

Define the access boundary of an OT AI pilot

A starting architecture that separates reading, recommendations and control authority.

In short

- A first OT AI pilot can read data and advise engineers without writing commands to production systems.
- Recommendations should be presented with supporting evidence, timestamp and model version, and model text must not be turned directly into PLC code or setpoints.
- Before launch, the pilot should rehearse stopping the service, losing the data feed and restoring the previous version.

01 / Limit initial authority

A first pilot can read data and advise engineers without writing commands to production. Record the data source, access account and collection gateway. Treat control-system availability separately from analytics availability. Inspect dependencies so an unavailable model service cannot interrupt process control.

02 / Draw the data path

Map the PLC or DCS, collection layer, intermediate network zone and analytics environment. Document direction, protocol, owner and purpose for each connection. Consider a bounded copy of necessary signals instead of broad network access. Site policy and risk assessment must determine the actual architecture.

03 / Keep engineering approval in the workflow

Show supporting evidence, timestamp and model version with recommendations. Record acceptance or rejection reasons for evaluation. Do not turn model text directly into PLC code or setpoints. Existing change review, test environments and engineering approval procedures continue to apply.

04 / Exercise recovery before launch

Test stopping the service, losing the data feed and restoring the previous version. Name the responsible person, record retention period and escalation route. This guide is not certification or a site-specific security assessment; it collects questions for designing the pilot.

Try it

Draw a read-only pilot in Flow Maker. Identify which connections are affected when analytics stops.

References and online guide

[Open the online guide](#)

NIST SP 800-82 Rev. 3

Proposed pilot steps do not claim field accuracy. Synthetic examples are not measurements from a production site.