A Safety Instrumented Function (SIF) may be typically required to shut-off electrical equipment such as pump, compressor motors, etc., to protect or avoid unwanted dangerous events, and reduce a specific risk to an acceptable level.

Usually the required action by the SIF final element is achieved by cutting or removing power to the motor, which is done through a motor starter, contactor, or other intermediate device that allows to stop the flow of current, (usually 3 phase power source to motor). (Low, medium voltage is understood to be 600 Vac or less).

The failure rate of a typical pump, motor starter is approximately $2.78 \times 10^{-6}$ /hour, (which is often an electromechanical relay).

In order to de-energize the control coil of the motor starter, which is the one that allows the current flow to the motor, it is necessary to interrupt the control circuit of the coil M1, (control circuit voltage is often 120Vac).

The control circuit resides in an enclosure called motor starter cubicle or “bucket” which usually is found in a motor control center, MCC. (The following control circuit is one of the most commonly found).

Figure 1: Typical Control Circuit Enclosure and Circuit Diagram
Figure 2: Typical Motor Control Centre (MCC) Enclosures

Motor control center (MCC)
When developing the Safety Requirement Specifications of the conceptual SIF, special attention should be given to the final elements in order to ensure that they execute shutoff correctly. The final element of the SIF is composed of,

- Cables to an interposing relay, (the majority of safety PLCs only provided 24 Vdc output modules and therefore an interposing relay is then needed),

- Interposing relay

- Motor starter.

The probability of failure on demand of each component should be determined individually, (i.e. 3oo3 for cable, interposing relay, and motor starter).

Installation Considerations: Special care should be given to the cable, circuit integrity, between PLC output module, the Interposing relay, and the motor starter. A good recommendation is to install the interposing safety relay inside the “bucket”, such that circuit integrity between the interposing safety relay and the motor starter is achieved by the protection provided by the motor starter cubicle.

If the safety function requires de-energize-to-trip, no further consideration is given to the circuit integrity between PLC output module and the normally open, (NO), interposing relay. However, if the motor starter requires energize-to-trip, the following are recommended.

- The safety logic solver should be supplied with a mechanism to test for cable integrity or

- A normally closed, (NC), interposing relay is used inside the “bucket”. This relay will be energized by the output module of the logic solver. In this way the logic solver needs to energize the circuit up to the interposing relay, while the output of the relay will be de-energized.

When the logic solver de-energizes the output signal from the output module, (or the cable is accidentally cut), the interposing relay will close, (energized to trip between relay and motor starter, while motor starter will cut power to motor). Note: If a Safety Integrity Level 2, (SIL 2), or higher is required for the SIF, then the hardware fault tolerance, HFT, tables from IEC 61511-1 must be followed.

Guillermo Pacanins
P.Eng., TÜV FS Engineer, TÜV FS Expert