What About? …Using Bypasses, DBB, and Other Process Features in SIFs

Mike Schmidt, Principal SIS Consultant

Tim Forbis, Process Safety Engineer

Where ideas become solutions.

Emerson Global Users Exchange '08

Presenters

- Mike Schmidt
- Tim Forbis

Introduction

- The safe state
- Complications
- Typical BPCS solution
- Recommended SIS solution
- SIL verification calculations
- Other considerations

Cases to Consider

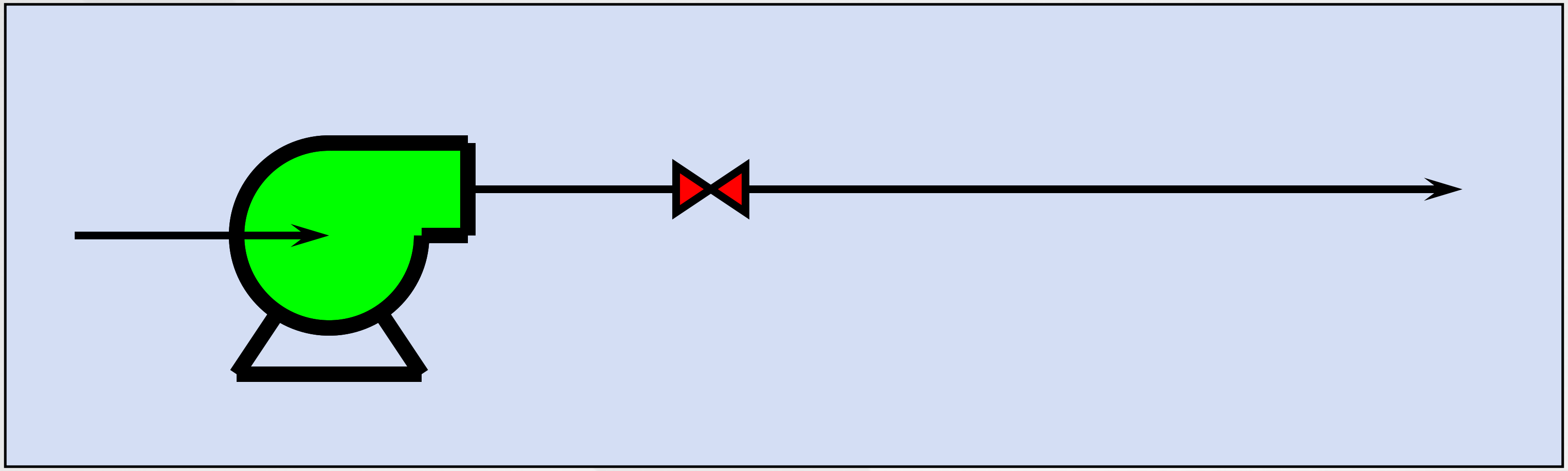
- Pump and discharge valve
- Multiple inlets
- Double block and bleed
- Unit bypass and isolate

Example SIL Calculations

At the end of each case

- Final control element (FCE) architecture
  - PFD_{AVG} calcs
  - $MTTF_S$ calcs
- Example results assume
  - $\lambda t = 0.02$ for valves
  - $MTTF_S$ = 18 years for valves
  - $\lambda t = 0.002$ for pump stop
  - $MTTF_S$ = 300 years for pump stop

Pump and Discharge Valve



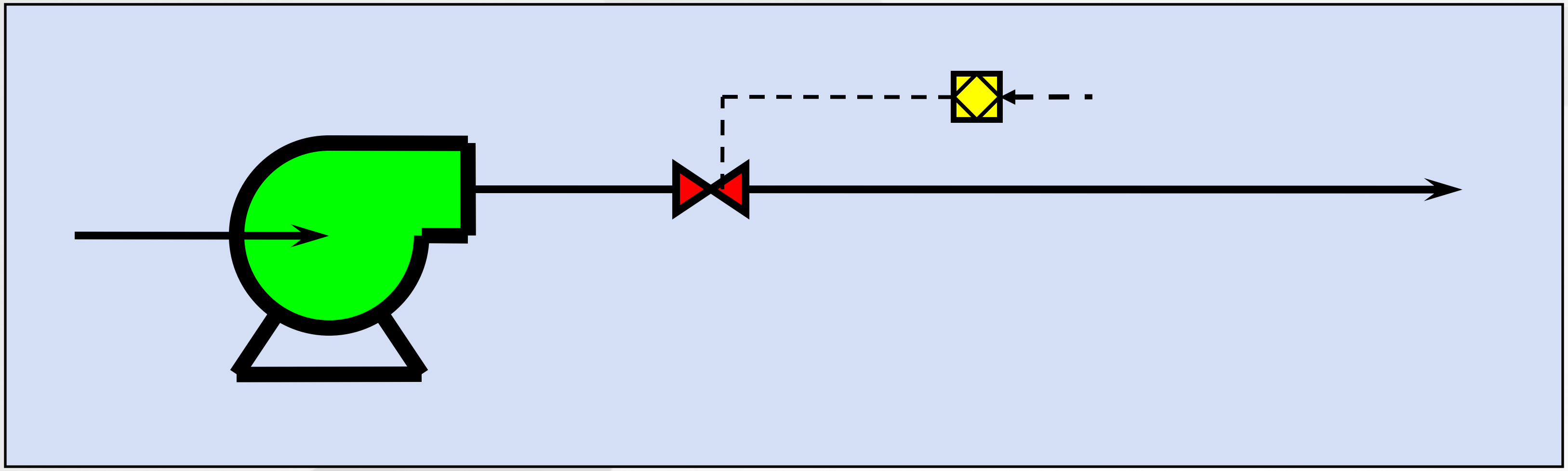
- Safe state: Flow stopped by closing pump discharge valve
- Complications: Pump deadheads against valve, resulting in pump damage
- Typical BPCS Solution: Stop pump if discharge valve is not open

Pump and Discharge Valve Recommendation

Recommended SIS solution: **Do not include pump in SIF**

Why not?

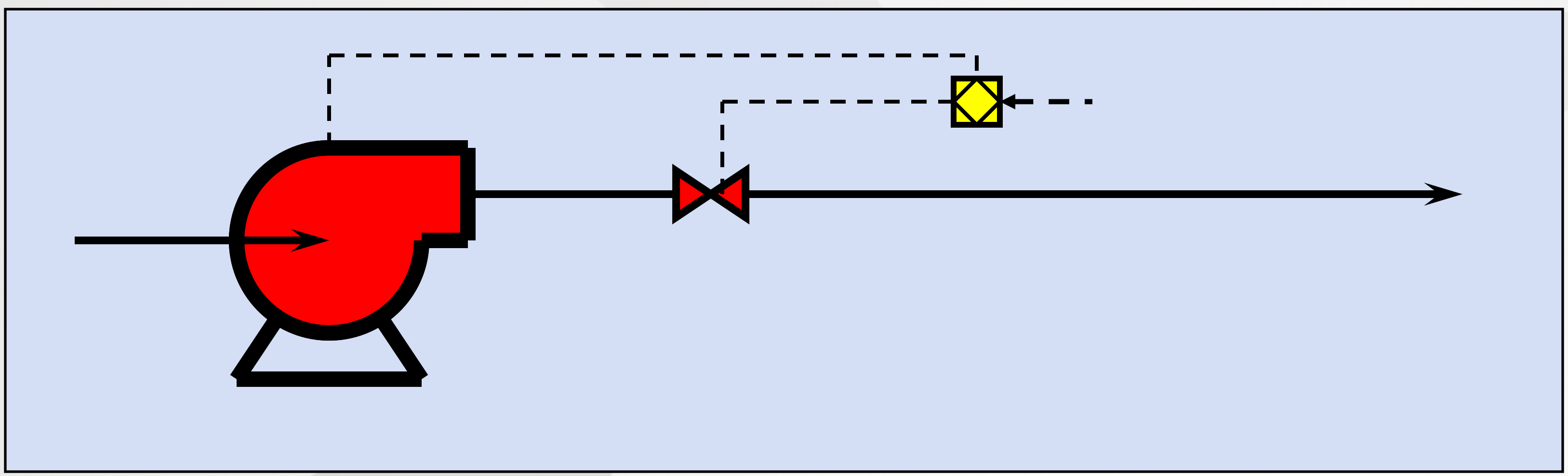
- Pump damage is not hazard protected against
- Pump damage does not warrant SIL-rated protection
- Less complexity means better spurious trip rate
- Pump stop may not contribute to SIF purpose—stopping flow
- Fewer components decreases cost—initial investment *and* operating cost



Pump and Discharge Valve Counter-recommendation

Reasons to include the pump in SIS

- Deadheading pump is its own hazard
  - Pump damage causes personnel injury
  - Overheating leads to fire.
- Redundancy
  - If pump stop does stop flow, including pump improves reliability



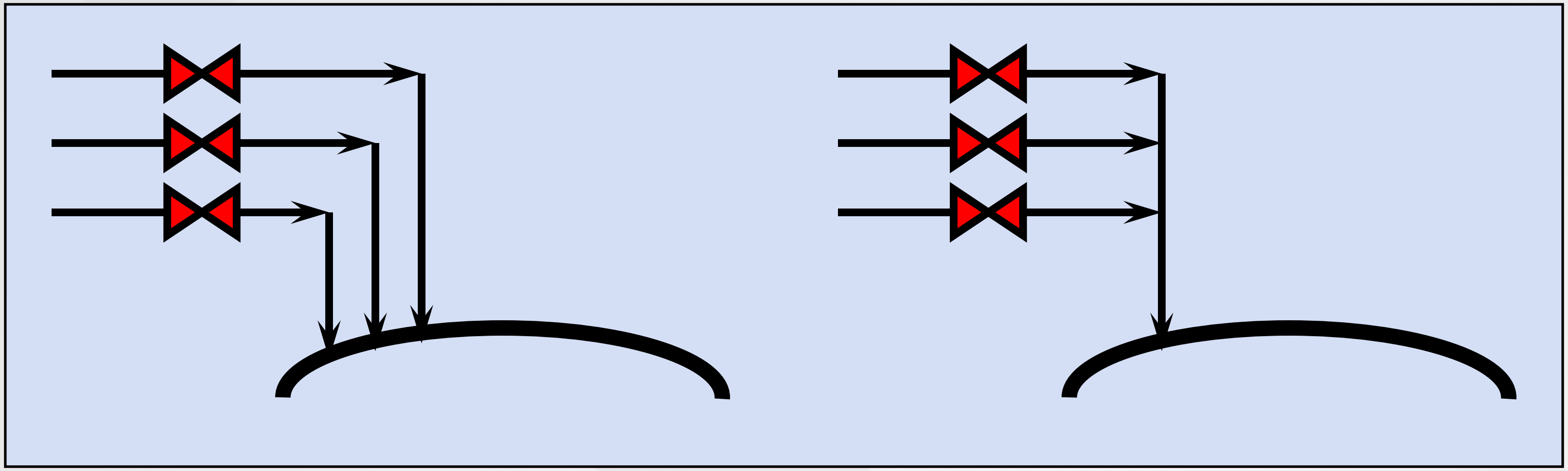
Pump and Discharge Valve SIL Calculations and Examples

- Recommended practice – SIF includes valve only
  - FCE Architecture is 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.01
  - FCE Architecture is 1oo1 for $MTTF_S$, $MTTF_S$ = 18.0 years
- Pump included, but not counted to stop flow
  - FCE Architecture is 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.01
  - FCE Architecture is 1oo2 for $MTTF_S$, $MTTF_S$ = 17.0 years
- Pump as redundant means for stopping flow
  - FCE Architecture is 1oo2 for PFD_{AVG}, PFD_{AVG} = 0.000013
  - FCE Architecture is 1oo2 for $MTTF_S$, $MTTF_S$ = 17.0 years

Pump and Discharge Valve Additional Considerations

- If deadheading pump is a separate hazard, use separate SIF with hazard-specific trip conditions
- If pump stop is included in SIF as redundant means to stop flow, trip on same condition as valve
  Note: Separate trip condition based on valve action
  - Adds complexity and cost
  - Compromises independence
  - Results in worse PFD_{AVG} and $MTTF_S$
- If logic solver has sequencing available, stop pump first, then close valve

Multiple Inlets



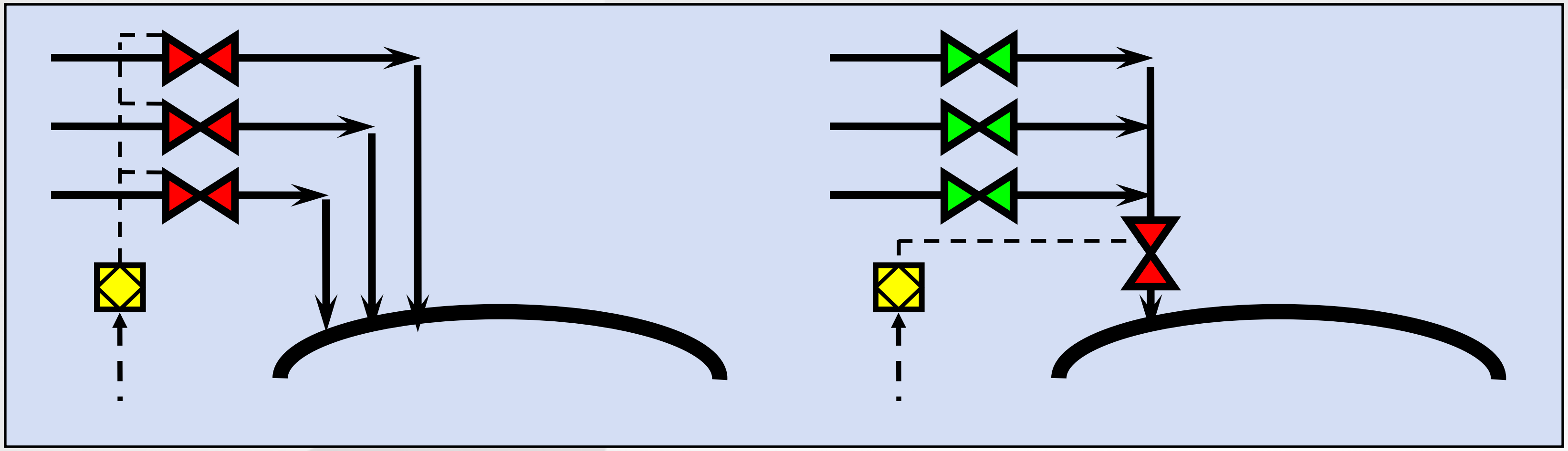
- Safe state: Flows from more than one source must each be stopped
- Complications: When any flow fails to stop, the safe state is not achieved
- Typical BPCS Solution: Separate final control elements (usually valves) on each line

Multiple Inlets Recommendation

Recommended SIS solution: **Group valves or use single header valve**

Why?

- Separate FCEs are not redundant, but independent opportunities to fail
- Fewer components mean better PFD_{AVG}
- Fewer components mean better spurious trip rate
- Fewer components decreases cost—initial investment *and* operating cost



Multiple Inlets Grouping Options

- Single relay to de-energize group of solenoids
  - Easiest way to group
  - Impact is primarily on I/O count to logic solver
- Single solenoid to de-energize group of valves
  - Depends on physical arrangement of valves
  - Has a more significant impact on PFD_{AVG} and $MTTF_S$
- Single valve on common inlet
  - May require new valve (installation and operating cost)
  - May be in congested area (constructability)

Multiple Inlets Counter-recommendation

Reasons to not group final control elements

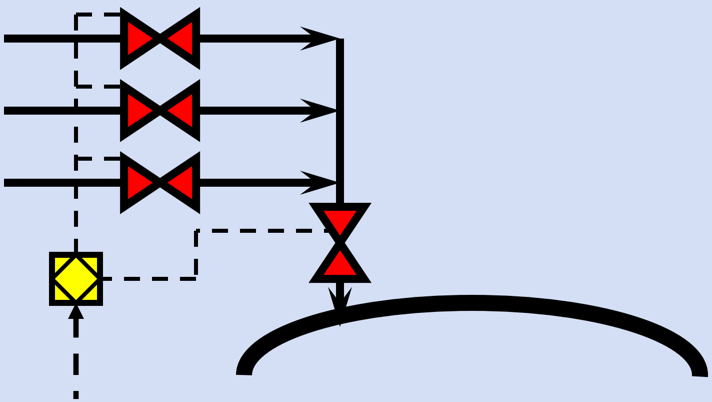
- Do not always act together
  - Example: A SIS may have one SIF that closes 6 valves and another SIF that closes only 2 of those. The 6 valves should not be grouped. Instead, the 2 valves should be grouped and tripped by both SIFs while the other 4 should be a separate group tripped by only the first SIF.
- Redundancy
  - Example: A pair of valves are installed to provide redundant shut-off and always act together. Grouped, they are no longer independent. Common cause failure compromises their redundancy.
- Proof-testing and maintenance
  - Example: Design of proof testing in a continuous process may only allow one valve to be stroked at a time, or repairs may require stroking of a single valve.

Multiple Inlet SIL Calculations and Examples

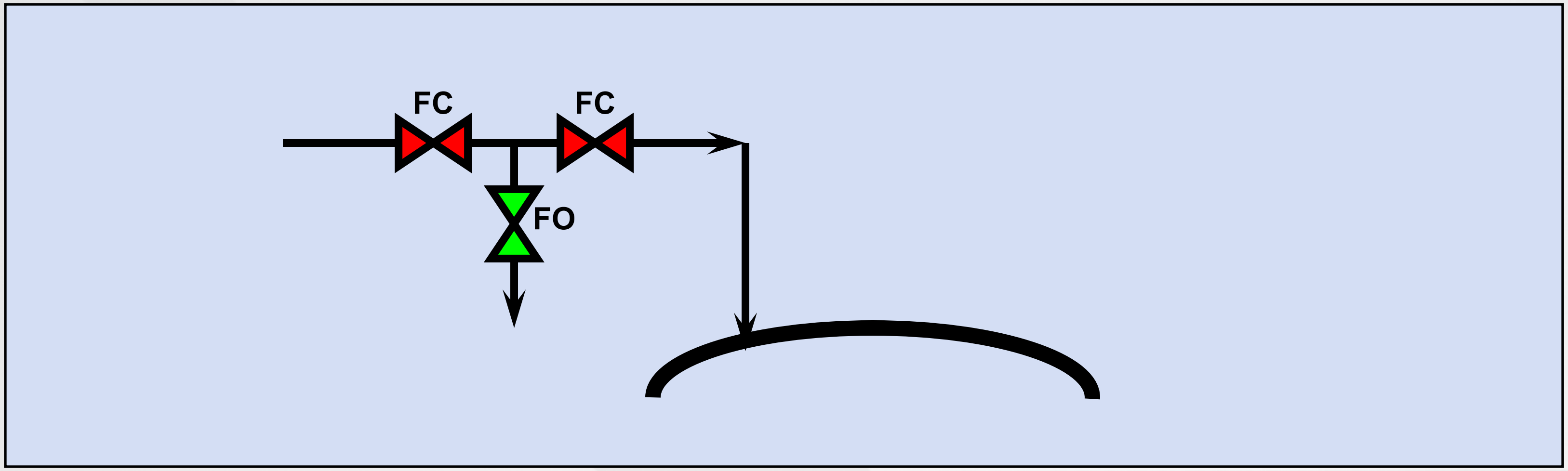
- Separate valves for stopping flow in X lines
  - FCE Architecture is X x 1oo1 for PFD_{AVG}, for three valves, PFD_{AVG} = 0.03
  - FCE Architecture is X x 1oo1 for $MTTF_S$, for three valves, $MTTF_S$ = 6.0 years
- Recommended practice – Flows grouped on single valve
  - FCE Architecture is 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.01
  - FCE Architecture is 1oo1 for $MTTF_S$, $MTTF_S$ = 18.0 years
- Recommended practice – Grouped on relay or solenoid
  - FCE Architecture is 1oo1 for PFD_{AVG}, to point of grouping
    FCE Architecture is X x 1oo1 for PFD_{AVG}, after grouping
  - FCE Architecture is 1oo1 for $MTTF_S$, to point of grouping
    FCE Architecture is X x 1oo1 for $MTTF_S$, after grouping

Multiple Inlet
Additional Considerations

- If mixing flows in a header introduces a new hazard, group at solenoid or relay.
- If a single header valve can be installed and the separate line valves grouped, 1oo2 architecture is possible.
  - Cost: One additional final control element
  - Benefits: Increased fault tolerance, better PFD_{AVG}
  - Drawback: Worse MTTFs and resulting cost of downtime
  - Gain: Less frequent proof testing.



Double block and bleed



- Safe state: Two block valves in series stop flow, with open valve between to confirm and bleed any slow leak
- Complications: Open bleed while block valves are open introduces a new hazard
- Typical BPCS Solution: Automate all three valves, sometimes with pressure indicator as tell tale

Double Block and Bleed Regulations and Standards

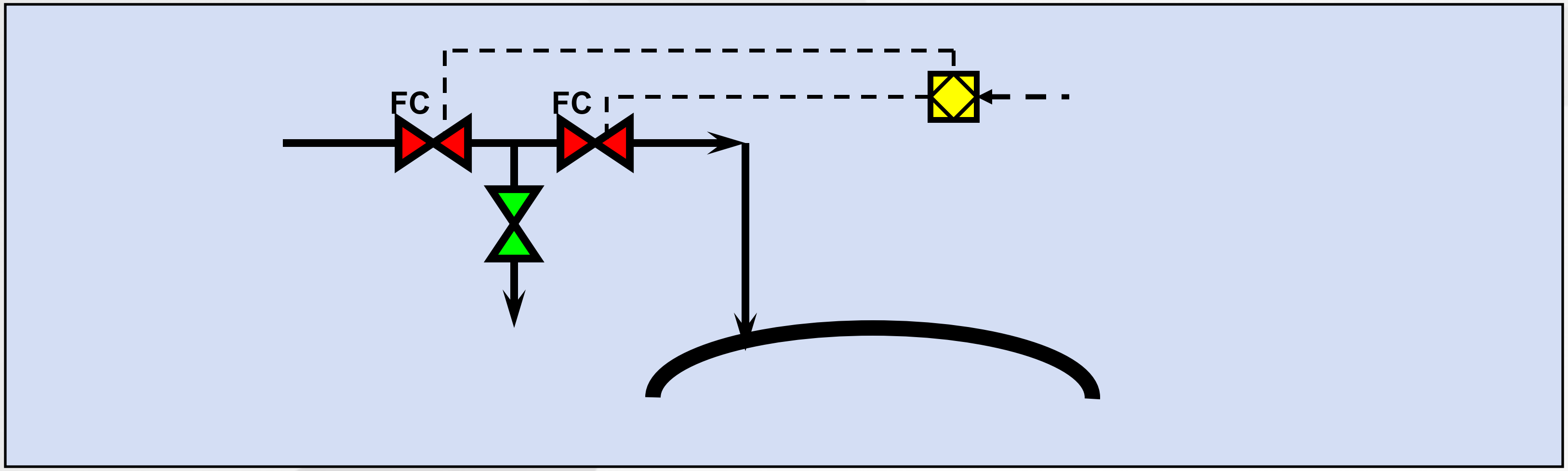
- OSHA's Permit-Required Confined-Space Entry Standard, 29 CFR 1910.146
  - Specifically recommended for isolating equipment before confined-space entry.
- OSHA's Control of Hazardous Energy Standard (Lockout-Tagout), 29 CFR 1910.147
  - Endorsed as a part of lockout-tagout procedures.
- Boiler and Combustion Systems Hazards Code, NFPA 85
  - Required on fuel lines as an automatic response to certain hazardous conditions to prevent accumulation of fuel in equipment.

Double Block and Bleed Recommendation

Recommended SIS solution: **Do not include bleed valve in SIF**

Why not?

- Spurious trip of bleed valve at full line pressure can create new hazard
- SIF purpose is to stop flow. Bleeding is non-emergency response.
- Bleed valve purpose—preventing slow accumulation in downstream equipment—achieved with manual bleed valve after SIF trip.
- Fewer components decreases cost—initial investment *and* operating cost



Double Block and Bleed Different Purposes

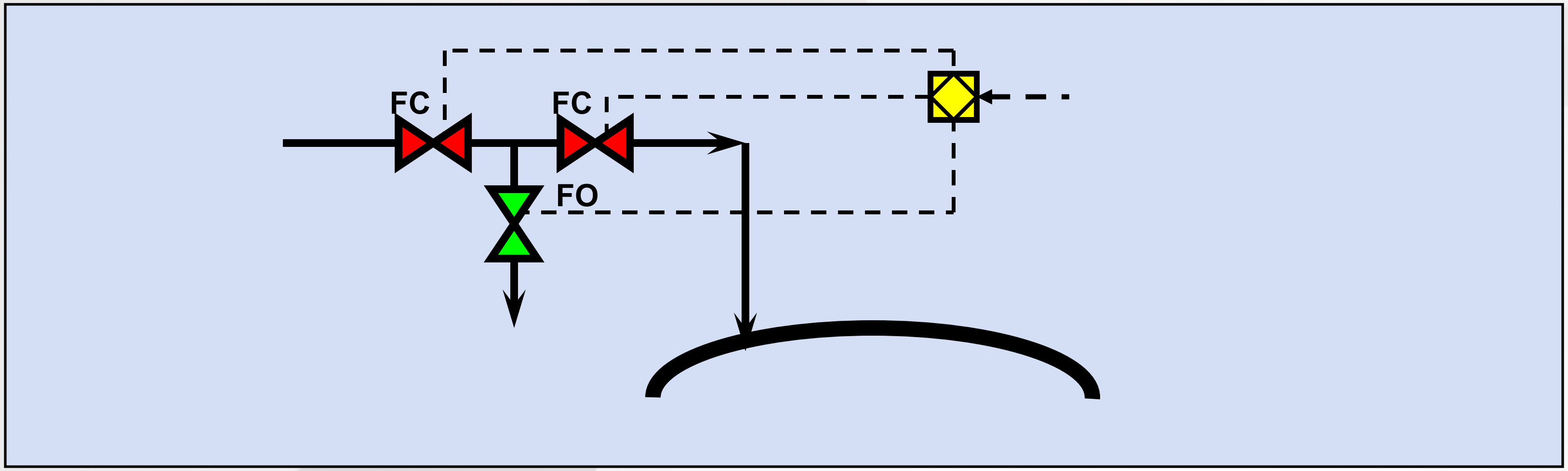
- SIF Purpose: Stop flow in emergency
  - SIF succeeds if either block valves closes, regardless of whether bleed valve opens or not.
  - SIF fails if both block valves fail to close, regardless of whether bleed valve opens or not.

  So, SIF success or failure is independent of bleed valve
  - No credit for bleed valve in PFD_{AVG} calculations.
  - $MTTF_S$ still must include bleed valve is part of SIF, making worse
- Bleed Valve Purpose: Prevent dangerous slow accumulation in idle downstream equipment
  - Time to respond is not seconds, but much, much longer
  - Lockout-tagout and confined-space entry require physical inspection and manual block in any case

Double Block and Bleed Counter-recommendation

Reasons to include bleed valve in SIF

- Hazard associated with minor leak into downstream equipment exceeds hazard associated with full discharge from the bleed valve.
- Required by standards or regulations



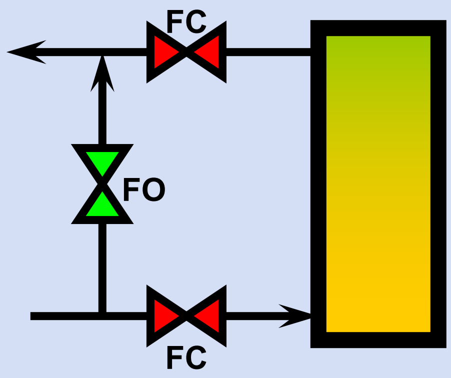
Double Block and Bleed SIL Calculations

- Recommended practice – SIF includes block valves only
  - FCE Architecture is 1oo2 for PFD_{AVG}, PFD_{AVG} = 0.00013
  - FCE Architecture is 1oo2 for $MTTF_S$, $MTTF_S$ = 9.0 years
- Bleed valve also included
  - FCE Architecture is 1oo2 for PFD_{AVG}, PFD_{AVG} = 0.00013
  - FCE Architecture is 1oo2 + 1oo1 for $MTTF_S$, $MTTF_S$ = 6.0 years

Double Block and Bleed Additional Considerations

- If block valves are partial stroke tested, an automated bleed valve allows more credit for partial stroke test coverage and may reduce class of valve required.
- If bleed valve must be included, use separate SIF with block valve position switches (or at least upstream valve position switch) as trip condition
- If bleed valve must trip on basic trip condition, group with downstream block valve
- If logic solver has sequencing available, close upstream block first, then close other two valves
- Size bleed line to accommodate full line discharge pressure and flow rate or install flow limiter

Unit Bypass and Isolation



- Safe state: Unit isolated with inlet and outlet block valves after bypass valve from inlet to outlet is opened
- Complications: Required response to emergency may be different from normal bypass-and-isolation
- Typical BPCS Solution: Automate all three valves

Unit Bypass and Isolation
Understand Purpose of SIF

- Case 1: Stop flow through unit
  - Requires only one valve: either inlet or outlet
- Case 2: Stop flow into unit
  - Requires two valves: inlet and outlet
- Case 3: Provide path around unit to maintain flow
  - Requires only one valve: bypass
- Case 4: Stop flow through unit and provide path around unit
  - Requires two valves: either inlet or outlet, and bypass
- Case 5: Stop flow into unit and provide path around unit
  - Requires all three valves: inlet, outlet, and bypass

Unit Bypass and Isolation Recommendation and Counter

Recommended SIS solution: **Only include required valves in SIF**

Why?

- Given that a spurious trip (open) of bypass does not shut down unit, additional valves increase spurious trip rate in most cases
- Fewer components decreases cost—initial investment *and* operating cost

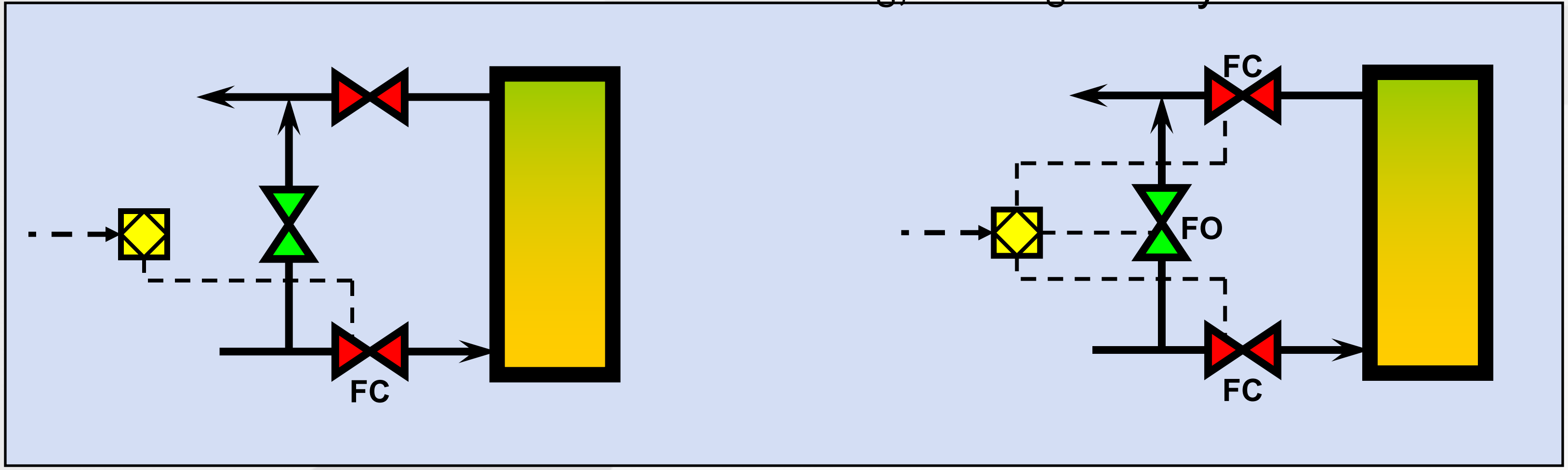
Reasons to include all valves in SIF, regardless of SIF purpose

- Uncertain nature of hazard in unit, so uncertain purpose
- When purpose requires stopping flow through unit (rather than into unit), including both inlet and outlet gives redundant FCEs

Unit Bypass and Isolation SIL Calculations and Examples

Case 1: Stop flow through unit

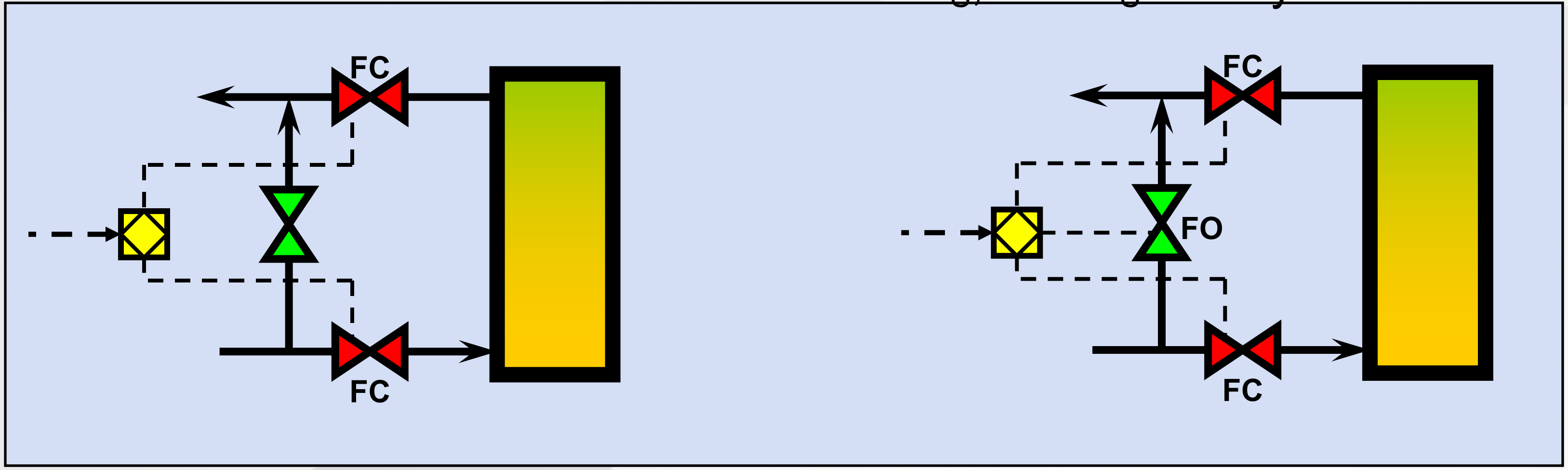
- Recommended practice – Only one valve in SIF, inlet or outlet
  - FCE Architecture is 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.01
  - FCE Architecture is 1oo1 for $MTTF_S$, $MTTF_S$ = 18.0 years
- Include all three valves in SIF
  - FCE Architecture is 1oo2 for PFD_{AVG}, PFD_{AVG} = 0.00013
  - FCE Architecture is 1oo2 for $MTTF_S$, $MTTF_S$ = 9.0 years



Unit Bypass and Isolation SIL Calculations and Examples

Case 2: Stop flow into unit

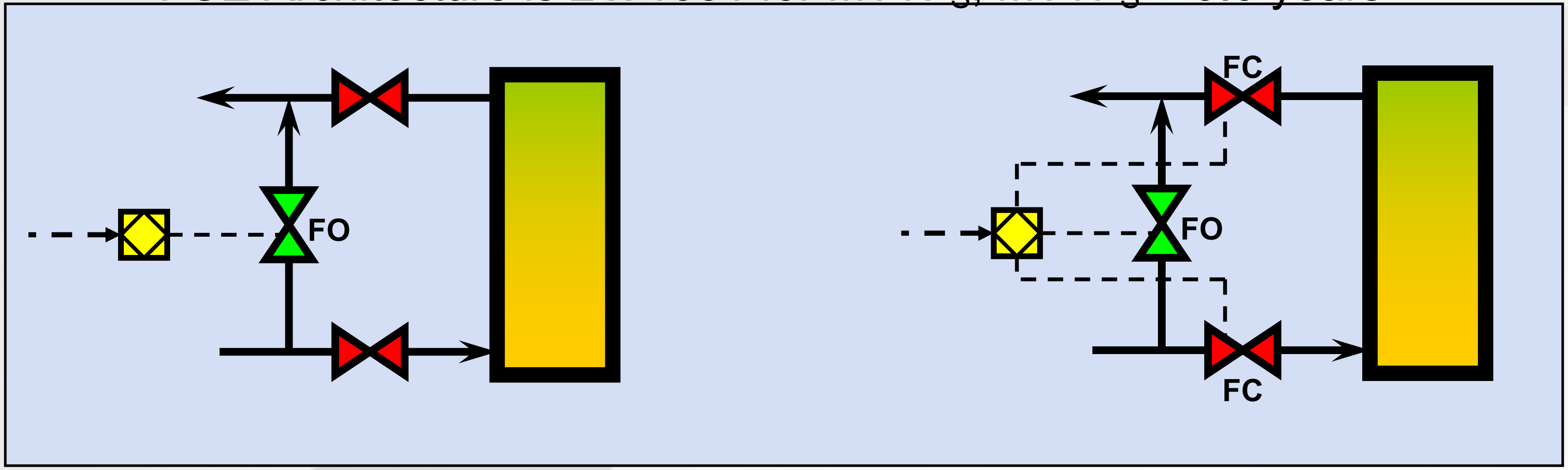
- Recommended practice – Both inlet and outlet in SIF
  - FCE Architecture is 2 x 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.02
  - FCE Architecture is 2 x 1oo1 for $MTTF_S$, $MTTF_S$ = 9.0 years
- Include all three valves in SIF
  - FCE Architecture is 2 x 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.02
  - FCE Architecture is 2 x 1oo1 for $MTTF_S$, $MTTF_S$ = 9.0 years



Unit Bypass and Isolation SIL Calculations and Examples

Case 3: Provide path around unit to maintain flow

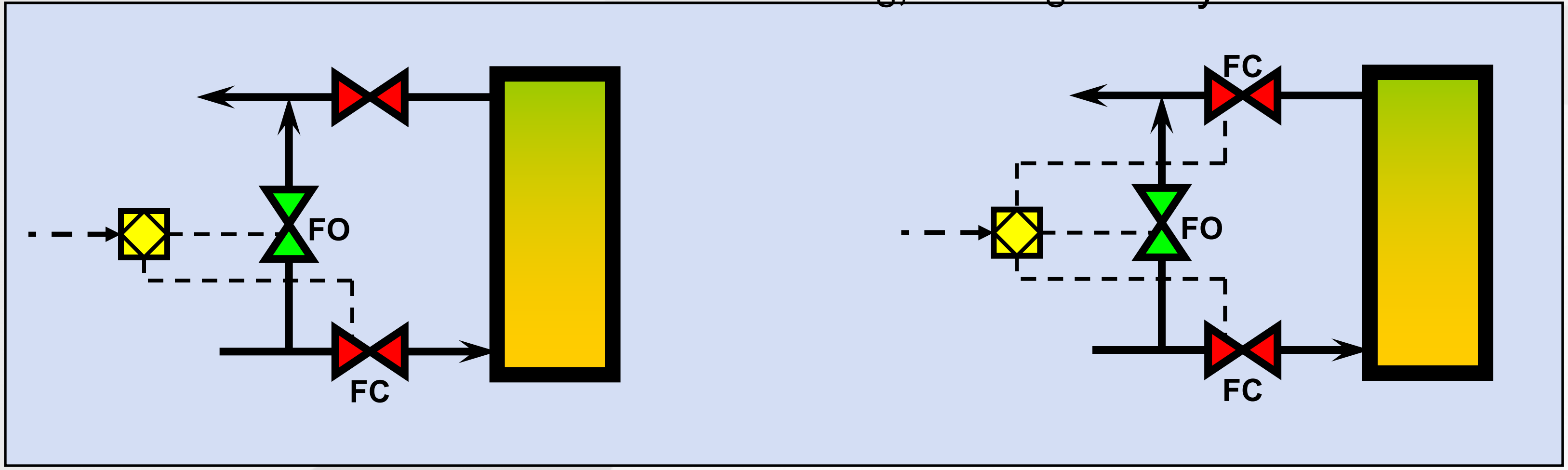
- Recommended practice – Only bypass valve in SIF
  - FCE Architecture is 1oo1 for PFD_{AVG}, $PFD_{AVG} = 0.01$
  - $MTTF_S$ does not shut down unit, $MTTF_S = \infty$ years
- Include all three valves in SIF
  - FCE Architecture is 1oo1 for PFD_{AVG}, $PFD_{AVG} = 0.01$
  - FCE Architecture is 2 x 1oo1 for $MTTF_S$, $MTTF_S = 9.0$ years



Unit Bypass and Isolation SIL Calculations and Examples

Case 4: Stop flow through unit and provide path around unit

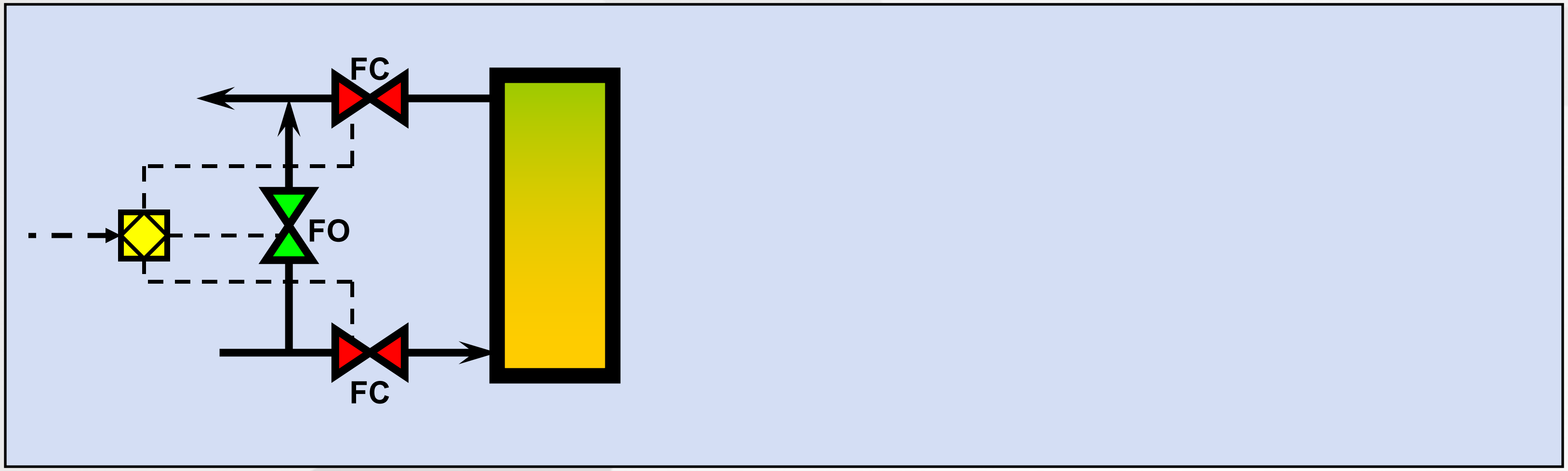
- Recommended practice – Bypass and one other valve in SIF
  - FCE Architecture is 2 x 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.02
  - FCE Architecture is 1oo1 for $MTTF_S$, $MTTF_S$ = 18.0 years
- Include all three valves in SIF
  - FCE Architecture is 1oo1 + 1oo2 for PFD_{AVG}, PFD_{AVG} = 0.01013
  - FCE Architecture is 1oo2 for $MTTF_S$, $MTTF_S$ = 9.0 years



Unit Bypass and Isolation SIL Calculations and Examples

Case 5: Stop flow into unit and provide path around unit

- Recommended practice – Include all three valves in SIF
  - FCE Architecture is 3 x 1oo1 for PFD_{AVG}, PFD_{AVG} = 0.03
  - FCE Architecture is 2 x 1oo1 for $MTTF_S$, $MTTF_S$ = 9.0 years



Unit Bypass and Isolation Additional Considerations

- If logic solver does not have sequencing available, group valves, to extent required by SIF
- If taking credit for 1oo2 architectures when preventing flow through unit, do not group inlet and outlet
- If using full sequencing, valves cannot be grouped
- If using full sequencing, open bypass first, close inlet second, then close outlet, to extent required by SIF
- If using partial sequencing, group bypass and inlet, trip grouped valves first, then close outlet
  Note: This still allows credit for 1oo2 architectures when preventing flow through unit

Summary

- The actions for SIFs may need to be different from the actions for process control in the same process
- The architectures for $MTTF_S$ calcs may need to be different from those for PFD_{AVG} calcs.
- FCEs in SIFs should be limited to those needed to accomplish purpose of each SIF
- General recommendations
  - With a pump and discharge valve, do not include pump in SIF
  - With multiple inlets, group valves or use single header valve
  - With double block and bleed, do not include bleed valve in SIF
  - With bypass and isolate, use only valves needed for purpose

Business Results Achieved

- SIF designs leveraged from process designs, but based on safety requirements
- Typically require fewer field devices and fewer I/O

- Lower PFD_{AVG}
- Longer $MTTF_S$
- Lower investment cost
- Lower operating and maintenance expense

Where To Get More Information

Bluefield Process Safety, (314) 420-9350

Emerson Process Management, SIS Consulting

- Refining and Chemical Industry Center

St. Louis, Missouri	(314) 872-9058
Overland Park, Kansas	(913) 529-4201
Houston, Texas	(281) 207-2800

- Hydrocarbon and Energy Industry Center

Calgary, Alberta	(403) 258-6200

About the Presenters

- Mike Schmidt, Principal SIS Consultant , Emerson Process Management
- Mike Schmidt is located at the RCIC in St. Louis. He works with customers to prepare SRSs and perform SIL calculations. Earlier in the safety lifecycle, he facilitates HazOps and other PHAs, LOPAs, and establishing RTC. Mike also consults on process design and optimization. He writes and teaches in all these areas. Mike is a registered PE in several states and a CFSE. He has worked in the chemical process industries since 1977, including working directly for Union Carbide (now Dow), Shipley (now Rohm and Haas), and Air Products.

About the Presenters

- Tim Forbis, Process Safety Engineer , Emerson Process Management
- Tim Forbis is located at the Refining and Chemical Industry Center in St. Louis, where he has been since completing his master's degree in Chemical Engineering at the University of Missouri – Rolla. He has worked on the preparation of SRSs for several clients, on HazOps, and is routinely called upon to perform SIL verification calculations, particularly for unusual architectures. He is training to become a Certified Functional Safety Expert.

Questions? Feedback? Comments?