Pinecrest Regional Water District (Sample)

Ignition MRI (Mapped Risk Inspection)

Backup taken	**2026-10-06**
Platform	**Ignition 8.1.44**
Report date	**2026-10-23**
Prepared by	**Artek Integrated Solutions · artek.io**

> Every risk found in the supplied gateway backup, ranked by severity and rated for effort to fix, with the evidence for each. The scan reads the backup only. It cannot see the PLC at the far end of a device connection, the database the queries run against, or the operator who clicks the wrong thing at shift change.

SAMPLE

1. Summary for the people who own the budget

This is a sample report. Pinecrest Regional Water District is a fictional organization. Every finding below is a type the MRI scan actually detects, drawn from patterns seen across real Ignition systems, but the names, counts and details are invented to show what a report looks like.

Pinecrest runs one Ignition gateway for its SCADA screens and reporting, with shared code in a parent project both inherit. The most urgent problem is security: three web endpoints hand any file on the server to whoever asks, with no login. Several problems fail silently instead: a data purge was written but never scheduled, six operator buttons do nothing when pressed, and a third of the tags have stopped recording history. On performance, one polling timer runs in three projects at once, and on recovery a restore would break every screen that uses a third-party chart module. The cheapest fixes this week take minutes each: schedule the purge, fix the buttons' script scope, fill in the Create Project permission, and turn on scheduled backups.

The review checks nine areas, and every one of them turned up something here:

AREA	CRITICAL	HIGH	MEDIUM	LOW
1. Scripts that fail quietly		2	1	
2. Security exposure	2	3	1	
3. Performance time bombs		1	2	
4. Database queries		1	1	
5. Tag and UDT structure		1		1
6. Alarm configuration		1	2	
7. Dead code and orphans			1	1
8. Upgrade readiness		1		1
9. Backup and recovery reality			2	1

SAMPLE

2. What we looked at

Backup	`Pinecrest_SCADA-backup-20261006.gwbk`, 61.4 MB, type DATA_ONLY
Gateway	Ignition 8.1.44, single gateway (no redundancy)
Projects	4 enabled and 1 inherited parent; 214 views; 88 named queries; 31 web endpoint resources
Tags	4,120 tags across 2 providers; 610 alarms; 1,380 with history
Databases referenced	SCADA_DB and Reports_DB on the district SQL Server. Contents **not** in the backup

3. Findings, ranked

#	SEVERITY	EFFORT	CATEGORY	FINDING
MRI-01	Critical	half-day	2	Three web endpoints hand any file on the server to whoever asks
MRI-02	Critical	half-day	2	Two passwords are written into the script library
MRI-03	High	quick-fix	1	A nightly data purge was written but never scheduled
MRI-04	High	quick-fix	1	Six operator buttons do nothing when pressed
MRI-05	High	half-day	2	Active Directory sign-in runs unencrypted
MRI-06	High	half-day	2	The gateway runs a build inside a published advisory range
MRI-07	High	half-day	2	The gateway reaches its database with the administrator account
MRI-08	High	quick-fix	3	The same polling timer runs in three projects at once
MRI-09	High	half-day	4	Fourteen database calls build SQL by pasting values into the query
MRI-10	High	quick-fix	5	1,340 tags send their history to a provider that no longer exists
MRI-11	High	half-day	6	Two alarm journals write to the same table
MRI-12	High	half-day	8	A restore breaks every screen that uses a third-party chart module
MRI-13	Medium	multi-day	1	214 error handlers hide failures instead of recording them
MRI-14	Medium	quick-fix	2	An audit profile exists but records nothing
MRI-15	Medium	half-day	3	38 query tags hit the database every five seconds, all day
MRI-16	Medium	quick-fix	3	Eleven screen bindings refresh every second
MRI-17	Medium	multi-day	4	Eleven named queries paste raw text into their SQL
MRI-18	Medium	project	6	Alarm priorities are upside down
MRI-19	Medium	half-day	6	412 alarms show no location when they fire
MRI-20	Medium	quick-fix	7	An old revision of the SCADA project is still running
MRI-21	Medium	quick-fix	9	Scheduled backups are switched off
MRI-22	Medium	quick-fix	9	Historian pruning is switched off
MRI-23	Low	various	5, 7, 8, 9	Housekeeping items, listed in one table

SAMPLE

MRI-01: Three web endpoints hand any file on the server to whoever asks

Severity Critical · **Effort** half-day · **Category** 2 Security exposure

What happens. Each of these endpoints takes a file path from the request and reads that file from the gateway server, with no limit on which folder it may reach. None requires a login. Each checks a token first, but the token is one fixed value shared by everyone, and the screens put it in the image links every operator's browser loads. Anyone who has opened those screens, or seen one of their links, can read the gateway's configuration files, its security keys and any other file the gateway service can open.

Evidence. `projects/SCADA_Shared/com.inductiveautomation.webdev/resources/file/` holds `serveFile`, `serveImage` and `thumbnail`. Each passes a request parameter to `system.file.readFileAsBytes` with no folder restriction, and each `config.json` has `require-auth=false`. The token is a memory tag that nothing in the backup ever changes. The endpoints sit in the inherited parent, so they are served on every inheriting project's address.

Fix. Look files up by an id from a table instead of accepting a path, or resolve every path against one fixed folder and refuse anything that leaves it. Require a login on each resource, and take the shared token out of links the browser receives.

Reference. Ignition manual, WebDev module and system.file functions.

MRI-02: Two passwords are written into the script library

Severity Critical · **Effort** half-day · **Category** 2 Security exposure

What happens. A mail server password and a historian database password are typed directly into script code. Anyone with Designer access can read them, and they travel inside every project export and every backup, including the one supplied for this review. Treat both as already disclosed.

Evidence. Library modules `shared.email` (line 41) and `shared.history` (line 18), each assigning a literal value to `password`. The values are not reproduced here.

Fix. Move both into a Secret Provider, read them at run time, then change both passwords.

Reference. Ignition manual, Secret Management.

MRI-03: A nightly data purge was written but never scheduled

Severity High · **Effort** quick-fix · **Category** 1 Scripts that fail quietly

What happens. A function that deletes data older than two years is written and correct, and its own comment says it should run nightly from a gateway timer. No timer calls it. Nothing errors and nothing is logged, so the tables it was meant to keep in check have simply kept growing. This is the most dangerous kind of problem a backup review finds, because the first symptom is usually the database hitting its size limit and the application failing to write.

Evidence. `shared.maintenance.purgeOldRecords`, documented "Run nightly from a gateway timer script". No timer or scheduled script references it.

Fix. Add the timer the comment describes. Before the first run, check how much it will delete, since years of backlog make it a long transaction; run that first pass in a maintenance window.

Reference. Ignition manual, Gateway Event Scripts.

SAMPLE

MRI-04: Six operator buttons do nothing when pressed

Severity High · **Effort** quick-fix · **Category** 1 Scripts that fail quietly

What happens. These buttons' scripts are set to run in the client. Perspective scripts run on the gateway, so a client-scoped action never executes: operators press the button and nothing happens, with no error on screen or in any log. Two of them acknowledge alarms.

Evidence. Six Perspective event scripts configured with `scope: "C"`, in `SCADA/Overview` and `SCADA/Alarms`.

Fix. Change each script's scope to Gateway.

Reference. Ignition manual, Perspective component events.

MRI-05: Active Directory sign-in runs unencrypted

Severity High · **Effort** half-day · **Category** 2 Security exposure

What happens. The gateway checks passwords against Active Directory over plain LDAP with encryption switched off, so every sign-in sends a domain password across the network in readable form.

Evidence. User source `PRWD_AD`, port 389, SSL off; two identity providers sign users in through it.

Fix. Switch to LDAPS on port 636, then change the directory service account's password.

Reference. Ignition manual, Active Directory user sources.

MRI-06: The gateway runs a build inside a published advisory range

Severity High · **Effort** half-day · **Category** 2 Security exposure

What happens. Ignition 8.1.44 is inside the affected range of CVE-2026-92817, rated 8.8 out of 10, which lets a signed-in user with access to a Vision project reach Designer-level rights and run code in the gateway. The Create Project permission is also blank, the condition of a second advisory, CVE-2026-77393.

Evidence. Backup version 8.1.44; both advisories are fixed in 8.1.55. Create Project role empty.

Fix. Fill in the Create Project role today; it takes minutes and closes the second advisory. Then upgrade to 8.1.55, checking third-party modules first.

Reference. CISA advisories ICSA-26-286-01 and ICSA-26-246-06.

MRI-07: The gateway reaches its database with the administrator account

Severity High · **Effort** half-day · **Category** 2 Security exposure

What happens. Any fault in the gateway, or anyone who obtains the stored credential, gets full control of the database server. Combined with MRI-09, a successful injection would run with that control.

Evidence. Connections `SCADA_DB` and `Reports_DB`, both as `sa`.

Fix. Give each application its own database login with only the rights it needs.

Reference. Ignition manual, Database Connections.

SAMPLE

MRI-08: The same polling timer runs in three projects at once

Severity High · **Effort** quick-fix · **Category** 3 Performance time bombs

What happens. An identical timer that polls every lift station runs in `SCADA`, `Reports` and the old `SCADA_rev2` project. Every poll happens three times, tripling the load on the gateway and the stations, and the three copies write the same tags in a race.

Evidence. Timer `PollLiftStations`, byte-identical in three enabled projects, every 2 seconds.

Fix. Keep it in one project and delete the other two copies. MRI-20 removes one of them already.

Reference. Ignition manual, Gateway Timer Scripts.

MRI-09: Fourteen database calls build SQL by pasting values into the query

Severity High · **Effort** half-day · **Category** 4 Database queries

What happens. These calls insert values straight into the SQL text. A single quote in a value breaks the statement, and a crafted value can change what it does to the database.

Evidence. Fourteen calls in live library modules, most in `shared.reports` and `shared.workorders`. Seven more sit in two old copies of the reports module, listed under MRI-23.

Fix. Rewrite each call to pass its values as parameters.

Reference. Ignition manual, system.db.runPrepUpdate.

MRI-10: 1,340 tags send their history to a provider that no longer exists

Severity High · **Effort** quick-fix · **Category** 5 Tag and UDT structure

What happens. These tags are set to record history, but the history provider they name was removed. Nothing errors visibly, and the trend charts simply show gaps that get blamed on the instruments. None of this history has been recorded since the provider was removed.

Evidence. 1,340 tags with `historyProvider` set to `Historian_Old`, which is not defined on the gateway. Most inherit it from four UDT types.

Fix. Repoint the four UDT types to the current historian; the tags inherit the change.

Reference. Ignition manual, Tag History.

MRI-11: Two alarm journals write to the same table

Severity High · **Effort** half-day · **Category** 6 Alarm configuration

What happens. Two alarm journals point at connections that reach the same database, so every alarm event is written twice, and the shorter of the two retention settings deletes records the other was meant to keep.

Evidence. Journals `Journal` and `Journal_Archive`, both writing `alarm_events` in SCADA_DB.

Fix. Keep one journal per table, with the retention you actually want.

Reference. Ignition manual, Alarm Journal.

SAMPLE

MRI-12: A restore breaks every screen that uses a third-party chart module

Severity High · **Effort** half-day · **Category** 8 Upgrade readiness

What happens. Forty screens use components from a third-party chart module. A gateway backup does not carry modules, so restoring onto a new server shows an error box in each of those places until the module is installed again at a compatible version.

Evidence. Third-party component types used across 40 views.

Fix. Record each third-party module's name, version and license with every backup, and keep the module files beside it.

Reference. Ignition manual, Gateway Backup and Restore.

MRI-13: 214 error handlers hide failures instead of recording them

Severity Medium · **Effort** multi-day · **Category** 1 Scripts that fail quietly

What happens. When one of these scripts fails, nothing is logged, so a screen shows empty data that gets blamed on missing data rather than on the script.

Evidence. 214 handlers that pass, return, or neither log nor re-raise.

Fix. Log a warning with the error in each, starting with the screens operators use most.

Reference. Ignition manual, system.util.getLogger.

MRI-14: An audit profile exists but records nothing

Severity Medium · **Effort** quick-fix · **Category** 2 Security exposure

What happens. The profile is defined, so auditing looks configured, but nothing writes to it. There is no record of who changed a setpoint, a project or a setting.

Evidence. Audit profile `PRWD_Audit` ; the gateway audit setting is empty and no project enables auditing.

Fix. Point the gateway and each project at the existing profile.

Reference. Ignition manual, Audit Profiles.

MRI-15: 38 query tags hit the database every five seconds, all day

Severity Medium · **Effort** half-day · **Category** 3 Performance time bombs

What happens. These tags run a SQL query on a fast fixed rate whether or not anyone is looking, about 657,000 queries a day. That load is constant, and it competes with the queries operators are actually waiting on.

Evidence. 38 query tags in a Direct tag group at 5 seconds.

Fix. Move them to a slower or Driven tag group, or fetch the values only when a screen needs them.

Reference. Ignition manual, Tag Groups.

SAMPLE

MRI-16: Eleven screen bindings refresh every second

Severity Medium · **Effort** quick-fix · **Category** 3 Performance time bombs

What happens. Each open screen re-runs these bindings every second. Four of them run a database query on each tick, so every additional operator adds load.

Evidence. Eleven expression bindings using `now(1000)`, four driving a query.

Fix. Slow them to 5 to 10 seconds, or update from a tag change instead of polling.

Reference. Ignition manual, Expression bindings.

MRI-17: Eleven named queries paste raw text into their SQL

Severity Medium · **Effort** multi-day · **Category** 4 Database queries

What happens. These queries use text parameters inserted into the SQL as written, including one that accepts a whole `WHERE` clause. If any caller passes user input, that is SQL injection.

Evidence. Eleven named queries in the inherited parent project, 23 text parameters between them.

Fix. Trace each caller and replace text parameters with value parameters.

Reference. Ignition manual, Named Query parameters.

MRI-18: Alarm priorities are upside down

Severity Medium · **Effort** project · **Category** 6 Alarm configuration

What happens. Good alarm practice keeps most alarms low priority and few high. Here 58% are High or Critical, so when something genuinely urgent fires it is lost in a screen already full of red.

Evidence. Priority distribution across 610 alarms: Critical 14%, High 44%, Medium 27%, Low 15%.

Fix. Re-rate alarms against a written priority definition, starting with the busiest areas.

Reference. ISA-18.2 alarm management; Ignition manual, Alarm Properties.

MRI-19: 412 alarms show no location when they fire

Severity Medium · **Effort** half-day · **Category** 6 Alarm configuration

What happens. These alarms have no display path, so the alarm table shows a bare tag name, and operators have to work out which station it belongs to before they can respond.

Evidence. 412 of 610 alarms with an empty Display Path.

Fix. Set the display path in the UDT types so every instance inherits it.

Reference. Ignition manual, Alarm Properties.

SAMPLE

MRI-20: An old revision of the SCADA project is still running

Severity Medium · **Effort** quick-fix · **Category** 7 Dead code and orphans

What happens. `SCADA_rev2` is an earlier copy of the SCADA project that was never disabled. Its timers and scripts still run, including one of the three copies in MRI-08.

Evidence. Project `SCADA_rev2`, enabled, with two running gateway timers.

Fix. Disable it, then delete it once nothing is found to depend on it.

Reference. Ignition manual, Projects.

MRI-21: Scheduled backups are switched off

Severity Medium · **Effort** quick-fix · **Category** 9 Backup and recovery reality

What happens. The newest backup is whenever someone last took one by hand.

Evidence. Scheduled gateway backups disabled.

Fix. Turn them on with a retention count, store them off the gateway host, and test a restore.

Reference. Ignition manual, Gateway Backup and Restore.

MRI-22: Historian pruning is switched off

Severity Medium · **Effort** quick-fix · **Category** 9 Backup and recovery reality

What happens. Tag history is never pruned, so the history tables grow without limit until the database or the disk stops them.

Evidence. Historian `Historian` with pruning disabled.

Fix. Turn on pruning with a retention period the district has agreed to keep.

Reference. Ignition manual, Tag History providers.

SAMPLE

MRI-23: Housekeeping items

Severity Low · **Effort** various · **Category** 5, 7, 8, 9 Several

What happens. None of these is urgent, but each is worth clearing during the work above.

Evidence. As listed below.

Fix. As listed below.

Reference. Ignition manual, as relevant.

ITEM	AREA	EFFORT
Two old copies of the reports module, holding seven of the string-built SQL calls	7	quick-fix
83 library functions with no direct caller, to review before removing	7	half-day
Tag names mix three different naming styles	5	project
142 calls to older tag functions that newer versions replace	8	half-day
The gateway is several releases behind the current 8.1	8	half-day
The backup holds no database data, so a restore alone gives no history	9	project
Single gateway with no redundancy	9	project

4. Quick wins

Everything rated quick-fix at Critical or High, in the order to do them.

1. MRI-03: schedule the purge job, after checking how much it will delete on its first run.
2. MRI-04: change the six buttons' script scope to Gateway.
3. MRI-08: delete two of the three polling timer copies.
4. MRI-10: repoint four UDT types to the current historian.

Three more quick fixes pay off immediately: filling in the Create Project role (the first step of MRI-06, which closes one advisory in minutes), MRI-14 (switch on auditing) and MRI-21 (switch on scheduled backups).

5. Acceptable as-is

- **No alarm notification pipelines.** The control room is staffed around the clock, so operators see alarms on screen without paging.
- **Gateway-to-gateway connections** use SSL and two-way authentication.
- **Stored database passwords** are encrypted; no clear-text password field is filled in.

SAMPLE

6. Scope and limitations

The scan read the backup only: projects, scripts, queries, tags, alarms and gateway configuration. It cannot see the PLCs, the databases behind the connections, how operators use the system, the load it actually runs under, or gateway logs, since a backup carries none.

CONTROL	EXAMINED
Script blocks	1,940
Inherited parent projects	1
Named queries	88
Inline database calls	1,210
Tags walked	4,120
Alarms	610
Web endpoint handlers	31

7. Method

The scanner was run against the unpacked backup, and every finding was checked against the source it names before inclusion. Advisory severities are the published CVSS ratings rather than our estimate.

About this sample. Artek runs an MRI from one gateway backup and returns a report in this format. Nothing is run against your system and we do not need access to your network. Backups are held only for the review and then deleted. Artek does not publish findings from client reviews; this report describes a fictional organization.

SAMPLE