

### F.3.5 Logic Solver Separation

In older installations, separation was assured because the PIS (or SIS) was typically implemented as an electrical system using electromechanical equipment housed in an access controlled (often locked) cabinet. Control functions were executed by pneumatic controllers. The BPCS and PIS were physically separate and were diverse in many aspects, including manufacturer, technology, installation, support systems, and even maintenance support.

The interaction between the BPCS and PIS is now much more complex. Field devices are often shared as discussed in Section F.4, and there may be extensive communication between the systems as discussed in Section F.6. However, experienced engineers and many good engineering practices continue to recommend implementing the PIS in a physically separate logic solver from the control functions. Some of the reasons for this include:

- Restricts communication to ensure that corrupted control system data does not corrupt the PIS,
- Limits the amount of logic to validate when software changes are made,
- Improves PIS application software integrity by ensuring that on-line changes to the control system software do not alter the PIS application software,
- Makes the PIS distinct, supporting access security and management of change, and
- Reduces the chance of human error (e.g., PIS typically require fewer changes than the control system).

SIFs cannot be implemented in the BPCS. When control functions and SIFs are implemented with a single system, all functions--control and safety--must be managed with the rigor of the SIS management system. The requirements of ISA 84.01/IEC 61511 apply to the entire system, including documentation, user approval, validation, access security, and management of change. If the control functions can place demands on SIFs executed in the same system, the system must meet the overall hazard rate requirements.

A major justification for separation is reduced long-term administrative costs. When layers are combined the management system of the highest layer applies. Means should be provided to restrict access, to limit communication to other systems and to control system changes. Generally the cost of separation is significantly less than the administrative cost to maintain the required rigor. The administrative rigor must be maintained for the life of the system, including the provision for necessary resources to verify and audit compliance.

Adequate separation is achieved by administrative controls and physical means. Physical separation is provided at the system level by executing the functions in separate and, often diverse logic solvers. Access security and management of change is enhanced by physically separate systems. When the

BPCS is physically separate from the PIS, the need to access the SIS is reduced and the BPCS can be managed under a less rigorous management system.

Separation ensures that the BPCS and PIS are not dependent on each other to operate. It also provides a clear and unambiguous distinction between the BPCS and PIS, which supports long-term access security and management of change. Separation also ensures that when maintenance and testing is conducted on one system the other remains available.

A common cause analysis should be performed on the BPCS and PIS to identify shared equipment. This analysis should consider the equipment necessary for operation of each function, such as the sensors, final elements, input/output (I/O) modules, main processors, utility, and application software, support systems, and communications. Functional separation is achieved when it is possible for all non-PIS components to fail dangerously and the process equipment still be taken to the safe state.