Paper No. 37c

Process Control Safety Standards as Institutional Memory

Edward M. Marszal, PE
President, Kenexis

Prepared for Presentation at the AIChE 2001 Spring National Meeting

Process Plant Safety Symposium

Session 37: Safety Standards for Process Control Systems

Process Control Safety Standards as Institutional Memory

Edward M. Marszal, PE
President, Kenexis
Ph: 614-451-7031
Fax: 614-451-2643
e-mail: edward.marszal@kenexis.com

Abstract:

Process incidents and accidents are often initiated, or least not prevented, by basic process control systems (BPCS). Much attention has been paid to Safety Instrumented Systems (SIS) due to recently ratified national and international standards on their design. The BPCS has as much, if not greater, impact on overall safety. The BPCS continuously keeps the process under control and allows the operator to manually move the process to a safe operational state before SIS "trip" actions are taken.

Design standards and guidance documents that are the basis for BPCS design should include an "institutional memory" of the incidents and accidents that have occurred in the plant and industry. All accidents should be analyzed to determine their root cause. The root causes of accidents should also be reviewed to determine how to prevent the accidents from occurring in the future. When the root cause or contributor to an accident is the result of a BPCS failure or design flaw, process control design documents need to be altered so that similar accidents can be avoided in the future.

The paper presents some real accidents or near misses. Failure of a basic process control system contributed to the occurrence of the incident in each case. For each incident, process control standard changes that might prevent future occurrences of these incidents are proposed. The paper also discusses additional sources of information that can be used to increase the size of your "institutional memory" based on accidents that happen in the overall CPI.

Introduction:

Basic Process Control Systems (BPCS) are responsible for ensuring that a process is consistently performing its design intent. For instance, if the design intent of a process section is to heat the process fluid to 500 °F then a BPCS is usually responsible for adjusting a heat input to ensure that a temperature of 500 °F is maintained. It is easy to see that problems occurring in the BPCS can quickly cause the process to violate design intent. If the heat input in the prior example were erroneously set to maximum, the results could be catastrophic.

In addition to performing "control" tasks, BPCS are also typically used as a first line of defense to bring the process to a safe state when process constraints are violated. BPCS are often designed to duplicate functions that are also performed in separate Safety Instrumented Systems (SIS); providing an additional independent layer of protection. As such, many of the requirements for SIS are also applicable to BPCS.

BPCS also have the characteristic of being inherently complex. Most BPCS are a combination of field sensors and actuators and control room based computers that communicate over a variety of hard-wired connections and digital communication buses. In addition to the main equipment, there is a host of supporting bits and pieces that are also required to make the system work, such as intrinsic safety barriers, lightning surge arrestors, relays, current monitor switches, and minor equipment items without which the entire system could not work effectively and safely. Design, installation, maintenance, and operation of this large assembly of programmable, configurable, temperamental, and sometimes-uncooperative collection of equipment leaves a lot of opportunity for error. Furthermore, a lot of these errors can reside inside the BPCS for weeks, months and years undetected, waiting for the perfect opportunity to evidence themselves when they can cause significant damage.

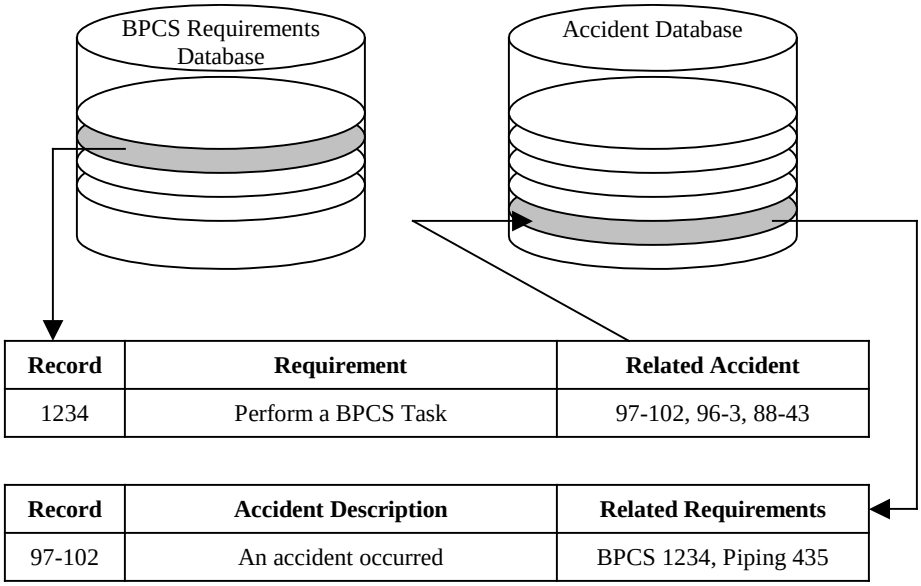
In order to minimize the likelihood that a BPCS contributes to initiating potential plant incidents, and hopefully is able to prevent other initiating events from propagating into unwanted accidents, the BPCS should be consistently designed using a solid set of corporate standards. This set of standards should not only enforce good engineering principles, it should also consider previous accidents and provide methods for preventing them in the future.

Digital Institutional Memory System:

At its root, a corporate standard for equipment design is simply a collection of requirements and procedures. As companies become more digitally enabled, they will also find that there is a benefit in moving corporate standards online. In doing so, they will be able to turn their requirement sets into databases, and their procedures into online tools. As more of a company's knowledge is placed online, they will be able to benefit from the synergies that interactions of those data sets and tools will allow. Specifically, databases of previous accidents can be related with databases of requirements to show how some requirements are related to previous accidents and also to show what engineering requirements have been created to prevent accidents from occurring in the future. This Digital Institutional Memory (DIM) system concept is demonstrated in *Figure 1*.

Web-based tools that are linked to relational databases also offer the advantages of global uniformity of design process, ease of deployment to multiple independent locations, consistency of information, and ease of data and application upgrades. Using newly available tools and standard protocols, providing access to databases through a standard web browser is nearly trivial.

Figure 1 – Requirements Database Concept



The concepts that are being discussed are not new, but the technology that can now be used to implement these paradigms has changed. For better or worse, computers are replacing the human element. The existing engineering design process relies heavily on experienced engineers and re-use of previous work. When designing a process, engineers will often use a "template" of a similar process unit as a starting point and as a reference when making design decisions. The engineer will then usually use a computerized tool to complete forms that describe the requirements for each equipment item. To some degree, these tools contain intelligence in the form of drop-down boxes and selection lists that are tailored to specific situations and other input.

Often during this process engineers will encounter novel or unfamiliar situations. They may even encounter situations where the computerized tool guidance or specifications in the template process seem strange. In these situations, engineers will often consult the organization's "institutional memory" to determine the reasons behind what may seem to be strange requirements. More often than not, the institutional memory is one or more engineers who have a combined experience that pre-dates the industrial revolution. When asked to explain the rationale behind the seemingly strange requirements they will almost invariably be able to tell a story of how something went wrong on a previous installation of equipment in the same service. After hearing the story the process engineer will usually have a much better understanding of the situation and wonder why she didn't think of this contingency.

This form of institutional memory has served us well for a long period of time, but there are a number of factors driving a move to a DIM system.

- More engineering work is being outsourced, but lessons learned must still be applied

- Senior engineers who hold the knowledge are leaving the company
- Employee tenures are becoming increasingly short
- Company's becoming more global

The Institutional Memory system that is currently being employed by most organizations is being destroyed by current market conditions. In order to survive, organizations are being forced to focus on their core skills and compete on a global landscape. This requires projects to be completed by bringing together teams that include outside experts, consultants and engineers, just in time. In addition, the team might be spread all around the world, but need to work from a common set of requirements to create a consistent product.

By using a DIM system, all engineers would work through uniform web-based tools and access a consistent set of requirements. This set of interconnected databases and tools will not only provide answers to questions about design basis, it will also provide a means of validating that all design requirements have been met during the validation or pre-startup acceptance test phase of a project.

Although a DIM system does not have all of the advantages of the experienced engineers that we have come to rely on, it does have its own unique set of advantages.

- DIM does not get sick, go on vacation, or retire
- DIM is available 24 hours a day to a virtually infinite number of people located globally
- DIM will not "forget" any previous incidents
- DIM recall of previous incidents will not change over time

While a DIM method for ensuring previous incidents are incorporated in new and existing process designs can never replace experienced

Scenarios:

The following scenarios are some examples of where accidents have occurred in the process industries where a requirement in a corporate standard or a requirements database could have prevented the accident from occurring. These scenarios demonstrate the type of information that could be used to populate an accident database, and the associated requirements that might be included in a BPCS requirements database.

<u>Incident #1</u>

INCIDENT TITLE: Failure of Centrifugal Pump P-101A at Unit A
LOCATION: USA (Company, City and State Withheld)
DATE AND TIME: December 01, 1997

SUMMARY OF INCIDENT:

At approximately 0700 hours on December 01, 1997, centrifugal pump P-101A pumping condensate from Tank 106 to the main storage tank TK-100 failed. The pump motor M-101A tripped on overload. Subsequent inspection of the pump revealed that its impeller and bearings were damaged.

BPCS RELATED ISSUES:

An investigation of the incident revealed that the pump failure was caused by loss of pump suction due to no level in Tank 106. The level in Tank 106 is controlled by level control loop LIC-1009. The transmitter measuring the level LT-1009 was a smart transmitter that failed, as was configured to fail high. The level controller therefore closed the condensate inlet valve causing the tank to run empty.

RECOMMENDATION FOR PREVENTION:

The failure mode of the transmitter to be changed to "fail low", and low and high level alarms are required in the control room for Tank 106.

APPLICABLE STANDARD REQUIREMENT:

Add the following clause to the Corporate BPCS design guidelines:

"An analysis of the failure modes of field transmitters shall be made during the engineering of loops in the BPCS to ensure that the most likely failure mode cannot lead to an unacceptable operating state."

Incident #2

INCIDENT TITLE: Damage to reciprocating compressor C-516
LOCATION: USA (Company, City and State Withheld)
DATE AND TIME: July 19, 1992

SUMMARY OF INCIDENT:

At approximately 1030 hours on July 19, 1992 the main control room operator for plant B got an alarm that C-516 compressor tripped on high discharge pressure. While speaking to the roving field operator to check the machine the operator got another alarm that the 600 HP motor driving the compressor tripped on motor overload. The controls and interlocks for the compressor motor are wired to a standard Programmable Logic Controller (PLC). Regulatory controls for the unit are handled by a DCS system.

Subsequent field inspections revealed that the compressor internals were damaged and that the high discharge pressure interlock contact in the PLC was "forced".

BPCS RELATED ISSUES:

The discharge pressure of the compressor became high because of the sluggish operation of a pressure control valve. The high discharge pressure switch wired to the PLC

detected the high pressure. The PLC digital output connected to the motor stop circuit did not operate due to it being "forced". Technicians would frequently force PLC I/O contacts in the PLC during the testing of field devices. It is essential that the forces be removed after the testing is completed. In this instance this was not done. The operator received the high-pressure alarm in the main control room because the alarm was connected to a separate output in the PLC. When he received the alarm he assumed that the compressor had tripped.

RECOMMENDATION FOR PREVENTION:

Install a hardwired alarm in the main control room to indicate that a PLC I/O or internal register in a forced/override state.

APPLICABLE STANDARD REQUIREMENT:

Add the following clause to the Corporate PLC design guidelines:

"**A dedicated hardwired alarm to be provided in the main control room to clearly indicate that a PLC I/O or internal reference is in a "Forced or override" state. A single alarm is required for each PLC.**

Incident #3

INCIDENT TITLE: Overheating and damage to Electrically heated furnace F-607
LOCATION: USA (Company, City and State Withheld)
DATE AND TIME: June 16, 1989

SUMMARY OF INCIDENT:

Electric furnace F-607 is use to carbonize metal powders at a temperature of approximately 2000 deg F. The furnace is 40 ft long, and 6ft wide and is internally lined with refractory bricks. A 4-20 ma electronic temperature controller located in a local panel controls the temperature. (T/C input and 4-20 ma output sent to an SCR panel that controls voltage to electric heaters.) The furnace also has a separate high temperature trip system set at 2200 deg F. During the commissioning of the furnace, the local electronic temperature controller was set to maintain the internal temperature of the furnace during the night at 800 deg F. When the operator inspected the furnace the following morning he noticed that the outer casing was glowing red. He immediately turned off all power to the furnace. The refractory bricks required replacing.

BPCS RELATED ISSUES:

An investigation of the incident revealed the following

- The thermocouple sensing the furnace temperature has failed during the night and the local temperature controller operated as if the temperature was 0 deg F. The electric heaters were therefore turned on to maximum.

- The backup high temperature safety shutdown system was disabled due to thermocouple problems.

BPCS RELATED RECOMMENDATION FOR PREVENTION:

- No system must be made operational unless all trip systems are functioning
- The temperature controller must be set for 0 ma output upon thermocouple burnout.

APPLICABLE STANDARD REQUIREMENT:

Add the following clause to the Corporate BPCS design guidelines:

"High or low temperature trip points are often configured within a interlock system using thermocouples as the source of temperature information. Since the primary failure mode for thermocouples is thermocouple burnout, burnout detection and alarm is mandatory on all temperature inputs."

"For thermocouples connected directly to electronic controllers for temperature control, the controller must have built in and configurable thermocouple burn out protection. This has to be set for all controllers so that the system can be placed in a safe mode if a T/C burnout occurs."

Incident #4

INCIDENT TITLE: Frequent nuisance trips at various units in refinery
LOCATION: USA (Company, City and State Withheld)
DATE AND TIME: Numerous

SUMMARY OF INCIDENT:

A petroleum refinery was experiencing frequent nuisance trips, especially to furnaces. The trips occurred whenever small dips in the control voltage to the trip circuits or open wiring occurred. These trips were having a major impact on the refinery production. A team was formed to recommend possible solutions to the problem.

BPCS RELATED ISSUES:

All trips were designed to be deenergize to trip. A drop in the control voltage or open wiring would cause the latching solenoids valves or relays to de-energize tripping the equipment. Maintenance technicians would some times inadvertently turn off the control voltage to the trip circuits causing a shutdown

BPCS RELATED RECOMMENDATION FOR PREVENTION:

Change the trip philosophy from de-energize to trip to energize to trip. Provide alarm in the main control room to alert operator on loss of control voltage to trip circuits.

APPLICABLE STANDARD REQUIREMENT:

Add the following clause to the Corporate PLC design guidelines:

"**In general, protective systems shall be of normally de-energized design to reduce potentially hazardous nuisance trips due to power failures, brownouts and open wiring. For microprocessor based systems considerations should be given to open wire fault detection. Normally energized protective systems are subject to special approval"**

Incident #5

INCIDENT TITLE: Hydrogen fire at rotary kiln
LOCATION: USA (Company, City and State Withheld)
DATE AND TIME: March 10, 1991

SUMMARY OF INCIDENT:

A rotary kiln 10 ft diameter and 100 ft in length was used as a reduction furnace. The oxygen in the material flowing through the kiln combined with the hydrogen at a high temperature to form water vapor. The hydrogen pressure in the kiln was controlled by a PID loop in a standard programmable logic controller (PLC).

On March 10 1991 the hydrogen pressure in the kiln became excessively high, and the hydrogen escaping through the seals in the kiln subsequently ignited. The kiln had to be purged with nitrogen to extinguish the fire.

BPCS RELATED ISSUES:

An investigation of the incident revealed that the PLC analog input and analog output cards were located in different racks and powered from different 110 volts power supplies. The 110 volts power to the analog input rack tripped causing the hydrogen inlet valve to open fully creating the high pressure i.e. the controller responded to a zero input signal.

BPCS RELATED RECOMMENDATION FOR PREVENTION:

Rewire PLC pressure control loop to a dedicated electronic controller. The pressure transmitter and valve to be powered directly from the controller.

APPLICABLE STANDARD REQUIREMENT:

Add the following clause to the Corporate BPCS design guidelines:

"PLC PID regulatory loops not to be used for critical control because of potential segregation of I/O and difficulties in tuning the loops."

Expanding Your Accident Database:

There is no reason that you should limit your accident database to accidents that have occurred in your plant. There are literally millions of chemical accidents from which your organization can learn lessons. In addition, a large number of these incidents are available and constantly updated from a variety of sources. *What Went Wrong?*, by Trevor Kletz, is an invaluable resource for process plant accidents. This book describes a multitude of accidents that have occurred, most of which could have easily been prevented. The book also describes the precautions that should be taken to ensure that these same accidents do not occur at your plant.

Another good source of the most current information on accidents is the chemical accident database maintained by the Chemical Safety Board. This database is the most comprehensive database of chemical accidents that are posted as they occur. Although the database has only been in operation for a few months, the data that it collects is invaluable in determining new and current operating problems. It is unfortunate that almost no week goes by that at least one new incident is not posted, but having access to the information is the best way to prevent this trend from continuing. The database is can be accessed over the internet at http://www.csb.gov/circ/.

Summary:

A BPCS has a lot of responsibility for not only maintaining product rates and specifications, but also keeping the process in a safe state. Due to the complexity and large number of interrelated components that comprise a BPCS, great care must be taken in its design.

Traditional design methods have relied on senior engineering staff to be an organization's institutional memory, retaining not only the knowledge of what requirements should be placed on their BPCS designs, but also why those requirements should be enforced. Many BPCS design requirements are the direct result of previous accidents.

For a number of reasons, replacing or enhancing senior engineering staff with a Digital Institutional Memory system is becoming an attractive option for many organizations. A Digital Institutional Memory system is a combination of databases and online tools that contain not only the requirements and procedures that are used to design processes, but also relate these requirements to previous incidents in an effort to provide background information for the requirements.

Employment of this type of system will push safety to a new level because the knowledge gained from previous incidents is crystallized into requirements for new and existing equipment. The knowledge will be employed if work processes systematically require that these requirements are systematically employed and validated.