# Redundancy Concepts in FOUNDATION™ Fieldbus H1

Tom Boyd
Senior Software Engineer
Fieldbus Inc.
Austin, TX 78759

Steve Vreeland
Senior Software Engineer
Fieldbus Inc.
Austin, TX 78759

## KEYWORDS

FOUNDATION fieldbus, Redundancy, Fieldbus, Control, Safety

## ABSTRACT

While FOUNDATION fieldbus H1 does not include approved specifications for media redundancy, there are ways of achieving various levels of redundancy within an H1 fieldbus system. This paper will examine several concepts and implementation techniques for redundant fieldbus systems.

## INTRODUCTION

Many engineers see redundancy as just media redundancy, duplicate wires running to a device. Given the number of possible failure points in a modern control system, system redundancy is a much larger issue. The dependability of the wire media from the power supply to the transmitter to the valve can be dramatically improved by the proper selection of conduit and wire routes. System redundancy, on the other hand, depends on the reliability of the power supply, the transmitter, the controller, the communications scheduler, the valve actuator and the wire. Of these failure points the wire has the lowest complexity level and, under normal conditions, has the lowest failure rate.

FOUNDATION fieldbus is a technology that enables a broader range of redundancy types than seen in more traditional control. From basic transmitter redundancy where the operator is presented with process variables from two or more transmitters (along with the status of the variables) to advanced system redundancy using specialized, distributed function blocks, FOUNDATION fieldbus can provide the appropriate level of redundancy for many applications.

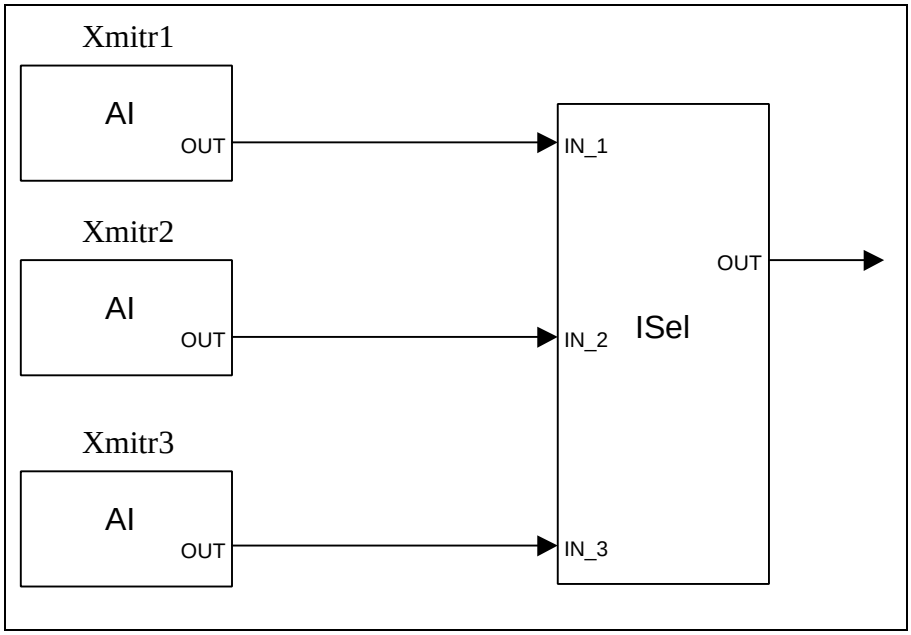


**Figure 1 - Multiple Transmitters with Selector Block**

## TRANSMITTER REDUNDANCY

Perhaps the simplest type of redundancy is the use of multiple transmitters. This is definitely nothing new. The operator is presented with process information from multiple transmitters and can choose to believe the signal his experience tells him is correct. However, with FOUNDATION fieldbus, each process variable has an associated status that tells the operator whether the device has determined that the signal it is presenting is good, bad, or uncertain. Furthermore, the device can alert the operator if it has detected any one of a multitude of conditions that may cause a loss of confidence in the information it is providing. And even beyond this, the device can possibly (and probably will) contain diagnostic information that the operator or engineer can review to determine the health of the device.

One method that can be employed to make the operator's job easier is to add a selector block that takes the process variables from several transmitters and presents a single output (still with an appropriate status) to the operator. In this case the operator does not have to look at several process signals, but can rely on the single output from the selector block. This is made possible due to the fact that bad inputs are not considered in the decision to select an output (unless all the input signals are bad, in which case the selector block will present a bad status on its output). So, the operator can monitor a set of redundant transmitters by watching a single signal, and if one transmitter fails, the output that the operator sees will still be accurate. Also, he can be informed of the failure either by the device that failed, or by employing other means.

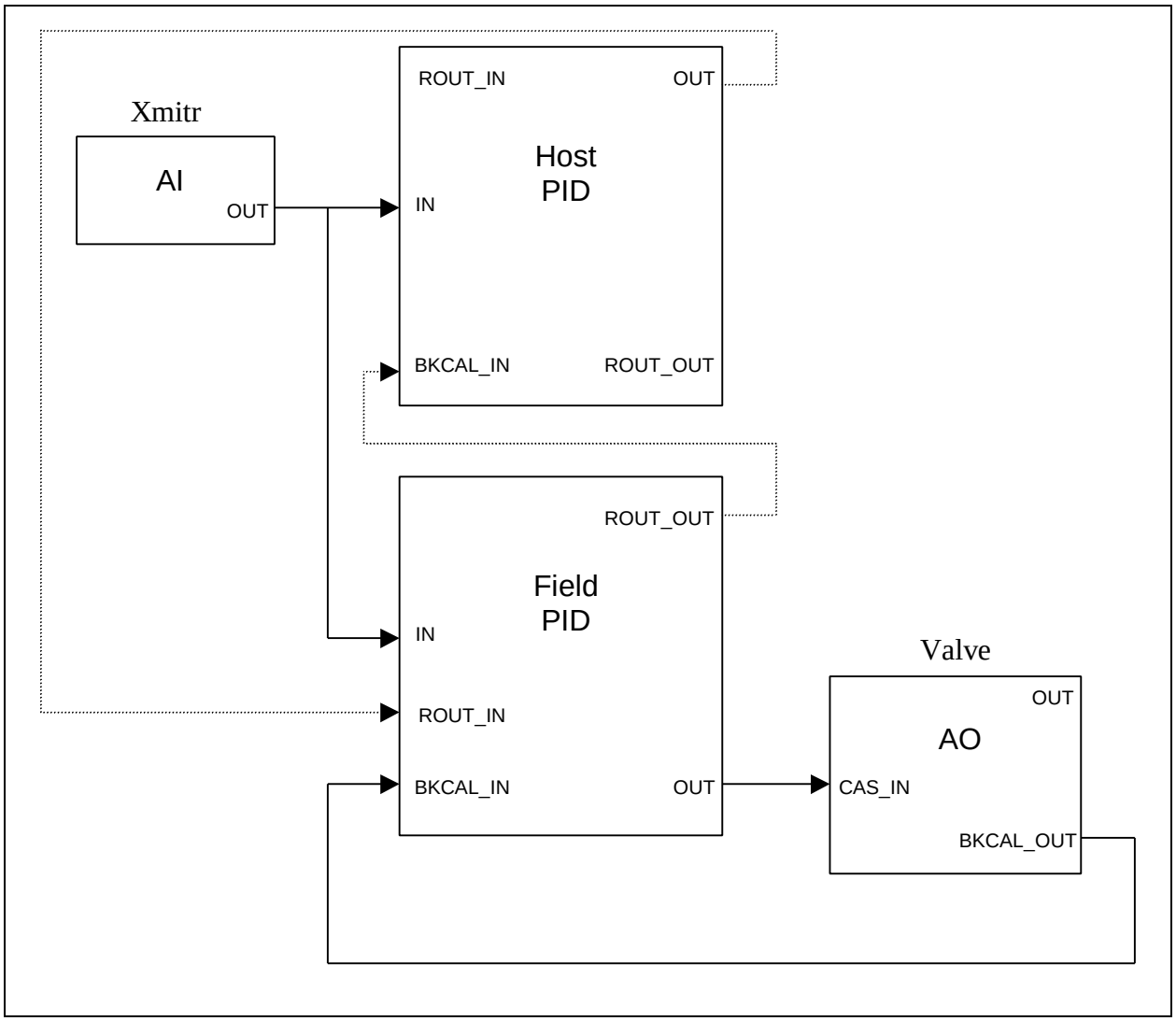


**Figure 2 - Field PID as backup to Host PID**

## CONTROLLER REDUNDANCY

FOUNDATION fieldbus enables the application of control in the field. With experience, users will realize distributing control to the field devices is more reliable than control in a centralized DCS or PLC. Users will soon appreciate the advantages of using a PID controller in a field device. Those slow to make the transition to control in the field may use the device PID controller as a backup to a host (DCS/PLC) PID controller. In the event of failure in the host system, control will switch to the field controller, and the process will continue without incident or bump. One simple way to accomplish this task is for the host to write the output from its PID to the ROUT_IN parameter of a PID in the field (see Figure 2 - Field PID as backup to Host PID). The PID in the field can be put into Rout mode, which will directly transfer the value written in its ROUT_IN parameter to its output. But, if the status goes bad on the data written by the host, or if the host gets too busy and does not get a chance to write the data in a configured amount of time, the field PID will switch to an automatic mode (determined ahead of time) and continue

operation. There is no bump because the PID has been monitoring the data from the host system as well as the data from the analog output block, and has been continually recalculating its internal variables so it will be ready to take over control when told to do so by an operator or by a set of conditions such as the ones described above.

While the above configuration will handle many problems, and would be sufficient for a number of applications, a more advanced technique can be employed that will provide an even higher level of redundancy.

Looking at Figure 3 - Using Redundancy Block and field PID to backup Host PID, we see the introduction of a new block, the redundancy switch or RSwitch block. One of the many features of this *custom* function block is that it can be used to switch to a backup PID controller based on conditions in the main PID controller, or based on conditions in the transmitter providing the process signal to the main PID controller. Taking an example where AI1 is in Transmitter1, AI2 is in Transmitter2 which is a backup transmitter to Transmitter1, AO is in a control valve, Host PID is in a DCS, Field PID and RSwitch are in a field device that happens to be a DIN box mounted in a NEMA 4 enclosure in the field. When operating under normal conditions, both AI1 and AI2 have good status, the Host PID is providing good data to the RSwitch block, and the RSwitch block is passing the value received from the Host PID to the AO block and to the Field PID. If there were a failure in Transmitter1 or in the DCS, the RSwitch would automatically switch to the Field PID, and control would continue without an interruption and without a bump.

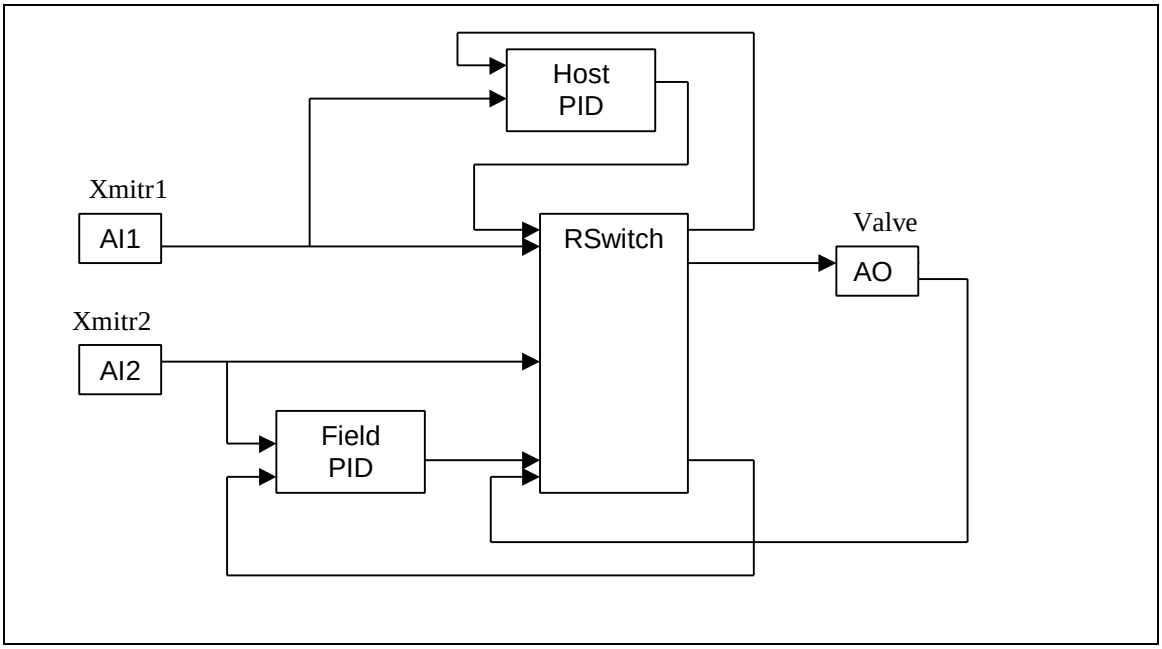


**Figure 3 - Using Redundancy Block and field PID to backup Host PID**

# VALVE REDUNDANCY

While valve redundancy is not as common as other types of redundancy, we will still present the possibilities. The simplest way to achieve valve redundancy is to have two valves in-line, both receiving the same signal from a controller. The main valve would be programmed to fail open, and the backup valve would be programmed to fail according to what would normally be done for the process. This solution is elegant in its implementation simplicity.

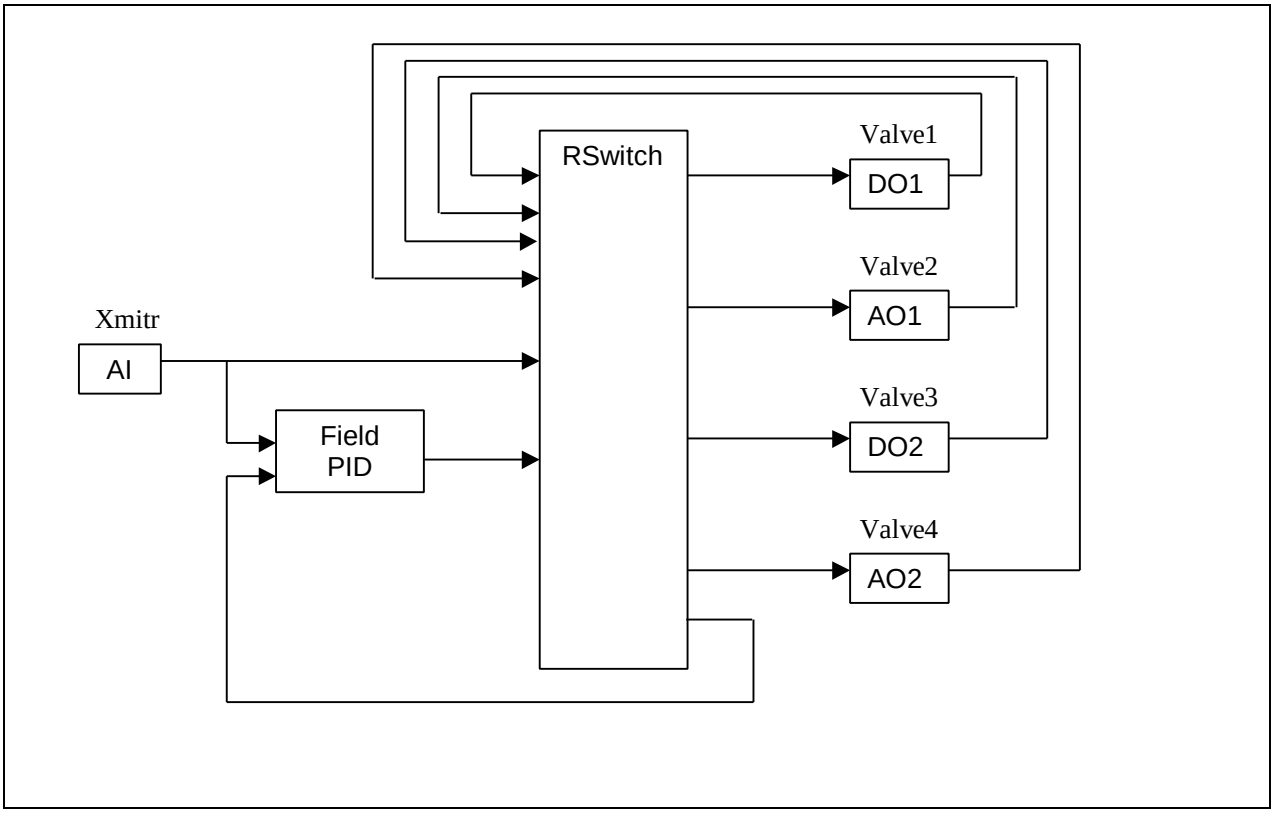


**Figure 4 - RSwitch and Redundant Valves**

An alternative involves a higher level of complexity and more hardware, but will provide more flexibility and reliability. Referring to Figure 4 - RSwitch and Redundant Valves, we see the RSwitch now connected to two throttling valves, each with an AO block, and two blocking valves, each with a DO block. This technique would require that the throttling valves be on parallel pipe sections downstream of a tee, and that the blocking valves are each in-line with their respective throttling valve as shown in Figure 5 - Parallel Valve Configuration. During normal operation, the output from the PID Controller is sent to AO1 and AO2. DO1 is opened and DO2 is closed. Normally AO1 is in control. If there is a failure detected by the throttling valve containing AO1, it will be communicated to the RSwitch block via the BKCAL_OUT parameter which is linked to the RSwitch Block's BKCAL_IN_1 parameter. If the valve or the RSwitch has determined that the error is sufficiently bad that it can no longer provide reliable service, DO1 is closed, DO2 is opened, and AO2 takes control. Also, the operator is informed of the failures using standard alarm features of FOUNDATION fieldbus.

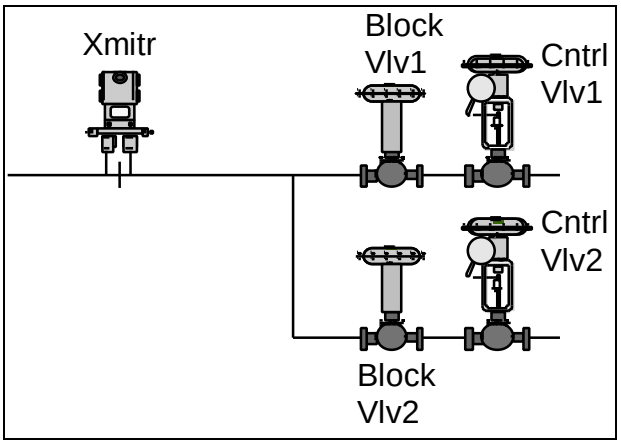


**Figure 5 - Parallel Valve Configuration**

## POWER REDUNDANCY

The most critical point in most control systems is power. Both electrical and pneumatic power are usually needed to keep a process under control. We will assume the systems engineer has dealt with the problem of redundant pneumatics or at least the system failure modes on the loss of air pressure. Electrical power is a little more interesting in so much as without it no device or human can tell what the current process situation is nor can they take action to rectify the problem. The electrical power supply to a FOUNDATION fieldbus segment has several potential failure points. While the power on the high voltage main coming into the plant is usually out of the control of the systems engineer, plugging in a second power supply into the same wall plug on the same circuit breaker on the same supply transformer only addresses the failure of the power supply itself. There are other possible points of failure which can be successfully addressed for many applications using one or more of several available techniques. Two of these methods are discussed here.

The first possibility is to have a backup power supply and battery backup in the same location as the main supply which is then switched on in the event of a failure in the main supply. An audible alarm could be sounded when this switch occurs. Also, FOUNDATION fieldbus enables the ability to add intelligence to the power supply. The power supply could contain a Resource Block that generates an alarm under certain conditions. Also, it could contain a Discrete Output block that sends a signal to the process when the battery is a configured number of minutes from being drained. This signal may be used to shut down the process in a known fashion before the battery in the power supply is exhausted.

Another technique that affords more protection is a secondary power supply at a separate location from the main power supply. When this power supply detects that the fieldbus voltage has dropped too low, it

will add a boost to the bus. Of course, it could contain alarms like the ones previously discussed. One of the benefits of having a backup power supply at a separate location is the addition of the ability to continue operation if the cable to the control room is accidentally cut. There are many issues to be dealt with in the use of a separately located backup power supply, such as where to put it, how to configure the terminators, etc. But, once these issues are properly worked out, this option provides a limited level of media redundancy in H1 fieldbus that is generally not recognized.

## LAS REDUNDANCY

A topic of great interest among our clients is LAS redundancy. The LAS, or Link Active Scheduler, in a fieldbus system is responsible for coordinating all communication on the fieldbus, i.e. it is in charge of the token. There can be one or more backup Link Active Schedulers on a fieldbus segment, in addition to the main LAS. If the active LAS fails, one of the backup LASs will automatically take charge of the bus. The one which takes over is a topic for another paper, so suffice it to say, one of the backups will take over, and it is a well ordered and reliable switch. The area of interest here is where to put the backup LAS(s). One possibility is in a secondary host such as a backup operator console, or a configuration device. This will provide backup in case of a hardware failure in the main host, but will probably not help in the event of a power failure to the control system.

Many people we talk to believe that every valve should have LAS capability since, without a valve, the process cannot be controlled (we do a lot of work with continuous process control). Since the role of the LAS is not a simple one, and is very cpu intensive, one of two things will be true of the valve with LAS capability. Either its performance characteristics will degrade to some extent when it takes over the role of LAS, or its performance characteristics will always be degraded to some extent when compared to the same valve without LAS capability. This performance degradation will not be a problem for many applications, but is something the user needs to seriously consider when assembling a redundant fieldbus segment.

Everything we just stated regarding valves is also true for transmitters.

With current technology the best place for a backup LAS is in a separate device that does not have any measuring or controlling functions. A field-based LAS whose only purpose is to take over the bus in the event of a failure in the main LAS. Furthermore, we believe that this backup LAS should be placed with each power supply. Simply put, if a power supply is lost and there is not a backup, it does not matter how may backup LASs there are, things won't work anymore. But, by placing an LAS with each power supply, maximum protection is achieved without adding more LASs than are needed.

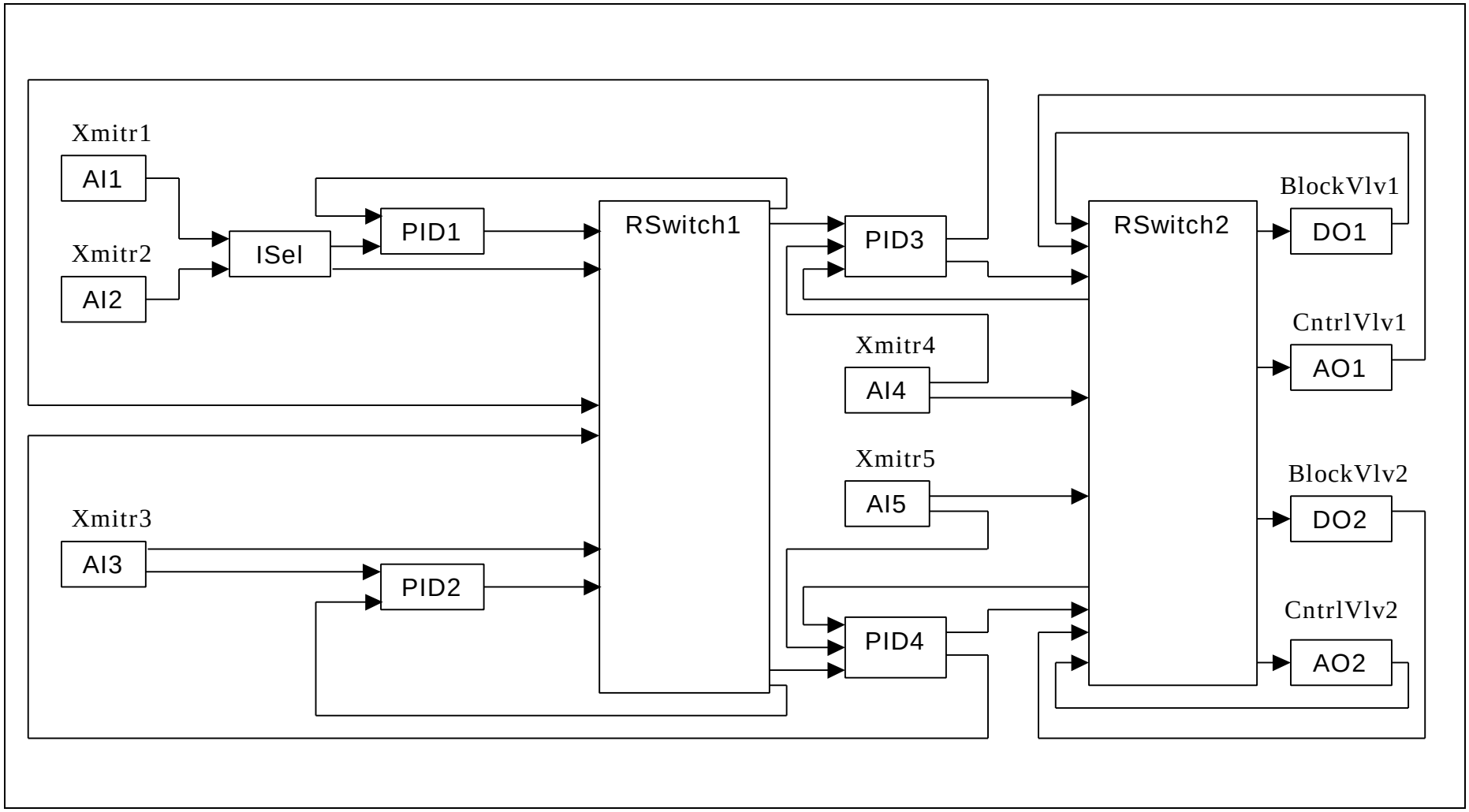


**Figure 6 - Example of Redundant Cascade Loop**

## EXAMPLE OF REDUNDANT CASCADE LOOP

**During normal operation of the example system shown in**

Figure 6 - Example of Redundant Cascade Loop and in Figure 7 - Redundant Cascade Transmitter and Valve Configuration, each output of AI1 and of AI2 is sent to ISel. The output of ISel is sent to PID1 and used as the controller's PV. The output of AI3 is sent to PID2 and used as the PV. The output of AI4 is sent to PID3 and used as the PV. The output of AI5 is sent to PID4 and used as the PV. Each output of PID1 and of PID2 is sent to RSwitch1 as is the output of ISel and the output of AI3. Using these inputs, RSwitch1 determines the correct output based on the inputs' status, and sends its output to PID3 and PID4 where the values will be used as each controller's setpoint. Back calculation values from RSwitch1 are sent to PID1 and PID2. The output of PID3, PID4, AI4, and AI5 are each sent to RSwitch2. RSwitch2 is connected to two control valves and two block valves and functions as shown in a previous example.

If either Xmitr1 or Xmitr2 fails, the ISel will take care of the backup switching. If the ISel fails, i.e. both Xmitr1 and Xmitr2 have failed, or if PID1 fails, RSwitch1 will switch to PID2. If AI4 or PID3 fails, RSwitch2 will switch to PID4. If RSwitch1 fails, PID3 and PID4 will automatically switch from cascade mode to auto mode allowing the operator to manually control the setpoint. If AO1 fails, RSwitch2 will close DO1 and open DO2 allowing AO2 to do the control. If RSwitch2 fails, all the valves would be set to their preconfigured fault state positions. And during all these failures, the standard alarm and status system would be informing the plant operator every step of the way.

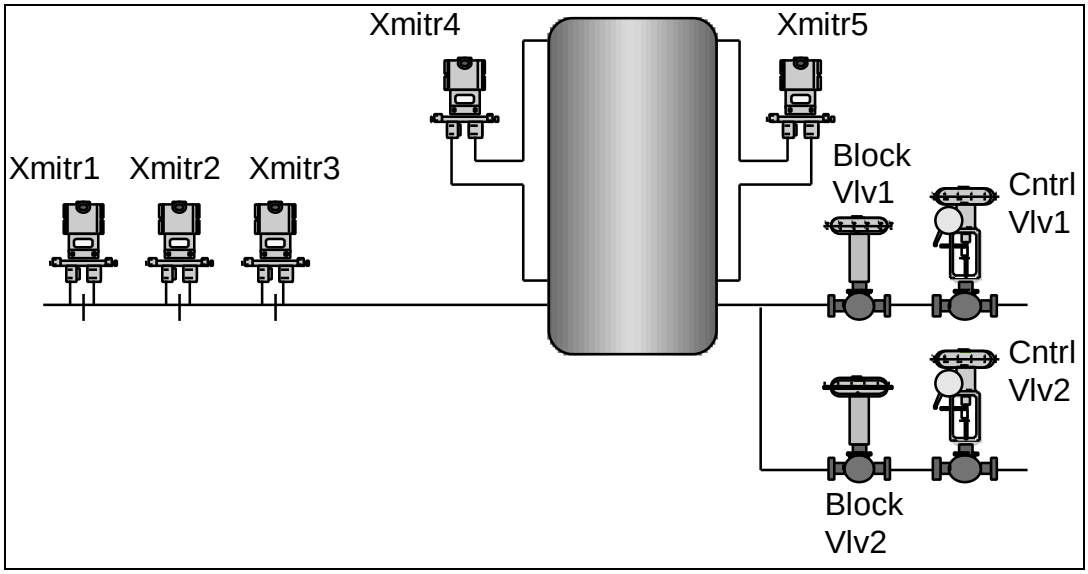


**Figure 7 - Redundant Cascade Transmitter and Valve Configuration**

## CONCLUSION

Something that the reader may or may not have noticed is that in some of the examples we do not show where many of the blocks reside. Other than the host controller examples, we do not show where the

controllers reside, we do not show where the RSwitch blocks reside, and we do not show where the ISel blocks reside. These are not shown because for most applications it does not matter where those blocks are located. We believe it is best if they are in the field near the process, but the engineer who is responsible for the application should decide where the blocks should be located dependant upon probable points of failure in that particular application. This is one of the strongest features FOUNDATION fieldbus has to offer. The system engineer has the flexibility to do what is best for each part of a particular application. He can determine the most likely points of failure, like the transmitter at the top of a tank that just doesn't seem to get as much maintenance as the other transmitters, and not put critical functionality there. He can hang controllers in DIN boxes in the control room, use the ones in the valves and in the transmitters, or hang one out in the field in a NEMA enclosure. Through this flexibility FOUNDATION fieldbus gives the engineer the ability to assemble a system that is best and safest for his unique application. With the examples presented here along with the many other redundant system possibilities that the flexibility of FOUNDATION fieldbus enables, a variety of redundant structures can be easily configured to provide a level of system availability consistent with a wide variety of requirements.