HEAVY MOVABLE STRUCTURES, INC.

SIXTEENTH BIENNIAL SYMPOSIUM

September 2016

FAIL-SAFE CONTROL SYSTEMS FOR HEAVY MOVABLE STRUCTURES

by

Mark VanDeRee, P.E.

of

WSP | Parsons Brinckerhoff, Inc.
2202 North West Shore Boulevard, Suite 300
Tampa, Florida 33607
813-520-4433

Tampa, Florida

September 2016

Fail–Safe Control Systems for Heavy Movable Structures

INTRODUCTION

Heavy movable structures can use many different control system architectures. These include hardwired electromechanical relays and various programmable electronic control systems such as the programmable logic controllers (PLCs), direct digital controllers, distributed controllers, or hybrids of each. The overall bridge control system architectural configuration may include control sub-systems dedicated to motor drives, hydraulic power units, navigation and signal lights, and other equipment. The control sub-systems may be separate, stand alone hardwired relays, PLCs, proprietary electronics, or hybrids.

It is necessary to design the overall bridge control system to include fundamental fail-safe characteristics regardless of the architecture used. A fail-safe system is one in which the failure of any component in the system will not prevent unsafe operation of the controlled equipment.[1] Typically, this means a fault will still allow equipment to be shutdown. More important, a fault should not cause the unintended operation of equipment. When analyzing the specific fail-safe requirements of the application, it may be necessary to exclude some control system architectures from consideration.

Circuits and programs used for starting and stopping equipment, machinery shutdowns, emergency stops, interlocks, permissives, and feedback control must be analyzed with regard to cause and effect for an overall fail-safe control system.

The objective of this paper is to explore different fault scenarios common to control circuits and systems. The focus is fail-safe control system design for heavy movable structures, and more specifically for movable bridges. Emergency stop control circuits that are both fail-safe and fault tolerant are presented. The techniques discussed can be extended to many other control system applications with success.

CONTROL SYSTEM ARCHITECTURES

Hardwired Electromechanical Relays

One of the most widely used control systems for all types of applications is the electromechanical relay control system. Relay control systems date back to the 1800s and remain popular today. An example of relay control architecture on a movable bridge is shown in Figure 1. Relays use an electromagnet to switch contacts from open to closed or closed to open (Figure 2). Springs are used to return the contacts to their de-energized position. Latching relays use dual electromagnetic coils to drive the contacts to either open or closed states. Latching relay contacts stay in the last position until the coil of the opposite state is energized.

Future reference to relays in this paper will imply the electromagnetic control relay unless stated otherwise. The energizing or de-energizing of relays and the switching of the associated electrical contacts provide a way to implement control logic by controlling and directing the flow of electrical energy. Fail-safe considerations for relays are primarily an analysis of what happens when a relay does energize and what happens when it de-energizes.

Electronic Control Systems

Programmable electronic systems include the PLCs (programmable logic controllers), DCSs (distributed control systems), network field bus types (Profinet, Profibus, Fieldbus, Hart, Modbus, Ethernet, etc.), direct digital or distributed control using mainframe computers, microcomputers, and personal computers. These digital electronic devices use microprocessor-based hardware to execute software and firmware application control programs developed by the control system engineer.

The PLCs and DCSs have gained the widest acceptance and use among the electronic control systems. DCSs are rarely used on movable bridges because their high costs outweigh their benefit for this type of application. PLCs are widely used on movable bridges (Figures 3 and 4).

The PLC is defined as a digitally operating electronic system designed for use in an industrial environment that uses a programmable memory for the storage of user-oriented instructions for

implementing specific functions such as logic, sequencing, timing, counting, and arithmetic to control various types of machines or processes, through digital or analog inputs and outputs.[2]

The PLC was developed in the 1970s to be a relay replacement device for discrete control. That is, control that can be implemented with logic states of "ones" and "zeros," "on" and "off," "high" and "low", and so forth. In the 1990s, PLC capability expanded to include the more sophisticated analog control that was previously available only in single loop controllers and distributed control systems.

Personal computers and microcomputers are advancing steadily in control system usage, but their reliability and fail-safe diagnostics lag behind the PLCs.

PLCs are developed with rugged hardware, and strict internal microprocessor diagnostics for software and firmware. Electronic devices do not necessarily fail to a logic state of "zero." PLCs are manufactured with built in fail-safe features. The operating system and application software used in PLCs are rigorously tested for efficiency and the "bloat-ware" commonly found in personal computers is typically not allowed by the PLC manufacturers.

Today, most movable bridges use PLC control, hardwired relay control, or a hybrid of the two. Drive systems are being manufactured more commonly with integral microprocessor based controls. This leads to the possibility that the embedded logic may not necessarily be fail-safe.

The engineer must develop fail-safe features in the relay control schematics, the PLC application programs and input/output configurations, and the drive system parameters.

Case History

The Hood Canal Bridge is a floating concrete pontoon bridge which spans the 330 foot deep Hood Canal connecting the Olympic Peninsula to the Kitsap Peninsula in western Washington. The floating portion of the bridge is 7,450 feet long and has two retractable draw spans in the center which can be opened to form a 600 foot channel for marine traffic. It carries one lane of traffic in each direction. On the evening Thursday, August 18, 2005 at approximately 11:30 PM the bridge was undergoing construction work to facilitate the widening of the west half of the bridge and the east and west approach structures. The WSDOT construction inspector noticed that the traffic had increased and saw that the east structures stop signals and traffic gate warning lights flashing. The bridge tender went to the control tower on the west half of the bridge and found that all of the

indicating lights on the control desk for the east half of the bridge were lit. When he was unable to gain control from the control desk in the west control tower, he went to the east control tower and found that all of the indicating lights on the east half of the control board were lit as well. Since he was still unable to control the bridge, he went to the PLC cabinet on the floor below and turned the primary and back up PLCs to "HALT" using the keyed switches which turned everything off at approximately 1:30 AM. He observed that the west end locks had rotated into the OPEN position, that the machinery rooms smelled like overheated motors and that the drive motors were hot to the touch.

A control system fault caused PLC outputs to energize without operator commands and without operators present. Electrical equipment, including motors, was energized and operating as a result. The drive motors were in a locked rotor condition for an extended period, destroying them. There were no PLC module failures identified. The PLC control system was reset by clearing all forced points. Later, the program was reloaded and system power was cycled off and then on. The PLC operations were tested and appeared to be functional.

The cause of the fault could not be repeated, isolated, or conclusively identified. It was more likely caused by equipment failure (hardware or firmware) than by a software failure. Direct human intervention was not the cause. It is possible that events leading up to the fault, such as testing the auxiliary generator or power surges and outages, may have caused, or contributed to, the fault. It may be possible for a power surge to have this effect even with good power filtration and a UPS for surge protection. A power surge could enter the system components through the input power feed, or back feed through the non-isolated output modules. There is one documented case from the manufacturer of a somewhat similar fault being caused by a power surge. Although, there were not enough details of the case to be conclusive. Poor quality control system grounding may also be a contribution factor.

Operator Control Stations

The operator control stations found on movable bridges are mostly hardwired hand switches, pushbuttons, pilot and indicating lights, and alarm displays. Engineering considerations must be given to the hand switch contact developments, spring returned hand switch contacts, captive key-lock hand switches, and dual pilot lights when designing the control console for fail-safe features. Push-to-test indicator lights are good to use when the lights are being used for alarms or to verify the position of machinery. Knowing that lamps are working is not only a helpful maintenance feature, but it allows the operator to know if the dark lamp indications are true. Fail-safe consideration for indicator lights includes using the actual machinery being monitored to give positive feedback directly to the indicating light. Using electrical control signals that command the

machinery to also control the indicating lights is an unreliable method of providing feedback to the operator. Additionally, where a device or piece of machinery travels to opposite positions; such as a valve (open/closed), a lock (driven/pulled), a leaf (open/closed), a brake (set/released); it is a good practice to sense both states independently. This provides the operator with an indication that the machinery is in travel or if it has failed during travel.

LED, LCD, or plasma flat screen based graphical operator interfaces have not been widely used on movable bridges for several reasons. Flat screen displays require redundancy because they are fragile when compared to a hardwired control console. Graphical displays on screen are easily washed out by sunlight that usually floods a control tower through the large windows needed for operator visibility. If the displays are left on continually without rebooting, screen burn-in will require their replacement every 2 years. If the displays are turned off between openings, there is a time delay required to warm up the monitor or to reboot the computer that is driving the graphics before operating the bridge.

Eventually these obstacles will be overcome and these operator stations will be used on more movable bridges. For example, high intensity enhanced LCD displays (liquid crystal display) or gas plasma displays could make graphical control stations more practical.

Fail-safe design considerations in graphical operator interface stations would include the performance of all actual control functions in a separate and dedicated PLC. The graphics station should remain strictly supervisory. With this architecture, fail-safe requirements are reduced to only needing the proper techniques to communicate between the graphics stations and the PLCs. The programming techniques of the PLC logic also become critical with this architecture.

FAIL-SAFE CONTROL SYSTEM DESIGN APPROACH

Control systems and devices have changed dramatically over the past 100 years. However, the fundamentals associated with the control systems required for safe operation and shutdown have not changed. It does not really matter if the machines, equipment, or processes being controlled are chemical plants, power plants, or heavy movable structures. It does not matter if the control system

architecture uses only mechanical devices, only electrical devices, only electronic devices, or if it is some type of hybrid. What does matter is that the control system is properly engineered to provide for the safe shut down of the machines and equipment in the event that one or more control system component fails. A control system must be engineered to achieve shutdown conditions in an orderly manner with minimum risk of injury or damage to the machines and equipment being controlled.

There should be no compromise between safety and cost when developing control system designs. Using fail-safe techniques does not usually require any significant amount of extra labor or materials. What should be considered instead is the cost of not being fail-safe if there is a failure.

Control system engineers freely adopt proven techniques from similar applications as being a prudent approach to design. Good engineering practice includes assessing whatever works for a specific application elsewhere and considering mirroring it in a similar application.[3] Some standards require a control system that is both fail-safe and fault tolerant. Generally, control system standards used for movable bridges do not accept designs where one or two faults of any kind can cause unintended operations or where a single fault will prevent equipment shutdowns.

Standards and Specifications

There are a few standards available for engineering movable bridge control systems. Guidance is taken from AASHTO publications (American Association of State Highway and Transportation Officials).[4, 5] The AASHTO, *Standard Specifications for Movable Highway Bridges* is the foundation on which the movable bridge is designed. However, AASHTO specifications and recommendations are somewhat limited in regards to control systems and need to be supplemented with additional standards. There are many industry standards, definitions, and symbols specifically dealing with control systems. Those most pertinent are listed as follows:

- AASHTO, *Standard Specifications for Movable Highway Bridges*, 5th Edition, American Association of State and Highway Transportation Officials, Inc., Washington, DC, 1988.

- AASHTO, *Movable Bridge Inspection, Evaluation, and Maintenance Manual,* 1st Edition, American Association of State and Highway Transportation Officials, Inc., Washington, DC, 1998.

- Code of Federal Regulations-CFR Title 33, Parts 118- Navigation and Navigable Waters.

- FHWA, *Manual on Uniform Traffic Control Devices (MUTCD)*, Federal Highway Administrator, 1988.

- ISA, *Instrumentation Symbols and Identification (ANSI/ISA-5.1, 1984)*, International Society for Measurement and Control, Research Triangle Park, NC, revised 1992.

- ISA, *Application of Safety Instrumented Systems for the Process Industries (ANSI/ISA-84.01, 1996)*, International Society for Measurement and Control, Research Triangle Park, NC, 1996.

- ISA, *Identification of Emergency Shutdown Systems and Controls That Are Critical to Maintaining Safety in Process Industries (ANSI/ISA-91.01, 1995)*, International Society for Measurement and Control, Research Triangle Park, NC, 1995.

- JIC, *Electrical Standards for General Purpose Machine Tools and Mass Production Equipment, (EGP-1-67 and EMP-1-67)*, Joint Industrial Council, McLean, VA, 1967.

- NEMA, *Industrial Control and Systems: Control Circuit and Pilot Devices, (NEMA ICS 7)*, National Electrical Manufacturers Association, Roslyn, VA, 1993.

- NEMA, *Programmable Controller Standard ,(NEMA ICS 3)*, National Electrical Manufacturers Association, Roslyn, VA, 1993.

- NFPA, *Electrical Standard for Industrial Machinery (NFPA-79, 1991)*, National Fire Protection Association, Inc. Quincy, MA, 1991.

- NFPA, *Hydraulic Fluid Power- System Standard for Stationary Industrial Machinery (ANSI/NFPA/JIC- T2.24.1, 1991)*, National Fire Protection Association, Inc. Quincy, MA, 1991.

The National Fire Protection Agency standards relating to electrical control systems include NFPA-70, *National Electric Code*, and NFPA-79, *Electrical Standard for Industrial Machinery.* NFPA standards are primarily concerned with protection against electrical shock and fire hazards. When NFPA-79 incorporated the Joint Industrial Council Standards in 1985, it only included those areas related to electrical shock and fire hazards. [2] NFPA-79 does provide definitions for the terms "Fault," Failure," and "Machinery Control Circuit," but does not define "fail-safe" as related to controls systems.

Additionally, the following standards address programmable control system safety:

- ANSI/ISA-84 Standard for Safety Instrumented Systems-(Instrumentation Systems and Automation Society).
- IEC-61508 Standard for Functional Safety- (International Electrotechnical Commission).

AASHTO Fail-Safe Requirements

AASHTO specifies that motor brakes for movable bridges must be fail-safe mechanically and electrically.[4] Motor brakes are to be held in the set position by springs and released when electrically energized. They are to set automatically whenever the electrical current is turned off. AASHTO also specifies that hydraulic pumps must fail to the zero pumping position and bypass valves must fail open.[4]

AASHTO also requires a level of redundancy in safety systems as for brakes and for safety related instrumentation. Some AASHTO requirements for equipment and associated control circuits are as follows:

- Auxiliary Power (recommendation).
- Two sets of Brakes; motor brakes and machine brakes.
- Two electric compressor type air trumpets and two smaller electric trumpets (requirement on bridges with electricity).
- Two drive motors with provisions for bridge operation by one motor (recommendation).

- Normal stopping controls, and emergency stopping controls.
- Reversing motors shall have mechanically interlocked reversing contactors.
- Span overspeed switches at nearly closed and nearly opened positions interlocked to set the brakes by removing power.
- Hand released brakes shall render the bridge inoperable.
- Disconnect switch to PLC input/output power.
- Master Control Relay (MCR) circuits to remove PLC input/output power.
- Position limit switches (and skew switches on lift bridges) to stop drive motors and set brakes at each end of span travel.
- Operational sequence interlocks: set traffic signals, lower gates, close barriers to block traffic, pull locks, release brakes, open span, etc.

Unfortunately, AASHTO specifications come short of mentioning how fail-safe or fault tolerant control systems are to be achieved.

The engineer should develop the control system plans and specifications in accordance with the applicable industrial standards. Even if not familiar with AASHTO, most reputable control system contractors are familiar with ISA, NEMA, and JIC. NFPA No. 79 and JIC No. EGP-1 standards and symbols for relay control systems are shown in Figures 5, 6, and 7.[1,2] These symbols include the familiar relay coil, timers, pushbuttons, pilot and indicator lights, and switches used in control circuits. JIC standards include symbols for control switches, sensors, and indicators with associated definitions. JIC standards and schematic ladder diagrams are used by most control system engineers, technicians, and electricians. PLC programming formats also include the schematic ladder diagram type of graphical programming adopted from the JIC standards. All symbols and standards rely upon the engineer for the proper application in developing fail-safe controls.

Instruments to detect flows, pressures, temperatures, and levels are used extensively on hydraulically operated bridges. Typically, the symbols used on hydraulic schematics are from NFPA/ANSI standards.[6] NFPA/ANSI nomenclature includes abbreviations for instrumentation and sensors like Float Switches (FS), Pressure Switches (PS), Temperature Switches (TS), and Limit (LS). The abbreviations from the ISA standards (International Society for Measurement and Control) are helpful when differentiating between a Flow Switch (FS), a Level Switch (LS), a

Position Switch (ZS), and a Pressure Switch (PS).[7] Control engineers must be careful not to mix symbols from conflicting standards identifying a Level Switch as "FS" for float switch, or a Position Switch as "LS" for limit switch or as "PS" for position switch. ISA, JIC, and NFPA instrument abbreviations conflict. The ISA standard provides the most comprehensive method for unique identification.

FAIL-SAFE CONTROL TECHNIQUES

There are many ways for control devices to fail to operate properly. While it is not impossible to design control systems that account for every possible combination of faults, it would be very expensive to do so. A more practical approach to designing fail-safe control systems is to account for the most probable modes of failures and provide control devices and techniques necessary for safety.

A fail-safe control device is one that will cause no unintended operations or unsafe functions if the device itself should fail. Figure 8 provides a generalization of some good and poor design practices. A common example is when using normally closed contacts on a control relay that is used in a motor starter circuit (Figures 9 and 10). An incorrectly engineered circuit, one that is not fail-safe, could result in the motor not being tripped if a control relay coil burns up or a fuse blows. A broken wire, or a bad relay coil should not cause a motor to start or prevent it from being stopped.

Another common example is shown in Figure 11 where a ground fault can start a motor unexpectedly if the controls are on the neutral side of the coil. This type of control is a National Electrical Code violation. [8]

Movable bridges use equipment that may become hazardous to the public if the controls should fail. A listing of some equipment and potential hazards follows:

- Traffic Gates and Barriers- A fault could cause the gate to unexpectedly operate with the bridge open to traffic or prevent the operator from stopping a gate operation.
- Center Locks- A fault could cause the lock to unlock with the bridge open to traffic.

- Drives and Brakes- A fault could cause the span to raise with the bridge open to traffic, or could prevent the operator from stopping the span from lowering with a vessel underway.
- Navigation Lights- A photoelectric relay circuit fault could turn off all of the navigation lights putting a vessel at risk of collision with the structure.

It is important to know how a sensor will be actuated and what that means for the associated machinery or equipment (Figure 12). For example: With a limit switch that is sensing the "released" position of a motor brake as required by AASHTO,[4] it is necessary to sense the "set" position independently from the "released" position. It is not the same to have a single switch make contact when the brake is in the "released" position and to assume the absence of a made contact indicates the brakes are "set." A loose switch or a loose wire would also appear to be an open contact to the control circuit and could result in unsafe control. When individual switches and circuits are used to positively sense when the brakes are "set" and "released," a circuit or switch failure can be detected more readily. Fail-safe interlocks and indications require a closed circuit to verify field condition. The absence of a signal should be interpreted as the absence of a control permissive and that conditions are not ready for operation. It is often just as important for the operator to know that a brake is not completely "set" as to know when a brake is fully "released."

In Figure 5, note the position limit switches and the temperature switches. They are available with normally open contacts "held" closed or normally closed contacts "held" open. It is the engineer's responsibility to define the contact development that is essential in designing a fail-safe system. The contact development must fit the application in the circuit for the desired operation during normal conditions and after a sensor or circuit failure. Position limit switch contact developments used on movable bridges are shown in Figure 13.

Figure 14 shows fail-safe and non-fail-safe methods for using position limit switches in a circuit for bridge leaf speed control. Design the circuit so the closure of the nearly open or nearly closed limit switch contact is a permissive signal to go to normal speed. The loss of the signal, whether caused by the limit switch contact opening or a broken wire, should cause the leaf to go to creep speed. The same is true for stopping the leaf using the full open and bridge seated limit switches. The absence of a signal should result in the leaf drive stopping.

In certain situations, consideration should be given to providing redundant switches for the full open or bridge seated limits. These would include situations where the limit switch arm may be prone to a mechanical failure or interference due to icing and other obstructions. The normally closed limit switch contacts are wired in series and are held in the open position when the bridge leaf is fully open or seated.

The temperature switch that is sensing a high temperature should be normally closed and should open upon high temperature conditions. This way a failed contact or broken wire, blown fuse, or loose terminal will result in a de-energized circuit (usually the safe case) and the high temperature interlock will close a valve, stop a pump, or allow a predetermined conditions to exist. The hydraulic pump motor control shown in Figures 9 and 10 illustrates this.

It is important to differentiate between controls used for alarms and indications only, and those needed for equipment shutdown safety. It is not always possible for an alarm to be generated by an open contact or by a de-energized circuit. Alarm conditions are usually annunciated by a light and a horn or buzzer, or by some other energized device. "Off the shelf" annunciators with built-in lights and audible devices are available which can be set to alarm upon sensing an opened contact. PLCs can be programmed to function the same way. Some owners who prefer to use relay control systems still use PLCs or microprocessor based annunciators for alarm handling because they are flexible and provide good historical data collection.

Figures 15 and 16 illustrate PLC control schemes for the hydraulic pump previously reviewed in Figure 10 using relay control. PLC triac outputs are acceptable for indication only. Triacs tend to fail in the short circuit mode. Such a failure would operate any device connected to the output if the control circuit has power up to the triac. For this reason, triac outputs are not recommended for motor control applications. Normally open PLC relay outputs are preferred.

Most PLCs are supplied with a watchdog timer that monitors logic circuits controlling the processor. If this timer is not reset in its programmed period of time (which is equal to one scan period), it will cause the processor to fault. Where a failure of the central processor can result in a significant hazard, an independent (external to the PLC) watchdog timer should be provided (Figure 17).

By programming an internal PLC cycle timer to start and stop external timers, the on and off cycling can be monitored as a "heart beat." The external timers provide a shutdown upon a PLC failure in either a high logic state (logic=1) or a low logic state (logic=0). Detection of unsatisfactory PLC operation should initiate an emergency shutdown. The external watchdog timers with a discrete input fed back to the PLC can be used to verify the operation of the input module, the central processor, and the output module.

There are some exceptions to using standard fail-safe controls. A different control system solution is needed when the equipment must remain energized during any fault condition. These applications are those that must be completely fault tolerant as opposed to fail-safe. This would be true for safety systems. A fire water pump is an example of one such system. The reason for this exception is that during a fire, it is likely for a control system to fault, but the fire is the greater risk. The design of such a circuit may need to consider special techniques including supervisory current to monitor circuit continuity and triple redundancy where two out of three devices can fail without consequence. Failure analysis for this type of system includes verifying the circuit can be turned on if one of the devices has failed, and that it can also be turned off. Sometimes when designing for one condition, the other is overlooked.

There will always be "exceptions to the rules" for the proper application of fail-safe control system techniques. It is therefore necessary for the engineer to assess each installation and application uniquely when developing the control system architecture.

FAULT TOLERANT CONTROL TECHNIQUES

A fault tolerant control system is one that has sufficient levels of redundancy to allow a single control device or group of devices to fail without affecting operations and the ability to control. A fault tolerant control system must be designed such that safety is not compromised in any way. The control interlocks must remain functional during the faults. Fault tolerant systems are often mandatory for the control of many chemical processes, burner management systems, and manufacturing systems where lost time of production or the safety risks outweigh the extra costs

associated with fault tolerant control systems. With these types of facilities, even if the controls are designed to fail safely and de-energize all machinery and equipment, sudden or frequent shutdowns may compromise the process equipment or the safety of the facility.

It is not usually necessary to provide fault tolerant control systems on movable bridges except for fire protection systems or similar safety systems. Some level of fault tolerance may be considered for bridges where the volume of roadway and marine traffic are high and a non-operational bridge could cause financial harm or impede emergency vehicles.

Until the 1980s, movable bridge controls were typically ungrounded. This made them fault tolerant for ground faults because if a circuit went to ground, it normally could not complete the short circuit to trip a breaker or blow a fuse, and the system would continue to operate. Operational safety is compromised with this concept since a second ground fault can result in unexpected operations. The NEC allows for ungrounded systems providing there is a ground fault indicator on the control circuit.[9] Some designs may have ground fault indication, but it is on the main service entrance, not on the control circuit. Because this type of system can "appear" to be operating normally, a ground fault can go unnoticed until there is a second fault. Generally, ungrounded control systems do not fail safely. There has been at least one incident resulting in a fatality caused by a second ground fault raising a bridge against moving traffic.[10]

Fault tolerance can also be achieved procedurally. Marine traffic is required to confirm that a bridge is fully open before proceeding underway through the structure. This is not always practical depending on the strength of the local tides, the navigational channel characteristics, and the size of the vessel. For large vessels, the bridge may need to be opened while the vessel is still a mile or more away so that if there is a fault in the control system, the bridge operator has time to employ emergency procedures.

It is a good engineering practice to include redundancy in the design for electrical power service, leaf drive systems, navigation lights, and traffic lights. There should always be an alternative means of operating the bridge. The AASHTO requirements and recommendations for redundancy, previously discussed, should be included in the control system design.

Emergency Stops

Emergency stops are required for all control systems. They are configured to remove power from machinery, equipment, and control circuits by opening hand switch contacts and contacts on master control relays (MCRs). This includes power to PLC outputs and other electronic output devices, and motor drives. Emergency stop circuits should be not be part of the normal operation. All of the emergency stop control devices should be dedicated to stopping all motors and removing control power from the motor controllers. In use, the emergency stop should cause all motors to de-energize and all brakes to set.

Some installations require the emergency stop circuits to be fault tolerant and fail-safe. In Figure 18, if a single MCR should fail, the shutdown circuit is not affected. It will require two MCR failures to affect a shutdown. Conversely, if a single set of MCR contacts become welded or seized together, or a spring fails; then the circuit will still provide a shutdown through the remaining two MCRs.

FAIL-SAFE AS AN ENGINEERING PHILOSOPHY

A lack of continuity in engineering safety techniques has been seen when comparing PLC control systems with hardwired relay control systems. Movable bridge control in some states has evolved from relays, to PLCs, and back again to relays. The knowledge of the engineers who once designed relay systems is not being passed along to the new engineers.

Certain design techniques that are fail-safe when using a PLC as a “relay replacer” are not fail-safe when using the same techniques with hardwired control relays. For example: In PLC logic, the software equivalent to a “normally closed” contact is often used in the control programs, and when the associated logical statement becomes “true,” the software contact is “opened.” This is acceptable in the PLC because internal self-diagnostics and “watchdog timers” constantly verify the PLC system is functional. A failure of any diagnostic test will result in the safe shutdown of the PLC system and all outputs are turned off. This is not the case for the equivalent hardwired control system (Figures 10 and 16). If there is a failure of the relay coil or a broken wire, the normally closed contact stays closed regardless of conditions that are supposed to open it.

It is the joint responsibility of the engineers and the owners to require fail-safe control systems. It is the responsibility of the engineers and their companies to be sure engineering techniques are defined, documented, and disseminated. The experience of the senior engineers must be passed to the engineering interns. At the same time, continuing education in control system safety for the senior engineers is necessary because control system devices are continually changing and being upgraded. Project schedules should provide adequate time for the control engineer to be thorough and complete in the application of fail-safe techniques. The control system symbols used in design look very similar (Figure 8). An improperly selected symbol, or a typographical error in a schematic or PLC program can result in catastrophe.

CONCLUSION

Engineering a control system to include fail-safe features requires knowledge of both the instrumentation and control devices, and the machinery to be controlled. It is necessary to design the control system architectures and circuits such that the machinery and equipment will de-energize upon a control device failure. It is also necessary to provide the engineering needed to ensure that electronic control system application programs and input/output configurations allow the same. While national and international standards address specific techniques, recommendations, and requirements to this end, it is still necessary for the controls engineer to make the final determination of the detailed design for each particular movable bridge facility.

Implementing engineering safety standards, alone, cannot assure absolute safety of operation. The ultimate safe operation and control of the system is in the hands of the contractor during construction, and the bridge tender and the maintenance personnel once completed. Fail-safe designs are not fail-safe if critical limit switches are defeated with jumpers or are bypassed. There is no substitute for diligent, capable, well-trained electricians, operators, and maintenance technicians.[11]

REFERENCES

1. JIC, *Electrical Standards for General Purpose Machine Tools and Mass Production Equipment, (EGP-1-67 and EMP-1-67)*, Joint Industrial Council, McLean, VA, 1967, pp. 32.

2. NFPA, *Electrical Standard for Industrial Machinery (NFPA-79, 1991)*, National Fire Protection Association, Inc. Quincy, MA, 1991, pp. 7.

3. Summers, A.E., *Safety Can Go Wrong- Fast,* InTech, Vol. 46, No. 11, November 1999, pp. 41-42.

4. AASHTO, *Standard Specifications for Movable Highway Bridges*, 5th Edition, American Association of State and Highway Transportation Officials, Inc., Washington, DC, 1988, pp. 36, 41, 47.

5. AASHTO, *Movable Bridge Inspection, Evaluation, and Maintenance Manual,* 1st Edition, American Association of State and Highway Transportation Officials, Inc., Washington, DC, 1998.

6. NFPA, *Hydraulic Fluid Power- System Standard for Stationary Industrial Machinery (ANSI/NFPA/JIC- T2.24.1, 1991)*, National Fire Protection Association, Inc. Quincy, MA, 1991.

7. ISA, *Instrumentation Symbols and Identification (ANSI/ISA-5.1, 1984)*, International Society for Measurement and Control, Research Triangle Park, NC, revised 1992.

8. NFPA, *National Electrical Code (NEC) (NFPA-70 , 1999)*, National Fire Protection Association, Inc. Quincy, MA, 1991, Article 430-73, pp. 271.

9. NFPA, *National Electrical Code (NEC) (NFPA-70 , 1999)*, National Fire Protection Association, Inc. Quincy, MA, 1991, Article 250-21, pp. 83.

10. Parsons Brinckerhoff, *Bridge Electrical Inspections*, PB Network, Issue No. 7, Vol. XV, No. 2, July 2000, pp. 40.

11. NFPA, *Ovens and Furnaces (NFPA-86, 1990),* National Fire Protection Association, Inc. Quincy, MA, 1990, pp. 17, 32.

LIST OF FIGURES