

The restore drill

Backup ≠ restore proof

One drill this month

1

Pick one controller or HMI

The one that would hurt most at 3 a.m.

2

Restore to spare hardware

A real target, not a file-open test

3

Time it, start to running

Measured, not estimated

4

Write down every surprise

The surprises are the deliverable

Then record the evidence.

Handover packages list restore proof: when, on what target, by whom, in how long.

What a drill exposes: firmware drift • missing licences • an engineering tool that won't run on any current laptop • drive parameters saved outside the program • access that works for one person, who is on leave.

Four questions per alarm

ANSI/ISA-18.2

IEC 62682

1

Cause

What condition actually fires it?

2

Consequence

What happens if nobody acts?

3

Action

What is the operator supposed to do?

4

Priority

Do consequence and response time justify it?

Expect the list to reorder.

Rank by count to find candidates — number seven may cost more attention than number one.

An alarm that can't answer all four isn't an alarm. It's a **notification wearing an alarm's clothes** — and it trains operators to acknowledge without reading.

Six things your redundant pair shares

Check before you claim redundancy

Power

One board, one UPS, one breaker upstream of both

Time

One source can disorder both histories at once

Configuration

The same latent defect, deployed twice

Engineering access

One laptop, one credential set, one session

Maintenance

One procedure, one technician, one shift

Common cause

Heat, water, vibration, EMC, a shared cable tray

Redundancy does not protect against a fault you installed twice.

Parallel maths assumes independence — the moment both channels depend on one thing, the calculation is fiction for every failure that thing can cause.

Diagnose a loop in this order

Tuning last

Every time

1

Measurement

Clean signal? Correctly ranged? Right for the duty?

2

Valve

Strokes smoothly? Travel at normal load? Positioner calibrated?

3

Design

Is the loop structure right for the disturbances it sees?

4

Tuning

Only once the three above are sound

No combination of P, I and D removes hysteresis or stiction. You only chase it — and the tuning hides the fault until it resurfaces as scrap or a trip.

Names a stranger can act on

Write for the 2 a.m. reader

~~M0.0~~ → **MOT_FEED_Running**

Boolean — type, area and state legible at a glance

~~%MW100~~ → **rTankLevel_pct**

Analog — type, name and unit carried in the name

Scattered tags → **Valve_101.Status**

Group related signals into a user-defined type

Hardcoded 4500 → **PRESET_FillTime**

Every consequential number gets a name and a source

Step_3_on → **STEP_Fill / ST_Running**

Modes, states, alarms and interlocks each get a form

M0.0 is a fact about memory. MOT_FEED_Running is a fact about the plant. The convention only works if it's written down and everyone uses the same one.

Four places a flat spot hides

IEC 62443 zones

One hunt this week

A device with two NICs

Quietly bridging what the firewall separates

An unmanaged switch

Added during a commissioning crunch years ago

A cellular gateway

Vendor-installed for “temporary” remote support

A maintenance laptop

Both worlds, one NIC, one login

The paths you didn't draw

Shared services, identity, time, wireless, portable media

Find it. Record it. Change nothing.

Log it through your site's cybersecurity process. A cable pulled by someone acting alone is how a survey becomes an incident.