

FIELD CASE STUDY — CONTROLLER DOWNTIME MONITORING

The Failure That Reports Nothing

How independent, around-the-clock monitoring of controller connectivity catches the one failure traditional systems can't see — the controller that goes offline and stops reporting

24/7 independent monitoring of controller connectivity — Kalder watches the controller itself, not only the data it sends	Real-time alerts the moment a controller stops reporting — caught before staff arrive in the morning, not after	0 silent outages — a controller that stops reporting can no longer go unnoticed	Overnight the unattended window where a silent outage would quietly spoil a full case, closed
---	---	---	---

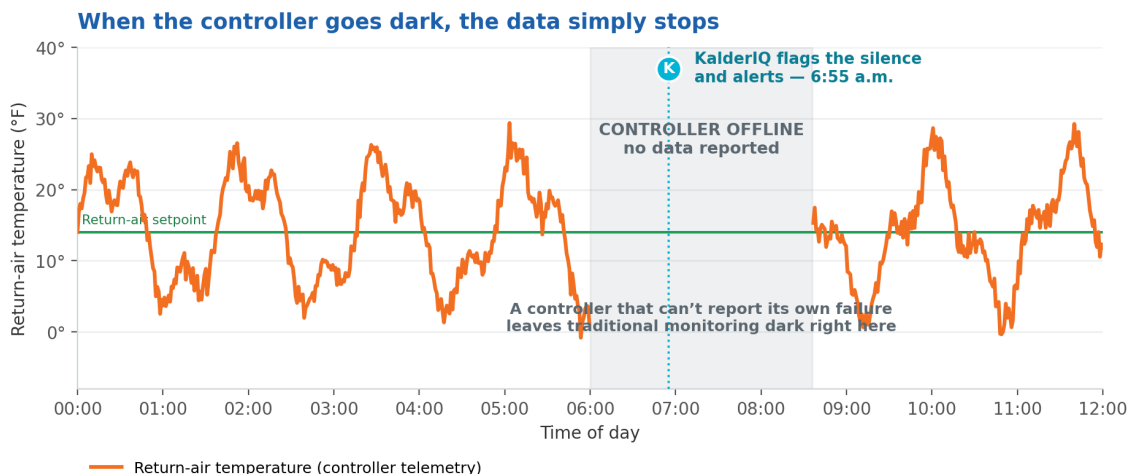
A refrigeration failure does not have to be dramatic to be expensive — it only has to go unnoticed. Early one Sunday morning, before 7 a.m., a monitored store's refrigeration controller stopped communicating. On a system that trusts the controller to announce its own problems, that kind of failure simply disappears from view: the trace goes quiet, nothing trips, and everything looks calm. KalderIQ — Kalder's AI monitoring system — watches controller connectivity independently of the controller, so it saw the silence and raised the alert while the store was still empty.

The outage that reports nothing

Most refrigeration monitoring depends on the controller to raise the alarm. That works for the failures the controller can see — a temperature crossing a setpoint, a defrost cycle that hangs. It does nothing for the failure where the controller itself goes offline: a hung logger, a dropped connection, a malfunctioning or powered-down controller. When the device that is supposed to report the problem is the problem, the alarm never comes.

The danger is that an absence of data looks exactly like calm. A blank or frozen trace does not trip anything, and overnight — with no one on site — an offline controller can sit unnoticed for hours. By the time a person physically notices, usually a warm case at store-open, the outage has already run its full length and product may already be gone.

“A failed controller can't raise its own alarm. The most dangerous outage is the one that reports nothing at all.”



Reconstructed return-air trace through the event. Telemetry cycles normally until the controller goes offline before dawn and the data simply stops — the shaded window is the outage. KalderIQ, monitoring connectivity independently, flagged the silence and alerted at 6:55 a.m.; a controller-dependent system shows nothing across the same window. Data resumes once the controller is restored.

What KalderIQ does differently

KalderIQ monitors controller connectivity and operational state continuously and independently — it watches whether the controller is reachable and reporting, not only what the controller says. The instant a controller stops communicating or malfunctions, KalderIQ registers the loss of signal itself as the event, rather than waiting for an alarm that, by definition, can no longer be sent.

On the Sunday in question, the store's controller went offline before dawn and stopped reporting. KalderIQ detected the dropped connection and alerted at 6:55 a.m., flagging the controller as offline or malfunctioning and prompting immediate response to restore communication — a remote reboot and, where needed, a service dispatch. Visibility was restored quickly, and the outage was measured by how fast it was answered, not by the hours until someone happened to walk past.

Why “going dark” is the failure that hides

A controller-dependent system has a structural blind spot: it can only report the failures the controller is alive to detect. Loss of the controller is the one failure it cannot announce — and it is among the most consequential, because every case and rack on that controller is unmonitored until it is back. The true cost of such an outage is set by its duration, and its duration is set by how long it stays invisible.

Monitoring connectivity independently closes that gap. KalderIQ treats silence as a signal: the moment telemetry stops, the clock that used to run unattended until morning instead runs for minutes. That converts an invisible, open-ended outage into an immediate, actionable alert — and restores the system visibility that every other layer of protection quietly depends on.

The bottom line

No one on site did anything wrong; the controller simply could not announce its own failure, and a system that waits to be told would have waited until morning. Independent connectivity monitoring removes the assumption that a quiet system is a healthy one. By watching the controllers themselves — around the clock, regardless of whether they can still report — KalderIQ catches the outages that would otherwise go dark, and keeps the rest of the monitoring honest.

Estimate basis & assumptions

Figures are illustrative and provided to convey behavior and scale, not to state values at a specific site. The event is based on a real controller-offline alert: on a Sunday morning a store's refrigeration logger reported its controller closed or malfunctioning and the monitoring software could no longer see current data, with the alert raised at 6:55 a.m. The return-air trace is a representative reconstruction of an outage of this kind, not raw telemetry; the data gap depicts the period the controller was offline and reporting nothing. KalderIQ monitors controller connectivity and operational state independently of the controller's own reporting, and initiates response — including remote reboot and service dispatch — to restore communication. The customer and site are described generically to protect confidentiality.