

# Plant Services

THE BENCHMARK FOR SUCCESSFUL PLANT SYSTEMS & MANAGEMENT

For info on this article make contact through [www.artzat.com](http://www.artzat.com)

## Power trans troubles?

**IMPROVE** RELIABILITY WITH PRE-ENGINEERED CONDITION MONITORING

Outwit four major control-system gremlins

Ammonia refrigeration is still cool

Resources to assure mechanical integrity



# Outwit

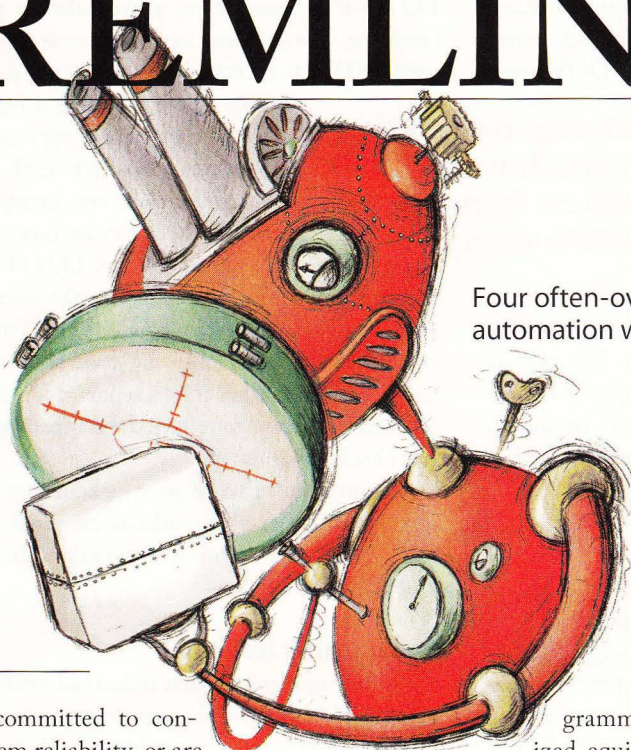
---

## CONTROL SYSTEM

---

# GREMLINS

---



Four often-overlooked flaws can creep into automation while you're not watching

By Arthur Zatarain, P.E.

**A**re you committed to control-system reliability, or are you merely involved? Ruthless oilman J.R. Ewing, of TV's "Dallas" fame, once explained the difference by saying, "It's like ham and eggs at breakfast. A chicken was certainly involved, but that pig was *committed*."

The folks who count on you to design and maintain a reliable control system won't expect quite such commitment from you. But they do expect a commitment to a control system that meets their expectations for performance, safety and economy. Although you know your systems inside and out, and often check their pulses, small problems can fly below radar to decrease reliability and dramatically increase downtime.

My experience in field service and forensic engineering has shown that ordinarily dependable systems can be jinxed by relatively minor oversights. Smooth-running systems might be the most vulnerable because they are rarely analyzed. The four situations discussed below range from obvious to obscure, but all of them might be closer than you think.

### Incompatibility

I've never seen a relay that stumped me, but I've certainly worked with my share of perplexing PLCs and other pro-

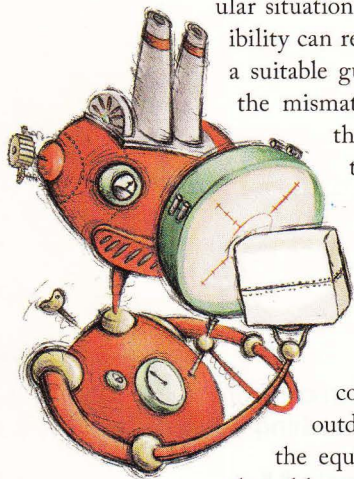
grammable devices. One certainty about computerized equipment is that every element must be 100% compatible: hardware, operating software, application programming and even interconnecting cables. Every aspect must fit perfectly to produce a reliable system.

With modern controls, even a small PLC can contain multiple processors, as well as several I/O and communications boards, each driven by onboard microprocessors. Those devices must have the proper operating codes (either ROM or firmware) to function properly with the particular variant of your application code. It's not always obvious that yesterday's program might be incompatible with today's apparently identical spare processor. Therefore, control-system reliability is quietly threatened by the continually evolving software provided on replacement parts.

I tripped over this anomaly while analyzing an accident on a circuit board manufacturing machine. The used equipment had been damaged in shipment, and the PLC processor had been replaced with an assumed compatible part — same brand, same part number — but with a later version of firmware. The machine operated normally for weeks before a safety switch failed to prevent automatic operation. The problem was traced to a "trick" in the ladder logic that had been used to work around a flaw in the firmware of earlier

controllers. Although the flaw was rectified on later controller boards, the earlier work-around was incompatible with the firmware. The manufacturer's literature explaining the situation had never made its way to the factory floor.

Merely installing a spare card, therefore, might introduce unanticipated operation that goes unnoticed until a particular situation arises. Even a known incompatibility can result in expensive downtime until a suitable guru can be located to coordinate the mismatched parts and programs. Even the best guru can have his hands tied until a vintage DOS-based



**The bottom line here is that although you have lots of spare parts on hand, they must be 100% compatible.**

computer can be found to run the outdated software needed to update the equipment. The bottom line here is that although you have lots of spare parts on hand, they must be 100% compatible. Will you be able to determine compatibility in real time while costly production slams to a halt? If not, then now's the time to work out a better plan.

### Fused ESTOP/LOTO

Although ESTOP and LOTO sound like space-age cartoon characters, they're better known as emergency stop and lockout-tagout — two essential components in any reliable control system. Both relate to halting an industrial machine or process effectively. However, ESTOP and LOTO serve significantly different purposes that can inadvertently work against each other if improperly coordinated. Careful consideration during initial design and later modification is essential for reliable control-system operation and maintenance.

ESTOP is aimed at producing a safe and immediate shutdown during any phase of operation. Its primary goal is minimizing harm to people, property, production and the planet. The details of performing an ESTOP vary greatly among situations, ranging from very simple (as in a drill press) to very complex (as in a roller coaster). Regardless of any particular design, every ESTOP system shares the common feature of simple and latched activation: once you push the red mushroom, it activates a safe mode, and nothing short of a manual reset will restart it.

LOTO, on the other hand, affects nonoperational maintenance concerns that are generally handled by specifically trained maintenance staff. LOTO usually occurs via a pre-planned process rather than as a single action, and applies primarily to offline equipment. Although some aspects of ESTOP and LOTO often overlap, a major philosophy difference is that ESTOP doesn't demand relief of stored energy.

In fact, stored energy is often required during ESTOP to prevent undesired motion.

Alternately, LOTO requires removal of all energy sources, such as electrical, pneumatic, hydraulic and mechanical. LOTO also requires a means to test its effectiveness before maintenance begins. That particular aspect is one area that can affect control-system reliability when ESTOP and LOTO functions overlap.

I once analyzed an accident involving mixed ESTOP and LOTO that occurred on a hydraulically powered foundry conveyor. The incident began when a maintenance worker used ESTOP to halt the power source and disable the actuator controls before servicing a high-pressure hose. Although the machine appeared dormant while the controls were tested, the energy trapped within the system was enough to remove his arm when the hose was disconnected.

One flaw in that LOTO process was the incorrect use of ESTOP to disable the solenoid valves. Subsequent testing after the ESTOP suggested that the conveyor was inert, but only the controls were dormant. The use of ESTOP, rather than a separate LOTO control mode, blocked the means to relieve the trapped pressure and properly check for stored energy.

If controls are part of your lockout-tagout process, make certain the entire plan works as expected. It's possible that working controls are needed to make sure the equipment is indeed locked out.

### Analog input isolation

It's widely recognized that industrial analog inputs are rated to withstand specific over-voltage conditions. A lesser-known aspect is the potential (and undesirable) interference with adjacent points on a multipoint analog input device. This isolation rating is far from standardized, and is sometimes difficult to determine without digging through the detailed technical specs.

Input systems designated as isolated are generally non-multiplexed and don't suffer from this limitation. However, many analog input systems, especially in lower-cost equipment, use multiplexing circuits that are subject to adjacent channel interference. The detrimental effects might be temporary, or they can persist until power is removed from the entire device.

This phenomenon might have caused a gas-detection failure in a supposedly fault-tolerant system based on redundant processors. Although the system correctly indicated a faulted input, the program had no means to sense the inaccurate measurements on other inputs that shared the same analog input multiplexer. This resulted in a high gas situation that went undetected until a flash fire destroyed a section of the facility. Had the operators known of the isolation problem, they could have disconnected the faulted input, thereby reinstating the integrity of the remaining inputs.

The gas-detection system was subsequently rebuilt using

more expensive and space-consuming isolated inputs — probably a good plan in any fault-tolerant system. Regardless, understanding this phenomenon and planning for its eventual occurrence is essential when using non-isolated analog inputs.

So, what's installed in your systems?

### Outdated panel layouts

No one intentionally plans a confusing panel layout, yet examples of poor designs are common throughout industrial installations. Sometimes no one seems to know what all the buttons and lights really mean. Some flaws are inherent in the original design, whereas others creep into the system because of well-intended but poorly executed field modifications. The poorly labeled controls that result can diminish reliability at the very time it's most needed.

I once investigated a horrific fatality caused by relocation of an existing panel to the opposite side of a battery recycling machine. Although the manual controls still functioned properly, they had been rotated 180° out of sync with the physical orientation of a multi-ton hydraulic ram — moving the lever left now moved the ram to the right. Under normal conditions this left-right disorientation was of little consequence. But when an equipment operator frantically pushed the control to free a trapped maintenance worker, the panicked rescue efforts actually made the situation worse. The result was a decapitation under manual control.

Improper field modifications are a frequent source of control-system problems. Perhaps a few replacement tags and minor wiring changes would have prevented that disaster. Are all your panels properly oriented and labeled?

### Bonus tip

Although the problems described above aren't insurmountable, they require focused attention that's difficult to schedule in a busy work environment. Here's one tip that won't cost you a bundle, and is so smart that you'll claim you thought of it yourself: Recruit a co-op student or summer intern to survey your systems, and then have him document what's both right and wrong.

A mid-level engineering or industrial tech student will be eager to delve into those systems you'd rather not revisit. Untainted eyes will spot illogical control layouts, missing documentation and incompatible spare parts. He'll be thrilled to salvage a vintage laptop and link it to a real-life PLC while building your disaster-recovery kit. And you'll make good use of the final report that details the good, bad and reliability-challenged aspects of all your control systems.

Don't just stay involved in control-system reliability — get committed. That way we'll never have to meet by accident. ☺

Arthur Zatarain, P.E., owns Artzat Consulting LLC and is vice president of TEST Automation & Controls, both in New Orleans. Contact him at [arthur@artzat.com](mailto:arthur@artzat.com).

## INDUSTRY DEMANDS, WE DELIVER!



Our CHARTS, PENS and RIBBONS enhance the operation of all leading chart recorders. Your data is only as good as the product it's recorded on.

For over 40 years, we have been supplying recording consumables manufactured to the highest quality to ensure your data is accurately captured.

Experience the difference.  
Trust your data only to the best!



**KOKUSAI CHART**

800-841-6870 [www.kokusai-usa.com](http://www.kokusai-usa.com)

Because Shepard Niles cranes and hoists last for decades, parts sourcing is critically important.

Today, Shepard Niles turns around 80 percent of parts orders in less than three days, with a huge inventory of genuine Shepard Niles parts in stock, available overnight.

We know exactly what you need, and we know you need it fast.

Shepard Niles equipment lasts practically forever. That's why we're looking for the oldest Shepard Niles crane or hoist still in routine use. Help us find it, and you can win \$250. cash for yourself and a voucher for \$500. in Shepard Niles parts for your company.

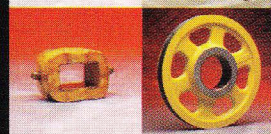
Deadline for entries is March 15, 2005. For details, call toll free or e-mail [contest@us.konecranes.com](mailto:contest@us.konecranes.com)

A service of KCI Konecranes  
220 N. Genesee Street  
Montour Falls, NY 14865  
(800) 481-2260

1 TON SHEPARD NILES  
#G 85001

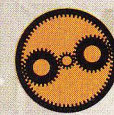
### We've Got It:

The world's largest inventory of in-stock parts for Shepard Niles cranes and hoists!



### Do You Have It?

The oldest Shepard Niles Hoist still in routine use today. If you do, you can win big!



**SHEPARD  
NILES**

[www.shepard-niles.com](http://www.shepard-niles.com)