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

10/21/2011

What happens when control systems fail? It is not so much the response, but the response planning that is crucial to failure situations. Like all other fields of engineering, control systems require careful planning and design to deal with every foreseeable situation, including failures, whenever feasible. No technology is perfect, so possible failure types must be identified and strategies developed for the handling of 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.

Why? Control system robustness and reliability have come a long way in the last 30 years. The automated control system is now considered to be a vital part of the infrastructure that helps ensure the smooth running of plants, pumping stations, utilities, and processing facilities. In all but the most specialized and small scale processes, the days of operators routinely turning valves, starting and stopping pumps by hand, and monitoring mechanical gauges are over. Low-level tasks are now typically handled by automated control systems.

Certain 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 (staff person) 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. If using a manual shutdown approach, careful consideration has to be given to how the operator would notice a failure and what the consequences would be if there was a time delay before the operator was able to shut down the process. For facilities without personnel and/or plants with limited alarm system capability, this approach can be difficult to use effectively.

2. Emergency stop: In many jurisdictions, processes must have emergency stop and/or process stop buttons installed. In the case of a control system failure, these can provide an easier method for an operator to quickly shut down a process. The downside is that these types of buttons typically initiate hard shutdowns, which may not always be the best response for certain types of control system failure. For example, in some water pumping applications having an operator start an auxiliary pump is preferable to an operator-initiated shutdown. Like the previously mentioned manual shutdown method, the manually initiated emergency/process stop approach also 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 have an operator switch the process equipment from automatic to manual mode and then continue to run the process in manual mode. Depending on process design, this may or may not be possible. While this approach may seem attractive for a process uptime perspective, simply running a process manually without the aid of the automated control system should only be considered with great caution. The process must be simple enough that an operator can run it manually without become overwhelmed, and the operator must be able to deal with any process upsets without the aid of the now-disabled control system. 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 before attempting to run a process manually. For some processes, the approach of having an operator run them in manual mode might not be acceptable due to the potential risk

involved.

4. Safety system shutdown: In processes that warrant automated independent safety systems, the safety system is another way that control system failures can be handled. For processes that use them, the safety system is typically designed to generate a hard shutdown. Safety systems can range from simple emergency stop circuits to highly redundant ISA84-style SIS (safety-instrumented-systems) that use multiple automatic shutdown techniques. The caveat with relying on the safety system to handle a control system failure is that the process often has to get out of control for the safety system to be activated. It is also a reactive approach rather than a proactive method of dealing with control system failures. The end result of a safety system being activated is almost always a hard shutdown, which has obvious impacts on process uptime.

The approaches above react to the results of a control system failure, rather than the control system failures themselves.

5. Redundancy: An alternate method to 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. Implementation challenges may exist in some primary control systems to provide for bumpless transfer among redundant system components.

6. Secondary redundancy: When having a fully redundant primary control system is not feasible, a slightly different approach is to have a secondary control system as a backup. Use of secondary control systems can be particularly well suited for applications where the cost of a fully redundant primary control system is prohibitive. A secondary control system is typically designed to "take over" the process in one or both of the following situations: (a) when a process value (such as a tank level) exceeds a value that the normal control system would prevent it from reaching, or (b) when a system health signal from the primary control system indicates that the secondary system needs to take over. Secondary control systems often have their own sensors, which have the benefit of being unaffected by instrumentation failures in the primary control system.

A secondary control system can also be triggered by a wired "failsafe," often an electrical signal, that indicates a failure 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 smoothly transition 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. When no redundancy and/or backup control systems are used, control system problems typically result in shutdowns. Furthermore, the response of 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 control system problems are almost always preferable to ones that require operator intervention each time a problem is encountered.

Effective plant design requires a diverse team of professionals and a multifaceted approach. Starting with knowledge of the process itself, the design team must consider the individual characteristics of the process and control system characteristics. 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 on how to deal with them.

- Graham Nasby, P.Eng., PMP, engineer, Eramosa Engineering Inc., Guelph, Ontario, Canada, is among *Control Engineering* Leaders Under 40, Class of 2011. Posted by Chris Vavra, *Control Engineering*, www.controleng.com

Nasby, a licensed professional engineer, has worked in various industries ranging from IT and software development to pharmaceuticals and semiconductor manufacturing. He designs automated control and monitoring systems for the municipal water/wastewater sector at Eramosa Engineering Inc. Graham is also a contributing member of the ISA18, ISA101, and CSC/IEC TC65 standards committees.

www.eramosa.com

Process Control Channel

<- Back to: Home