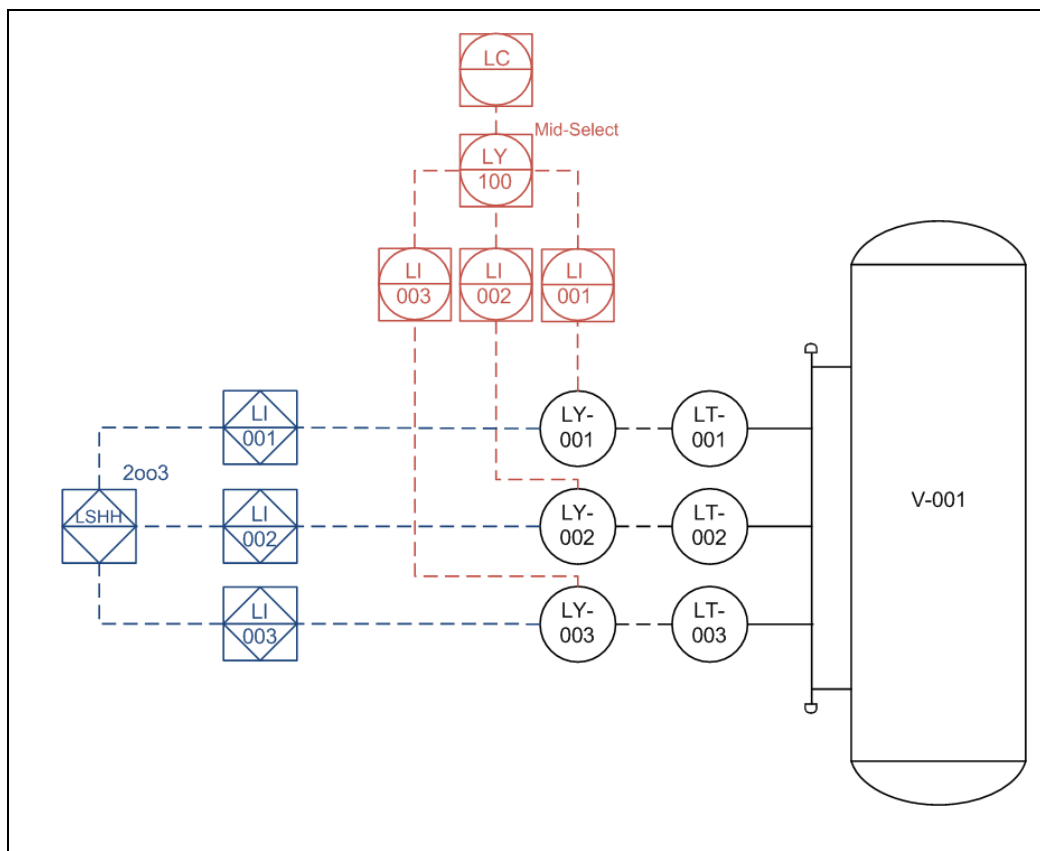


## Memorandum

From:	Kevin J. Mitchell
To:	Professional Staff, Technical Memo File
CC:	
Re:	Acceptable Sharing of BPCS and SIS Field Measurements
Date:	4 Dec 2008
Reference:	TM010.emm
Keywords:	

Many users of safety automation equipment employ a practice of using redundant field devices on safety-critical process measurements (e.g., level transmitters, flow transmitters, pressures transmitters, etc.). These users, who are often in the petroleum refining industry, typically use these measurements in a 2oo3 (two-out-of-three) vote to shutdown using triplicated field instruments, with this logic being implemented in the Safety Instrumented System (SIS) logic solver. Less commonly, some also use these same three signals as inputs to the basic process control system (BPCS), usually with a mid-select function for feedback control of a process variable. This practice involves splitting each of the three signals with one analog input to the Safety PLC and one analog input to the BPCS. Signal repeaters are typically powered by the SIS. This is shown in the diagram below.



ISA and IEC standards for SIS encourage users to separate field devices used in BPCS from field devices used in the SIS. The intent is to ensure that no device that is used in BPCS can fail in a way that inhibits or degrades the performance of the SIS. This position would argue that the shared transmitter practice of shared BPCS and SIS transmitters in a 2003 vote is not compliant with ISA and IEC standards for SIS. The ANSI/ISA 84.00.01-2004 standard *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* (harmonized with the IEC-51511 standard) states:

*Clause 11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependence between the SIS and BPCS, and the SIS and other protection layers. And*

*Clause 11.2.10 A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable.*

Therefore, allowance is made for situations where sharing BPCS / SIS field devices is suitable from the perspective of risk. In precise terms used in risk analysis, shared signals for BPCS and SIS only become a problem when there is a potential for a transmitter failure that inhibits or degrades the performance of the SIS while simultaneously creating a demand for the SIS to take action by causing the BPCS to malfunction in a way that initiates a hazardous condition. For example, if loss of liquid level in a vessel could result in a hazardous "gas blow-by" event, a single level transmitter that is used for both control and safety could fail in place above the set point. This would falsely indicate a high level. In this scenario with a single transmitter and a 1oo1 vote to trip, the SIS would be unaware of any subsequent low level conditions. Simultaneously, the BPCS would sense high level and take action to drive the level in the vessel lower. Because the transmitter has failed in place, the level would continue to drop until a hazardous low level condition occurred. Clearly, this is not an acceptable level transmitter configuration for safety-critical applications.

Conversely, shared signals for BPCS and SIS are not an issue in risk analysis terms when there is no potential failure mode of the BPCS control loop that would place a demand on the SIS. One example in would be backflow prevention safeguards afforded by shared flow transmitters. The SIL Selection team identified no failure modes for flow control loops that could result in a potential hazardous backflow condition occurring. This hazard would only occur if charge pump fails. No demand would occur for the SIS to trip even if flow transmitter(s) were in a failed state.

In the refining industry, we commonly observe use of three transmitters in a 2oo3 vote to trip in the SIS and a mid-select function in the BPCS. When 3 transmitters are operational, no single transmitter failure would simultaneously inhibit the SIS and initiate a hazardous condition that would place a demand on the SIS. However, not all

transmitter modes-of-failure that would traditionally be safeguarded by a typical 2oo3 vote to trip are being safeguarded by this practice.

Kenexis has identified the following failure modes that are unprotected by the SIS:

- Two transmitters failed in a dangerous undetected mode such as “fail-in-place”. This would defeat the protection afforded by the SIS. In this case, the demand for the hazardous condition would occur simultaneous with the failure of the second transmitter. Because three transmitters are used to sense the same process variable, deviation alarms could be used to diagnose a single transmitter being failed-in-place.
- A common cause failure mechanism that simultaneously defeats all three transmitters. Note: this failure mechanism could not be argued to be safeguarded against by providing additional transmitters that physically separate the BPCS and SIS.
- The SIS has degraded to a 1oo1 vote due to diagnosed failures of two out of three transmitters. Repair to either transmitter has not yet occurred. In this time interval, a single transmitter is now being used for both control and SIS protection. If this transmitter were to fail dangerous undetected mode (e.g., fail-in-place) prior to repair of the remaining two, the SIS would be inhibited and the BPCS would simultaneously initiate a hazardous condition that would result in a demand on the SIS. Using administrative procedures that ensure faulted transmitters are repaired within a relatively short time-frame (e.g., 72 hours) would greatly reduce the likelihood of this scenario. This would be covered under procedures for defeat of critical safety systems and temporary operation with Safety Instrumented System in bypass.

Kenexis advises our customers that ISA / IEC standards do not promote use of the practice of sharing BPCS/SIS transmitters. Further, Kenexis advises our customers on the potential failure modes which are not protected by the SIS when using this practice, which are limited to the above four identified interlocks.

Some customers consider these risks to be tolerable given the engineering design and strong administrative controls that are in place for these systems. Others prefer the more traditional separation of BPCS and SIS transmitters. ANSI/ISA standards on SIS allow sharing, but require additional analysis of failure modes, the likelihood of failure, and an assessment of the risk.

For additional information, contact Edward Marszal or Kevin Mitchell at Kenexis.