

## Memorandum

From:	Kevin J. Mitchell
To:	Professional Staff, Technical Memo File
CC:	
Re:	When is Separation of BPCS and SIS Necessary?
Date:	06 September 2005
Reference:	TM005.emm
Keywords:	Separation, Combined Systems

"Separation of Basic Process Control and Safety" is an overriding principal that – to great a extent – governs the design of safety instrumented systems (SIS). Design standards such as *Application of Safety Instrumented Systems for the Process Industries* ISA 84.01 state that it is generally necessary to provide separation between basic process control and SIS functions. While this is usually a prudent design practice, it is reasonable to ask what circumstances require strict separation, and what situations would reasonably allow for the a safety instrumented function using one or more components defined to be within the Basic Process Control System (BPCS).

To answer these questions, consider some of the principals that guide designers of safety shutdown systems. One guiding principal is that the SIS should continue to protect the plant in the presence of partial or total failure of the BPCS. More precisely worded, no safety function (SIF) in the SIS should be allowed to be inhibited by a failure of any component the BPCS. This is a mantra of control system designers which generally leads to a standard – yet often excessively conservative – design; but, it has little or no basis in the principals of hazard and risk analysis.

From the perspective of the risk analyst, a safe process design is one that reduces the risk of a specific hazard to a level that is considered tolerable. The risk of a hazard can be expressed in terms of the likelihood of the event and the potential hazard severity. The SIS most-often reduces the likelihood of an undesirable consequence, but only after an initiating event (or cause of the hazard) has already occurred. The initiating event is the beginning of the chain of events that could ultimately result in a hazard – and it is identified as being a failure of the BPCS. The safety shutdown function is one of (possibly several) independent protection layers – or the opportunities to break the chain of events before a hazard occurs. In order to be reasonably assured that the safety shutdown provides 'real' risk reduction, the failure resulting in the initiating event and the failure of the safety shutdown should be 'independent events'. Any single point of failure, such as failure of a transmitter, failure of a logic solver I/O module / processor, or failure of a final control element should be evaluated to determine if it violates this criterion.

If any component of the BPCS could fail in a manner that simultaneously defeats the protection provided by the safety function and initiates the hazard scenario, we have a design that presents the opportunity to short-circuit a defense in depth philosophy

toward reducing risk. Most companies that have experienced an accident as a result of this type of failure have taken the position that no single point of failure should simultaneously inhibit protective functions and initiate an accident scenario.

Consider a pressure protection system that shuts down a distillation column on high pressure. The designers intend for this system to protect against a high pressure event caused by BPCS malfunction. In this example, the designers improperly used the same pressure transmitter for distillation column pressure control and to initiate the high pressure shutdown of heat input to the column's reboiler. If this transmitter fails in place below the set point, the control system will attempt to increase column pressure, while at the same time the safety shutdown will be inhibited – the sensed pressure would never exceed the trip point. This would be prime example of a situation where strict separation of BPCS and SIS would be warranted. A sound basis for SIS design would require separate sensors, separate logic solvers, and separate final control elements.

Consider a similar, but slightly different example. Designers intend to install a high pressure shutdown not to protect against overpressure of the distillation column itself, but against overloading the flare system on total loss of plant power. Under this scenario, numerous other columns and other equipment would attempt to simultaneously relieve to the flare system, thereby overloading it. In this case, the malfunction of the BPCS remains a credible scenario that could result in overpressure and relief to the flare, but adequate emergency pressure relief capacity exists without the benefit of the high pressure shutdown function. Although the high pressure shutdown function could benefit this situation, it is not necessary nor is the design intended to safeguard against BPCS control malfunction. In this example, the only initiating event of concern is total plant power failure – a scenario that is completely *independent* from the BPCS. The use of a BPCS pressure transmitter might be permissible for this example, subject to other restrictions on achieving the required Safety Integrity Level or SIL for this function.

Usually, separation of BPCS and SIS is a prudent design practice. However, Kenexis has analyzed numerous process hazards and control system configurations where strict separation of BPCS and SIS is not necessary, and - in some cases – is not warranted. By examining the specific hazard being prevented, the initiating event(s), and the level of risk, a design with an appropriate degree of safety will be achieved. By understanding the practical requirements for separation of BPCS and SIS, limited resources for SIS design and maintenance can be allocated more efficiently.