MITIGATING RISKS:
Fail-Safe Design Principles in Modern Automated Facilities

Robert van Akelijen, P.E., CFEI S-E-A

In 2005, there was an explosion at a Texas City refinery, which resulted in 15 deaths, 180 injuries and 43,000 people were ordered to shelter in place. The plant was going through a startup process and an instrument mounted on a chemical separation tank was not properly calibrated, resulting in an improper hazardous liquid level reading in the tank. This led the operators to believe the liquid level was much lower than it actually was. A secondary level-sensing switch on the tank failed to trigger a high-level alarm that began a chain of events, which ultimately led to the explosion.

How often do we turn on the news and the lead story is similar to this scenario about an explosion, fire, spill or chemical release from a manufacturing/process facility? The results of the event can be devastating with consequences such as poisonous gasses being released into the atmosphere, land being polluted, fish and wildlife endangered or killed, or people being evacuated from their homes. No one wants to experience the fallout of such an event, and no one ever intends for something like this to happen. Within almost every manufacturing/process facility is an automation system designed and programmed to control the process and mitigate the likelihood of a catastrophic event. Automation and control systems are used in power plants, wastewater treatment plants, oil refineries, pulp and paper, pharmaceuticals and many more. Fail-safe is defined as, "incorporating some feature for automatically counteract-

ing the effect of an anticipated possible source of failure." How can a fail-safe design and configuration help potentially mitigate and prevent these scenarios?

Automation and control systems consist of devices that gather information about how the process is operating and make decisions about how to control the process safely and efficiently. Another requirement of these systems is to identify when the process is wandering outside normal operating parameters towards a hazardous situation and to make major corrections or terminate the process if and when that occurs. The information gathered from the system might consist of pressures, flow rates, temperatures or some other measurable characteristic. These are the inputs to the system. The control or shutdown of the process may be opening or closing valves, turning on or off heaters, or starting and stopping pumps. These are the outputs of the system. Both the inputs and outputs are considered the first level of the automation and control system. The next level is the controller, which is programmed to manage the outputs based on the status of the inputs. This is typically an industrial computer referred to as a programmable logic controller (PLC). For a given system, there may be multiple PLCs based on the size and complexity of the facility. The next level in an automation and control system is the visualization of the system. This is achieved by presenting the information via graphical representations and alarms to the person operating the process that details how the process is proceeding and what corrections the PLC is making to keep the process running.

Fail-safe automation should be considered at all levels, starting at the design phase. During this phase, automated equipment should be specified such that it is fail-safe, i.e., so that in a failure event such as when energy is removed, the equipment is able to move to its safest state. The failure may be a power outage, a loss of instrument air pressure, a tripped circuit breaker, a blown fuse or anything that prevents the PLC from controlling the end output devices.

An example of a device that can have a fail-safe design is an air-operated valve. Air-operated valves are typically specified as fail-closed (air to open) or fail-open (air to close) (See Figure 1). The system designer must determine the safest position of the valve if system air is lost and specify the valve so that it moves to that position when there is a loss of control. A common assumption would be that the default specification is fail-closed as that should be the safest position, but what if that valve was providing cooling fluid to an engine? A fail-close valve would close on the loss of system air, preventing cooling fluid from getting to the engine to keep it cool.

Think of the valve that supplies water to our refrigerator ice maker. These products require electrical power to open the valve (fail-closed) to provide water to the ice maker, but what if the ice maker requires electrical power to close the valve (fail-open) and there is a power outage? In the event of a loss of power, the valve would open, allowing water to flow, which would cause potential flood damage to our homes. This example would not be a fail-safe design of the refrigerator ice maker. In a simple system such as this, it may be easy to specify the correct fail position of the valve, but in complex process plants, that design decision may not be so clear.

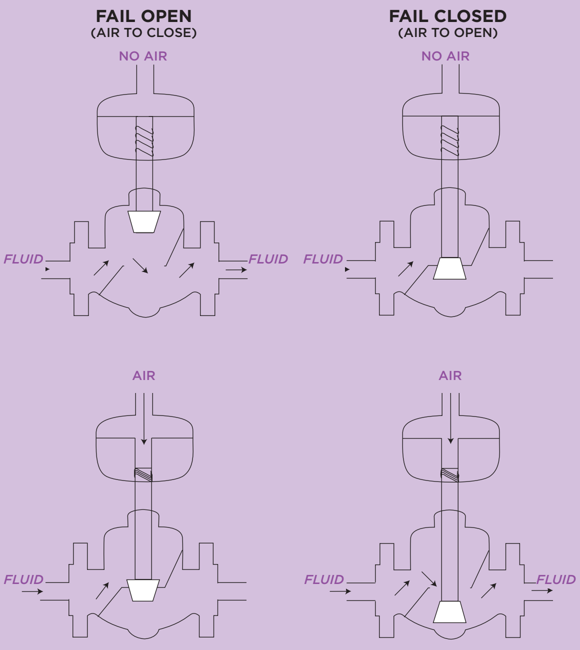

FIGURE 1 – Valve positions without air and with air for fail open & fail close configurations

All input signals should be wired in a manner that the PLC is receiving an input signal when the process is normal. This is considered fail-safe because in the event of a tripped breaker, blown fuse or severed signal wire, the loss of the normal input signal would trigger the PLC to take an action. This action may simply be to generate an alarm to an operator, or it may be critical enough to shut down part or all of the process entirely.

Everything discussed so far is part of the normal design of an automation and control system, but what else can be done to make the system safer from failures? Building redundancy into the design is one of the ways in which a system can be made safer. Redundancy is defined as, "serving as a duplicate for preventing failure of an entire system upon failure of a single component." Every component in an automation and control system can be designed with redundancy. The PLC can also be designed in a redundant configuration. In this scenario, a second PLC is synchronized with the controlling PLC and can seamlessly take over control of the system in the event of a failure of the controlling PLC. Power supplies that provide power to the PLC and to field instrumentation can be redundant, so one power supply failure does not shut down the system. The actual field instrumentation can be redundant as well. The system designers of the automation and control system need to analyze what components are critical enough to warrant redundancy to make the system safer in the event of a particular failure.

An Uninterrupted Power Supply (UPS) can also play a useful role in allowing the PLC extra time to shut down the system processes to a safe state. A PLC with backup UPS power can be programmed to recognize a power outage and take the control action necessary to shut down the process to its safest state. Additionally, while motors and pumps will stop and air compressors will no longer deliver pneumatic air to systems during a power outage, the PLC should be programmed with a safe shutdown sequence. The PLC should also be programmed with a safe startup sequence after any shutdown to prevent equipment from starting prematurely.

Even with our best efforts, failures are still possible. A properly specified air-operated valve may not move to its fail-safe position due to an unknown internal or mechanical failure. However, a properly designed, installed, configured and maintained fail-safe automation and control system can help a facility prevent the loss of life, environmental damage and/or damage to equipment resulting from these unexpected failures.

Robert van Akelijen, PE, CFEI is an electrical engineer with S-E-A. He is an experienced automation specialist with a demonstrated history of working in the oil and energy industry. At S-E-A, he investigates electrical faults and malfunctions and analyzes and evaluates a wide array of automation systems to determine the cause of loss, malfunction, and/or poor performance.