New regulations and their effect on high-availability monitoring and control systems

THOMAS A. WALCZAK

The first half of the 1990s has brought new concerns and demands for change in safety practices for the process industries.

The proposed Occupational Safety and Health Administration (OSHA) guidelines for safety practices in the process industries, introduced Sept. 11, 1991, and revised in 1992, have been finalized and are due to be fully mandated in 1996. This new standard addresses a global spectrum of process hazards.

The Environmental Protection Agency (EPA) introduced an expanded proposed list of hazardous chemicals in 1994. This list, due to be finalized this year, has expanded ten-fold the previous list of proposed hazardous chemicals.

The original focus for the guidelines was primary chemical manufacturers and handlers: the large producers who use automated processes and critical processes. Targeted users now include those industries having one or more included process hazards.

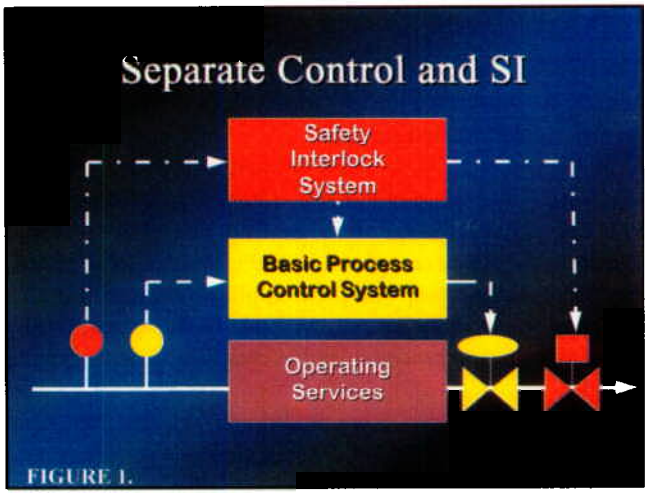
For the pulp and paper industry, the process hazards include a host of items: boiler controls and management systems, power generation gas and steam turbines, chlorine dioxide generators, bleach-handling equipment, large paper machine rotating equipment, and others. Pollution of land and water resources are also an issue.

This article describes existing technologies for meeting safety, environmental, and economic concerns and which benefit employees, government, the public, users, and producers.

OSHA activity

OSHA's process safety management standard has already been felt to a major degree in the petrochemical process industry *(1)*. The standard applies to companies that produce or use, store, manufacture, or handle hazardous chemicals or which have critical processes. Although this standard applies to more than 28,000 firms, those businesses most affected include chemical plants, refineries, food and pharmaceuticals, pulp and paper mills, and incendiary manufacturing. OSHA has specifically targeted a program for petrochemical facilities.

1. Separate control and safety interlock system

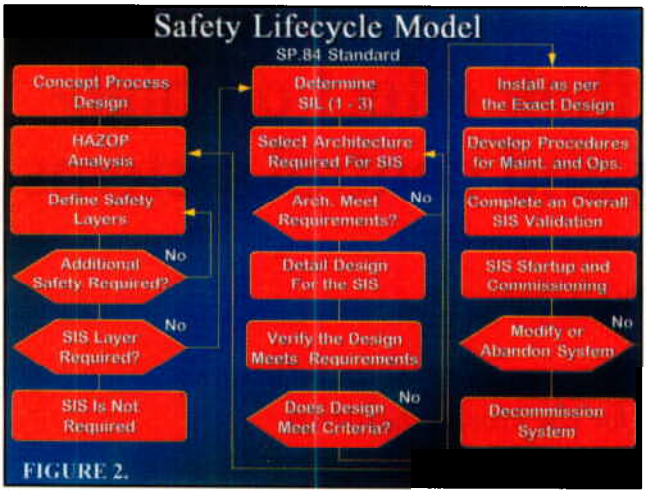


Process safety management has been brought to the U.S. public's attention, particularly during the past decade, by news reports of industrial accidents. Releases of chemicals, explosions, and fires at petrochemical processing facilities have claimed many lives and caused many injuries.

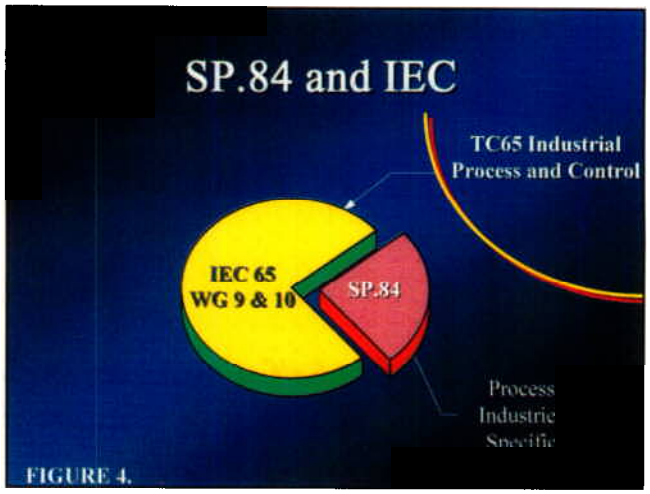
Chemical hazards are not the only risks. Machine guarding, control safety interlock, releases of airborne craft and liner products, among others, are also hazards within a facility. These hazards can be reduced by applying risk reduction control techniques.

The final OSHA ruling 29 CFR (Code of Federal Regulations) 1910.119 was released Feb. 24, 1992. The OSHA document is broad ranging, covering many aspects of safety management including proper documentation of procedures, identification of hazards, and response training. These activities are designed to meet a total response to the requirements of risk reduction.

2. Safety life cycle model



3. IEC standard recognizes the commonality for the processes industries.



EPA activity

The EPA has the responsibility for protecting the public health and the environment through enforcement of federal environmental regulations and statutes.

At the end of 1993, the EPA released a proposal in association with SARA (Superfund Amendments and Reauthorization Act) activity. Adoption of the EPA risk-reduction listed chemicals should be completed in 1995. Hazardous chemicals are used in various pulp and paper applications including CIP (cleaning-in-place) operations, antiscale boiler agents, dyeing and recomposition processes, and in bleaching systems, among others.

Bleaching processes using traditional chlorine for paper whitening are now considered ozone unfriendly. Newer processes using ClO_2 (chlorine dioxide) are being touted as environmentally sound replacements. However, the safety concerns associated with handling chlorine are amplified with chlorine dioxide. Chlorine dioxide is listed in SARA title III, in the consolidated chemical list, CAS 10049-04-4, Sec. 313, and is four times more lethal than its counterpart chlorine in the same concentrations.

OSHA and EPA

These two agencies continue to exchange information and data, as well as training for agency personnel. Acting according to the 1992 "Memorandum of Understanding" (MOU) that banded the agencies together, EPA and OSHA have mutually enforced statues and regulations at plants. They also have shared technical and professional assistance for coordinating compliance and enforcement activities.

Process safety management

The ISA (Instrument Society of America) SP.84 Committee "Programmable Electrical-Electronic Systems (PES) for Use in Safety Applications" has attempted to quantify the requirements for meeting the new standards over the last several years. The requirements for meeting guidelines and standards have been often elusive or continually evolving, almost preventing a final resolve. The current date for the final SP.84 standard release will be mid-1996.

1. IEC safety integrity levels

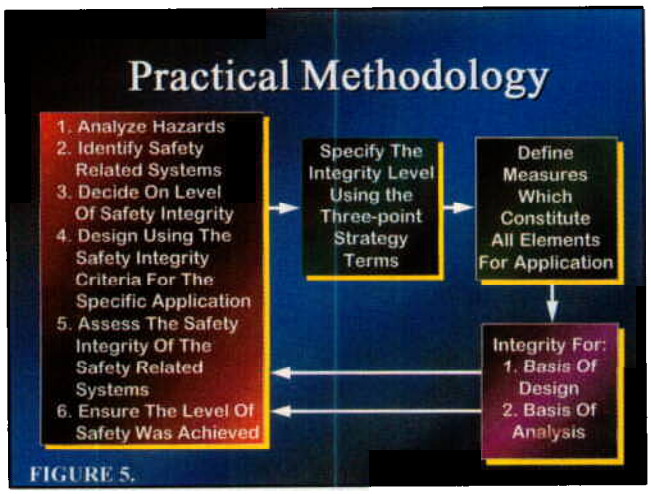
Safety integrity level	*Continuous control of dangerous failures per hour*	*Safety protection probability of failure to perform on demand*
4	10^{-9} to $<10^{-8}$	10^{-5} to $<10^{-4}$
3	10^{-8} to $<10^{-7}$	10^{-4} to $<10^{-3}$
2	10^{-7} to $<10^{-6}$	10^{-3} to $<10^{-3}$
1	10^{-6} to $<10^{-5}$	10^{-2} to $<10^{-3}$

In 1993 the IEC (International Electrotechnical Commission) approved the ISA proposal to use SP.84 as the basis for developing an IEC safety standard specific to the process industry. The standard encompasses IEC SC65A/WG10 Functional Safety: Safety Related Systems part 1 "General Requirements" and part 2 "PES Requirements," and IEC SC65A/WG9 Functional Safety: Safety Related Systems part 3 "Software Requirements."

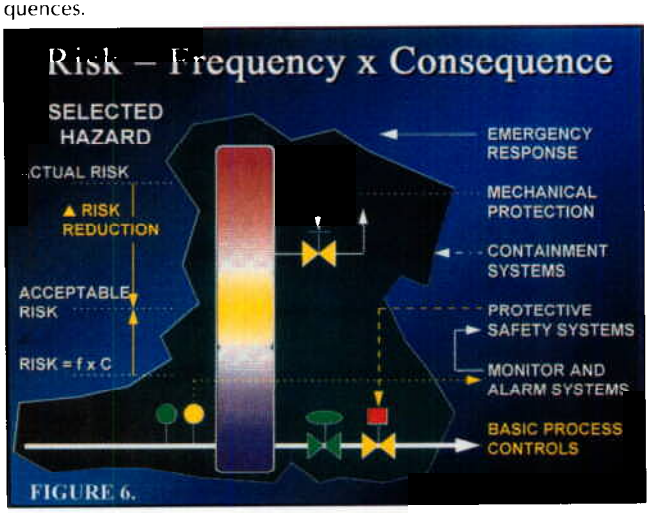
The safety standard:

- Has been developed for the process industries
- Separates control and safety and alarm interlock systems (**Photo 1**)

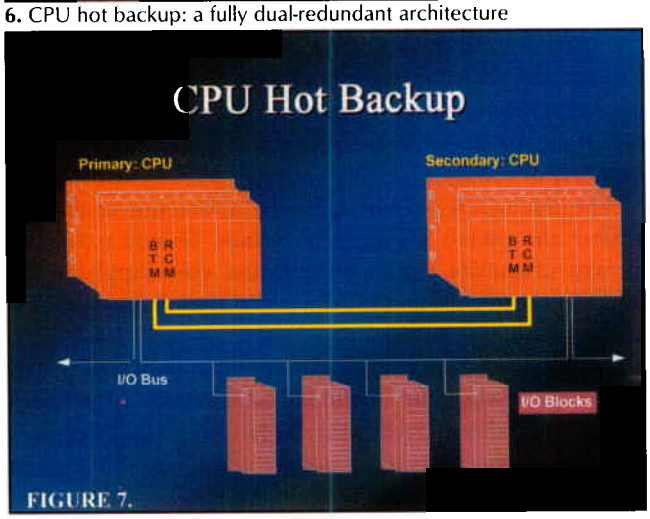
4. Common process-oriented LCM (life cycle model) systematic engineered approach



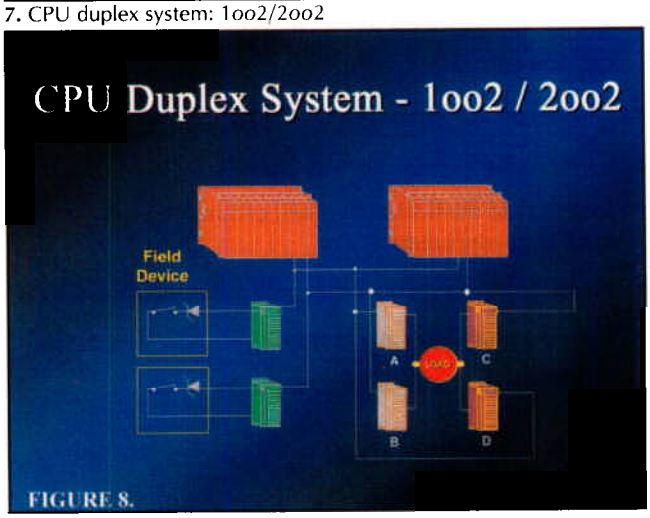
5. A qualitative or quantitative approach for identifying, analyzing, and determining hazards for a given process. Risk = frequency x consequences.



6. CPU hot backup: a fully dual-redundant architecture



7. CPU duplex system: 1oo2/2oo2



- Includes electrical, electronic, and programmable electronic systems
- Considers the inclusion of sensors and final elements in addition to the PES
- Is based upon the IEC safety life cycle model (**Photo 2**) and the four IEC safety integrity levels (**Table I**).

The IEC standard covers many applications (e.g., machines, industrial process, medical, electronics, railroads) and industries, but segregates and recognizes the commonality for the processes industries (**Photo 3**).

ISA SP.84-IEC SC65A

The formation and purpose of the committee activities are to promote:

- A common basis of measure for SIS systems
- Common definitions and terminology for technical discussions
- A quantifiable measurement for risk as per the OSHA guideline
- A logical engineering approach to remove "emotions"
- Elimination of the basis of confusion for safety parameters, measures, and technology
- Use of a common process-oriented LCM (life cycle model) systematic engineered approach (**Photo 4**).

The documentation includes:

- A safety life cycle design approach methodology
- A relative SIS (safety interlock system) to BPCS (basic process control system) design relationship

8. System architecture using fault-tolerant 2oo3 voting design

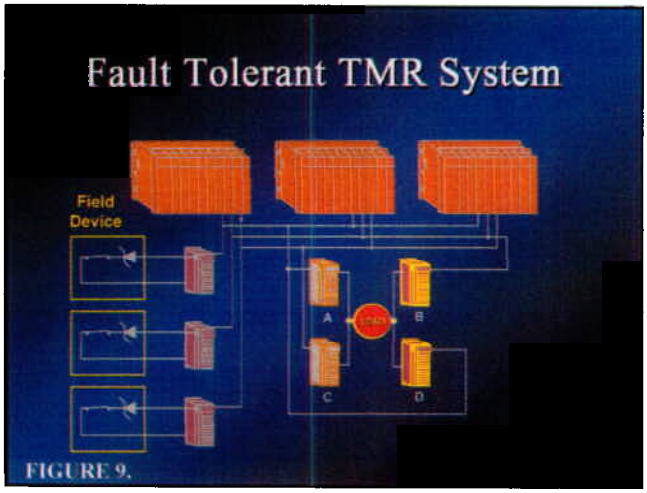


FIGURE 9.

9. Failure-state analysis using Markov modeling techniques where OK = ok, SDN = safe/detected, SUN = safe/undetected, DDN = dangerous/detected, DUN = dangerous/undetected, FS = fail to safe, and FD = fail to danger.

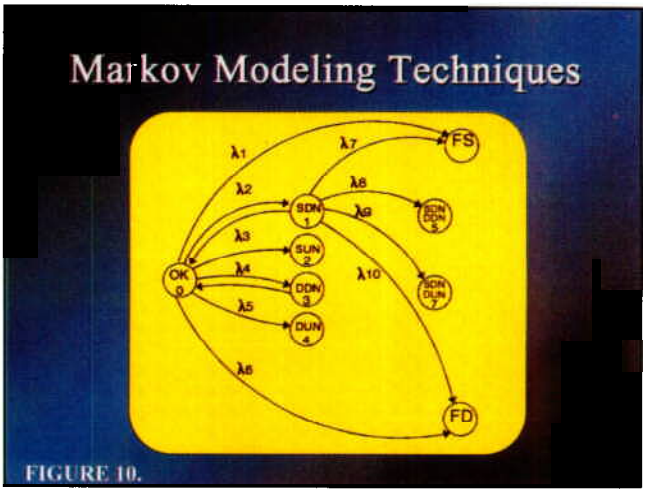


FIGURE 10.

- Availability and reliability analysis based on common failure data *(2)*
- The overall system diagnostic coverage requirements *(3)*
- Control system hardware and software security
- Interfaces to the field devices and communications to other intelligent controllers
- Operational and maintenance guidelines and procedures
- Training procedures and manuals
- Additional documentation as required.

Process hazard analysis

A qualitative or quantitative approach for identifying, analyzing, and determining hazards for a given process must be established. The guidelines are a function of the causes, consequences, demand rates, and frequency as a relative measure against a risk-reduction factor (**Photo 5**).

Documented and proven methods for analyzing the process hazards include HAZAN (Hazard Analysis), HAZOP (Hazard and Operability Study), Fault Tree, FMEA (Failure Modes and Effects Analysis), and others. There is much documentation readily available to support the process of conducting any of these analyses.

Once the process has been analyzed, risk reduction must be examined. After all practical means of reducing hazards within the constraints of the process have been examined and implemented, a target risk reduction methodology may be developed based upon the safety level specified and the integrity level required *(4)*.

Validation is an absolute must, and system testing must follow the guidelines of any functional test procedure for completeness.

Providing control system integrity

Considering the criteria achieved, is additional safety in the control system required? If not, then the task is done. However, if the risk has not been reduced to an acceptable level, it is necessary to continue.

The next logical step is to define the architecture required to achieve the overall system performance. Several types and formats of control system architectures exist. Applying the information in SP.84 and LCM, the necessary design considerations apply.

Techniques such as redundancy, configuration, quality, and diagnostic coverage are important contributors to increased system availability and reliability. Redundancy (applying more than the single element) is usually considered for control system elements that have *(5)*:

1. A low or unreliable operational record
2. Catastrophic effects upon loss or failure
3. Unacceptable alternate operation potential.

The design philosophy of how redundancy is implemented will ultimately contribute to determining the operational availability and reliability of the control system. For example, the combination of duplicating all elements in a system does not begin to develop an operational strategy as to how the system will function. In a fully dual-redundant architecture (**Photo 6**), a transfer of control using a backup operation, or an active voting mechanism, could exist; this is typically found in mill boiler applications.

If an on-line bumpless transfer from a failed to a backup operational component is configured, the system availability—its ability to continue to operate and not shut down due to a failure of a single component—will have increased. However,

reliability has not been increased equally. The system is configured to operate on only single components and it is no more reliable than a single control system.

Voting elements are usually accomplished by taking the sensor signals and comparing them in the CPU executing the application logic. The actuator signals are then directed to the outputs where the signal for the actuator is either electrically or logically solved, or both. For simple dual voted configurations, two votes are available. The logic can be voted either 1*oo*2 (one-out-of-two) or 2*oo*2 (two-out-of-two) from the state of the signals *(6)*.

For a system using a control voting logic of 1*oo*2, the convention used will be that only one of the two votes need be present to operate. A system that lost the ability to receive one of the two signals, or process it, would be able to continue to operate with the other signal. The availability of this system would be increased (**Fig. 7**), since a shutdown would not occur. However, upon closer examination of the system reliability, a signal read incorrectly would result in uncontrolled operation, potentially resulting in a FTD (failure-to-danger) fault state. This unsafe operation is not desirable for the critical processes requiring reliable control.

Voting a dual system 2*oo*2, where both signals are required to be present for operation, will increase reliability (where the safe state is off or nonoperational). This is desirable for the safe operation of critical processes and machines. However, availability is compromised because of the potential for a single loss of a component causing the system to shut down.

Methods are available to vote 1*oo*2 and 2*oo*2 within the same system. It is also possible to have hybrid fault degradation schemes to reduce nuisance trips *(7)*.

A more favorable system architecture uses a fault-tolerant 2*oo*3 (two-out-of-three) voting design (**Photo 8**). This configuration allows the benefit of higher availability from fault degradation operation as follows:

2*oo*3 operation

on first failure to

1*oo*2 <or> 2*oo*2 operation

on second failure to

1*oo*1 operation (optional)

on third failure to

default FTS configuration

The failure state analysis in **Photo 9** uses Markov modeling to demonstrate system failures. The lines connecting the successful and failed components represent a failure or repair. Many tools can be used to represent a statistical display of system performance between system configurations.

Quality in the design of hardware and software is essential to a critical control system. Random and systematic failures can be reduced by using proven technology, highly tested components, and equipment with sound experience records.

Diagnostic coverage can greatly improve availability and reliability of system performance by:

- Effecting repairs quickly
- Detecting failures and responding appropriately and automatically
- Reducing potential maintenance errors
- Providing historical data
- Reducing FTD faults.

Process system design summary

Once a system architecture has been selected, a design for the system should be completed. Verification of the final design should meet the requirements of the original specification and original design. Care should be taken to ensure that the installation and maintenance meet the requirements originally designed. Testing and validation will assure that the system meets the anticipated operational requirements.

Conclusion

Process design parameters that meet emerging guidelines and regulations for system design criteria have the following benefits:

- Safe, reliable operation performance
- Improved product quality
- Increased productivity
- Reduced downtime
- Raised profit levels.

Designing and upgrading control system operation makes good sense all around. ■

Literature Cited

1. Bureau of Business Practice, *Safety Managers Guide*, Prentice Hall, 1994.
2. Talmor, M., "A practical approach to system reliability modeling and calculations," GE Fanuc Paper, 1992.
3. O'Connor, P., *Practical Reliability Engineering*, Wiley & Sons, New York, 1991.
4. Walczak, T. A., *ISA Proceedings*, Vol. 2, Houston, 1992, #92-0457, p. 321.
5. Anon., "Programmable Electronic System (PES) For Use in Safety Applications," Draft 16-6E, ISADS84.01, ISA, Research Triangle Park, N.C., July 1994.
6. Holscher, H. and Rader, J., "Microcomputers in Safety Technique," TÜV Research Report.
7. Walczak, T. A., *ISA Proceedings*, Chicago, Sept. 23, 1993, #93-515, p. 517.

Walczak, P.E., is senior critical control system engineer, GE Fanuc Automation, N.A., P.O. Box 1235, Sugar Land, TX 77487-1235, Fax: (713) 980-5391.