A message from Javad Rahimian, MCE Chief Executive Officer: This is a "must read" article for those who are impacted by the ***ASME A17.1-2000/B44-00 Safety Code for Elevators and Escalators*** *– including inspectors, consultants and field adjusters. Understanding and meeting the intent of the new code is a very time consuming and difficult task, and yet, it is extremely important to ensure compliance. Throughout this article, we will point out common misunderstandings and compare these against a design methodology that we have found to be effective at meeting the requirements of the new code. We appreciate ELEVATOR WORLD for providing this forum to educate our industry on issues of importance.*

ELEVATOR CONTROLLERS:
Common Misunderstandings Related to Compliance with *ASME A17.1-2000/B44-00 Safety Code for Elevators and Escalators*

by Pat Fleming

Introduction

At Motion Control Engineering, Inc. (MCE), *how* we respond to new elevator safety code requirements has changed dramatically since our company's early days. In the past, a few engineers would put their heads together and spend a few hours modifying our controller design to meet new code requirements. This simplistic process changed with the introduction of the *ASME A17.1-2000/B44-00 Safety Code for Elevators and Escalators.* These same engineers – now joined by a handful of others – would be involved in day-long meetings, some lasting well into the night, trying to understand just the *intent* of new language added to the code. The intent was so well hidden, that we were forced to submit requests for interpretation **before** the official release date. In addition, we hired code experts from the industry to help us with our task of interpretation and implementation of this new code. Never had we worked so hard to understand the reasoning behind the words.

Now that it's all said and done, we want to share a brief version of our experience with the industry. Clearly, to design a compliant controller, there can be no substitute for a thorough understanding of the A17.1-2000 Code.

Critical Operating Circuits

The 2000 Code defines a "Critical Operating Circuit" as one that is covered by a specific area of the code (see Rule 2.26.3). If electromechanical contactors or relays are used to implement any of these critical operating circuits, and if contacts on these contactors or relays are used to monitor their own status, then they must be contactors or relays of the "force-guided" type. These circuits include, but are not restricted to, those involving any electrical protective devices (EPDs) such as door locks, car gate contacts, overtravel limit switches, emergency stop switches, governor overspeed switch, emergency terminal stopping devices, buffer switches, ascending car overspeed protection and the device to prevent "unintended car movement."

These "critical operating circuits" also include circuits that restrict any car movement beyond leveling zone when door locks are not closed, speed monitor function circuits such as leveling overspeed detection and circuits that perform overspeed detection while on access or inspection operation. They also include circuits that prevent the car from reverting back to normal operation while on access, inspection, or any of the door bypass operations, and circuits that prevent bypassing of door locks or car gate contacts when the access mode or door bypass functions are returned to normal.

While this may not be a complete list, this provides a good idea of the majority of items that are covered by the very stringent new requirements of the 2000 Code. Many well-known items new to the code are being listed as EPDs, and this sudden increase in existing items becoming EPDs is a huge factor in the dramatically increased complexity of controllers that are truly compliant with the new 2000 Code.

When a single failure of any one of these critical operating circuits occurs, this **must not prevent** the circuit from safely performing its required function, and if the elevator is moving at the time of failure, it is permitted to go to the next landing and stop normally and then it will be prevented from running again. One alternative to this is as follows: at the **instant** that the single failure first occurs, if the related critical circuit is now no longer properly functional, then **the car must be shut down at that instant**. All of these requirements result in what is commonly termed "redundant safety operation" and the tests that detect the failures are sometimes referred to as "redundancy checks."

For example, if a single "standard" relay contact is used to bypass the emergency stop switch, a code violation results because the failure of this single contact could bypass the stop switch and create an unsafe condition. If the welding of a single contact would compromise safety, as a minimum, two contacts would need to be placed in series (redundancy). The same concept applies to solid-state devices used to bypass EPDs.

But this is still not sufficient, as the type of relay used in critical operating circuits is also defined by the new code. Note that a single force-guided relay could be used to bypass the emergency stop switch as long as it is

Continued

monitored and there is some *other* means to stop the car if it turns out the relay is stuck in the energized position. We will discuss later how we employ this method on MCE controllers.

Force-Guided Relays

When a relay is used in place of an EPD, it must be of the "force-guided" (FG) type. This means that if any single contact of the relay fails to change state, all of the other contacts must be prevented from changing state as well. In other words, welding of a normally open contact will prevent all of the normally closed contacts from making up. This enables the monitoring of any single FG relay contact to ascertain the state of all other contacts. The only alternative to the FG relay requirement is to monitor the contact that is carrying out the function of the EPD.

Returning to the stop switch example: 1) At least one FG relay must be used, and 2) when only one FG relay is used, the state of the relay *and* the stop switch itself must be monitored.

Another code requirement states that further operation of the elevator must be prevented after the first detected failure in any critical operating circuit. So if one of the relays being used to bypass the emergency stop switch fails to drop out, further operation of the car must be prevented.

MCE uses a single FG relay to bypass the in-car emergency stop switch. In Figure 1, note the location of the ESB relay and the single (normally open) contact that shunts terminals 18 to 20. Notice that the stop position of the in-car stop switch at RSTOP must be monitored in order to tolerate the single failure of this contact. When the stop switch is turned to the stop position it is expected that the STOP input will be deactivated. If this is not the case, the software system will stop further operation of the elevator by turning off the MPSAF and CSAF outputs (Figure 4), which drop the main safety relays and prevent further operation of the car.

But more must be done than simply monitoring the position of the stop switch.

Cycle Testing

Another requirement states that while on automatic operation, all critical operating circuits must be checked before the car is allowed to start. At MCE we have coined the term "operating cycle." During a floor-to-floor run, we define *operating cycle* as the time from which the controller picks a direction to the time when that direction is dropped. Certain circuits will change state as a result of moving from one floor to another. The door zone, leveling and direction relays circuits are examples of circuits that normally change state. Circuits that may not change state during a run need to be forced to change. We do this by using our cycle test logic to force all critical operating circuits that may not normally change state to change state once during each operating cycle.

For the emergency stop bypass logic we do this by picking and then dropping output ESBYP as part of our cycle test routine (refer to Figure 2). During the cycle test, we monitor a normally closed contact of relay ESB with input RESBYP and expect it to change state. If it does not, we prevent further operation of the car by turning off relays SAFR1 and SAFR2. This way any single failure of the input or output circuitry (latches, transistors, triacs, ribbon cables, connectors, etc.) or associated relays will be detected. Similar logic is performed for all FG relays.

Continued ▶

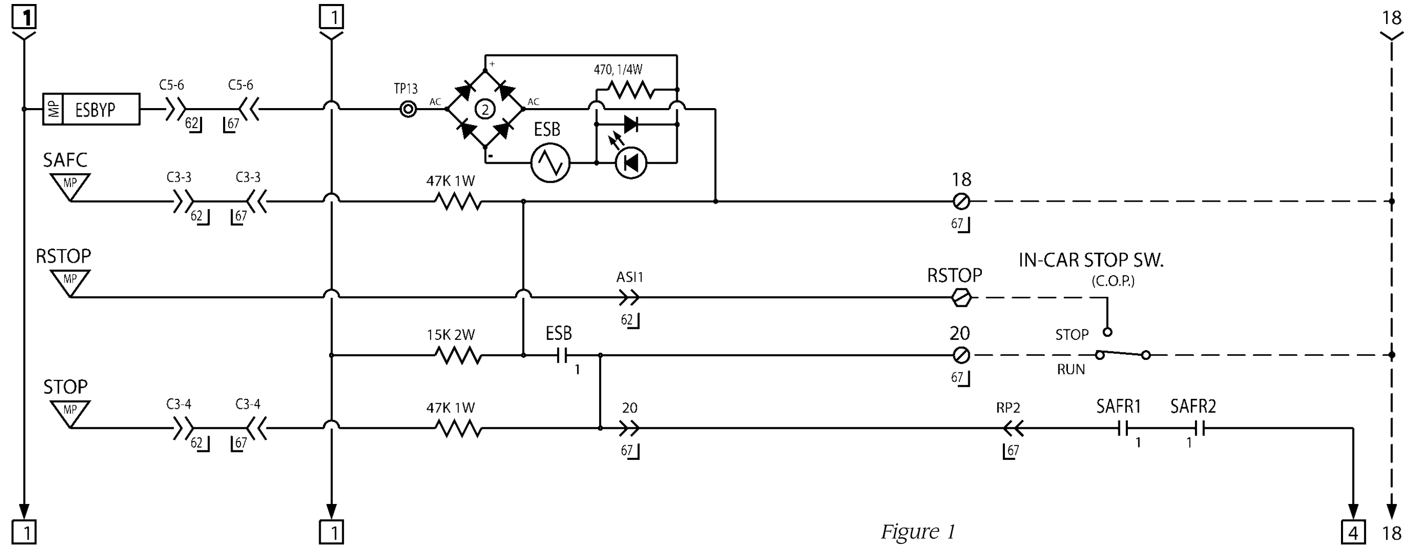

Figure 1

Continued

Door Lock Logic

Door lock circuitry is an example of a critical operating circuit that warrants special concern. Since ASME's introduction of car door and hoistway door lock bypass circuitry, many manufacturers have chosen to install relays in their controllers to carry out the function of the lock bypass switches. But even before the introduction of door lock bypass logic, the door locks were routinely bypassed to allow releveling at the floor with both of the hoistway doors in the open position. This was typically accomplished by placing a combination of leveling and door zone relay contacts around the door lock circuitry.

The new code now defines the hoistway door and car door electric contacts as electrical protective devices. This means any relays used to bypass these circuits must be of the force-guided type and must be monitored. These include the door zone, door lock bypass, leveling and inspection access relays. Some manufacturers are still using standard relays for these circuits, and are failing to monitor for the first failure.

For all of the circuits just mentioned, MCE uses force-guided relays and monitors these same relays. We even go one step further. For example, when a car makes a no-call stop, parking with doors closed, the door lock relays will not drop out. This is why we include cycle testing logic to force the drop out of all the relays associated with the door electric contacts. We monitor contacts of these FG relays and expect a state change during cycle testing. Again, this process is necessary in order to meet the requirement that all critical operating circuits are checked before the car is allowed to restart.

Software System Monitor

Language was added to the 2000 Code that requires controller manufacturers to monitor for a "software system failure." Simply driving a standard relay with a microprocessor output, which was standard practice on pre-2000 products (refer to Figure 3 – CSAF output), is not sufficient. The software monitor must be separate and independent of the software system. If the software monitor drives a relay, it must be a force-guided relay that is monitored at least once per operating cycle.

In order to meet this requirement, MCE has made extensive changes to our software and microprocessor support logic. Since we use the software system to monitor for single failures of solid-state devices, relays or other components used in critical operating circuits, it becomes essential to monitor for a failure of the software. In this way, we prevent a software system failure from compromising control system safety.

MCE uses a timer called a "watchdog" to monitor the software system for proper functionality. We do this by first breaking the software program into small modules. Each module, as part of its routine, sends a pulse to the watchdog, but only if certain "check sum" logic is validated first. If the watchdog fails to receive a pulse in 200 mS (i.e., the software is not executing its program correctly), the output of the timer is turned off, and relay SAFR2 (refer to Figure 4) is dropped, which shuts down the car. Since it is part of a critical operating circuit, the functionality of the watchdog must be checked once per operating cycle. This is part of the cycle testing logic.

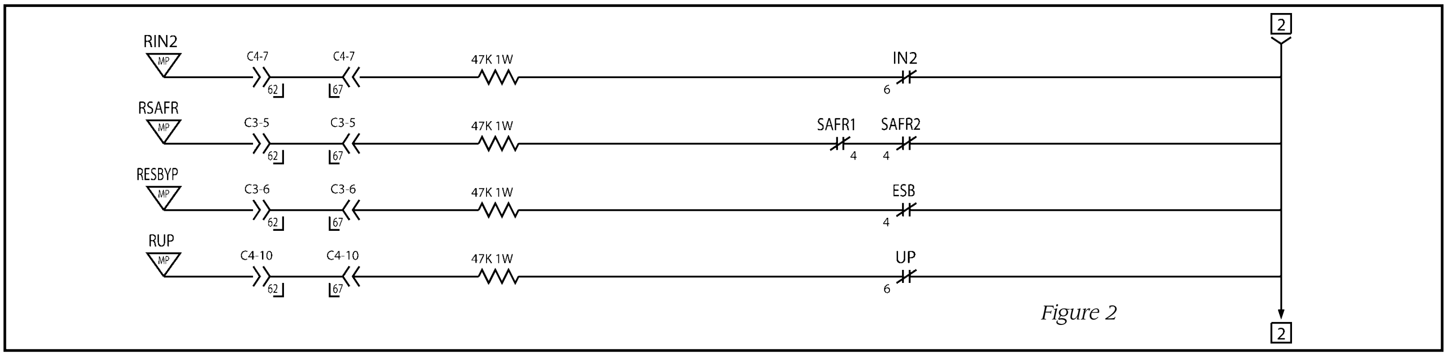

Figure 2

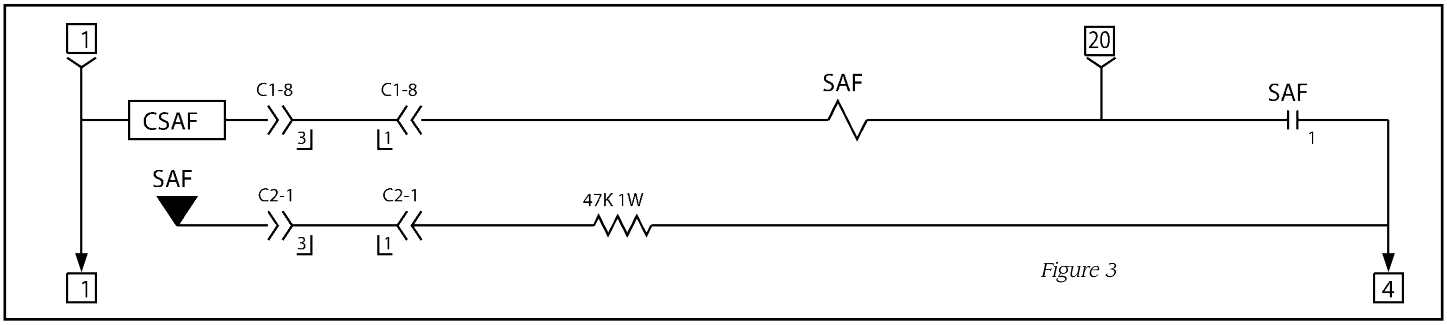

Figure 3

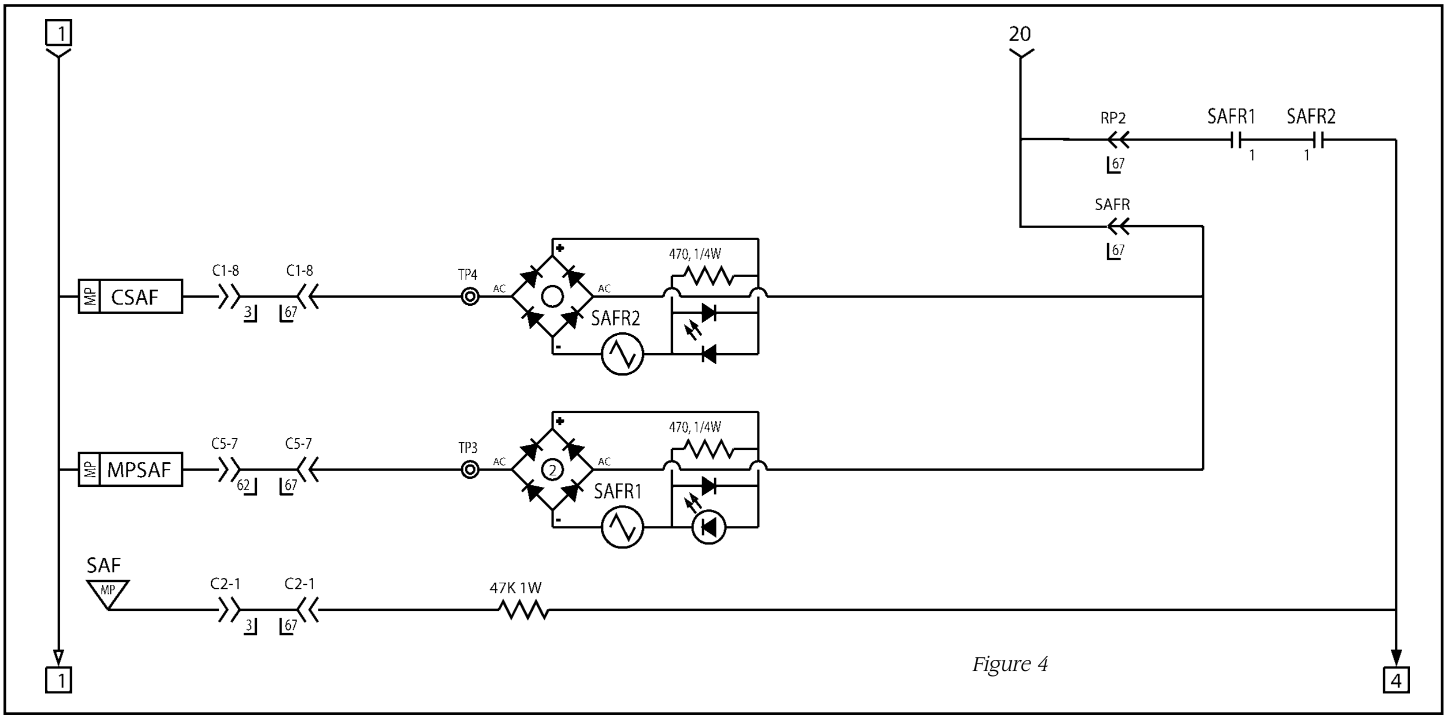

Figure 4

MCE takes this logic one step further during cycle testing. First the processor stops sending pulses to the watchdog and expects that the FG relay, SAFR2 (controlled by the watchdog output), will turn off. This causes input SAF to go low (refer to Figure 4). Next, the processor drops out relay SAFR1. Both primary FG safety relays having dropped out result in input RSAFR turning on (refer to Figure 2). Once the processor sees this input activated, it resumes sending pulses to the watchdog and expects input RSAFR to go low. Finally, the processor picks up relay SAFR1, which reestablishes the safety circuit.

Note that during the drop out of the safety relays, all critical operating circuit components connected to the #4 bus will be dropped out. Normally closed contacts of these FG relays are monitored and if any fail to release as intended, the system is shut down. Of course, we have logic that allows for slow relays to drop out and if a single failure is detected, we will cycle the logic again (four attempts are made) to try to free up any problematic contacts, thus averting intermittent service calls. (Note: any time a single contact fails to release, an "event" will be stored to memory. This event prompts the maintenance mechanic to execute preventative maintenance and thus avert a potential shutdown.)

Final Motion Control Means

Looking at the valve operating circuitry, some manufacturers use contacts of standard relays to energize the valve solenoids from a voltage source that is not qualified by the safety circuit, door locks or limit switches. A failure of these non-force-guided relays could allow the car to run without regard to the status of the safety circuit or door locks.

The control voltage supplied to the valve coils on an MCE hydraulic controller is first routed through the safety circuit, then the door locks and finally through contacts of force-guided relays that are monitored for proper operation. This design methodology provides maximum safety to the elevator riding public.

Electromagnetic Immunity

A further requirement of the new code states that the completed controller will be subjected to high levels of radio frequency interference (RFI). This testing must be performed by an independent testing laboratory and needs to prove that the elevator responds in a safe manner to such levels of RFI-as specified by the code.

In summary, when replacing the function of an electrical protective device with solid-state devices, relays or software systems, the circuit used to replace the EPD must be designed so that a single failure of one of the components does not compromise safety. Second, the resultant critical operating circuit must be monitored so that the first failure of any component is detected and further operation of the car is prevented until the failure is corrected. Third, failure of the software system must not in any way compromise safety. Fourth, all critical operating circuits must be checked once per operating cycle. Finally, high levels of RFI must not compromise the safety of the complete controller. If any of these steps has been neglected, the resultant control system does not comply with *ASME A17.1-2000/B44-00 Safety Code for Elevators and Escalators*.

Pat Fleming *is a senior design engineer*
at Motion Control Engineering.