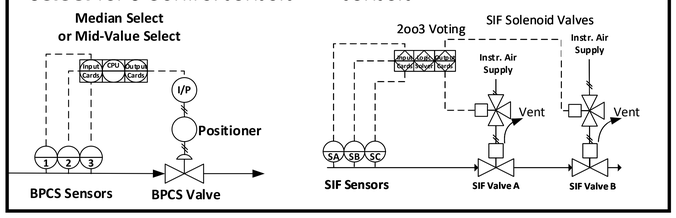
What Is the Real Risk Reduction for 3 Sensors Using the Mid-Value for Control and 2oo3 Voting for Safety?

SPRING21 +17TH GCPS
A Joint AIChE and CCPS Meeting

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute

What happens to the risk when two good ideas are combined?

- **Median (or mid-value) Select** for 3 control sensors
- **2oo3 voting** for safety sensors

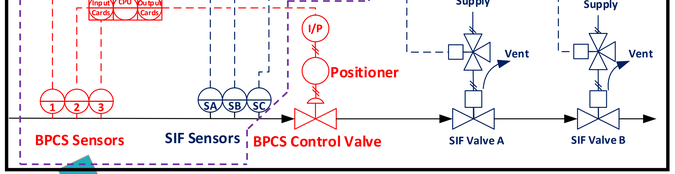


Advantages of each independent configuration

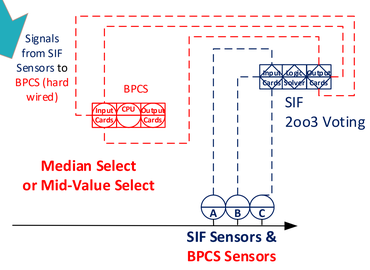
- **Median (or mid-value) Select** for 3 control sensors
- Reduced trips from transmitters that drift or that have bad PV
- **2oo3 voting** for safety sensors
- Reduced spurious trips
- Lower PFD than 1oo1 voting

BPCS Loops are Red; SIF Loops are Blue

Control & SIF are independent! (Required by [1, 2])



Sensors shared between SIF and BPCS



How to Estimate Relative Risk of Sensors Shared?

- Fault Tree Analysis could be used, but it is difficult to model failure modes and failure sequences in time.
- Markov models can handle different failure modes and failure sequences in time.
- A **Markov model** was used [3].
- For simplicity, the model was limited to the sensors configuration.

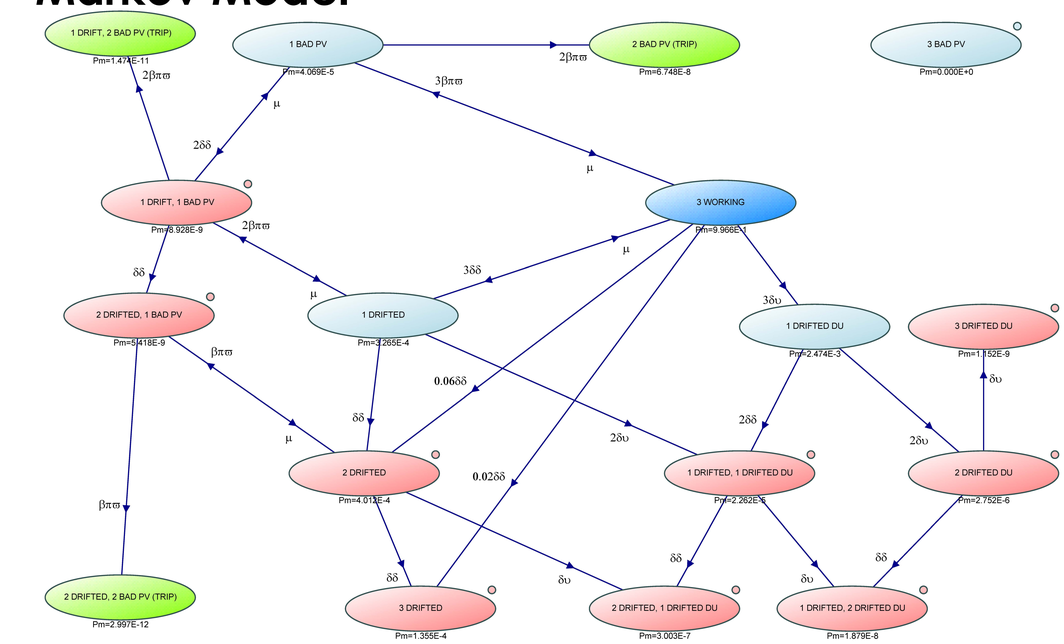
States were selected for each degradation path

- 3 sensors working – **dark blue**
- 1 sensor failed, drift (dangerous detected or dangerous undetected), bad PV (detected) – **light blue** – control & SIF are still functional
- Unavailability states with 2 or 3 sensors failed. – **light red**
- Tripped states – **light green**

Transitions between states

- Based on failure rates (and number of sensors that have not yet failed) and repair rate.
  - Sensor failure rate, λ = 1.67E-2/year
  - DD Drift, δδ = 0.8* λ = 1.34E-2/yr.
  - DU Drift, δυ = 0.1* λ = 1.67E-3/yr.
  - Bad PV, βπω = 0.1* λ = 1.67E-3/yr.
  - Repair rate, μ = 121.67/yr. (72 hr. MTTR)
  - Proof Test Interval = 1 year

Markov Model



O = unavailability state
Mean unavailability states (PFD) = 5.6E-4

Pm = Mean probability of a state
Mean availability states = 9.99E-1

Conclusions

- For 2oo3 sensor voting, the Probability of Failure on Demand (PFD) is 5.62E-4. **This is a reasonable value for the sensor part of an SIF**.
- For median select or mid-value select for control sensors, the expression PFD = λT/2 is solved for λ. For a 1 year test interval, **the failure rate, λ, for the control sensors is 1.12E-3/yr, an order of magnitude lower than the single sensor failure rate of 1.67E-2/yr.**

Recommendations

- **If the SIF trips** on the 2oo3 sensors, the BPCS control loop shall be automatically placed in **manual** and the output to the valve shall be **set to 0**. Required to avoid a "race" condition in which the control loop sees a 0 PV and attempts to open the control valve.
- The **loops** for each of the three sensors shall be **powered by the SIF logic solver**.
- There are **other schemes** to share process variables between the SIF and the BPCS but analysis of their failure modes is **beyond the scope** of this paper.
- Provision should be made for the BPCS to **calculate the mean value correctly** when the **sensors are in a degraded state**
  - 1 sensor with bad PV (detected)
  - 1 sensor drifted (detected)
- It is critical that **detected failures be repaired within 72 hours.**
- **Future work**: include more explanation for human factors that introduce errors during testing [4].

References

1. IEC 61511-1:2016+AMD1:2017 CSV, Consolidated version: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements, International Electrotechnical Commission (IEC), 2010, Geneva, Switzerland.
2. ANSI/ISA-61511-1-2018 / IEC 61511-1:2016+AMD1:2017 CSV, Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, definitions, system, hardware and application programming requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT), International Society of Automation, Research Triangle Park, North Carolina.
3. CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment*, American Institute of Chemical Engineers, New York, New York, 2001.
4. ISA-TR84.00.02-2015, Safety Integrity Level Verification of Safety Instrumented Functions, Annex E, Markov Analysis. International Society of Automation, Research Triangle Park, North Carolina.
5. "SIL-3, SIL-2, and Unicorns (There Is a High Probability Your SIL 2 and SIL 3 SIFs Have No Better Performance Than SIL 1)", A.M. (Art) Dowell, III, W. Bridges, M. Massello, and H.W. (Hal) Thomas, *15th Global Congress on Process Safety*, New Orleans, LA, AIChE, March 31-April 3, 2019

Glossary

Acronym	Definition
1oo1	1 out of 1 voting
2oo3	2 out of 3 voting
BPCS	Basic Process Control System
βπω	Bad PV failure rate
CPU	Central Processing Unit (or Controller Card)
DD	Dangerous Detected
DU	Dangerous Detected
δδ	Drift dangerous detected failure rate
δυ	Drift dangerous undetected failure rate
I/P	Current to pneumatic transducer
λ	Failure rate, per year
mA	Milliampere
MTTR	Mean Time To detect and Repair, years. 1/MTTR = μ
μ	repair rate, per year
PFD	Probability of Failure on Demand
PV	Process Variable
SIF	Safety Instrumented Function
SIL	Safety Integrity Level

Calculations done by

- The **Markov Model** Module in **Reliability Workbench** 13.0.2.0 provided by **Isograph LTD.**

ART DOWELL, III **Principal Process Safety Engineer**
adowell@piii.com

Art has a BA and BS in Chemical Engineering and has more than 50 years of process safety experience, including 42 years at Rohm & Haas; now The Dow Chemical Company. Art has published more than 50 papers, many on PHA, LOPA, and SIS implementation.
PII has helped more than a hundred companies implement process safety since 2003. This includes leading hundreds of PHAs for both new projects and existing plants and training more than 4000 PHA leaders and scribes. PII staff has performed more than 1000 LOPA and more than 1000 SIL Verification.