Factory IoT Readiness Checklist

This checklist helps plant heads, operations managers and Chief Technology Officers (CTOs) decide whether a factory is ready for an Industrial Internet of Things (IIoT) pilot. It covers business goals, machine and programmable logic controller (PLC) data access, network and operational technology (OT) security, data definitions and the people who will act on the data, so gaps are fixed before money is spent on hardware.

Technically reviewed by the EmbedCrest engineering team Updated November 16, 2026

How to use this checklist

Walk through each section with production, maintenance and information technology (IT) or OT staff in one session. Mark every item as confirmed, partly confirmed or unknown. Unknown items on the pilot machines become the scope of a site survey, and anything marked partly confirmed gets an owner and a date.

Business goals and scope

- [ ] Is one measurable problem chosen, such as unplanned downtime, Overall Equipment Effectiveness (OEE), energy or scrap, rather than a general digitalisation goal?
- [ ] Is the baseline for that problem measured, including the measurement window and data source?
- [ ] Are two to five pilot machines selected, including the constraint machine of the line?
- [ ] Is a business owner named who will decide whether the pilot succeeded?
- [ ] Are success criteria and the pilot duration agreed before any hardware is ordered?
- [ ] Is the cost of downtime per hour estimated for the pilot machines?

Machines and data access

- [ ] Is the controller make, model and firmware version recorded for every pilot machine?
- [ ] Is it known whether each controller exposes Modbus, OPC UA (Open Platform Communications Unified Architecture), EtherNet/IP, PROFINET or a vendor protocol?
- [ ] Are PLC programs and tag lists available, or can the machine builder supply them?
- [ ] Is written permission from the machine builder needed before connecting to the controller?
- [ ] Are machines without accessible controllers identified for sensor retrofit, such as current or vibration sensors?
- [ ] Are signals for run state, cycle count, alarms and good versus rejected parts identified?
- [ ] Is read only access confirmed, so the pilot cannot change machine behaviour?

Network and infrastructure

- [ ] Is a network drawing available showing OT, IT and any existing remote access paths?
- [ ] Is wired Ethernet or reliable wireless coverage available at each pilot machine?
- [ ] Is there a powered, protected location for an edge gateway near the machines?
- [ ] Is it decided whether data stays on site, goes to a cloud platform or both?
- [ ] Is store and forward buffering required for periods when the uplink is down?
- [ ] Are time synchronisation sources, such as Network Time Protocol (NTP) servers, available for consistent timestamps?

Security and governance

- [ ] Is the OT network segmented from the office network with defined firewall rules?
- [ ] Will the gateway use outbound only connections rather than open inbound ports?
- [ ] Is it agreed who owns gateway credentials, certificates and software updates?
- [ ] Is the IT or OT security team involved in approving the architecture?
- [ ] Are data ownership and retention rules agreed with any external platform provider?

Data definitions and people

- [ ] Are planned production time, stop categories and reason codes defined in writing?
- [ ] Is it agreed who enters stop reasons that machines cannot report automatically?
- [ ] Is a person named on each shift to act on alerts during the pilot?
- [ ] Is there a plan for dashboards at the line, for supervisors and for management?
- [ ] Is time budgeted for operators and maintenance staff to learn the new tools?
- [ ] Is a review meeting scheduled at the end of the pilot to decide on scale up?