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

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2021 Spring Meeting and 17th Global Congress on Process Safety
Virtual
April 18 - 22, 2021

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

Arthur M. (Art) Dowell, III, PE
Process Improvement Institute, Inc.
2437 Bay Area Blvd, PMB 260
Houston, TX 77058-1519
Adowell@piii.com

Keywords: SIF, SIS, SIL, safety instrumented function, LOPA, process control, median select, mid-value, 2oo3 voting

Abstract

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

To reduce spurious trips of SIFs (safety instrumented functions), many plants moved from 1oo1 or 1oo2 voting on the sensors to 2oo3 voting -- a good idea. To improve stability for critical process control loops, many plants went from one or two sensors to three sensors using the mid-value for control (also called median-select) -- also, a good idea.

Without really analyzing it, some facilities combined the two ideas, using the mid-value of three sensors for a control loop and then, using the same three sensors voting 2oo3 for an SIF. The intent of the SIF was to protect against consequences that could be caused by a failure of the control loop as well as other causes. This arrangement violates the fundamental premise of LOPA (layer of protection analysis) and ANSI/ISA 84.00.01 (ISO 61511); an independent protection layer shall be independent of causes of the consequence that the layer protects against.

The new configuration must be evaluated by Markov analysis. The Markov analysis considers sequential failures of each of the three sensors (and repairs, where failures are detected) and determines which of the remaining devices in the SIF can detect the scenario. The PFD

(probability of failure on demand) is calculated for the 2oo3 sensors voting in the SIF and compared with the PFD of the totally independent 2oo3 sensor SIF.

The paper suggests guidance for appropriate use of the combined configuration and suggests how to approximate the risk reduction.

1 Introduction

To reduce spurious trips of SIFs, many plants moved from 1oo1 or 1oo2 voting on the sensors to 2oo3 voting as shown in Figure 1 -- a good idea.

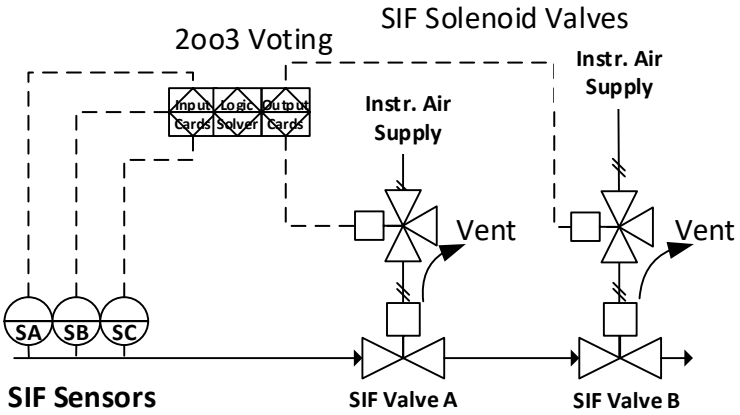


Figure 1: 2oo3 Voting for Safety Sensors (Courtesy of Process Improvement Institute, Inc., all rights reserved)

2oo3 voting avoids the spurious trip rates of 1oo1 or 1oo2 voting for safety sensors. While 2oo3 voting does not have as low a PFD as 1oo2 voting, its PFD is low enough for use with reasonable test intervals. The tradeoff between low spurious trip rates and reasonably low PFD makes 2oo3 voting popular for critical SIFs.

Additionally, 2oo3 voting allows diagnostic comparisons between each sensor and the median value with an alarm for any sensor that differs from the median value (for example, by more than 5% for more than 5 minutes). The operator response to the alarm is to initiate troubleshooting with repairs completed within 72 hours.

In the BPCS (basic process control system), to improve reliability, some facilities went from a single sensor for a critical control loop to three sensors with mid-value for control (also called median-select) as shown in Figure 2 -- also, a good idea. A sensor that develops a significantly different value for the process variable from the other two sensors would be ignored and the deviation alarm would initiate operator response for troubleshooting and repairs completed within 72 hours.

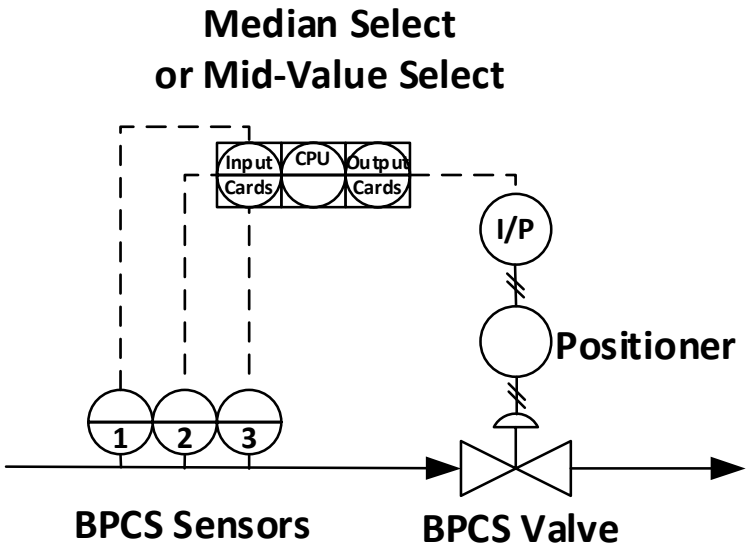


Figure 2: Median or Mid-Value Select for Control Sensors (Courtesy of Process Improvement Institute, Inc., all rights reserved)

What happens if these two ideas are combined? The SIF standards [1, 2] and the simplified risk assessment tool, LOPA (layer of protection analysis) [3], require independence between the control loop (which can be an initiating cause for a dangerous scenario) and the SIF loop (which detects the process variable deviation and manipulates final elements to prevent the scenario). Combining the two ideas with the required independence is shown in Figure 3.

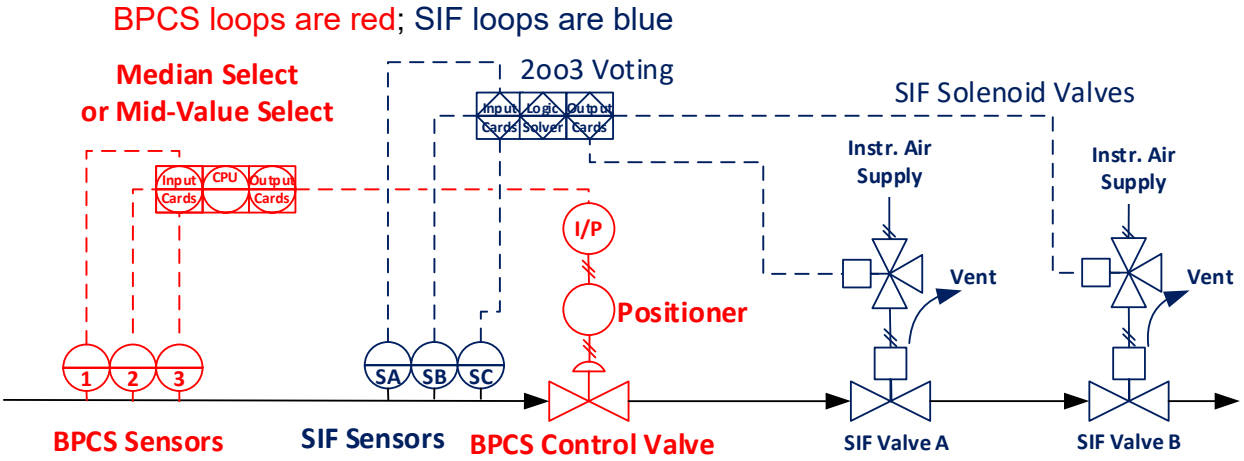


Figure 3: Control and SIF Are Independent (Courtesy of Process Improvement Institute, Inc., all rights reserved)

Today, we are seeing some facilities who are using three sensors for both control and safety. For control, the BPCS is using median select (mid value) select. The SIF is using the same three sensors for 2oo3 voting to detect the scenario, as shown in Figure 4.

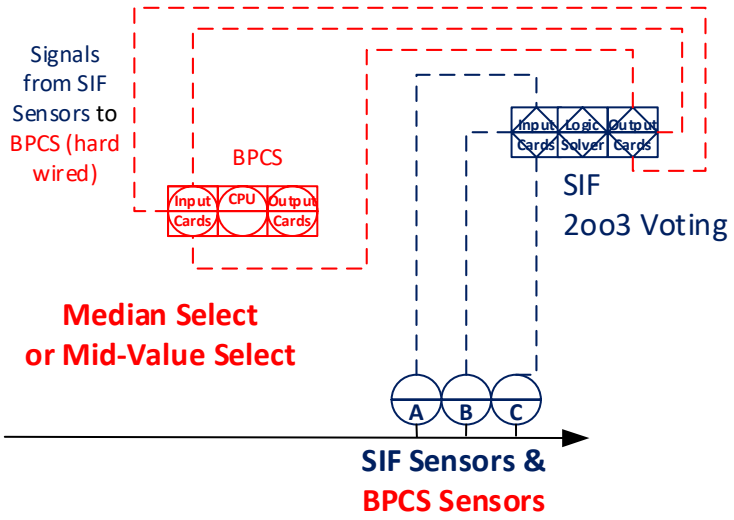


Figure 4: Sensors shared between SIF and BPCS (Courtesy of Process Improvement Institute, Inc., all rights reserved)

2 Analysis

Qualitatively, failures of the three sensors that are initiating causes of a dangerous scenario will be reduced significantly by the median select control strategy. The three sensors voting 2oo3 for the SIF will be very effective in detecting initiating causes that are independent of the three sensors. The challenge is how to estimate the relative risk of scenarios that arise from the shared sensors.

Initially, it was planned to use fault tree analysis to estimate the PFD of the three sensors in SIF service and to estimate the dangerous failure rate of the three sensors in control service. It was found to be difficult to model the various failure modes and failure sequences in time. Some failures are undetected and cannot be repaired (until the scheduled proof test detects the failures and repairs are made). Some failures are detected and can be repaired. Because of the transitions from states where the SIF could work correctly to states where the SIF is impaired, and the transition from impaired states back to states working correctly, a Markoff model was used for the analysis [4]. For simplicity, the model was limited to the three sensors configuration.

The Markoff model starts with all three sensors working correctly. Then degradation paths are developed for each of the possible dangerous failures (detected or undetected). The degradation paths result in states 1) with one sensor failed or 2) unavailability states where two or three sensors are failed. The unavailability states are conditions where the three sensors are unable to detect a scenario. Where repair paths are available, the sensors are moved from a degraded state back to a functional state. The states for the Markoff model are shown in Table 1 and Figure 5.

Table 1: Markoff Model STATES for the Three Sensor Group

State	Functional capability	Color (Figure 5)
3 sensors working	Everything working as designed	Dark blue
1 sensor failed, drift (dangerous detected or dangerous undetected), bad PV (detected)	Control and SIF are still functional	Light blue
Unavailability states with 2 or 3 sensors failed	SIF is not functional	Light red
Tripped states	SIF logic has moved the final elements to the tripped or safe state	Light green

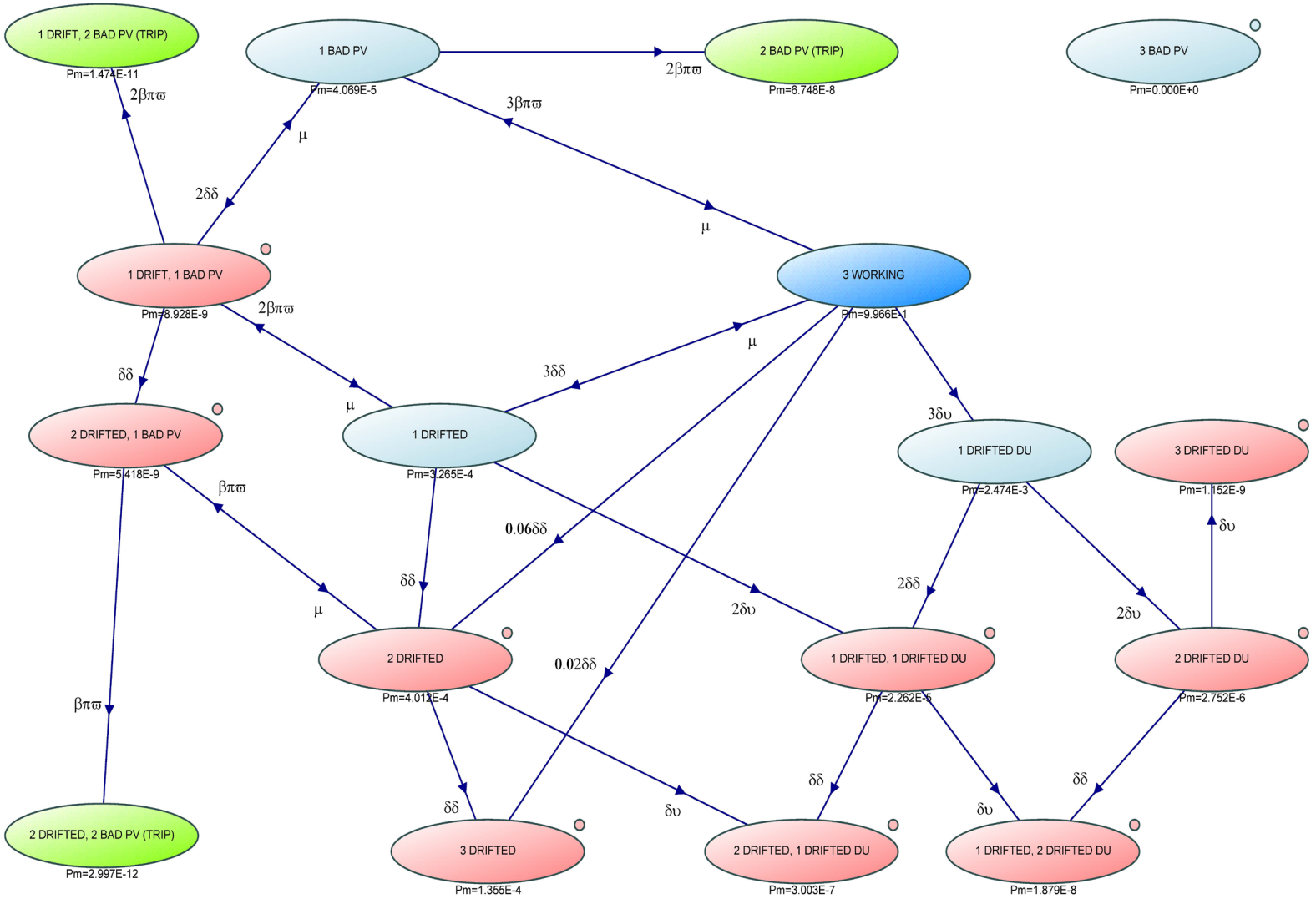
Next, transitions between states were identified, as shown in Table 2. Transitions along the degradation paths are based on the failure rates and the number of sensors that have not yet failed. Transitions along the repair paths from a detected failure are based on the repair rate. The sensor failure rate, λ = 1.67E-2/year, was taken from typical industry values [4]. For a specific installation, failure rates that apply to the equipment should be used. Three different failures were modeled for each sensor, dangerous detected drift, dangerous undetected drift, and bad PV (process variable -- <4mA or >20mA). These three types of failures were allocated to sum up to the industry failure rate value. The repair rate was based on a MTTR (mean time to repair) of 72 hours. An annual proof test interval was assumed for the sensor group.

Table 2: Markoff Model TRANSITIONS for the Three Sensor Group

Description	Symbol	Value	
DD Drift (detected)	$\delta\delta$	0.8*λ=1.34E-2/yr	
DU Drift (undetected)	$\delta\upsilon$	0.1*λ=1.67E-3/yr	
Bad PV	$\beta\pi\omega$	0.1*λ=1.67E-3/yr	
Repair rate	μ	121.67/yr	MTTR=72 hours

The Markoff model is shown in Figure 5. The three sensors group begins with the dark blue state of three working sensors. Since there are three sensors, the DD Drift, DU Drift, and Bad PV degradation paths from this state show the failure rate multiplied by a factor of three. The model also includes transitions to the 2 Drifted and 3 Drifted states, representing human error during calibration. The failure rates for the human error are based on [5]. For degraded states where the failure can be detected, the model includes a transition back to the previous state, using a repair rate of 121.67/yr (MTTR = 72 hours).

The Markoff model was created in and was solved by the Markoff model module in Reliability Workbench 13.0.2.0 provided by Isograph LTD**.** The Reliability Workbench also includes fault tree analysis**.**



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

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

Figure 5: Markoff Model

3 Conclusions

For 2oo3 sensor voting, the 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 = $\lambda T/2$ is solved for λ. For a 1-year test interval, the failure rate, λ, for the three control sensors group is 1.12E-3/yr, an order of magnitude lower than the single sensor failure rate of 1.67E-2/yr.

Based on this analysis, we conclude that the configuration of three sensors used both for control (using median select) and for safety (using 2oo3 voting) offers a probability of failure on demand for the sensor group that is reasonable for a SIL 1 or SIL 2 SIF. Note that the SIL verification calculation must be performed for the complete SIF, including sensors, logic solver, and final elements.

We also conclude that the failure rate of the sensor group used for control is an order of magnitude lower than the single sensor failure rate.

These conclusions are subject to the recommendations shown below.

4 Recommendations

The following recommendations must be followed to support the conclusions drawn from this analysis.

4.1 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. This step is required to avoid a "race" condition in which the control loop sees a PV value of 0 and attempts to open the control valve.

4.2 The loops for each of the three sensors shall be powered by the SIF logic solver.

4.3 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.

4.4 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)

4.5 It is critical that detected failures be repaired within 72 hours.

4.6 Future work: include more explanation for human factors that introduce errors during testing [5].

5 Glossary

Table 3 has definitions for acronyms.

Table 3. 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

6 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), Geneva, Switzerland, 2017.

[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, 2018.

[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, 2015.

[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.