Integrating Control and Safety: Where to draw the line.

Robin McCrea-Steele, TÜV FSExpert
Invensys-Premier Consulting Services

New digital technology now makes it feasible to integrate process control and safety instrumented functions within a common automation infrastructure. While this can provide productivity and asset management benefits, if not done correctly, it can also compromise the safety and security of an industrial operation. This makes it critically important for process industry users to understand where to draw the line. Cyber-security and sabotage vulnerability further accentuate the need for securing the Safety Instrumented System (SIS).

Certainly, a "common platform" approach, using similar hardware and software dedicated for control and safety functions, respectively, can arguably provide some cost savings. However, it is widely acknowledged that utilizing separate, independent, and diverse hardware/software for safety and control is the optimal way to protect against potentially catastrophic common cause and systematic design and application errors.

Different vendors offer varied degrees of integration and solutions. The question is how to provide an integrated control and safety solution with advanced functionality and productivity, without compromising safety and security. So where do users draw the line?

The answer may lie in a recent "Zoomerang" survey of chemical, oil, and gas process plant operating companies conducted by Invensys. The survey responses revealed that 78% of the over 200 respondents adhered to strict separation of safety and control for safety protection. Additionally, 74% of respondents indicated that independent protection layers (IPL) were critical and 66% gave common cause as a major concern.

In the same survey, only 8% indicated that "diversity" was not a concern, while 89% of users said that their ability to choose best in class for both safety and control was important.

The results of this survey, combined with in-depth discussions with a much larger population of process industry end-users around the world, clearly indicate that the majority of end-users draw the line at maintaining independent layers of protection and diversity between their safety instrumented and process control systems.

The importance of Independent Layers of Protection

The whole basis for the concept of "defense in depth (D3)" and "independent protection layers (IPL)" at the heart of all the international safety standards (including IEC 61508 and IEC 61511), is that every layer of protection, including both control and safety,

should be completely independent. Some of the reasons for this basic requirement are to avoid common cause faults, minimize systematic errors and provide security against unintentional access, sabotage and cyber-attacks. Merging two layers of protection is a safety incident waiting to happen.

A recent University of California at Berkeley Civil Engineering study reported that the Engineers Corp. in charge of building and supervising hurricane levees, started to change their culture from safety to efficiency in the mid 1970's. Hurricane Katrina uncovered the systematic engineering design problems 30 years later. In the processing industry, the ramifications of the current temptation to cross "the line" by merging the IPLs' may be only revealed by a major chemical disaster in the future.

Those process industry users who currently find themselves at a crucial fork in the road should thoroughly understand the potential ramifications of compromising safety and security by merging independent layers of protection. Keeping these layers independent is clearly the path of zero compromise; the path that will reduce risk to a level as low as reasonably practicable (ALARP).

Interpreting the Safety Standards

Performance based standards, such as IEC 61508, IEC 61511 and ANSI ISA-S84.00.01-2004, are intended to open the doors to creative engineering implementation. Rather than dictating a specific configuration, these standards set performance criteria goals. The problem arises when the performance criteria are taken selectively or out of context.

Some control systems vendors seem to have been stung by the "creativity" bug. However, rather than having process safety being driven by technology, we should be using new digital technology to integrate at the information, predictive maintenance and HMI level.

IEC 61511-1 clause 11.2.4 states that the BPCS (Basic Process Control System) shall be designed to be separate and independent to the extent that the functional integrity of the SIS is not compromised.

Several automation vendors seem to have selectively interpreted this paragraph to mean that the standard does not require physical separation or diversity.

However, another section of the same standard IEC 61511-1, clause 9.5, addresses the requirements for preventing common cause, common mode and dependent failures. Clause 9.5.2 states that the assessment shall consider (a) independency between protection layers, (b) diversity between protection layers, (c) physical separation between protection layers and (d) common cause failures between protection layers and BPCS.

The question is, how do you conform to clause 11.2.4 without physical and diverse separation? IEC 61508 and IEC 61511 acknowledge that it is virtually impossible to assess the failure rate of software and furthermore cannot quantify a target criteria goal for systematic failures.

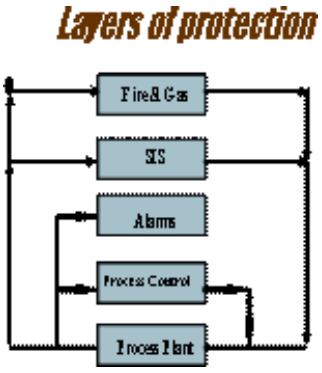
Attempting to overcome the problem of separation and diversity with increased reliability and self diagnostics is definitely not the right approach. Focusing only on the PFD, reduces the criteria to reliability engineering, which cannot accomplish safety on its own. Systematic errors, common cause errors and software errors form an integral component of the overall safety assessment.

ISA TR84.00.04 part 1 is designed to be a guideline for the interpretation and implementation of IEC 61511. This technical report has many good recommendations, including Annex F section F.4 where it addresses physically separate and diverse SIS logic solver as a having served the industry well and a way to virtually eliminate common mode failures.

Although no one really challenges the advantage of physical separation and diversity, the issue, for some, seems to have come down to "how far can I push the interpretation of the standard?" Designing your systems down to selective paragraphs while ignoring the intent of the standards, is not conducive to providing a safe working environment through good engineering practices.

The difference between "risk-based" and "risk-informed" decision making is that the numbers should only be used as one input to the decision making, rather than an absolute measure. "Defense in depth" should be a cornerstone of any safety system design.

As a user, with responsibility over process safety, one should not get blinded by new marketing terminology such as "integrated functionally separate safety and control". Physical separation and diversity are the only ways to guaranty complete independence of layers of protection. Commingling control and safety only exacerbates the problem……and the risk. Compromising safety for design flexibility or a lower price is unconscionable.



Other Prescriptive Application Standards on Separation

In addition to the performance based standards discussed above, a number application specific prescriptive standards also will apply. For example:

- NFPA 85 - Boiler and Combustion Systems Hazards Code 2001- clause 1.9.3.2.3 Requirements for Independence. *"The logic system performing the safety function for burner management shall not be combined with any other logic."*

- API 14C - Basic Surface Systems for Offshore Production Platforms- Paragraph 3.3 and 3.4 page 11. *"Two levels of protection should be independent of and in addition to the control devices used in normal operation."*
- API Recommended Practice 554 (1995)-Process Instrumentation and Control *"The shutdown and control functions should be in separate and idependent hardware"*
- IEEE 1993 Standard for Digital Computers in safety of Nuclear Power Generating Stations 7-4.3.2 - *"Isolation needs to be considered in order to prevent fault propagation between safety channels and from a non-safety computer."*
- IEEE 1992 Standard 384 - Standard Criteria forIndependenceof Class 1E Equipment. *"Class 1E circuits shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of a failure of non-safety equipment"*

If process safety is your concern, physical and diverse separation / isolation between the SIS and the BPCS is good engineering practice, conducive to a safe working environment.

Effect of integration on the SIL requirement

The level of control-safety integration may affect your SIL requirement. For example, if you used LOPA or another SIL assignment method that incorporates credits for external layers of protection, and credit was taken for the control system's integrity and reduction of demands on the SIS, you may need to re-assess the study.

An integrated control/safety system which has crossed the line of separation of independent layers by either embedding a same technology SIS logic solver in the control system or using the same operating system, may have systematic design and common cause errors that invalidate any credit taken for the independence of the BPCS layer. The bottom line is that the safety integrity of the safety instrumented function may have been compromised.

If the HAZOP/SIL assignment process determined that a certain safety function required a SIL2, and now no credit can be taken for the BPCS as an IPL, then the new assessment will most likely determine an increased requirement (i.e. a SIL3) for that safety function.

Any cost savings of the integrated control/safety system would, in this case, be wiped out. As a matter of fact, the costs would increase if additional field redundancy and proof testing is required to meet the new target SIL.

Cyber-security concerns

We are all well aware of how hackers, viruses, trojans, worms, etc can penetrate firewalls, break password securities, and in general create havoc in a computer network system.

The vulnerability of a safety system "integrated" with a control system that in turn is connected to a site LAN and/or corporate WAN is increased exponentially.

Remote process monitoring as well as remote diagnostics, maintenance and asset management through web connectivity have become an efficient tool. However, firewalls and passwords are only another challenge to hackers. In time and with focus, they are routinely broken. The safety system, as a last line of defense, needs to be secured.
A computerized waste treatment plant in Queensland, Australia, was hacked by an individual who had worked for the contractor that installed the system and was angry over a rejected job application. The hacker managed to divert millions of gallons of raw sewage in to city waterways and rivers.

Insiders, disgruntled employees, web hackers and terrorists are all real threats to the process industry. Media Corp-News Asia- reported on October 4th, 2005 that 500 computer hackers in North Korea were given a five year military university training program with the objective of penetrating the computer systems in South Korea, USA and Japan.

Even multiple firewalls and intrusion detector systems are not enough. All systems are vulnerable. There is no such thing as absolute security, only layers of protection.

Q

The Question:
How to provide an integrated solution with advanced functionality and productivity without compromising safety and security?

Most plant operators in the chemical, oil and gas industry (as shown by the Zoomerang survey conducted by Invensys, referenced earlier) believe that the answer is to maintain strict physical separation and diversity between the process control and safety instrumented functions, while facilitating secure integration at the information, diagnostics, configuration, and HMI levels. This is where the line should be drawn. Process industry users should demand this level of integration from their automation vendors.

Solutions that advocate functional integration with the SIS "embedded" in the control system and based on the same technology, are prone to systematic, common cause and cyber-security issues. It is not enough to dedicate separate mission specific modified DCS modules for the SIS logic solver within the control system.

Furthermore, any level of integration that merges layers of protection will have a detrimental effect on the target SIL of the safety instrumented functions.

Users are not about to compromise safety and security of their plant.

The bottom line is that the independent layers of protection need to be just that. Independent.

Robin McCrea-Steele, TÜV FSExpert
Invensys-Premier Consulting Services
Irvine, California- USA

Senior Safety Consultant / Director of PCS Business Development.
Certified TÜV Functional Safety Expert I. D. 0101/04 and approved instructor for the TÜV ASI Rheinland Functional Safety Program.
AIChE Member, ISA Senior Member and SP84 committee member working on the Safety Field Bus task force.
Specialized in process safety consulting and risk assessments
Robin has presented multiple technical papers at industry symposiums and has been published in various safety related magazines, such as InTech, Control Solutions International, Hydrocarbon Engineering, Control Magazine, etc.