ATTACHMENT B

FAIL-SAFE DESIGN OF PROCESS CONTROL LOOPS GUIDANCE

(PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	11/17/03	Initial issue.	Mel Burnett, FWO-DECS	Gurinder Grewal, FWO-DO
1	10/27/06	IMP and ISD number changes based on new Conduct of Engineering IMP 341.	Mike Clemmons, *FM&E-DES*	Kirk Christensen, *CENG*
2	09/29/14	Administrative change. Changed from Appendix to Attachment.	Allen Hayward, *ES-EPD*	Lawrence Goen, *ES-DO*

CONTACT THE I&C STANDARDS POC

for upkeep, interpretation, and variance issues

Section D3060/F1050 App B	**Instrumentation & Controls POC/Committee**

1.0 PURPOSE

This appendix provides guidance for designing fail-safe process control loops.

2.0 SCOPE

Fail-safe protection is considered for loss of electrical power or air supply to any element in the instrument loop and for loss of the control signal to any valve or instrument in the control loop or between interconnected loops. The effects of sensing element failures are also discussed, as well as the affect of digital controller configuration details on loop reliability and safety. Items not considered are internal failures in instruments and retaining the last valve positioned after a failure.

3.0 DEFINITIONS

Direct Action – A device in which the value of the output signal increases as the value of the input (measured variable or controlled variable) increases.

Fail-Safe – A design characteristic by which a unit or system will attain a safe state and remain safe if a system or component loses its activation energy.

Intrinsically Safe – Equipment and wiring that are incapable of releasing sufficient electrical or thermal energy under normal or abnormal conditions to cause ignition of a specific hazardous atmospheric mixture in its most easily ignited concentration.

Overrange – Any excess value of an input signal above it upper range value or below its lower range value. The overrange limit is the maximum input that can be applied to a device without causing damage or permanent change in performance.

Reverse Action – A device in which the value of the output signal decreases as the value of the input (measured variable or controlled variable) increases.

Sensor – A device that responds to a physical stimulus from a process variable and converts the measurement into an electric or pneumatic signal.

Transmitter – A device that responds to the value of a measured variable and transmits a resulting signal. A transmitter may contain a sensor to directly monitor a process variable.

4.0 FAIL-SAFE ANALYSIS

A. The fail-safe analysis should establish the potential faults of each individual component within the process control loop and evaluate their effects on the final control element and the process.

B. The fail-safe analysis should determine the “safe direction” of the process medium that is measured to establish the desired response of the process control loop for potential faults and component failures. The Hazards Analysis, or other safety analyses, should be consulted for this information and reviewed as part of the fail-safe analysis. As an example, the safe direction when measuring temperature or pressure is usually toward lower temperature or pressure. However, for other measured mediums, the opposite direction may be safest.

C. The fail-safe analysis should identify the motive force(s) required for the operation of each component within the process control loop (e.g., power supplies, instrument air, hydraulics, etc.). In analyzing the ability of a process control loop to fail in the safest direction, the potential failure of the motive force(s) should be evaluated not only for their effect on the individual components but also for their effect on the final output response of the process control loop.

D. The fail-safe analysis should evaluate the effects of a loss or failure of the control signal on the individual components and the resulting effect on the final output response of the process control loop. The control signal is considered to be any command, actuation, alarm, or data signal(s) that is required to start, stop, or continue some operation.

5.0 FAIL-SAFE DESIGN PRINCIPLES

A. Fail-safe design can generally be implemented through the use of either direct action or reverse action sensors. A reverse action sensor should be used when a high value of process variable is unsafe and a direct action sensor should be used when a low value of process variable is unsafe. The fail-safe analysis should make the determination which type sensor is required and ensure that it results in a fail-safe condition. In some instances it may appear that the use of either a direct action or reverse action will result in a fail-safe process control loop, but this is not always the case. For example, a thermistor has a negative temperature coefficient of resistance and would seem to qualify as a reverse action sensor. However, since short circuits and open circuits would produce opposite results at the receiver, it is not fail-safe. Only when the sensor produces it own outputs can both short circuits and open circuits result in output signal loss (e.g., thermocouples).

B. Where a reverse action sensor is preferred but not available, signal reversal should take place as soon as possible in the process control loop. For example, an application involving a thermocouple-to-pneumatic converter in which reverse action is necessary, the reversing action should take place in the signal amplifier rather than in the current-to-pressure (I/P) transducer. In most applications, however, a reverse action transmitter will ensure that signal reversal occurs at the nearest possible point within the process control loop.

C. In addition to the implementation of direct action or reverse action sensors / transmitters, the design of a fail-safe process control loop should take into consideration the following design principles.

1. Design Integrity and Quality
2. Redundancy or Backup Systems
3. Isolation of Systems, Components, and Elements
4. Reliability
5. Failure Warning or Indication
6. Maintainability

6.0 FAIL-SAFE TRANSMITTER CONFIGURATION

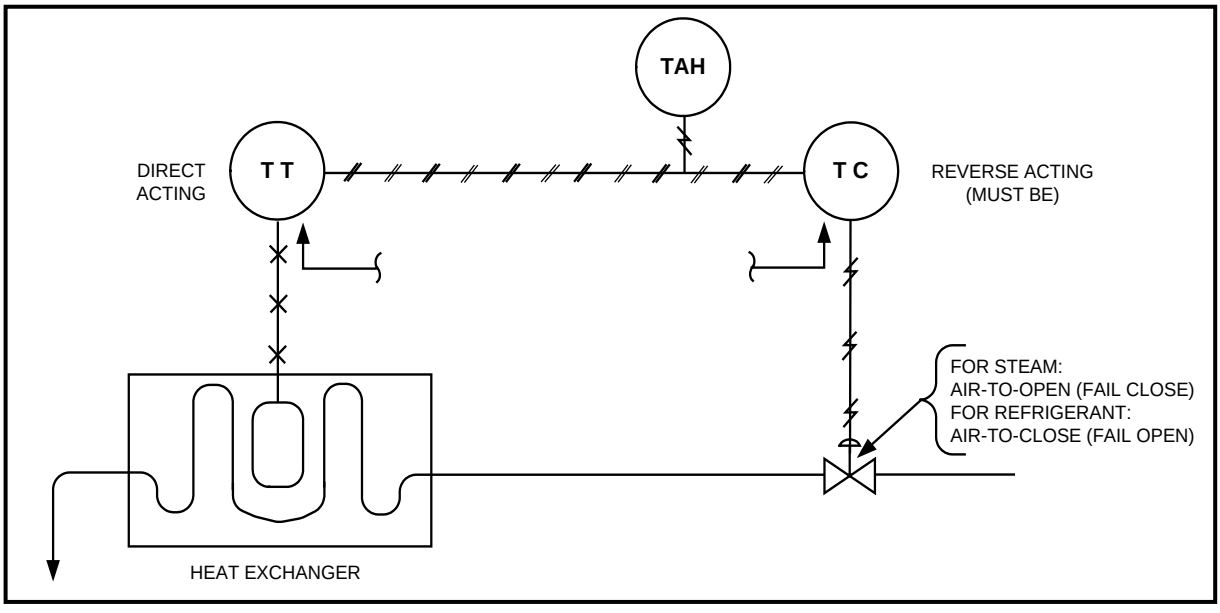
A. The loss of a transmitter output signal should cause a fail-safe action. A transmitter is considered to be any device that responds to the value of a measured variable and transmits a resulting signal. The transmitter may contain the sensor.

B. Short circuits, open circuits, and grounds may all cause the loss of a transmitter output signal. For a four-wire transmitter, the transmitter power is brought in on one pair of wires and the output signal is brought out on another pair. All 3 types of electrical failures in either the power or signal wiring pair result in loss of signal to the receiver. Partial shorts will lower the signal for either a current or voltage output signal. Under certain circumstances, full or partial shorts between particular power and signal wires could cause erroneous high signal indications. However, the likelihood of this latter occurrence is small.

C. For a three-wire transmitter, the output and power circuits share a single common conductor, but otherwise the considerations are the same as for the four-wire transmitter.

D. The unsafe action of an instrument loop due to the loss of the transmitter output signal can be illustrated by using a pneumatic temperature control loop as an example, see Figure 1 below. Assume that high temperature is unsafe and a direct action transmitter is used in the loop. A high pneumatic signal will therefore represent a high temperature. Accordingly, the controller interprets a full or partial loss of signal as a low temperature and attempts to correct the condition. The high-temperature alarm would not be actuated for this condition.

Figure 1: Simple Pneumatic Temperature Control Loop

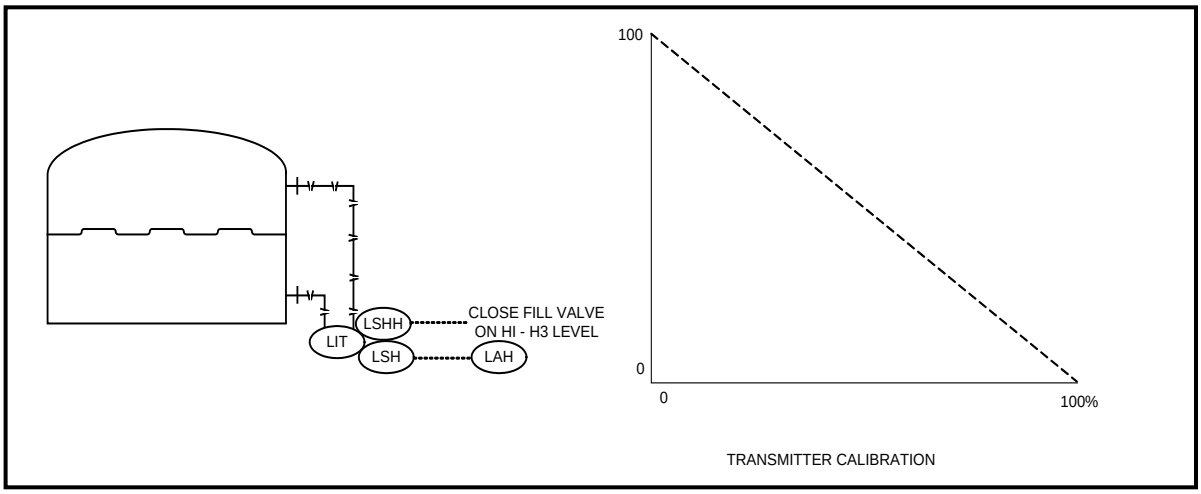


E. In the above example (Item B), the addition of a low-signal detector (alarm) may appear to be a solution, but this does not provide protection for any condition except the abrupt loss of signal. A gradual loss of the signal will cause the controller to compensate by increasing the process temperature, but there will be no indication that an abnormal condition exists. The addition of a redundant alarm circuit connected directly to the sensor (primary element) would detect this condition and would be recommended for this circumstance.

F. Where the use of a reverse action transmitter is preferred but not available, an alternative is the installation of a direct action transmitter close coupled with a reverse action relay. This may improve safety at the expense of system reliability and accuracy. This design, however, is inferior to a transmitter with built-in reverse action.

G. Reverse action may be obtained from a standard differential-pressure transmitter equipped with an elevation suppression kit. In this application, the high and low inputs are reversed and the suppression is adjusted such that zero differential produces one hundred percent output and full span differential produces zero percent output, see Figure 2 below.

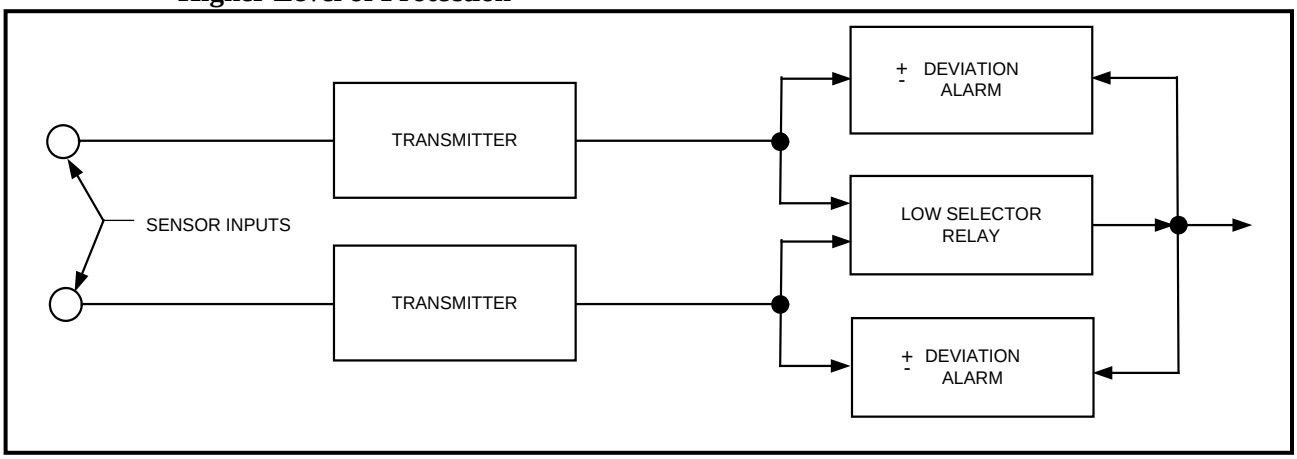
Figure 2: Differential - Pressure Transmitter Reverse Connected for Fail-Safe Operation



H. The fail-safe analysis may reveal that transmitter failures or unpredictable sensor faults will defeat fail-safe objectives. In such instances redundancy should be considered in addition to the above mentioned fail-safe design guidance.

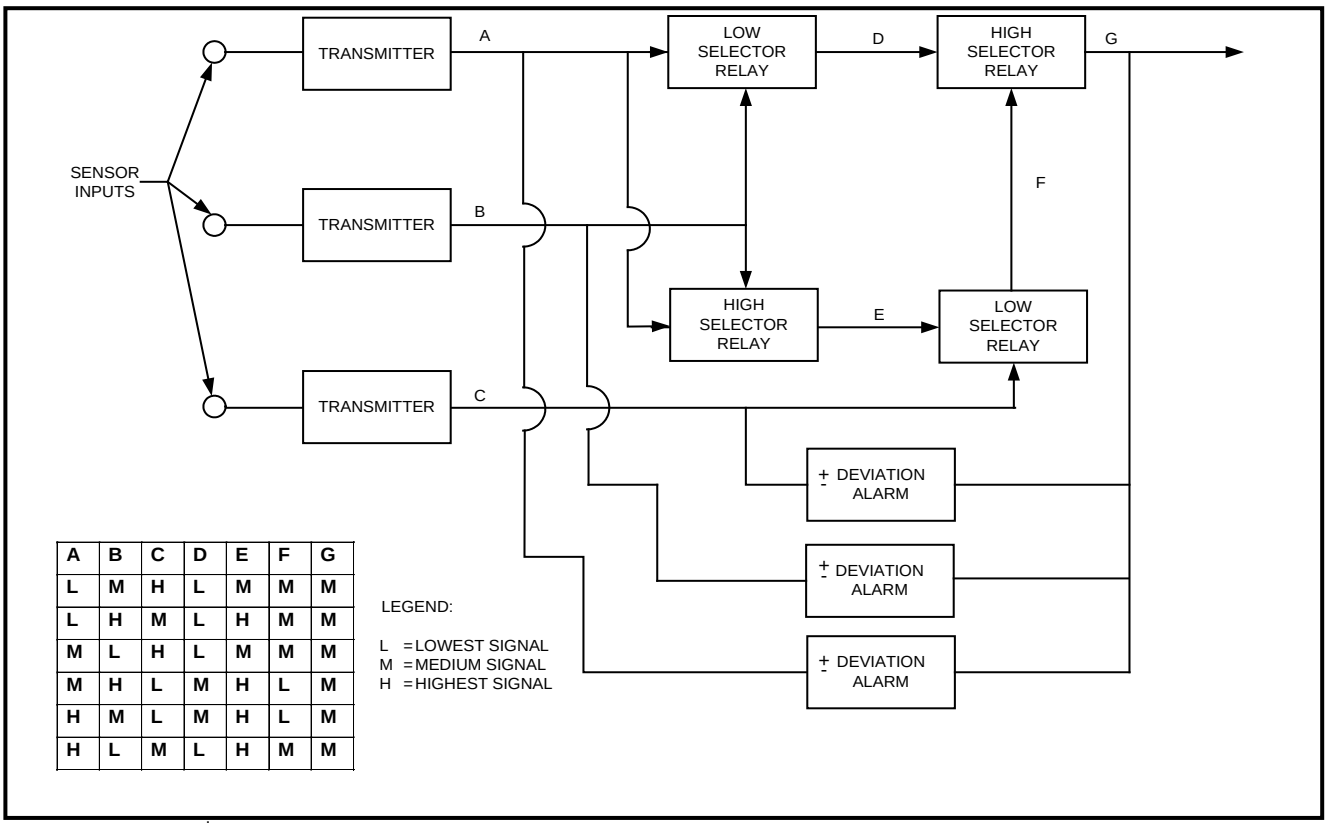
I. The fail-safe design of a process control loop with redundant transmitters should consider the addition of a low select relay on the output of the transmitters. As shown in Figure 3 below, the low select relay detects the lowest output of the two redundant transmitters. The resulting value is then compared to the output of each transmitter. If the comparison yields a deviation that is not within a preset acceptable range, the deviation alarm will be activated indicating a lost in transmitter redundancy. The deviation alarms will also detect possible failures of the selector relay, which will generally cause a deviation large enough to active the alarm. Only when both deviation alarms are tripped should an interlock shutdown be necessary.

Figure 3: Redundant Fail-Safe Transmitters With Low Selector Relay and Alarms for Higher Level of Protection



J. A three-transmitter median selector system is shown in Figure 4 below. The median selector is made up of two high selector relays and two low selector relays. A plus or minus deviation alarm comparing each transmitter output with the final output detects a transmitter failure.

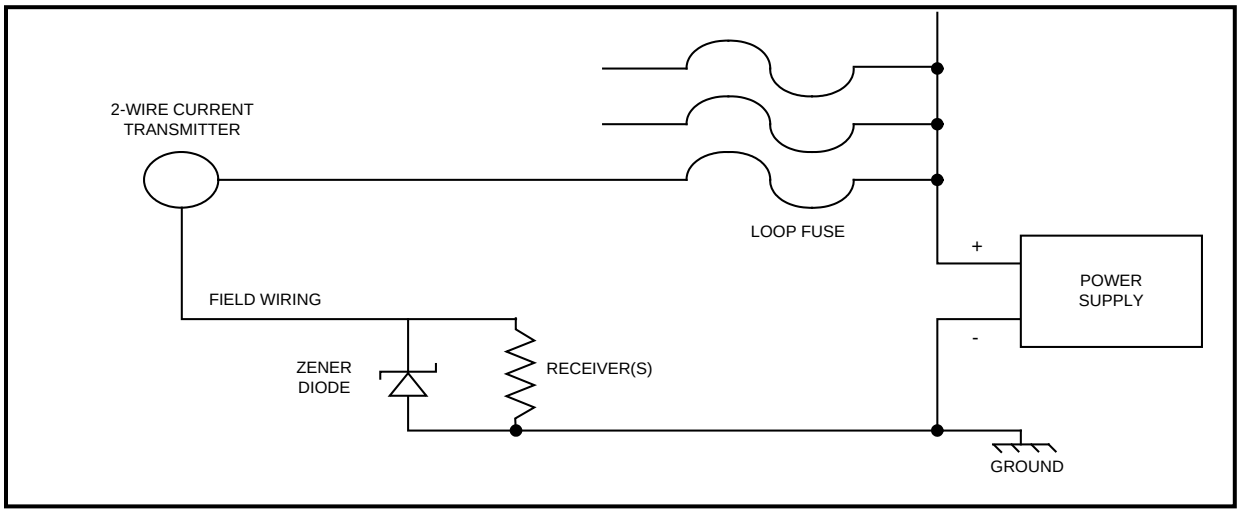
Figure 4: Three Parallel Transmitters with Median Selector and Alarms



A	B	C	D	E	F	G
L	M	H	L	M	M	M
L	H	M	L	H	M	M
M	L	H	L	M	M	M
M	H	L	M	H	L	M
H	M	L	M	H	L	M
H	L	M	L	H	M	M

K. Components of a process control loop that are located within a hazardous area should be made intrinsically safe. A two-wire transmitter is shown in Figure 5 below with an intrinsically safe barrier. The addition of a zener diode and a fuse to the circuit protects against all but partial short circuits (leakage) across the transmitter terminals. The zener diode will not allow the voltage across the transmitter input to exceed the rated zener voltage. Excess voltage will cause the zener diode to conduct, which will blow the fuse. The zener voltage is selected so that conduction begins at a reasonable overrange of signal. Intrinsically safe transmitter circuits often add resistors in the loop to limit any fault current to a moderate overrange of signal. It may be difficult, however, to obtain a fuse that will blow under this circumstance.

Figure 5: Increased Protection for 2-Wire Systems



7.0 FAIL-SAFE CONTROLLER CONFIGURATION

A. The fail-safe analysis should acknowledge that the failure mode of some digital controllers is unpredictable.

B. Digital controllers implemented through a fail-safe design should have features such as self-diagnostics, field device diagnostics, internal redundancy, and integrated event recording and alarm notification.

C. In the event of loss of power, most digital controllers can be configured for any of several different ways to restart on power restoration. Controllers also provide configurable options on whether or not to use set point tracking. While these combinations of features can provide some powerful advantages, some combinations of the selected configuration parameters could result in a possible unexpected and unsafe operation on restoration of power. The configuration of the controller should be carefully selected to obtain the desired fail-safe response of the process control loop.

8.0 FAIL-SAFE CONTROL ELEMENT CONFIGURATION

A. It is essential that the final control element be properly specified to assure that failures in its signal or energy source produce a safe process state.

B. The direction of action for a fail-safe control element (e.g., air-to-close or air-to-open) can be chosen based upon knowledge of the controlled variable. For example, if a valve positioner pressure booster relay, or current-to-pressure transducer is used, it should not reverse the relationship between the transmitted signal and valve actuator pressure. Loss of supply or transmitted signal should result in a safe direction of action for the control element.

C. Loss of supply or transmitted signal should result in a safe direction of action for a control element. Process interlocks or alarm should be configured to alarm on loss of signal.