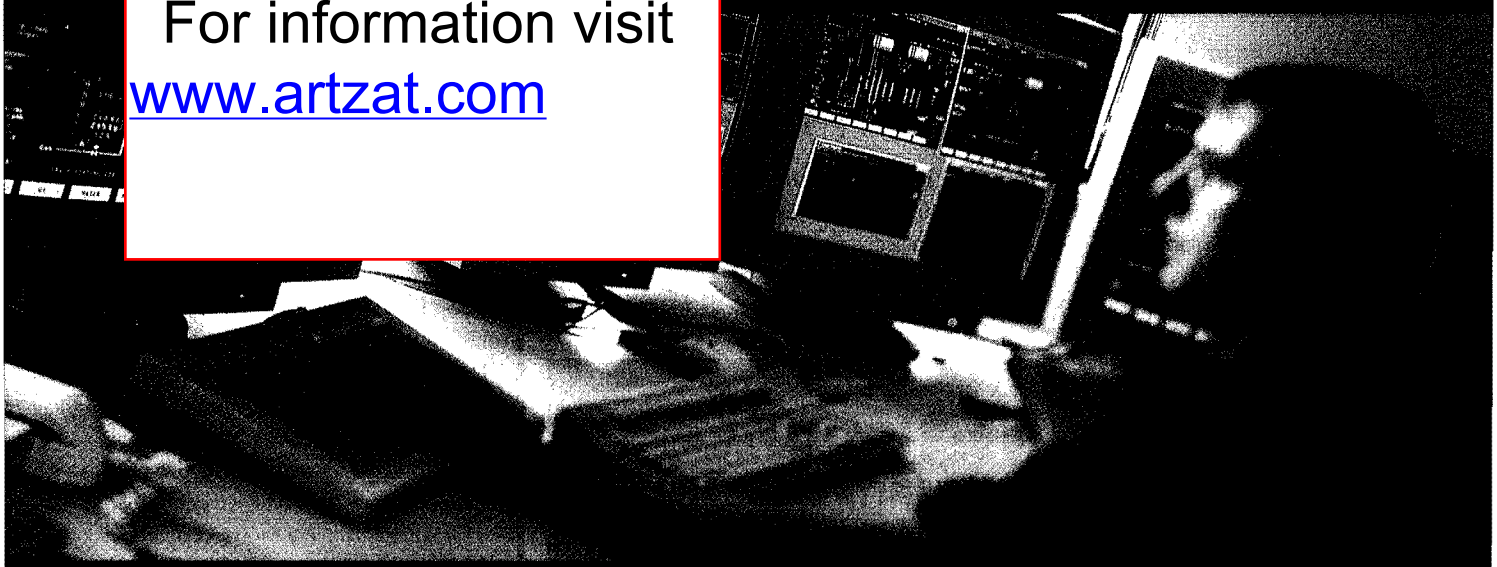

HOW TO VALIDATE

BY ARTHUR ZATARAIN, P.E.

TAKE ADVANTAGE OF MISSED OPPORTUNITIES TO TEST REDUNDANT AND BACKUP SYSTEMS

Many of us are inclined to ignore the time honored adage, "If it ain't broke, don't fix it." Sometimes our handyman instincts can't leave well enough alone. Yet that same intuition also encourages us to believe, "If it ain't broke, don't test it." This reluctance is especially evident when it comes to testing the redundant and backup features of our critical control systems. At best, failures resulting from inadequate testing will only cost you lost production. At worst, insufficient testing can cost you your job.

Get hip to R&B

Although the terms redundant and backup (R&B) are often interchanged, each represents a different aspect of reliability design. A redundant system uses multiple similar components in a configuration that permits simultaneous performance of the same (or similar) function. A redundancy failure causes no reduction of system operation or capability. Simple examples include parallel power supplies and series shutdown valves. A more sophisticated example is a redundant PLC system: a microchip fails, a warning light comes on and production continues normally. A key aspect of redundant systems is that multiple components do the same job at the same time.

A backup system takes a different approach to reliability by providing an independent means of performing all or part of the overall control function, usually in a primary and standby configuration. Manual or automatic transfer mechanisms determine which component takes the lead. For increased reliability, backup systems can use alternate configurations and technologies to improve resistance to single-point and common-mode failures. For example, a simple local controller that can operate without assistance from a plant-wide control system is a common instance of backup technology. The local system may lack bells and whistles, but at least it can maintain safe production should the primary system go offline.

Backups also can be found within the control system's support structure. A frequent example is an uninterruptible power supply (UPS) that delivers reliable energy to many electronic control systems. If the primary power goes away, the UPS instantly takes over to maintain essential control functions — at least as long as the batteries hold out.

Note that redundancy and backup are not mutually exclusive. Many control systems have separate elements of both, and some even combine them into so-called redundant backup systems that have high levels of fault tolerance. Such systems include two or more similar control entities, each having full capability, but based on different technologies. Having two independent and diverse control systems is often considered the best protection against unanticipated failures.

In addition to improving reliability, R&B controls can simplify routine operating facility maintenance and avoid downtime. R&B concepts allow portions of the control system to be repaired offline while the controlled process remains in service. Special operating modes such as manual supervision may be required, but the ability to perform online testing of items like relief valves and meter runs is a valuable benefit of high-reliability systems.

Test to ensure safety

Some industries, such as aerospace and nuclear, routinely test redundant and backup systems because reliable technology is essential to their high-risk business. But less-risky industrial users don't always adopt a mission-critical approach to testing R&B performance. Everyone in industry has heard war stories of redundant and backup systems that failed to do their job, explained with statements such as, "The UPS should have kept us going," or, "The redundant processor had an outdated program." The subsequent diagnosis is often performed through a rear-view mirror, with perhaps some adjustment to future maintenance procedures. But in reality, proper testing of R&B systems remains on the back burner of many maintenance programs.

Of course, the less exotic elements of R&B systems, such as inputs and outputs, are often tested during routine control system maintenance. However, such checks are often limited to calibration and physical care. This level of maintenance may test the heart of an R&B system, but not its soul. A true test requires simulation of the specific transient conditions for which the R&B systems are designed. Proper R&B testing requires more than simply faking a process fault to verify that the system performs its normal role. R&B testing also should include challenging their unique nonstop features to verify reliable performance even while partially disabled.

Simulations that merely pull the plug might not represent realistic failure modes.

Further, the requirement to routinely verify R&B operation is becoming increasingly important because of safety-related standards such as IEC 61511 and ANSI/ISA S84-2004. These internationally accepted guidelines define Safety Integrity Levels (SIL) and Safety Instrumented Systems (SIS) that generally rely on redundant and backup systems. Merely designing controls to meet those standards isn't sufficient to satisfy existing and pending regulations. Proper testing and verification of specific redundant and backup features is essential for meeting both the spirit and letter of those standards.

Test under operating conditions

A proper test of redundancy and backup requires producing operating conditions that mimic failures of the control system and its various support systems. These tests must go beyond the manual or automatic diagnostics built into many R&B systems (i.e. the UPS "test" button). Those diagnostics are generally local to the device and might not adequately test responses to external problems. Although built-in tests help verify operation of an R&B component, they can't verify reliable system operation for situations that involve interconnected units.

A true test requires simulation of the special transient conditions for which the R&B systems are designed.

So how can the R&B functions best be tested? There's no easy answer. Every redundant and backup system has its own requirements. But a common theme is to simulate fault conditions that are unrelated to the controlled machine or process. A significant goal is testing the redundant or backup system's ability to maintain operation during and after a transient condition that interrupts normal operation, including loss of the primary control system. Therefore, testing one part of an R&B system usually requires disabling other parts under conditions that simulate real-world failures.

Another key testing goal is to validate the R&B system's ability to alert operators to a partial failure. In addition to seamlessly maintaining operations, the R&B system must accurately indicate that it or its partner is impaired. Without such notification, corrective action may be delayed or overlooked until after the remaining portions fail.

Fortunately, functional testing of R&B systems is usually more fun than routine maintenance work. Rather than calibrating transmitters or greasing actuators, we get to kill half of a redundant system and suffer nothing beyond a warning light. Or we can disable a remote speed control and watch the lowly backup governor maintain operation. And then there's everyone's favorite — pulling the plug on a UPS and grinning when nothing bad happens. Can testing really be that simple? Maybe not.

The UPS example may seem like a good idea, but many UPS manufacturers will disagree. An often-overlooked effect of simply pulling the plug is disconnection of important ground and neutral references that help the UPS monitor primary power. A better UPS test procedure is to remove power at the circuit breaker or other convenient upstream point to introduce transients similar to a power outage. Only then can the ability of a UPS system to sense, switch and supply be truly field-tested.

Likewise, simulations that merely pull the plug on an input, communications link or processor might not represent realistic R&B failure modes. Input signals don't usually go away, but they do drift out of specification. Similarly, communications links don't always go quiet — in fact, they're more likely to get noisy when they fail. And processors are rarely known to leap from their happy home in the electronics rack. A more realistic procedure will mess with the power or communications going into a processor, or to an output coming from the processor, to determine if its R&B control partner can carry on.

Establishing adequate test procedures therefore requires careful consideration and planning. The tests can't merely be convenient or arbitrary — they need to be realistic. And they need to be part of the facility's regular maintenance plan.

Test during maintenance

In theory, we should be able to test redundant and backup systems anytime we want. If they work properly, there's nothing to fear. In reality, R&B testing for a non-shutdown event rarely occurs until after the system fails to perform. Perhaps the lapse is from fear that the R&B system won't work. No one wants an unexpected shutdown noted in their permanent file. The logical solution is to combine R&B testing with other maintenance procedures in which an unexpected shutdown can be tolerated.

For example, many off-line maintenance activities begin with a functional test of the emergency shutdown (ESD) system. Few maintenance tasks are more satisfying than watching an automatic control system stop a complex machine or process in a safe, organized sequence. Similarly, a planned shutdown is an ideal time to test the failure modes of redundant and backup systems to verify that they don't interrupt a process. Functional R&B tests are therefore usually best accomplished just before performing the scheduled ESD.

If you suspect shortcomings in your R&B maintenance, consider building a multi-disciplined team to raise awareness and evaluate your needs. Proper testing likely will require input from many sources. Be sure to include the usual suspects — plant utilities, communications, engineering and operations. But also include lesser players such as safety, training and administration, all of whom share your interest in seeing redundancy and backup systems perform as planned. There's little doubt that attainable goals can be set. But chances are, the path to those goals begins with you.

Arthur Zatarain, P.E., consults in technology and intellectual property through Artzat Consulting, LLC (www.artzat.com). Contact him at arthur@artzat.com.

MORE AT WWW.PLANTSERVICES.COM/THIS MONTH

Fuzzy logic for process control — "Fuzzy logic"
Ultrasonic leak detection — "Getting to the source"
Condition monitoring — "The power of decentralization"
Electrical test equipment — "Testing, testing"
Performance — "A new way to think about control loops"

For more, search www.plantservices.com using the keywords failure, redundancy and UPS.