INOVIQ
TECHNOLOGIES
Engineering Intelligent Industry

INDUSTRIAL INTERNET OF THINGS (IIoT)

A PRACTICAL CUSTOMER GUIDE

Connecting assets for quick, measurable benefits in new and legacy plants
Companion to the INOVIQ Digital Transformation Primer and Maturity Self-Assessment

Contents

1 Executive summary
2 What Industrial IoT is, and what it is not
3 Reference architecture: five layers
4 Building blocks: sensors and connectivity
5 Reference architecture: retrofitting legacy assets
6 Quick wins: practical starting points
7 A 90-day plan from idea to results
8 Security essentials
9 Building the business case
10 Pitfalls to avoid and next steps

1 EXECUTIVE SUMMARY

Industrial IoT connects machines, equipment and utilities to software through low-cost sensors and secure networks, so that people see what is happening as it happens and act before small problems become costly ones. It works in brand-new plants and in plants where much of the equipment is decades old.

The fastest returns rarely come from large platforms. They come from a few well-chosen measurements on assets that already cost money every day: energy-hungry compressors, critical pumps and motors, bottleneck machines, storage tanks and temperature-controlled rooms. Most of these can be monitored without touching control systems, often within weeks.

Key messages

- **Start with a problem, not a technology:** unplanned stops, energy waste, manual rounds, product loss.
- **Retrofit before you replace:** clamp-on, battery-powered sensors and gateways add data to old assets non-invasively.
- **Keep it separate and secure:** a dedicated IIoT network zone, read-only access to control data, outbound-only links.
- **Design to scale:** open standards and a common asset model so each quick win becomes a building block.

2 WHAT INDUSTRIAL IOT IS, AND WHAT IT IS NOT

Industrial IoT (IIoT) is the network of sensors, instruments and machines that collect operational data and share it with software for monitoring, analysis and decision-making. It complements existing automation rather than replacing it: control systems keep running the process, while IIoT widens what can be seen and analyzed.

Aspect	Traditional automation (control)	Industrial IoT (insight)
Main purpose	Run the process safely and consistently	Monitor, analyze and improve the process and assets
Typical data	Signals the control logic needs	Additional data: asset health, energy, environment, utilities
Response time	Milliseconds; deterministic	Seconds to minutes is usually enough
Connectivity	Wired, closed control networks	Wired and wireless, often battery-powered, via gateways
Cost per point	Higher: engineered I/O, cabling, panel space	Lower: retrofit sensors installed in minutes
Who uses it	Operators and control engineers	Maintenance, energy, quality, operations and management
Change risk	Changes need careful management of change	Read-only and separate, so low risk to production

3 REFERENCE ARCHITECTURE: FIVE LAYERS

Every IIoT solution, large or small, can be described in five layers. Thinking in layers keeps choices independent: a sensor can be changed without redesigning the platform, and a new application can reuse data already collected.

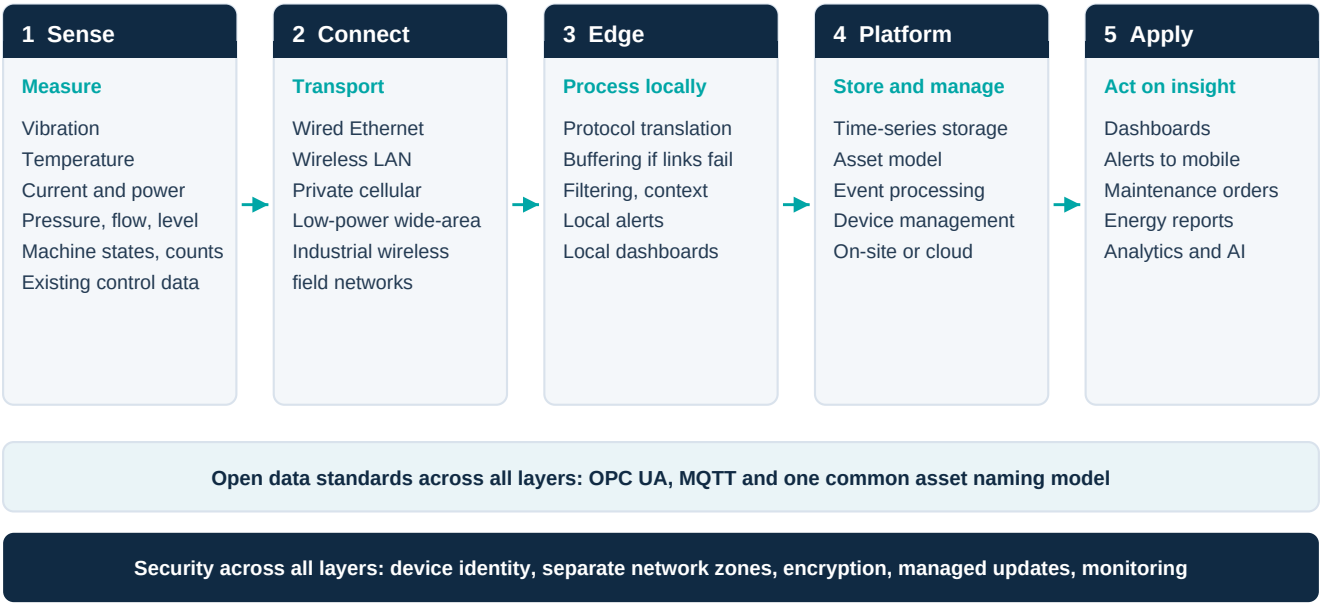

Figure. Data moves from sensing to action through five independent layers. Open data standards and security apply to every layer, not only to the network.

- **Sense:** measure what matters. Reuse existing control data where possible and add sensors only where data is missing.
- **Connect:** pick the simplest network that meets range, data rate and power needs (Section 4).
- **Edge:** process data close to the asset so alerts still work if the wider network or internet is down.
- **Platform:** store time-series data with its asset context and manage devices centrally, on-site, in the cloud or both.
- **Apply:** put insight in front of the person who acts: a technician's phone, a shift dashboard or a work order.

4 BUILDING BLOCKS: SENSORS AND CONNECTIVITY

Sensors

Retrofit sensors are now small, battery-powered and quick to fit. Choose by the failure or loss you want to see.

Measurement	What it reveals	Typical retrofit method
Vibration	Imbalance, misalignment, bearing wear, looseness	Magnetic or stud-mounted wireless sensor on bearing housing
Surface temperature	Overheating motors, bearings, panels, steam traps	Adhesive or magnetic sensor; thermal camera for surveys
Electrical current and power	Running/idle/off state, load, energy use, overload	Split-core clamp on cables; no rewiring or shutdown
Pressure and flow	Leaks, blockages, pump performance, air demand	Insertion or clamp-on sensor; tap into existing ports
Level	Tank contents, consumption rate, overfill risk	Non-contact radar or ultrasonic sensor on tank top
Temperature and humidity (ambient)	Cold-chain, storage and clean-area conditions	Wireless room sensor; minutes to install
Machine signals	Cycle counts, stops, alarms, stack-light status	Read from controller via gateway, or light/current sensing

Connectivity options

Connectivity option	Range	Data rate	Power	Best for
Wired industrial Ethernet	Plant-wide (cabled)	Very high	Mains	Machines with existing controllers; high-volume data
Wireless LAN	Tens of meters per access point	High	Mains or rechargeable	Indoor areas with existing coverage; mobile devices
Private 4G/5G cellular	Site-wide	High	Mains	Large sites, moving equipment, many devices
Low-power wide-area (LPWAN)	Several kilometers	Very low	Battery, years	Tanks, remote utilities, environmental sensors
Industrial wireless field networks (IEC 62591, ISA100)	Plant-wide mesh	Low	Battery, years	Process plants; instrument-grade monitoring
Short-range wireless	A few meters	Low	Battery	Handheld data collection, commissioning

5 REFERENCE ARCHITECTURE: RETROFITTING LEGACY ASSETS

Older plants do not need new control systems to benefit from IIoT. The pattern below adds data alongside the existing equipment, leaves control untouched and keeps the new devices in their own secured network zone.

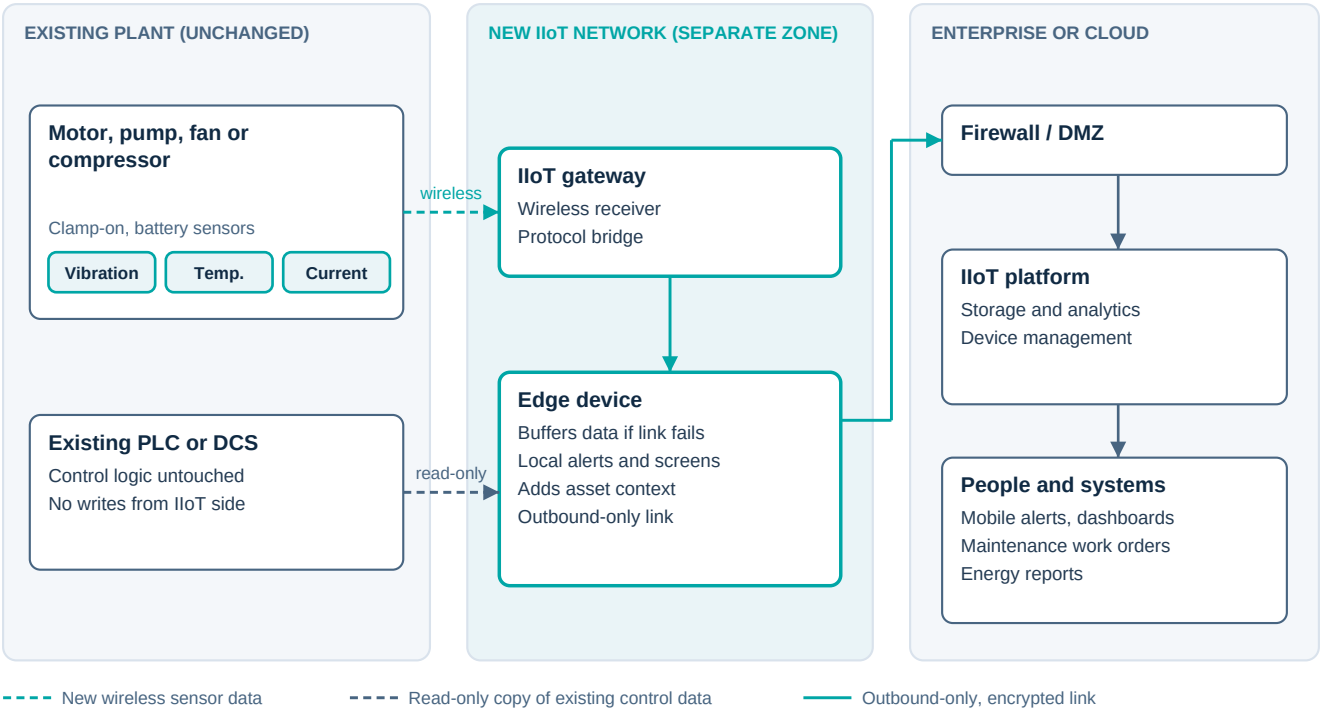

Figure. New sensors and a read-only copy of control data flow through a separate IIoT zone to the people who act on them. Nothing is written back to the existing control system.

- **Non-invasive first.** Clamp-on, magnetic and adhesive sensors avoid shutdowns, rewiring and changes to certified equipment.
- **Read-only from control.** Where controller data is useful, copy it through a gateway or edge device; never write back without formal change management.
- **Separate zone.** Gateways and edge devices sit in their own network zone, linked outward through a firewall. Control networks gain no new inbound paths.
- **Local resilience.** The edge device buffers data and keeps local alarms working when the wider network is unavailable.

6 QUICK WINS: PRACTICAL STARTING POINTS

These use cases share three traits: they need little or no change to existing equipment, they address costs that occur every day, and they show results within weeks. Benefits depend on the site; measure a baseline first.

Quick win	Problem it solves	What to install	Typical benefit	Time to value
Energy sub-metering of major loads	Energy bills with no breakdown; equipment left running when idle	Clamp-on power meters on compressors, chillers, furnaces, large motors	Visible idle and out-of-hours waste; energy per unit tracked	2–4 weeks
Condition monitoring of critical rotating equipment	Unexpected pump, fan or motor failures; manual vibration rounds	Wireless vibration and temperature sensors with alert thresholds	Early warning of failures; planned rather than emergency repairs	4–8 weeks
Automatic machine-state and downtime capture	Downtime recorded late, inaccurately or not at all	Current sensing or stack-light/controller signals via gateway	Accurate downtime reasons; live availability and OEE	2–6 weeks
Compressed air monitoring	Leaks and over-pressure waste energy unseen	Flow and pressure sensors on headers; power on compressors	Leaks found and fixed; pressure set-point optimized	2–4 weeks
Remote tank level monitoring	Manual dips, stock-outs, overfills, late deliveries	Non-contact level sensors on raw material, chemical or fuel tanks	No manual rounds; reorders triggered by actual level	1–3 weeks
Cold-room and storage environment	Product loss and compliance gaps from unnoticed excursions	Wireless temperature and humidity sensors with mobile alerts	Excursions caught in minutes; automatic records for audits	1–2 weeks

Worked example: compressor room

A plant runs three air compressors around the clock. Clamp-on power meters and a pressure sensor on the main header are installed in a morning, without stopping production, and data flows through a wireless gateway to a simple dashboard. Within two weeks the data shows the compressors running at weekends with the plant idle, pressure set higher than any user needs, and a steady demand that points to leaks. The team schedules weekend shutdowns, lowers the set-point in steps and runs a leak survey, then tracks energy per unit produced to confirm the saving.

7 A 90-DAY PLAN FROM IDEA TO RESULTS

A short, time-boxed pilot proves value quickly and builds the foundation for scaling.

Period	Activities	Outcome
Days 1–15: Select	Choose one or two quick wins; agree owner, baseline and success measure; walk the area; confirm network zone and security rules	Approved pilot scope and baseline
Days 16–45: Install	Fit sensors and gateway; connect edge and platform; set naming and asset model; configure alerts and dashboard with users	Live data and first alerts
Days 46–75: Use	Run daily with the team; tune thresholds; act on findings; record every intervention and its effect	Measured improvements
Days 76–90: Decide	Compare against baseline; calculate payback; document lessons and standards; decide to scale, adjust or stop	Scale-up plan and template

8 SECURITY ESSENTIALS

Every connected device is a potential entry point. Building security in from the first pilot costs little and avoids expensive rework when scaling. The IEC 62443 series is the main reference for industrial systems.

- **Separate network zone** for IIoT devices, with a firewall between it, the control network and the enterprise.
- **Outbound-only, encrypted connections** from the edge to the platform; no inbound access from the internet.
- **Read-only access** to control systems; any write-back requires formal management of change.
- **Unique device identity and credentials;** change all default passwords before installation.
- **Managed firmware updates** and an up-to-date inventory of every device, gateway and account.
- **Supplier remote access** only through a managed, logged, multi-factor gateway.
- **Data ownership** written into contracts: your operational data stays yours and can be exported in open formats.

9 BUILDING THE BUSINESS CASE

Keep the first business case simple: annual benefit divided into total first-year cost gives a payback period that operations and finance can both check. Include sensors, gateways, installation, software subscriptions, and the time people spend acting on the data.

Quick win	Benefit to measure	KPI
Energy sub-metering	Energy and cost avoided	kWh per unit produced; idle-time consumption
Condition monitoring	Failures avoided, repair cost, lost output	Unplanned downtime hours; MTBF; planned-to-reactive ratio
Machine-state capture	Recovered production time	Availability; OEE; top downtime reasons
Compressed air monitoring	Energy saved from leaks and pressure	kWh per cubic meter of air; leak count fixed
Tank level monitoring	Labor and logistics saved; stock-outs avoided	Manual rounds removed; stock-out events
Environment monitoring	Product loss avoided; audit effort	Excursion count and duration; response time

10 PITFALLS TO AVOID AND NEXT STEPS

1 Buying devices before defining the problem and the person who will act on the data.

2 Collecting data nobody looks at: every measurement needs an owner and an action.

3 Setting alarm thresholds once and never tuning them, causing alert fatigue.

4 Connecting devices directly to control or business networks without a separate zone.

5 Choosing closed, proprietary devices that cannot share data in open formats.

6 Running pilots without a baseline, so benefits cannot be proven.

7 Ignoring battery life, signal coverage and maintenance of the sensors themselves.

8 Scaling before naming standards and an asset model are in place.

Next steps

- ☐ List the five assets or areas that cost the most in energy, downtime or product loss
- ☐ Pick one or two quick wins from Section 6 and name an owner for each
- ☐ Record a baseline for the chosen KPIs before installing anything
- ☐ Agree the IIoT network zone and security rules with IT and OT
- ☐ Run the 90-day plan and decide on scale-up with real numbers

Important: This guide is general guidance, not a design specification. Benefits and timelines are indicative and depend on site conditions. For a site assessment or a quick-win pilot, contact INOVIQ Technologies at www.inoviqtech.com.