Control System Failure **Survival Strategies**

When bad things happen to good control systems, it's best to know in advance which of several strategies will be used, why, and how.

Graham Nasby

What happens when control systems fail? It is not so much the response, but the response planning that is crucial to failure situations. No technology is perfect, so possible failure types must be identified and strategies developed to handle each one of significance. This is not to say that an engineered approach is required every time, but factors such as how the system is monitored, alarm system capabilities, availability of operators, process uptime requirements, probability of occurrence, possible consequences, and process safety, just to name a few, must always be considered.

> "No technology is perfect, so possible failure types must be identified and strategies developed to handle each one of significance."

Why? Control system robustness and reliability have come a long way in the last 30 years. Automated control systems are now considered to be a vital part of the infrastructure that helps ensure the smooth running of plants, pumping stations, utilities, and processing facilities.

Several approaches are commonly used to deal with control system failures:

1. Manual operator shutdown: Perhaps the simplest response to a control system failure is to have an operator shut down the process manually. In some systems where there are no significant safety concerns, operators are always available, and there is a way the operator can easily notice a problem, an operator-initiated approach is sometimes used. But make sure you know how the operator would notice a failure and the consequences if there was a time delay before the operator shut down the process.

2. Emergency stop: In many jurisdictions, processes must have emergency stop buttons installed. In the case of a control system failure, these can provide an easy method for a quick manual shutdown. The downside is that these typically initiate hard shutdowns, which may not always be the best response. Since this is still a manual shutdown method, it depends on the operator noticing the problem and being able to react to it in a timely manner.

3. Automatic to manual: Another option is to switch the process equipment from automatic to manual mode and then continue to run the process. While this may avoid a shutdown, running a process manually without the aid of the automated control system should only be considered with great caution and when potential risks are acceptable. The process must be simple enough that it won't overwhelm an operator, even during an upset. Furthermore, any potential safety risks must be carefully identified, evaluated, and managed. Likewise, any potential impacts on the alarm system and/or reduced data logging capability also must be carefully considered.

4. Safety system shutdown: Processes that warrant automated independent safety systems will often respond to a failure by generating a hard shutdown, but not always as a direct result of the failure. Safety systems can range from simple emergency stop circuits to highly redundant ISA84-style SISs (safety instrumented systems) that use multiple automatic shutdown techniques. However, the SIS may not respond until the failure lets the process get out of control and trips an alarm. It is a reactive approach rather than a proactive method of dealing with a failures, and will likely result in a hard shutdown.

5. Redundancy: An alternate method for dealing with control system failures is to make the control system less prone to failures by using redundancy. Redundant components such as backup power supplies, multiple processors, fault-tolerant I/O cards, dual-trunked networks, and backup instrumentation, along with automatic fail-over logic, can significantly reduce the chance of control system failure. By handling failures with built-in redundancy in the primary control system, costly hard shutdowns can often be avoided. This approach does come with a cost since implementing redundancy into a control system can often be an expensive undertaking.

6. Secondary redundancy: When a fully redundant primary control system is not feasible, consider a secondary control system. A

ONLINE

For more information, visit:
www.eramosa.com

"When a control system failure occurs, it is usually preferable to rely on control system redundancy and/or backup control systems, otherwise control system problems typically result in shutdowns."

secondary control system can take over the process when a process value (such as a tank level) exceeds a point that the normal control system would prevent it from reaching, or when the primary system indicates a fault. Secondary control systems often have their own sensors, which have the benefit of being unaffected by instrumentation failures in the primary control system.

For example, a sewage pumping station with a sewage holding tank could use a PLC with a level transmitter for its primary control system, and a set of float switches with electric relay logic as its backup control system. If the PLC or level transmitter fails, the float switches and relays would then take over control of the pumps. In many systems, a well-implemented secondary control system can result in significant uptime improvement at an attractive price-point. However, implementing secondary backup control systems can present challenges when designing how output devices, such as pumps and valves, are to transition smoothly from primary to secondary control when required. Being able to transition output devices and final control elements in an automated fashion requires careful planning and system integration.

Choose among options

In general, when a control system failure occurs, it is usually preferable to rely on control system redundancy and/or backup control systems, otherwise control system problems typically result in shutdowns. Furthermore, having an operator continue to run the processes in manual mode is not always an option due to staffing levels and potential safety concerns. Systems that can auto-recover from minor problems are almost always preferable to ones that require operator intervention.

Effective plant design requires a diverse engineering team and a multifaceted approach. Starting with knowledge of the process itself, the team must consider the characteristics of both the process and control system. Control system failures are a possibility that we all have to be aware of. The key is to make sure that when they happen, there is a solid plan and strategy in place for how to deal with them. **ce**

Graham Nasby, P.Eng., PMP, engineer, Eramosa Engineering Inc., Guelph, Ontario, Canada, is among Control Engineering Leaders Under 40, Class of 2011.