the same SIS (SIL 3) can have maximum RRF=10000
  - The maximum risk reduction for a BPCS function is 10
  - Two independent BPCS functions can be claimed in LOPA as per IEC 61511

- **A.9.3.1** The BPCS may be identified as IPL
  - When a BPCS is the initiating source,
    no more than one BPCS protection layer may be claimed
  - When the initiating source is not BPCS failure,
    no more than two protection layers may be claimed

MTBF<=100y

RRF<=100

SIS vs. BPCS Reliability

- Source: exSILentia database for SIS
  - Yokogawa ProSafe-PLC 1oo2D — λ_{DU} = 2.37E-08 — MTBF = 4 822 years
  - Honeywell FSC 2004D (QMR) — λ_{DU} = 9.95E-09 — MTBF = 11 465 years
  - ABB AC800M High Integrity SIL 3 — λ_{DU} = 7.24E-10 — MTBF = 157 652 years

- Assumptions for BPCS
  - Certification for safety reliability not required
  - Failure rates and modes generally not available

  - At least equivalent to minimum SIL 2

    PFDavg = 0.01 or RRF = 100 low demand — λ_{DU} = 1.14E-06 — MTBF = 100 years

    PFH = 10E-6 (1000 FIT) continuous demand — λ_{DU} = 1.00E-06 — MTBF = 114 years

  - Maximum should be less than a SIS (SIL 2)

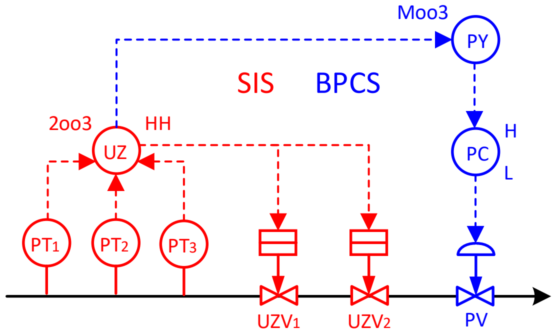
    Generic SIL 2 certified PLC (exSILentia) — λDU = 2.00E-07 — MTBF = 570 years

Assumption of PFH between 200 and 1140 FIT

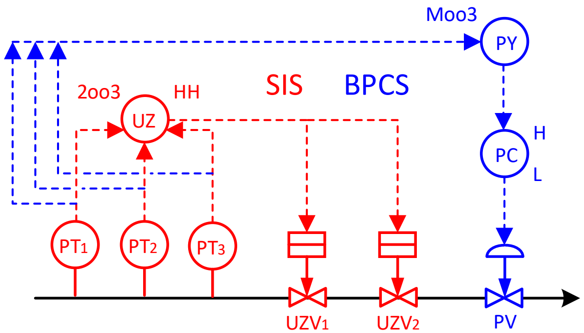
FLUOR®

Case study – 2oo3 voting

- 2oo3 preferred voting
  - High Reliability (SIL 3)
  - High Availability (MTTFS)



- Moo3 in BPCS
  - Analogue transmitters can be continuously monitored
  - Instrument failure and repair without process disruption
  - Alarm availability extremely high (1oo3 voting)
  - Control based on Moo3 is more reliable



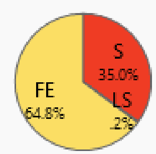
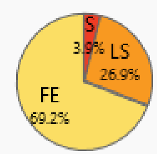
- Limitation
  - BPCS is a valid IPL with RRF=10, or
  - SIS credited as SIL 3 and RRF=10000

FLUOR®

Calculations 2oo3/Moo3

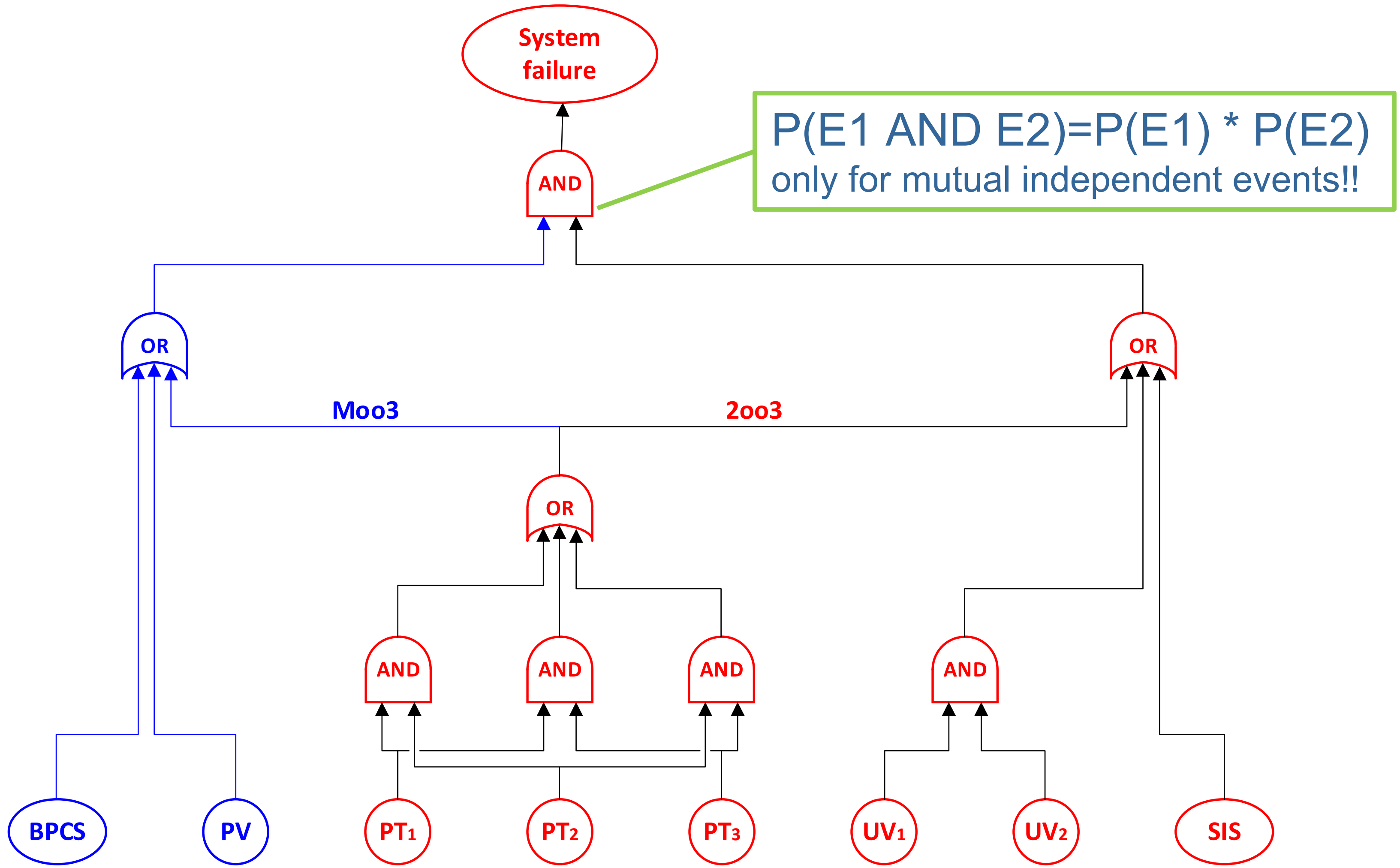
- SIS Sensors (2oo3)
  - PT, Yokogawa EJA, E Series & J Series
  - Ti=1 year, Cv=90%, Lt=15 years, β=0.1
- Logic solver
  - Yokogawa ProSafe-PLC 1oo2D
  - Ti=1 year, Cv=90%, Lt=10 years
- Final elements (1oo2) β=0.1
  - Generic quick exhaust valve:
  - Ti=1 year, Cv=98%, Lt=10 years
  - Flowserve Norbro SR actuator:
  - Ti=1 year, PST=1 month
  - Swagelok 60 Series 2 Way

- BPCS Sensors (Moo3)
  - Continuous demand mode!
  - Sensor (Moo3) failure PFH=5.83E-8
- Logic solver
  - No option in exSILentia
  - Generic PLC (SIL 2) λ_{DU} = 200 FIT
  - BPCS PFH<1/100 years ➔ λ_{DU} < 1141 FIT
- Final element (control valve)
  - Generic Globe Valve, λ_{DU} = 1000 FIT
  - Generic Pneumatic Actuator, λ_{DU} = 600 FIT
  - Generic I/P Transducer, λ_{DU} = 2400 FIT
  - Overall PFH=3.11E-6 MTBF=36.7 years

<table>
<tr><th></th><th>RRF</th><th>PFDavg</th><th>MTTFS</th><th>SIL PFDavg</th><th>SIL AC</th><th>SIL SC</th><th>Resp. Time [ms]</th><th>PFDavg Contrib.</th><th>MTTFS Contrib.</th></tr>
<tr><td>SENS</td><td>3,570</td><td>2.80E-4</td><td>2829.85</td><td rowspan="4">3</td><td>3</td><td>3</td><td rowspan="4">4000.0</td><td rowspan="4">
</td><td rowspan="4">
</td></tr>
<tr><td>LS</td><td>640,536</td><td>1.56E-6</td><td>408.84</td><td>3</td><td>3</td></tr>
<tr><td>FE</td><td>1,924</td><td>5.20E-4</td><td>158.85</td><td>3</td><td>0</td></tr>
<tr><td>SIF</td><td>1,248</td><td>8.01E-4</td><td>109.95</td><td>3</td><td>0</td></tr>
</table>

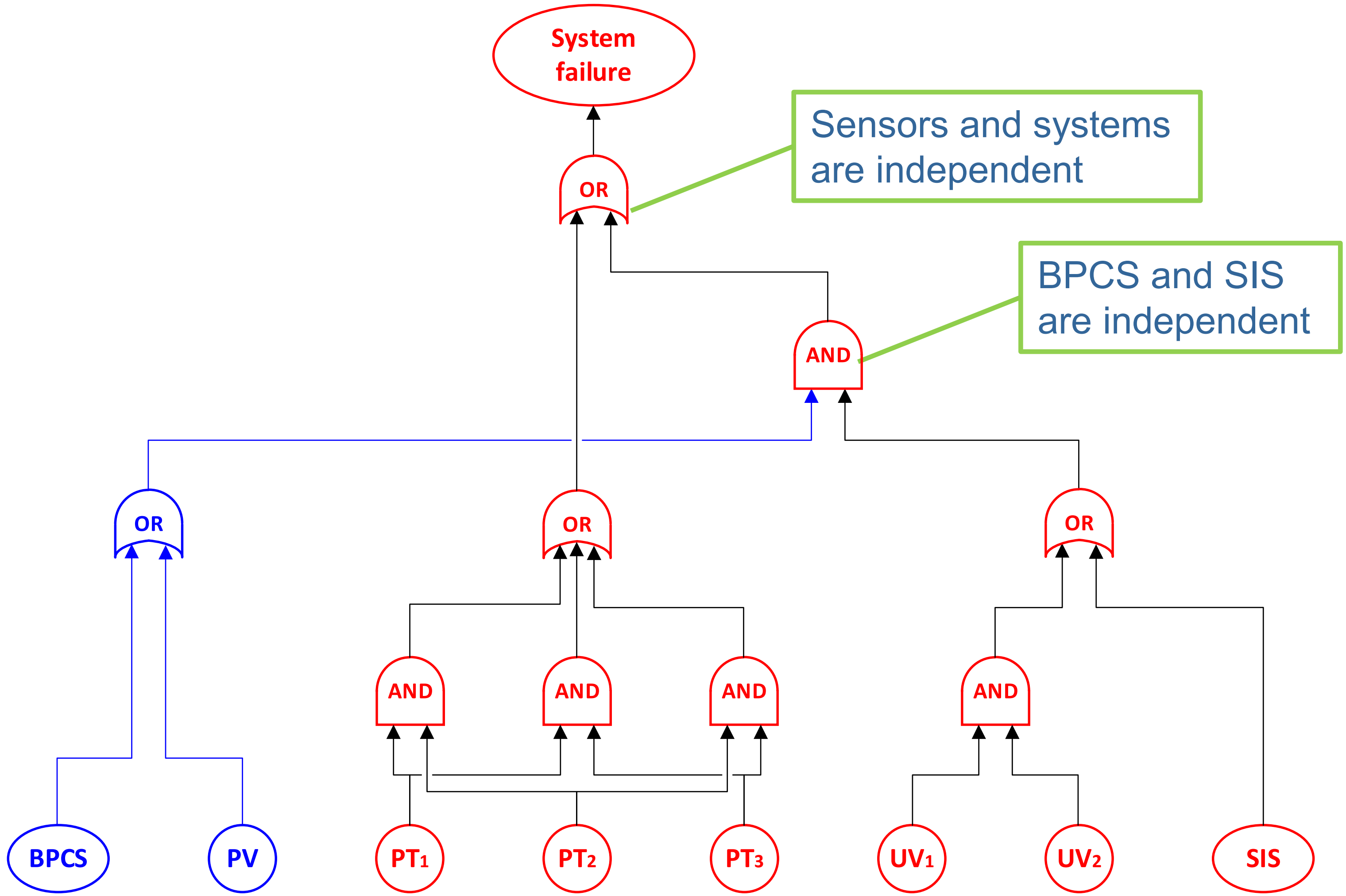
FLUOR®

Functional FTA 2oo3/Moo3



FLUOR

Calculation FTA 2oo3/Moo3



Results 2oo3/Moo3

- Cause in BPCS
  - Control valve (PV) failure
  - No credit for BPCS
  - SIF only protection

    Sensors PFDavg = 2.8E-4

    SIS PFDavg = 1.6E-6

    UZV's PFDavg = 5.2E-4
  - Overall PFD_{avg} = 8.0E-4

  SIL 3 & RRF=1248

- Conclusions
  - LOPA scenario → SIL verification
  - Cause likelihood exclusive sensors
  - Failure of SIFs shall be excluded
  - Use exSILentia / no credit for BPCS

- Cause independent on BPCS
  - FTA with increased reliability of SIS+BPCS

    Sensors PFD_{avg} = 2.8E-4

    BPCS+PV PFD_{avg} = 0.029 to 0.037

    SIS+UZV's PFD_{avg} = 5.2E-4

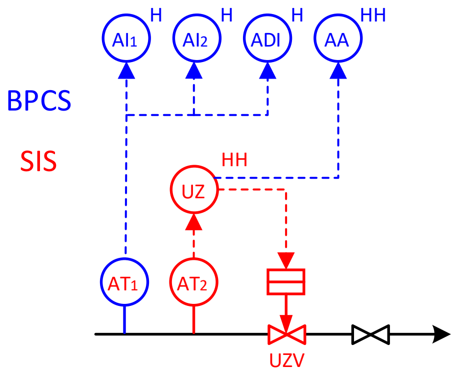
    SIS+BPCS PFD_{avg} = 1.51E-5 to 1.94E-5
  - Overall PFD_{avg} = 2.97E-4

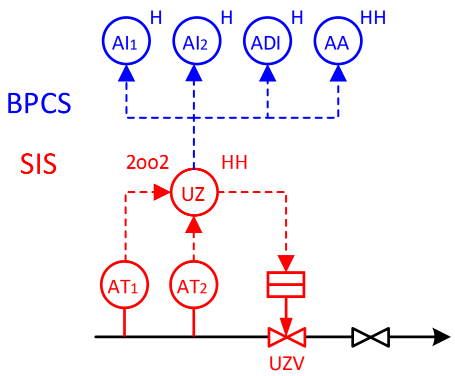
  SIL 3 & RRF=3361 (excl. operator errors)

- Conclusions
  - BPCS control valve → increased reliability
  - BPCS contribution is 3361/1248 = 2.7
  - Use a solenoid on control valve
  - Use exSILentia / no credit for BPCS
  - SIL 3 & RRF= 3255

Case study 1oo2/2oo2

- Analyzers
  - Low reliability
  - Used in low SIL applications
  - LOPA requires RRF=100
- Design intent
  - BPCS alarm as 1oo2
  - Deviation alarm
  - 2oo2 in SIS / availability
  - SIL calc. / independent
- Question
  - Is it better to be independent?
  - Or to share instruments?





FLUOR®

Calculation 1oo1(SIS) / 1oo1(BPCS)

- SIS Sensors (1oo1)
  - SERVOTOUGH Oxydetect 2222
  - Ti=2 year, Cv=91%, Lt=10 years, β=0.1
  - PFD_{avg} = 7.61E-3 RRF = 132
  - MTTFS = 148 years
- Logic solver
  - Honeywell FSC 2004D (QMR)
  - RRF = 835817
- Final elements (1oo3)
  - Two shut-off valves
  - Control valve with solenoid valve
  - PFD_{avg} = 1.98E-3 RRF = 505
- SIL 2 with RRF = 104

- BPCS sensor (1oo1)
  - Continuous demand mode!
  - Sensor failure rate 564 FIT
  - Sensor (1oo1) failure PFH=4.92E-6
  - MTBF = 23 years
- Logic solver with operator action
  - Assumption of λ_{DU} = 200 FIT
  - Operator failure estimated PFH=6.29E-6
- Overall risk reduction
  - BPCS PFH=1.14E-5 or RRF 10
  - SIS demand 1/10

  RRF: 104 x 10 = 1040

FLUOR®

Calculation 2oo2(SIS) / 1oo2(BPCS)

- SIS Sensors (2oo2)
  - SERVOTOUGH Oxydetect 2222
  - Ti=2 year, Cv=91%, Lt=10 years, β=0.1
  - PFDavg = 1.44E-2 RRF = 69
  - MTTFS = 1490 years
- Logic solver
  - Honeywell FSC 2004D (QMR)
  - RRF = 835817
- Final elements (1oo3)
  - Two shut-off valves
  - Control valve with solenoid valve
  - PFDavg = 1.98E-2 RRF = 505
- SIL 1 with RRF = 61

- BPCS sensors (1oo2)
  - Continuous demand mode!
  - Sensor failure rate 564 FIT
  - Sensor (1oo2) failure PFH=2.3E-6
  - MTBF = 49 years
- Logic solver with operator action
  - Assumption of λDU = 200 FIT PF
  - Operator failure estimated PFH=6.29E-6
- BPCS overall protection
  - BPCS PFH=1.14E-5 or RRF 13
  - SIS demand 1/13
  - With SIS overall RRF = 793

FLUOR®

Conclusions – sharing instrumentation

- Follow client specifications
  - Do not take credit for BPCS as safeguard
  - Take credit for BPCS, but limit overall RRF to 10000

- Simplify risk assessment
  - Documented in LOPA ToR and agreed with the client
  - Consider only failure of BPCS and control valve as cause
  - Consider failure of shared instruments as initiating event / no protection

- Benefits
  - Better availability for process control
  - Less demand for safety system
  - BPCS improving the safety of the plant can be demonstrated

Q&A