

Wellsite Automation Without Open Ports

Connecting RTUs, flow computers, and lift controllers at remote pads, with an audit trail the measurement group and the regulators can both use

Fireball Industries · September 30, 2026 · 23 minute read

It is 5:40 in the morning and the pumper is already forty miles from the yard. His route sheet has thirty-some stops on it. At most of them he will open the gate, look at the tank gauge, glance at the plunger arrival count on the controller display, check the chart or the flow computer screen, sniff for gas, and drive on. Two of those stops actually need him today: a plunger that has stopped arriving and a tank that will be full before the haul truck gets there. He won't know which two until he reaches them. Meanwhile the SCADA tech is trying to explain to the measurement group why a meter's event log has a gap from the night the cell modem dropped, and somebody in IT has just found out that the RTU on a gathering compressor answers to the internet.

None of these is a new problem. Wellhead pumpers earned a mean of \$33.62 an hour in May 2023, and 11,550 of the country's 18,230 worked in Texas [17]. The IRS business mileage rate is 72.5 cents a mile for the first half of 2026 and 76 cents for the second [18]. Consider an illustrative route of 150 miles a day: that is roughly \$109 to \$114 of vehicle cost per day before wages, fuel spills, or the day the truck gets stuck. About three-quarters of US producing wells are marginal wells making 15 barrels of oil equivalent a day or less, and together they supply about 5 percent of US oil and gas [19]. On those wells the drive is often the largest controllable cost.

The security side has a shorter fuse. In May 2025 CISA, the FBI, EPA, and DOE warned that unsophisticated actors were going after ICS and SCADA in oil and natural gas through internet-exposed devices and default credentials [1][3]. In February 2026 Dragos reported that a threat group it tracks had compromised Sierra Wireless AirLink cellular gateways across US midstream pipeline operations and pivoted to engineering workstations [6][7].

This paper is written for the production engineer, the automation or SCADA tech, and the person who manages the lease operators. It gives you a self-check you can run on your own field, a list of what is worth connecting at a pad and why, a reference architecture that works over cellular, radio, or satellite without opening a single inbound port, a step-by-step path that starts with the cheap fixes, the ways these projects go wrong, and how the design lines up with API 21.1, OOOOb, and the TSA pipeline directives.

A self-check for your field

Try to answer these about your own operation today, without asking anyone to go look.

1. How many devices at your pads and compressor stations can be reached from the public internet right now: RTUs, flow computers, cell modems, radios, solar charge controllers? How do you know?
2. When a cell modem drops for six hours, what happens to the flow computer's hourly records, and does the host back-fill them automatically or does someone re-poll by hand?
3. Can your measurement analyst pull the configuration log, event log, and alarm log for any meter, for any day this year, in under ten minutes?
4. What share of yesterday's pumper stops found nothing that needed doing?
5. Who can change a plunger lift setpoint or a rod pump controller's pump-off setting remotely, how is that change logged, and does the log name the person?
6. If an RTU firmware or modem patch broke polling, how many sites would you have to drive to before you could roll it back?
7. For each pad subject to OOOOb, where is the record of the last AVO survey, what it found, and when the repair was done?

If more than two of these took a phone call to answer, the rest of this paper is aimed at you.

What needs to be connected, and why

A typical pad already has most of the data you need. It is locked in devices that were installed to run locally and were connected later, usually through whatever modem was cheapest that year. The job is to read them reliably, keep their records intact, and give the right people the right slice.

SOURCE	TYPICAL PROTOCOL	WHAT TO BRING BACK	WHY IT MATTERS
Flow computer (EFM)	Modbus RTU/TCP, BSAP, vendor protocols	Hourly and daily quantity records, configuration log, event log, alarm log	API 21.1 audit trail; allocation and sales volumes; meter freeze-offs and liquid loading show in the trends
Pad RTU	Modbus, BSAP, DNP3	Tubing and casing pressure, separator pressure, valve positions, ESD status, solar battery voltage	The pad's state at a glance; dead batteries are a common cause of "comm failure"
Plunger lift controller	Modbus	Arrival times, cycle counts, open and close times, non-arrivals	Non-arrivals and slow arrivals predict a loaded-up well days before it dies
Rod pump controller	Modbus	Dynamometer cards, pump fillage, strokes per minute, run time, pump-off events	Fluid pound, worn pumps, and parted rods show up in the cards first
Tank level gauges	Modbus, 4 to 20 mA through the RTU	Oil and water levels, interface, temperature, high-level alarms	Haul scheduling, run tickets, and spill prevention; thief hatch events
Gas detection and leak sensors	4 to 20 mA, Modbus, vendor cloud	Concentration, alarm states, continuous monitor alerts	Safety and OOOOb fugitive records
Combustor and flare controllers	Modbus, discrete I/O	Pilot flame status, alarm states	Pilot-out events are emissions events

SOURCE	TYPICAL PROTOCOL	WHAT TO BRING BACK	WHY IT MATTERS
Compressor panels	Modbus, vendor protocols	Suction and discharge pressure, run status, shutdown codes	Gathering pressure drives back-pressure on every well upstream
Backhaul gear	SNMP, vendor APIs	Signal strength, uptime, data usage	Separates “the well is down” from “the link is down”

The flow computer’s audit trail deserves more attention than it gets. API MPMS Chapter 21.1 expects unedited quantity transaction records kept in enough precision to recalculate, hourly records of no more than 60 consecutive minutes, daily records summed from the hourly, a configuration log of the constant flow parameters, an event log that captures the parameter changed with old value, new value, and timestamp, and an alarm log of operating exceptions [15]. The standard itself does not set a retention period; contracts, tariffs, and regulations do [15]. Any system that polls a flow computer and keeps only the latest values has thrown away the part an auditor asks for.

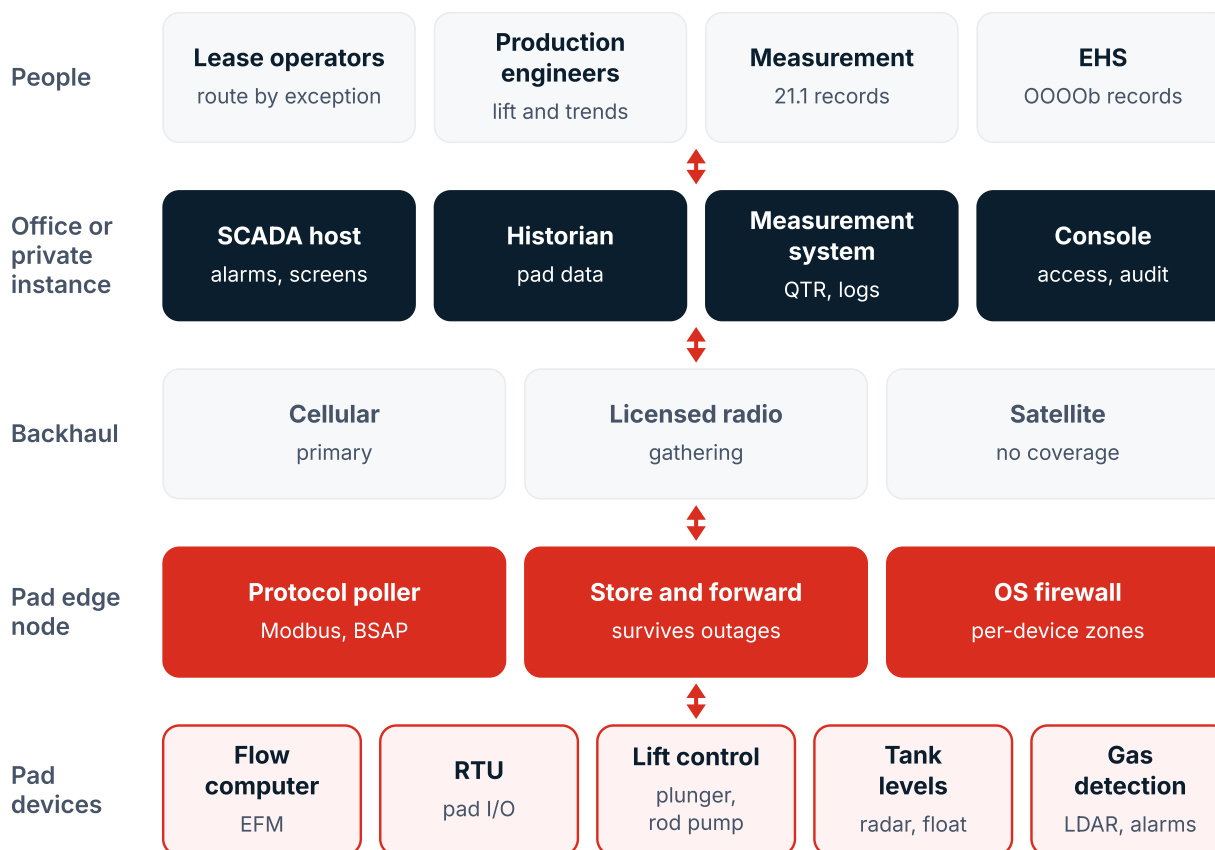
A reference architecture: pad to people

Figure 1 shows the shape that works at remote pads. It has four ideas in it.

- 1. One small node per pad, sitting in front of the existing devices.** It polls the flow computer, RTU, lift controllers, and tank gauges over their native serial or Ethernet ports, and nothing else on the pad needs to change. The flow computer keeps doing its own calculations; the node collects its records.
- 2. Store and forward at the pad.** The node keeps everything it collects on local storage and forwards it when the link is up. With local buffering, a six-hour cellular outage delays the records by six hours and loses none of them.
- 3. Outbound-only connections.** The pad initiates every connection to the office or private instance over a single outbound port. Nothing at the pad listens for connections from the internet, so a scan of the cellular carrier’s address space finds nothing to log in to.
- 4. Identity-based access with a log.** People and applications reach a pad device by name and role through the console, and every session and every write is recorded.

FIGURE 1

Reference architecture: pad to people



Every connection is initiated from the pad outward. Nothing at the pad listens for inbound connections from the internet.

Figure 1. Reference architecture for a connected pad: devices, a pad edge node, any backhaul, and the office systems the people use.

Backhaul is whatever the pad has: cellular where there is coverage, licensed radio on many gathering systems, satellite in the gaps. The node buffers through outages and always initiates the connection, so the choice doesn't change the design.

On EmberNet. An EmberNode is installed in front of the pad's existing RTU and flow computer, and those devices keep running unchanged.

EmberFLUX makes outbound connections only, on 443, so no inbound port is opened at the pad and there is no VPN to configure; traffic is encrypted, including post-quantum encryption, and devices are reached by identity.

The pollers, historian, and broker run as containers on the node, chosen by the operator.

At the office, the SCADA host, historian, and measurement system stay. They reach the pads through the same outbound-initiated fabric, with access granted per person and role: the measurement analyst sees meters, the lease operator sees his route, and the compressor contractor sees that compressor for the length of the job.

On EmberNet. EmberCORE is the single console for every pad and every app: role-based views, tenant scope for a joint venture or a contract operator, the App Store, and the audit trail. Ignition Edge, Node-RED, an MQTT broker, InfluxDB, and Grafana run side by side on the same node as containers, with the operator's own containers alongside; a crashed app does not take down the node.

Doing the work, step by step

The order below runs from what costs nearly nothing to what takes a project budget. Each step is useful on its own.

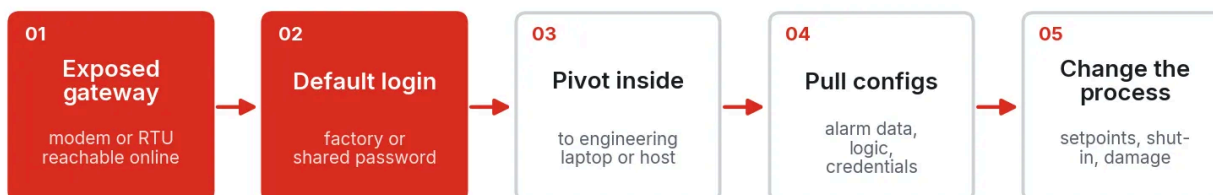
Step 1: Find what's exposed and close it

Start with the inventory. List every device at every pad with an IP address, including modems, radios, and solar controllers. Then check which of them answer from outside. CISA's December 2023 advisory on Unitronics PLCs described actors logging in to internet-exposed controllers over the default TCP port with default passwords or no password at all, compromising at least 75 devices across several sectors, energy among them [4]. The May 2025 joint fact sheet lists the first moves plainly: remove OT

connections to the public internet, change default passwords, secure remote access with phishing-resistant multifactor authentication, segment IT from OT, and keep the ability to run manually [2][3].

FIGURE 2

How an exposed pad gets used



Chain assembled from CISA joint advisory AA23-335A (2023, updated 2024), the CISA/FBI/EPA/DOE fact sheet of May 2025, and the Dragos 2026 OT report.

Figure 2. How an exposed pad device gets used, from the first login to a process change. Assembled from CISA advisory AA23-335A, the May 2025 CISA/FBI/EPA/DOE fact sheet, and the Dragos 2026 report.

Pay particular attention to cellular gateways. They sit at the edge where nobody watches, and they often have management interfaces enabled by default. Dragos's 2026 oil and gas briefing recommends auditing every Sierra Wireless AirLink gateway in the fleet after the VOLTZITE activity, and found default credentials still in place on field devices at 26 percent of oil and gas sites it assessed [6].

This step needs a spreadsheet, a few days of the SCADA tech's time, and the carrier's private APN settings. No new hardware.

Step 2: Fix polling and keep the records

Next, make sure the data that comes back is complete. Move polling for each pad onto a local node that keeps its own copy. For flow computers, collect the full 21.1 set: hourly and daily quantity records, configuration log, event log, and alarm log [15]. Confirm that after a link outage the host receives the missed hourly records in order, with their original timestamps, and that nothing is recalculated on the way.

For BSAP devices on older Bristol and ControlWave installations, and for vendor-specific flow computer protocols, plan for real integration work: a poller per protocol, a tag map per device type, and a test against a bench unit. Read-only polling comes first; writes come later, under change control.

Step 3: Route by exception

Once a pad's data is trusted, the route sheet can change. Use the data you now have to decide which stops a pumper needs to make today:

1. A tank approaching its haul level, with the projected fill time.
2. A plunger with consecutive non-arrivals or arrival times drifting long.
3. A rod pump with falling fillage, rising pump-off events, or a changed card shape.
4. A meter with a frozen differential, a stuck static pressure, or a flow time short of 60 minutes in the hour.
5. A pilot-out alarm on a combustor, or a high reading on a gas detector.
6. A pad with low solar battery voltage, before it goes dark.

Everything else becomes a scheduled visit at a lower frequency. One remote-monitoring vendor claims its customers cover three times more sites with less windshield time [21]; treat that as a vendor figure and measure your own by logging, for a month before and after, which stops found something actionable.

Haul tickets belong here too. Match the level transmitter's reading at pickup to the run ticket, and hauler disputes get shorter while theft shows up as a level drop with no ticket.

Step 4: Close the loop on lift, carefully

With reliable data and logged access, remote setpoint changes on plunger and rod pump controllers become reasonable. Keep control in the controller: it opens and closes the motor valve, and the remote layer only changes its settings. Tie every write to a named user, log old and new values, and ask the lift vendor which registers are safe to write mid-cycle.

Step 5: Put emissions records on the same footing

EPA's 2024 rule for new, modified, and reconstructed sources (40 CFR 60 Subpart OOOOb, published March 8, 2024, effective May 7, 2024) set fugitive monitoring schedules by well site type, as summarized in Figure 3 [8][9][10]. The rule also requires natural-gas-driven process controllers at new sources to have zero emissions, and 95 percent reduction from storage vessels above its thresholds [9]. It allows advanced detection technologies, both periodic screening and continuous monitoring, as alternatives to optical gas imaging, and it set a super-emitter program for remotely detected events of 100 kilograms per hour of methane or more [8][13].

FIGURE 3

OOOOb fugitive monitoring for new well sites

Site type	Survey method	Frequency	Repair window
Single wellhead only	AVO	Quarterly	15 days first try
Small well site	AVO, plus hatch and dump valve checks	Quarterly	15 days first try
Multi-wellhead only	AVO plus OGI or Method 21	Quarterly AVO, semiannual OGI	30 days first try
Major production equipment	AVO plus OGI or Method 21	Bimonthly AVO, quarterly OGI	30 days first try

Figure 3. OOOOb fugitive monitoring for new well sites by site type. Source: EPA summary of key requirements (2023) and Encino Environmental's summary of 40 CFR 60 Subpart OOOOb.

The dates have moved since. EPA's interim final rule of July 2025, finalized in November 2025 and published December 3, 2025, extended a set of OOOOb deadlines [11]. Per one environmental consultancy's summary, compliance deadlines for process controllers, storage vessels, control devices, equipment leaks, covers and closed vent systems moved to January 22, 2027 [12]. In April 2026 EPA finalized revisions that loosened some flare and vent-gas provisions [22]. Your environmental group owns the current applicability for each site.

What the connected pad adds is the evidence. A pilot-out alarm on a combustor, a thief hatch opening with no haul ticket, a pressure signature that says a dump valve is stuck open, a continuous monitor's alert: each is a timestamped record that can be routed to the right person, tied to a work order, and closed out with a repair date. The 2018 study published in *Science* estimated US oil and gas methane emissions at about 13 million metric tons a year, roughly 60 percent above EPA's inventory at the time, and found that most of the emissions came from leaks, equipment malfunctions, and other abnormal operating conditions [14]. Those are the conditions a pad's own instruments often see first.

On EmberNet. EmberCORE's audit trail records who reached which device, when, and what they changed. For a site's OOOOb and API 21.1 programs, that log sits next to the device data itself, so the record of a setpoint change or a repair visit does not depend on someone remembering to write it down.

Step 6: Patch the fleet without driving it

Most fields skip this step. A bad patch on remote pads costs a truck roll to every site it touched. The answer is a pipeline (Figure 4): test on lab hardware identical to the field, soak-test the pad workload, release to a few canary pads on one route, then roll out in waves by area, with a way to return a node to its last known-good state without a visit.

FIGURE 4

Patching a fleet of pads without a truck roll

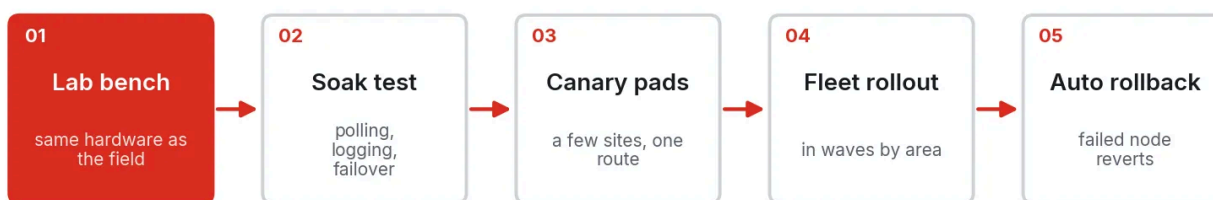


Figure 4. A patch pipeline for remote pads: identical lab hardware first, then canary pads, then waves, with automatic rollback.

On EmberNet. EmberRTOS is an immutable edge operating system with automatic rollback patching: a node that fails after an update returns to its previous image on its own. Patches are tested on lab hardware identical to field deployments before they go out, and the firewall built into the OS segments each pad device at the operating-system layer.

Where these projects go wrong

Most wellsite automation projects that disappoint fail in one of a few predictable ways.

1. Connecting first, securing later. The modem goes in with a public IP and the vendor's default password because the start-up crew needs to reach it from the truck. Two years later it is still there. This is exactly the condition CISA has warned about in successive advisories [1][4].

2. Treating the cell gateway as plumbing. Dragos found that cellular gateways at unmonitored OT edges let adversaries bypass perimeter controls, and reported that 29 percent of its oil and gas engagements found poor IT/OT segmentation, the highest share of any sector [5].

3. Polling the values and dropping the logs. A system that collects current flow rate and today's volume but not the 21.1 event and configuration logs produces nice trends and an audit finding [15].

4. Assuming the link is always up. Without local buffering, every cellular outage leaves a hole in the hourly records, and someone ends up estimating volumes.

5. No owner for the route change. The data arrives, nobody changes the route sheet, and the pumper drives the same loop.

6. Writes without change control. Remote setpoint changes made from shared logins leave no record of who did what, which is a problem in a lift dispute and a bigger one after an incident.

7. Patching by hand or not at all. Dragos reported vulnerability management findings in 31 percent of its oil and gas engagements, again the highest of any sector [5]. When a patch requires a site visit, it waits.

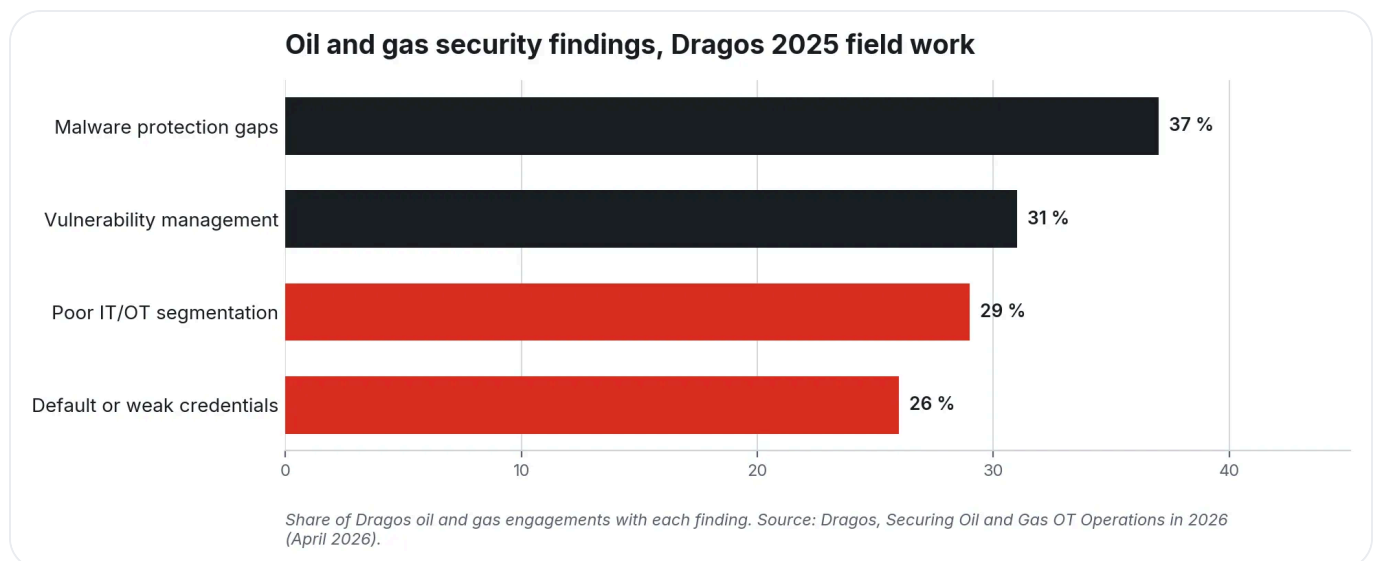


Figure 5. Share of Dragos oil and gas engagements with each finding. Source: Dragos, Securing Oil and Gas OT Operations in 2026 (April 2026).

Security and compliance in your regulators' terms

The site's compliance program decides what applies and owns compliance. The architecture's job is to make the controls practical.

CISA, FBI, EPA, and DOE guidance

The May 2025 fact sheet's mitigations are the baseline for a connected pad [2]. An outbound-only design removes the internet-facing listener at the pad, identity-based access ends shared logins, and

per-device segmentation on the pad node limits what a compromised device can reach.

TSA pipeline security directives

TSA's Security Directive Pipeline-2021-02 series is directed at hazardous liquid and natural gas pipeline owners and operators. Version 2021-02D, issued July 27, 2023, required policies that keep operations running if IT or OT is compromised, documented zones and controls that prevent unauthorized communication between them, MFA or equivalent controls, least privilege and separation of duties, continuous monitoring with logging, and risk-based patch management with alternative mitigations where a patch would degrade operations [16]. Version 2021-02E took effect July 27, 2024, and was ratified in August 2024 [20]. Where a gathering system is not covered, those outcomes are still a good yardstick, and Figure 1 maps to each: zones at the pad, one outbound conduit, named-user access, logged sessions, and a patch pipeline with rollback.

NIST SP 800-82 and IEC 62443

NIST SP 800-82 Revision 3, published September 28, 2023, is the federal guide to OT security, including industrial control systems [23]. Segmentation into zones with controlled conduits between them, the approach also used in the IEC 62443 series, is the vocabulary most operators' security teams use. A pad node that segments each device at the OS layer and carries all traffic through one authenticated conduit fits that model.

API MPMS 21.1 and OOOOb

For measurement, the controls are records: unedited quantity transaction records, configuration logs, event logs, and alarm logs that an auditor can use to recalculate [15]. For emissions, they are survey, detection, and repair records with dates, along with continuous monitoring records where an operator has chosen that path [8][10]. In both cases the design goal is the same: the record is collected at the source, buffered through outages, and kept with a log of who touched it.

On EmberNet. The same architecture has been used to reach a controller from far away without opening the site: on September 29, 2026, an engineer in Austin, Texas, downloaded a PLC application from the CODESYS IDE to a virtual PLC running in a container on an industrial PC in Cleveland, Ohio, over EmberNet, with no VPN and no inbound port opened. The same outbound-only path serves a pad RTU or flow computer.

A phased rollout

FIGURE 6

Phased rollout

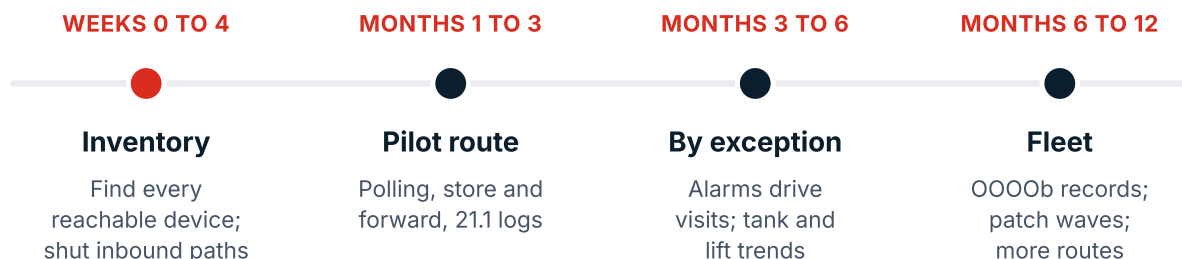


Figure 6. A phased rollout from inventory to fleet-wide operation over roughly a year.

- 1. Weeks 0 to 4: inventory and close.** List every networked device at every pad. Find which answer from the internet and close those paths. Change default passwords. Move modems to a private APN where the carrier offers one.
- 2. Months 1 to 3: one route.** Pick one pumper route, ideally the longest or the one with the most callouts. Put a node on each pad, poll every device read-only, buffer locally, and collect the full 21.1 record set from each flow computer. Log, by hand, which stops each day found something actionable.
- 3. Months 3 to 6: route by exception.** Build the exception list from Step 3 with the pumper who runs the route. Change the route sheet. Add tank-level-to-run-ticket matching. Introduce logged remote writes for lift settings with the production engineer's sign-off.
- 4. Months 6 to 12: emissions records and the fleet.** Route pilot-out, hatch, and detector alarms into work orders that close with repair dates. Stand up the patch pipeline with lab hardware matching the field. Expand route by route.

What to do Monday

Pull the list of public IP addresses your carrier has assigned to your field modems and check which of them answer. Change every default password you find this week. Then pick the route you argue about most, ride it once with the pumper, and write down at each stop whether he did anything other than look. A month of that log will tell you which pads to connect first and what to put on the exception list. None of it requires a platform or a capital request.

About Fireball Industries

Fireball Industries is EmberNet's master integrator. Fireball's engineers design, build, and support wellsite and gathering automation of the kind described here: surveying pads and backhaul, integrating existing RTUs, flow computers, and lift controllers, standing up the pad nodes and office systems, and running the patch and rollout program with the operator's production, measurement, and EHS teams.

Sources

1. Cybersecurity and Infrastructure Security Agency (CISA). "Unsophisticated Cyber Actor(s) Targeting Operational Technology." May 6, 2025. <https://www.cisa.gov/news-events/alerts/2025/05/06/unsophisticated-cyber-actors-targeting-operational-technology>
2. CISA, FBI, EPA and DOE. "Primary Mitigations to Reduce Cyber Threats to Operational Technology." May 2025. <https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology>
3. SecurityWeek. "US Warns of Hackers Targeting ICS/SCADA at Oil and Gas Organizations." May 7, 2025. <https://www.securityweek.com/us-warns-of-hackers-targeting-ics-scada-at-oil-and-gas-organizations/>
4. CISA and partners. "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities" (AA23-335A). December 1, 2023, updated December 18, 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>
5. Dragos. "Securing Oil and Gas OT Operations in 2026." April 16, 2026. <https://www.dragos.com/blog/oil-gas-cybersecurity-threats-2026>
6. Dragos. "2026 OT Cybersecurity Year in Review: Oil and Gas Executive Briefing." 2026. https://hub.dragos.com/hubfs/2026_YIR_ExecutiveBriefing%20O_G.pdf
7. Dragos via Business Wire. "Dragos OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure." February 17, 2026. <https://www.businesswire.com/news/home/20260217364132/en/Dragos-OT-Cybersecurity-Report-Adversaries-Increase-Real-World-Impact-Map-Control-Loops-Across-Industrial-Infrastructure>
8. US Environmental Protection Agency, Federal Register. "Standards of Performance for New, Reconstructed, and Modified Sources and Emissions Guidelines for Existing Sources: Oil and Natural Gas Sector Climate Review." March 8, 2024. <https://www.federalregister.gov/documents/2024/03/08/2024-00366/standards-of-performance-for-new-reconstructed-and-modified-sources-and-emissions-guidelines-for>
9. US Environmental Protection Agency. "Summary of Key Requirements" table, oil and natural gas final rule. December 2023. <https://www.epa.gov/system/files/documents/2023-12/summary-of-key-requirements-table.pdf>
10. Encino Environmental Services. "EPA's Updates to 40 CFR Part 60 Subpart OOOOb: Fugitive Emissions Monitoring Requirements." 2024. <https://encinoenviron.com/epas-updates-to-40-cfr-part-60-subpart-oooob-fugitive-emissions-monitoring-requirements/>

- 11.** US Environmental Protection Agency. "2025 Interim Final Rule to Extend Compliance Deadlines." 2025. <https://www.epa.gov/controlling-air-pollution-oil-and-natural-gas-operations/2025-interim-final-rule-extend-compliance>
- 12.** ALL4. "U.S. EPA Finalizes Oil and Gas Compliance Deadline Extension." January 8, 2026. <https://www.all4inc.com/4-the-record-articles/u-s-epa-finalizes-oil-and-gas-compliance-deadline-extension/>
- 13.** Electronic Code of Federal Regulations. "40 CFR Part 60 Subpart OOOOb." Current edition. <https://www.ecfr.gov/current/title-40/chapter-I/subchapter-C/part-60/subpart-OOOOB>
- 14.** NOAA Chemical Sciences Laboratory. "U.S. Oil and Gas Methane Emissions 60% Higher than Estimated." June 21, 2018 (reporting Alvarez et al., *Science*). https://csl.noaa.gov/news/2018/238_0621.html
- 15.** Keith Fry, American School of Gas Measurement Technology. "Auditing Electronic Gas Measurement per API MPMS, Chapter 21.1." 2023. https://asgmt.com/wp-content/uploads/2023/09/2023_EGM_Auditing_Per_API-21.1.pdf
- 16.** Industrial Cyber. "Network segmentation, MFA among cybersecurity measures laid down in TSA Security Directive for pipeline operators." July 2023. <https://industrialcyber.co/transport/network-segmentation-mfa-among-cybersecurity-measures-laid-down-in-tsa-security-directive-for-pipeline-operators/>
- 17.** US Bureau of Labor Statistics. "Occupational Employment and Wages, May 2023: 53-7073 Wellhead Pumpers." 2024. <https://www.bls.gov/oes/2023/may/oes537073.htm>
- 18.** Internal Revenue Service. "Standard Mileage Rates." 2026. <https://www.irs.gov/tax-professionals/standard-mileage-rates>
- 19.** RMI. "Marginal Wells 101: What Are They, Where Are They, and Why Do We Need to Assess Them?" April 23, 2025. <https://rmi.org/marginal-wells-101-what-are-they-where-are-they-and-why-do-we-need-to-assess-them/>
- 20.** Transportation Security Administration, Federal Register. "Ratification of Security Directives." January 17, 2025. <https://www.federalregister.gov/documents/2025/01/17/2025-01243/ratification-of-security-directives>
- 21.** Twin Eagle Solutions (vendor). "Remote Pumper." Accessed September 2026. <https://www.twineaglesolutions.com/remote-pumper>
- 22.** Harvard Environmental and Energy Law Program. "EPA VOC and Methane Standards for Oil and Gas Facilities" (regulatory tracker). Accessed September 2026. <https://eelp.law.harvard.edu/tracker/epa-voc-and-methane-standards-for-oil-and-gas-facilities-2/>
- 23.** National Institute of Standards and Technology. "SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security." September 28, 2023. <https://csrc.nist.gov/pubs/sp/800/82/r3/final>