MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

18th Annual International Symposium
October 27-29, 2015 • College Station, Texas

Diversity and Independence with Regard to BPCS and SIS Systems

Arvin B. Creef, Jr.
TUV/FS Eng 5209/12
HIMA Americas, Inc.
bcreef@hima-americas.com

Abstract

We live in a dangerous world. We work in a dangerous industry.

Albert Einstein is quoted as saying, “The world is a dangerous place to live; not because of the people who are evil, but because of the people who don’t do anything about it.”

As safety professionals, it is our job to do something about it. Yet, in the interest of ease of implementation or due to some belief that communications might be easier or for the more base reason that there might be a cost saving, we find ourselves making too many compromises.

This paper will postulate that the Integrated Control and Safety System is one of those compromises. Since the beginning of this industry, separate and diverse systems have been the rule in processing facilities. Such systems provide the ultimate in safety and security.

This paper will make the case for Independent and Interconnected Control and Safety Systems that will provide the ultimate in safety and cyber security.

Introduction

As long as human beings have built hazardous devices and processes, we have attempted to make them as safe as possible. The principal of separation and diversity between control and safety systems is almost as old as the concept of safety itself. Using different technologies provided protection against common cause. A decade or so ago the process industries began to hear of the concept of an Integrated Control and Safety System. Using similar technologies from one vendor that do both control and safety may save implementation cost or training cost or provide increased ease of use. All of those things are nice and desirable but what about safety?

ISA, IEC, and other agencies have created standards that we use to ensure the safety of our processes. But, the standards leave it up to user to interpret the standard and to make intelligent decisions regarding the safety of their own facility. If you are reading this, there is a very good chance that you are aware of standards such as ISA 84, IEC 61508, and IEC 61511 and that, in your everyday life, you try to implement those standards at your facility. In addition to

calculations you make and data that you accumulate, you also depend on certifications provided by third party laboratories to assist you in making these decisions.

However, it is important to know what these certificates guarantee and what they do not guarantee. And, it is important to understand that no matter what data or what consultants you

rely on, in the end, the responsibility for the safety of your facility rests with you, the end user. You cannot delegate that responsibility and, in the end, you can't share it with anyone. Should an event occur, it is solely your responsibility.

That being said, we should look at all of the prescriptive standards as we look at the minimum speed limit on a highway. They represent a MINIMUM level of safety for your facility. Our goal should be to make your facility as safe as possible not to just meet a standard. That being said, let's look at the standard.

The Standard

ANSI/ISA 84.00.01 is the standard that we, in the US, are generally attempting to adhere to. Let's examine a few of its statements.

> **9.5.1** The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative.

> **9.5.2** The assessment shall consider the following:
>
> - Independency between protection layers;
> - Diversity between protection layers;
> - Physical separation between different protection layers;
> - Common cause failures between protection layers and between protection layers and BPCS

11.2.4 If it is intended not to qualify the basic process control system to this 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.

NOTE 1: Operating information may be exchanged but should not compromise the functional safety of the SIS.
NOTE 2: Devices of the SIS may also be used for functions of the basic process control system if it can be shown that a failure of the basic process control system does not compromise the safety instrumented functions of the safety instrumented system.

It would seem clear that the intent of the standard is that there should be:

- Complete independence between protection layers
- Diversity between protection layers, and
- Low risk of common cause failures.

Common Cause

ISA 84 defines a common cause failure as: failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.

This definition is usually applied to a multiple channel system; redundant sensors, redundant modules, etc. In those cases, we examine the likelihood of a common cause failure per ISA 84 paragraph 9.5.1 quoted above. It is interesting that the standard says the assessment may be qualitative or quantitative. For our purposes, let's substitute objective for quantitative and subjective for qualitative.

Based on our objective or subjective analysis, we apply a Beta (β) factor to the risk of common cause. The β factor is basically the percentage of all the failures that we would expect to be the result of common cause.

In his book, *Functional Safety Basic Principles of Safety-related Systems*, Dr. Josef Börcsök, Chief Technology Officer of HIMA Paul Hildebrandt, states that at some level common cause failures "render the increase of the number of channels at a specific number meaningless."

Common cause failures, if they exist in high enough levels, can erase the benefits of redundant layers.

Note that common cause is almost always applied to redundant or multiple channel systems. But let's consider that in the event of a dangerous upset in a refinery or a chemical plant, the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) share a common mission, to keep the plant in a safe state, even in case of occurrence of failures or mal functions

of the equipment. Therefore, in that situation, the BPCS and the SIS can be considered to be a multiple channel system with one common function.

Quantitatively or qualitatively, we need to "ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers."

Analysis of Common Cause

Let's divert for a minute to a recently published study that introduces some interesting facts and terms.

SINTEF Technology and Society recently published a study entitled *Common Cause Failures in Safety Instrumented Systems*. The study is interesting in that the authors investigated all of the maintenance notifications at six facilities looking particularly for Common Cause Failures. It should be noted that the study did not include BPCS's or PES's. It was only a study of sensors and actuators. Both dangerous detected and dangerous undetected failures may be caused by Common Cause Failures. The study only considered dangerous undetected failures. The table below is reprinted from that study.

Equipment group	**Total population**	N_{DU}	$N_{DU,CCF}$	**New suggested β**	**β from PDS 2013 data handbook (for comparison)**
ESD/PSD valves (incl. riser ESD valves)	1120	279	68	**12 %**	5 %
Blowdown valves	228	73	17	**12 %**	5 %
Fire dampers	458	44	23	**20 %**	5 %
PSVs	2356	148	32	**11 %**	5 %
Gas detectors (point and line)	2239	74	20	**15 %**	7 %
Fire detectors (flame, smoke and heat)	5921	65	19	**15 %**	7 %
Process transmitters (level, pressure, temperature and flow)	1746	112	32	**15 %**	6 %

The table is shown only to demonstrate the difference between the β Factor estimated from the PDS 2013 handbook, the subjective β factor, and the β Factor suggested by the research, the objective β factor. Certainly the substitution of the experienced β Factor which is even higher than the suggested β Factor could have affected the design of the SIS.

While this study did not investigate Control and Safety Systems, it should cause us to be very skeptical of our subjective estimation of Common Cause Failures.

Both this study and Dr. Börcsök's book (cited above) discuss what the study calls coupling factors or coefficients of coupling. The study is quoted below.

"A **coupling factor** is a characteristic of a group of components or parts that identifies them as susceptible or vulnerable to the same causal mechanisms of failure. Such characteristics may be related to the use of common procedures, common design principles, the same environmental exposure and/or operating environment, and the same personnel involved in design, installation, operation, or maintenance."

Basically a coupling factor is a characteristic that makes the components or parts susceptible to Common Cause Failures.

Basic Process Control Systems and Safety Instrumented Systems and Coupling Factors

Turning back to the subject of this paper, traditionally Basic Process Control Systems and Safety Instrumented Systems were designed and manufactured by different people at different companies using different design criteria, different components, and different manufacturing concepts. Basically, there were NO COUPLING FACTORS.

Over the past decade or so, that has changed.

In the name of lower engineering cost or ease of use, the BPCS and the SIS have, in many cases, become ever more tightly integrated. These tightly integrated systems are even called Integrated Control and Safety Systems. While there MIGHT be savings in engineering costs and/or ease of use, we must be careful not to sacrifice safety in the name of savings.

The standard response is that these devices are third party certified so they meet the standard. But we need to look beyond certificates. Certificates do not relieve us of our responsibility. Remember that the responsibility for safety belongs to the End User, not the certification laboratory and remember that the certificate does not include an analysis of possible common cause failure modes or coupling factors between SIS's and BPCS's. The certificate only says that applied alone, the SIS meets the requirements for a SIL-X application.

This paper is not intended to be an indictment of Integrated Control and Safety Systems. But it is intended to suggest that there often are coupling factors that should be investigated and that we should be very conservative in dismissing or diminishing the significance of those factors. Remember the SINTEF study above and how it demonstrates the enormity of Common Cause Failures observed compared to the number expected.

So what coupling factors might exist?

If the BPCS and the SIS share a common configuration tool, is that a coupling factor? Would a bug or a human error in that tool impact both systems? Possibly in a dangerous manner?

If I/O technology is shared or partially shared between the BPCS and the SIS, should that be considered a coupling factor? Again, could an error in the I/O system design or operation affect both systems? Do we need to consider it as a coupling factor?

Is a common network a coupling factor? What about a common I/O database? Do these things cause us to do additional investigation and/or risk analysis?

Certainly a common design team or two design teams that share technologies and/or personnel could be a coupling factor.

It would seem to be incumbent on the user to investigate the possibility of common cause failures in any of these cases.

And remember from Dr. Börcsök's book that at some point the possibility of common cause failures renders the number of channels meaningless. Might we have to reduce the credit we take for the Integrated Control and Safety System if we find enough coupling factors?

Conclusion

While the advent of the Integrated Control and Safety System seems to have made our lives easier and possibly reduced our cost of engineering, it may be that they have introduced issues that have been hidden from our investigation.

If we are going to use Integrated Control and Safety Systems, it seems necessary that we investigate any coupling factors that exist to ensure that those factors don't increase the risk of a common cause failure that would render the both systems ineffective.

Since the responsibility for safety rests with the end user, the end user has to be responsible for this investigation. Assurances from suppliers cannot be accepted without further investigation.

Perhaps it is time for the trend to move back to what could be called Independent and Integrated Control and Safety Systems where data can be shared but coupling factors and the need to investigate them are reduced.

Perhaps we had it right to begin with.

Epilogue

While this paper did not address Cybersecurity, it is worth noting that the IEC 62443 committee has developed a model for a typical plant that emphasizes defense in depth and suggested "conduits" between layers. As the safety layer and the control layer migrate closer and closer, does that increase the susceptibility to cyber-attacks? Just a question for another time.

References

1. ANSI/ISA 84.00.01-2004 Part 1
2. Hauge, Stein, Hoem, Asa Snilstveit, Hokstad, Per, Habrekke, Solfrid. Lundteigen, Mary Ann; *Common Cause Failures in Safety Instrumented Systems, 2015-05-20*
3. Börcsök, Josef, *Functional Safety Basic Principles of Safety-related Systems,* ©2006