Don’t Compromise on Safety

Definitions

Safety – The quality of averting or not causing injury, danger, or loss.

Compromise – An agreement reached by adjustment of conflicting or opposing claims, principles, etc. – An endangering, especially of reputation; exposure to danger, suspicion, etc.

This paper will examine these two words and how they are/do not/should not coexist in the Process Industry.

The Responsibility for Safety

The first thing that must be understood when discussing safety is who is responsible for the safety of a process plant? Is it the EPC? NO! Is it the Main Automation Contractor? NO! It is the owner of the facility. Safety is the owner’s responsibility and the owner’s commitment to the people working the plant, to the community where the process equipment is located, to the shareholders, and to the long-term wellbeing of the environment.

This is not a responsibility that can be delegated or passed off to another entity. The Owner/Operator has complete and sole responsibility for the safe operation of the process equipment and facilities it owns and operates.

It is the owner’s responsibility to avert or not cause injury, danger, or loss.

The Consequences

The consequences of not averting injury, danger, or loss are vast.

- In 1984, an incident in Bhopal, India killed between 3,000 and 5,000 people. Total deaths attributable to this incident to date exceed 23,000.
- In 1988, 167 people died when the Piper Alpha platform exploded in the North Sea.
- In 2005, 15 people died as the result of equipment failures at Texas City, Texas.

These incidents might seem extreme and scattered over time. It might be easy to believe that they are isolated incidents, but look at the facts. As of September of 2012, the Chemical Safety Board lists 14 ongoing investigations. Every year approximately 100 process plant personnel are killed and several hundred are injured globally.

The consequences of inadequate safety, while infrequent, are far too high to ever make compromises regarding its implementation.
A Little History

Faced with the issue of potential death and injury, not to mention lost production and reduced availability of resources, asset owners began in the 1960s to attempt to build systems that would shut plant operations down quickly and safely in the event of emergencies.

These systems, called ESD (Emergency Shut Down) or SIS (Safety Instrumented Systems), were designed from scratch to be independent of the basic process control system and operate from redundant controllers with redundant field devices that could be tested independently of the operation of the plant.

As the basic process control system (BPCS) grew into the modern distributed control system (DCS), and communications between field controllers and the control system master became faster and began to use common digital bus protocols like Modbus and Ethernet, engineers at vendor companies began to see how SIS systems could be interconnected with the DCS on a common platform and a common bus, but with separate but equal operation.

Several DCS vendors now have combined DCS and SIS control system offerings. The argument is that the redundancy of the SIS removes the potential for single point of failure issues, and that the common engineering and operations platform, in this age of fewer trained and experienced individual workers outweighs any potential for interactive failure modes between the DCS portion and the SIS portion of the system.

The operative theory is that this is a workable compromise that benefits both the safety and reliability engineers and the operators and process control engineers. It also benefits the control system vendor, who now has the ability to provide both the BPCS and the SIS. The question is, does it really benefit the asset owner with increased safety or reliability or asset availability?

A Little More History

In the time period from about 1960 to 1980, most process companies had their own central engineering department, which handled design, integration and commissioning of the automation systems (both BPCS and SIS Systems) for their assets. Beginning in about 1980, however, the economic situation became one of layoffs and cutbacks, and such central engineering organizations became rather thin.

There was, however, still a need for a knowledgeable organization to integrate the systems, write whatever code was necessary, build marshalling cabinets and junction boxes, and assemble, test and commission the automation system in a plant, whether it was a new plant or an upgrade.

Enter the MAC

In order to optimize the use of their own products and to fill the engineering void, first one, and then another and finally all the major DCS vendors announced programs to compete with the EPCs and the Control Systems Integrators—these programs are called “MAC” (Main Automation Contractor) or “MIC” (Main Instrument Contractor) or, occasionally, “ICSS” (Integrated Control and Safety System). In other
words, the BPCS vendor offers to stand as the control system integrator as well as the system designer. We will call this the MAC concept.

Studies has shown that proper implementation of the MAC concept, while increasing the Capital Expenditure, can actually save money for the End User through reduced cost of procurement, lower operating expense, and a reduction in the number and cost of change orders.

On the other hand, the MAC who is also the manufacturer will always plan to furnish its own products. Indeed this is part of the attractiveness of this concept to the BPCS companies who supply this service. Addressing this point, Frost and Sullivan has said, “the end user must also be wary that at times the MAC may potentially provide a product/technology that may not be the optimum product/technology desired. Hence, on occasions the end user might have to stipulate the procurement of certain products/technologies from certain specific companies to the MAC.”

The Compromise

So, by employing the MAC concept, what happens to the End User’s responsibility for safety? Nothing. While that responsibility remains with the end user, the implementation is passed on to the MAC and the MAC’s safety offering often gets no more interrogation than his selection of instrument pipe fittings.

Examining the standards that apply to Process Safety Systems, we find the following.

Part 1 of ISA84.00.01/2004-IEC61511 clearly states:

“11.2.4 If it is intended not to qualify the basic process control system to the ISA84.00.01/2004-IEC61511 standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.”

“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, in Part 2, “Diverse separation offers the additional benefit of reducing the probability of systematic failures and reducing common cause failures.

There are four areas where separation between the SIS and BPCS is generally provided:

1. field sensors;
2. final elements;
3. logic solver;
4. wiring.”

Let’s consider the compromises:
• By accepting a single vendor solution, is the End User compromising on the separation of BPCS and SIS? Are paragraphs 11.2.4 and 11.2.9 above fully considered?
• By accepting a single vendor solution, is the End User more susceptible to common cause failures? Note all the quotes from the standard above. Can the user be sure that proper separation is being maintained?
• By accepting a single vendor solution, is the End User compromising on the safety solution being provided to protect its employees and equipment?
• By accepting a single vendor solution, is the End User compromising on his vendors commitment to safety and to the changing standards and needs of process safety?

Many users may feel that the only choice they have it to accept the MAC concept and the compromises inherent in that choice or to bid all items separately and accept the increased life cycle costs and change order costs inherent with that decision.

But, where safety is concerned the cost of that compromise is too large. In safety compromise may cost lives. It may destroy productivity. I may even ruin businesses.

Many companies have learned that they can have the benefit of the MAC/MIC/ICSS while maintaining control of critical items such as Safety Systems.

Consider the following:

• At the Rio de Janeiro Petrochemical Complex, Comperj, Petrobras decided to go with the MAC concept but Petrobras specified the SIS vendors who would be acceptable. They gained the advantages of the MAC methodology while refusing to compromise on the safety of their people and resources.
• On the Ichthys Field Project, Inpex decided to go with the MAC concept but Inpex specified the SIS vendors who would be acceptable. They gained the advantages of the MAC methodology but they did not compromise on safety.
• When Bayer Chemical decided to upgrade the safety and control systems at their Baytown Refinery, they wanted a single point of responsibility but they specified the SIS vendor that provided the maximum safety. Another user that refused to compromise.

Conclusion

So, the point isn’t that MAC is bad. The point is that compromise is bad; at least it is when the compromise has to do with safety.

Safety should be the one area is our industry where there is no compromise. The consequences are just too large.

It should be incumbent on each End User to examine every option and to insure that every avenue has been explored to insure the maximum safety of every process implemented. That might well mean that the safety system and the Basic Process Control System should come from different manufacturers to insure independence.