COMPUTER CONTROL OF INDUSTRIAL PROCESSES

INTRODUCTION

PRC.17.10 is referenced in this document and is considered an integral part of this PRC Guideline. Please use it as a reference for additional information.

Unlike more common electronic data processing centers used in business or financial operations, computer systems controlling industrial processes couple computers to instruments and controls using signal networks. They may be in either complete or partial control of a process or series of processes. They may also vary in size from microcomputer to minicomputer and occasionally to main frame.

Although programmable logic controllers (PLC) can control industrial processes, they do not have the processing capacity and peripherals associated with computers. PLC are solid state electronic switches controlled by a microprocessor which can be programmed to respond to external incoming signals in a prescribed manner. PLC do not usually require any special consideration or protection.

Protection for computers controlling industrial processes differs from that for data processing centers. Reasons for this include:

- The equipment used is more likely to be specially adapted or designed to perform functions that may be unique to the particular application. Therefore, replacement of a destroyed or seriously damaged computer may be more difficult.
- The option of using computers at another site does not exist (as in common business applications) because of the obvious need to be tied into the signal/control networks to the process. In-house redundancy is an alternative.
- Using the computer requires maintaining the integrity of the signal network and the wiring interface between the computer and the network.
- Recorded data points sources and processing scenarios are more numerous. Accuracy and efficiency of the computer can only be as good as the input from instrumentation at the process equipment.
- The limited need for printed output and infrequency of program changes should help minimize the amounts of combustibles within the computer room.

POSITION

Management Programs

Pre-Emergency Planning

Preferably, use a dedicated computer for control operations. In any case, make sure there is an arrangement for monitoring the variables under computer control so that operations can safely be switched over to manual operation in the event of impending computer failure. In some cases, redundant computer systems may be the only alternative. A proper hazard analysis will help identify process weaknesses.

Program the system so that when total or partial failure of critical computer functions occur, including input signal, the process goes into a fail-safe mode and brings the process to a safe condition. For example, if one of the functions of a process control computer is to monitor combustion control equipment, loss of this monitoring function should result in a cessation of fuel flow and a purging of the combustion chamber or the release of critical control to the next lower level of control. The combustion unit may have its own control system, which could be a PLC.

In the case of computer controlled machining, it may be desirable to place control in a “locked” condition. This preserves the last set of values until released by subsequent manual correction or by the return of the process to computer control. In chemical process control, critical instrumentation loops, such as cooling, heating or agitation, may need to be left to operator control with a certain degree of flexibility to bring chemical reactions involved in the process to a safer condition.

Provide an uninterruptible power supply (UPS) so that, in the event of a failure of the primary power supply to the computer, the process may be continued.

Each task under computer control must notify the operator when a variable under control exceeds previously established parameters.

To bring a relieving operator up to date at a shift change, provide a method for reviewing the situation existing at that time regarding critical variables.

Protection of Vital Records

Beyond the usual requirement for protection of programs and information files, duplicate critical network wiring diagrams and store them in a remote location. In the event of fire involving the signal and control networks, this information will be needed to affect speedy restoration, particularly at the computer and network interface.

Equipment Maintenance

Computer or operator control of plant processes can only be effective when correct readings are produced by sensing, measuring or recording instruments, and there is a correct response by controlling equipment. It is essential that a detailed, systematic program of testing and maintenance be followed for these devices.

Computer cabinet and circuit layout design should permit rapid and convenient troubleshooting and maintenance in the event of computer failure. Maintenance of the computer is considerably more important than the additional space requirements involved.

In processes that are particularly hazardous and could be a threat to the safety of the plant and its personnel, duplicate the sensing and measuring devices used in process control so that any partial malfunction of one device will not permit a dangerous condition to go undetected. Arrange valves or other control devices to move to a safe position in the event of failure. Locate all instrumentation so it can be safely inspected and maintained.

General Arrangement

The area housing the process computer should meet AXA XL Risk Consulting recommendations for non-process related computers found in PRC.17.10. The following clarifications or exceptions under each indicated heading apply.

Location

The location is of primary importance when the computer is controlling hazardous processes or equipment. Locate the computer such that exposure from fire and explosion within equipment or structures will be minimized. Do not overlook the danger from possible flammable or corrosive liquid spills or vapor release.

Construction

Use only noncombustible construction materials. Avoid the use of decorative wood paneling and plastic grid ceilings.

When exposure to a potential explosion cannot be avoided, incorporate the following construction features into the computer control center:

- For exterior walls, use steel-framed or reinforced concrete nonloadbearing construction designed to withstand anticipated explosion overpressures.
- Avoid windows if possible. Where deemed vital, minimize their size and use laminated safety glass or wired glass.
- Avoid suspended ceilings as they may be displaced by external blast waves, endangering operators and equipment below them.

Equipment

Equipment protection considerations must extend beyond the computer system to include the signal network. Pay particular attention to the wiring interface that connects the computer, the main manual control station and the signal/control network. Destruction of this interface could lead to complete loss of control of the process.

Fire Protection

Because of the importance of computer controlled process equipment, a more aggressive approach to fire protection must be taken, especially for the computer and the wiring network within the computer room. Provide automatic sprinkler protection on an Ordinary Hazard Group 1 basis throughout, in accordance with NFPA 13 and PRC.12.1.1.0. Control the presence of Class A combustibles in the computer room. If there are sufficient combustibles to propagate a fire in the underfloor space, provide an automatic total flooding gaseous agent system such as carbon dioxide. Design the system to meet the requirements of NFPA 12 and PRC.13.3.1, or NFPA 2001 and PRC.13.6.1. Critical equipment may be protected by a gaseous agent system as follows:

- Install smoke or products of combustion detectors throughout the computer room and underfloor space. Design underfloor detection systems so only an alarm is produced by the operation of a single detector, and agent is discharged as a result of actuation of a second, confirming detector.
- Provide automatic CO_2 or clean agent fire extinguishing system for the underfloor space and within the computer room, if operations and safety considerations allow the installation. Actuation of extinguishing system should occur upon activation of the smoke or products of combustion detectors. In critical occupied areas, carbon dioxide total flooding of the computer room may be considered, if the occupants receive appropriate training and safety equipment.
- Provide smoke detection of the air-sampling type and automatic CO_2 extinguishing system inside of important equipment cabinets.
- Use a design concentration of 50% and maintain the concentration for at least 10 minutes for CO_2 system. For clean agent extinguishing systems, refer to NFPA 2001 and PRC.13.6.1 regarding design guidance.
- If the air conditioning unit for the computer control room is located within the area and is used solely for that purpose, it may be left in operation during discharge of the extinguishing system. Take agent loss into account in the design to allow for normal fresh air makeup.

- If the computer equipment power can be interlocked to shut down on extinguishing system operation, locate a means of manual interruption of all computer power at all exits from the computer room. See power supply concerns under Pre-Emergency Planning. If management intents to keep the computers operational or to go to a manual partial shutdown, provide proper breathing apparatus for occupants and do not install interlocks at exits to shutdown power to the computer.
- Provide emergency mechanical venting to exhaust smoke and corrosive fumes to the atmosphere. Base fan capacity on 3 cfm/ft² (0.914 m³/min/m²) of floor area. Locate manual controls for the necessary fans immediately outside the computer room in a readily accessible, clearly identified location. Delay emergency mechanical ventilation system operation until after the gaseous extinguishing system has operated for the appropriate soak period, if appropriate.
- Protect cable interconnections between the computer and the signal/control networks by an automatic extinguishing system, actuated by a properly arranged smoke detection system.

Air Conditioning

Proper location of fresh air intakes for the computer control center is very important. Place them at a high elevation in an area that will minimize the possibility of pulling in smoke, flammable vapors or corrosive fumes during normal or abnormal operations.

For very critical facilities, it may be appropriate to incorporate two widely separated intakes to avoid contaminated air infiltration. Use of pressurization techniques and the use of high efficiency filters may be incorporated.

Electrical Wiring

Route all signal and control wiring and tubing from the control center so as to avoid possible fire and explosion exposure from buildings, equipment or flammable liquid spills. Where such exposure cannot be avoided by routing or burial, provide suitable protection by automatic fixed-water spray, fire-resistive encasement or both. Another acceptable arrangement is to provide redundant circuitry routed over different paths.

Pneumatic tubing, using transducers, is often used in control circuits. Where massing of plastic tubing cannot be avoided, or such tubing exposes or is exposed by cable troughs, provide automatic fire protection, fire-resistive encasement or both. Evaluate the importance of the control circuit and the consequences of losing it before using plastic tubing.