Comparison of Voting Arrangements in SIS

One of the key design parameters in safety instrumented system (SIS) design is the architecture or voting arrangements of the various subsystems that comprise a safety instrumented function (SIF). The architecture, or voting arrangement, is essentially the use of redundant pieces of equipment for the purpose of creating the ability to tolerate a failure of one component and still have the SIF perform its action. Selection of an appropriate voting arrangement will consider the failure modes of the SIS equipment, the level of safety that must be achieved and the rate of spurious failures and the associated consequences (financial or otherwise) of a spurious trip.

In process industry SIS design there are several common voting arrangements. For the purposes of this discussion I will focus on the sensor subsystem, but the same discussion will also apply to the logic solver and final element subsystems. The most common voting arrangements used in industry are as follows:

- One-out-of-one (1oo1) – a.k.a., simplex
- One-out-of-two (1oo2)
- Two-out-of-two (2oo2)
- Two-out-of-three (2oo3)

There are two parts to the voting arrangement description. The first number is the number of devices that must "vote" to cause a trip for the trip to occur. The second number is the total number of devices. Thus, in a 2oo2 voting arrangement, 2 devices must vote to trip, out of a total of two device for the shutdown action to be taken.

Before discussing the value of the different voting arrangements in different situations, it's important to first understand the failure modes of SIS equipment. SIS equipment can fail in one of two ways

- Safe (Spurious, Initiating, Overt)
- Dangerous (Inhibiting, Covert)

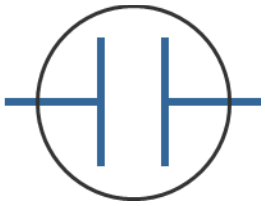
When an SIS suffers a safe failure, the SIS will cause the SIF to activate and shutdown the plant when there was no actual demand or need to shut the plant down. These failures are often referred to as spurious failures or nuisance failures since production was unnecessarily stopped. The are also called initiating failures because the initiate the action of the SIF when it was not required, and overt failures because the failure is overt- meaning it announces its presence by causing a shutdown of the plant. As an example, a safe failure of a shutoff valve could include breakage of the instrument air connection, which then causes the actuator to depressure and the valve to fail to its closed position. In this case a shutdown occurred unnecessarily when there was no hazard present.

Dangerous failures are the opposite. Dangerous failures are also called inhibiting failures because they inhibit the SIF from taking action when it is called to do so, and covert failures because the failure does not reveal itself, laying in wait until the SIF is called on to take its safety action but it cannot. As an example, a dangerous failure of a valve could include the ball of a ball valve getting jammed against the seat preventing it from turning. The failure itself does not cause anything to happen and will not evidence itself until the SIS calls on the valve to close, but since the valve is jammed it will not close and thus inhibits or prevents the SIF from taking the required safety action. Knowing these two failure

modes is critical because the use of redundancy can only affect one of these modes depending on the voting arrangement.

Now that failure modes of been described, let's go through each of the voting arrangements and describe them physically and compare their probability of failing dangerously as well as their spurious trips.

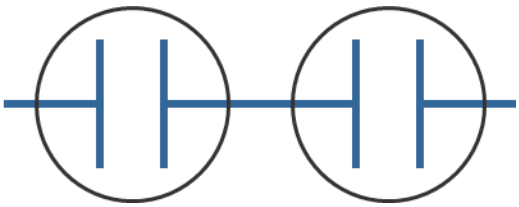
1oo1 Voting



One out of one voting represents a single device. This is the most common voting arrangement as well as the cheapest and easiest to maintain. If safety goals and nuisance trip avoidance goals can be achieved by a simplex device, that is the arrangement that should be used. Only if a single device cannot achieve one of the performance metrics should redundancy be considered. In the figure you will see a 1oo1 voting switch, such as a switch that might be contained in a pressure switch or a level switch. In SIS, we typically employ a de-energize-to-trip, fail-safe circuit design. With this design when power is removed from the circuit it will default into the position that the trigger the plant shutdown and safe condition. For switches in this configuration the failure mode of "contacts welded closed" is a dangerous failure because the failure prevents you from de-energizing the circuit and causing the plant shutdown. On the other hand, the failure mode of "open circuit" where the switch or related wiring open and interrupt the power of the circuit is a safe or spurious failure. The component failure causes the plant to shutdown when there was no real demand to do so from the process. The probability of failure and spurious trip rate are functions of the reliability of the specific piece of equipment. In a 1oo1 voting arrangement there is no failure tolerance to either dangerous failures or safe failures. For purposes of comparison, we have set a value of PFD (average probability of failure on demand) and STR (spurious trip rate) to set a baseline so that we can compare the characteristics of the different voting arrangements.

Voting Arrangement	PFD	STR
1oo1	***3.3E-2***	***4.5E-6***

1oo2 Voting

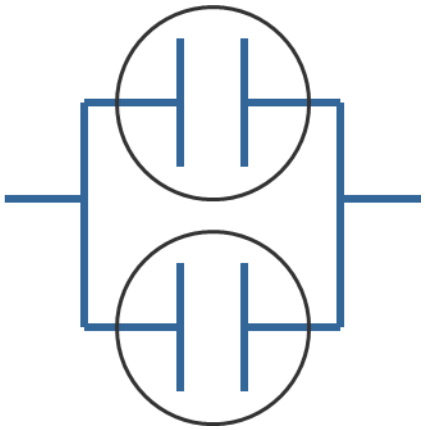


One-out-of-two voting (1oo2) employs two devices instead of one. In this arrangement of two device only one vote to shutdown from either one of the two devices will cause the shutdown action to occur. Physically, this is represented by two switches in series. If either the "A" switch opens the circuit (i.e., votes to trip), or the "B" device does a shutdown action is taken. This arrangement is the "safe" arrangement because for the system to fail dangerously both of the individual switches would have to fail dangerously. This arrangement is tolerance to one dangerous failure because if the "A" switch contacts were welded close, the "B" switch could still open to de-energize the circuit and bring the plant back to a safe state.

While this arrangement is tolerant to one dangerous failure it is not tolerant to any safe failures. Thus, if the "A" switch alone suffers a safe failure (i.e., open circuit) the entire system will fail spuriously. The addition of second device makes whose spurious failure can also cause a system spurious failure means that while 1oo2 voting improves safety, the spurious trip rate is twice as high. In the table below, you can see the effect of the voting arrangement mathematically. 1oo2 voting has a much lower probability of failure (more than an order of magnitude improvement), but the spurious trip rate doubles. The doubling of spurious trip rate makes logical sense because you have double the number of components whose failure causes a spurious trip of the system. Ultimately, 1oo2 voting is used if more safety is required, i.e., the system cannot achieve its SIL target, but the increase in spurious failure rate is tolerable.

Voting Arrangement	PFD	STR
1oo1	3.3E-2	4.5E-6
1oo2	***1.4E-3***	***9.0E-6***

2oo2 Voting



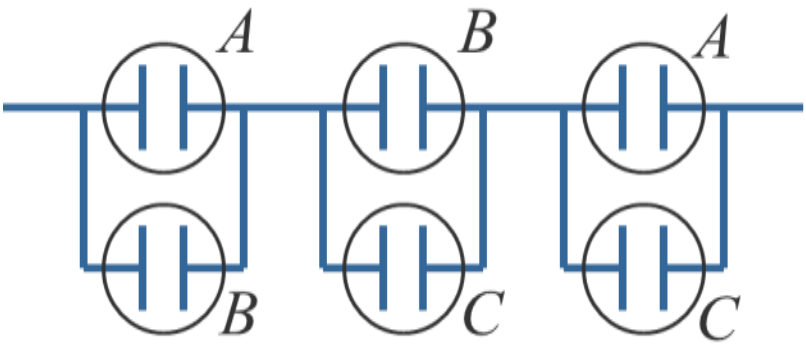
Two-out-of-two voting (2oo2) also employs two devices. In this arrangement, of the two devices, both devices must "agree" to cause a shutdown before the shutdown will occur. I.e., both devices must vote to trip to cause a trip action. This is physically represented by two switches in parallel. De-energizing either the "A" switch or the "B" switch alone will not cause the entire circuit to de-energize. Only when

both switches open is the circuit de-energized and the plant moved to a safe state. This arrangement does not have any tolerance to dangerous failures. A failure of the "A" device in the welded closed mode by itself will result in a dangerous failure of the overall system, and the same is true for the "B" device. While this arrangement does not have any tolerance to dangerous failures, it does have one degree of tolerance to safe failures. If the "A" device were to spuriously fail in the safe open-circuit mode, power will still be conducted through the "B" switch, preventing a spurious shutdown. The same is true for a spurious failure of the "B" switch.

As a result of being tolerance to one safe failure but no dangerous failures, this voting arrangement is commonly used to improve resistance to spurious failures at the cost of decreasing safety performance below what it would be if only a single device were used. As you can see in the table below, use of 2oo2 voting provides for a drastically reduced spurious trip rate, but that improvement in resistance to spurious trips comes with the cost of decreased safety. Specifically, the probability of failure on demand of a 2oo2 voting arrangement is twice as high as for a single device. As a result, this voting arrangement can only be used to reduce spurious trip rates for systems with low SIL requirements e.g., SIL 1.

Voting Arrangement	PFD	STR
1oo1	3.3E-2	4.5E-6
1oo2	1.4E-3	9.0E-6
2oo2	***6.6E-2***	***2.9E-9***

2oo3 Voting



Two-out-of-three voting (2oo3) employs three devices instead of one or two. As a result, this arrangement is the most costly and complex. In this arrangement, if any two switches vote to cause a shutdown, a shutdown will occur. This arrangement is a little hardware to visualize conceptually because each switch needs to have two contacts, as shown in the figure above. Essentially, there are three sets of parallel switches in series. While this arrangement does not provide two degrees of fault tolerance in any mode, its advantage is that it provides one degree of tolerance to safe failures and also one degree of tolerance to dangerous failures. Therefore, if any one switch suffers the dangerous welded-closed failure mode, the other two switches will still be able to move the process to a safe state.

Similarly, if any of the three switches suffers the safe open-circuit failure mode, the other two switches will be able to prevent the entire system from being spuriously energized.

Mathematically, the system operates like three 1oo2 systems for safety and three 2oo2 systems for spurious trip avoidance. As you can see in the table below, the 2oo3 systems has good performance in comparison with a simplex 1oo1 voting arrangement with respect to both safety and nuisance trip avoidance. Even so, the PFD of the 2oo3 voting system is 3x higher than the PFD of a 1oo2 system, and the spurious trip rate is 3x higher than for a 2oo2 system. While the 2oo3 system is the most complex and costly it is still very popular when higher SILs (i.e., SIL 2 and SIL 3) need to be achieved, but the plant cannot tolerate the high spurious trip rate associated with 1oo2 voting.

Voting Arrangement	**PFD**	**STR**
1oo1	3.3E-2	4.5E-6
1oo2	1.4E-3	9.0E-6
2oo2	6.6E-2	2.9E-9
2oo3	***4.3E-3***	***8.7E-9***