



INDUSTRY + OPERATIONS

MANUFACTURING AI PLAYBOOK

Select one operational problem. Run a bounded pilot. Retain the evidence. Decide from measured value and risk.

For plant leaders, operations owners, production supervisors, quality, safety, IT/OT, cybersecurity, workforce and executive sponsors.

SELECT

One recurring, lower-risk workflow with a named owner.

TEST

Approved data, qualified review, baseline and stop condition.

DECIDE

Continue, revise, pause or stop from a retained record.

ORIENTATION

CONTROL THE WORK BEFORE THE TOOL

A bounded pilot begins with an owner, an allowed data boundary, a reviewer, a baseline and a stop condition.

ORIENTATION CONTRACT

WHO

Plant and operations leaders; production, quality, maintenance, supply chain, safety, training, IT/OT and cybersecurity owners.

WHEN

A recurring delay, error, rework burden or information task has a measurable current process.

OUTPUT

A signed pilot charter and retained decision record.

LEAVE WITH

One decision-ready record naming the workflow, owner, baseline, approved system and data boundary, reviewer, evidence, stop condition and next review.

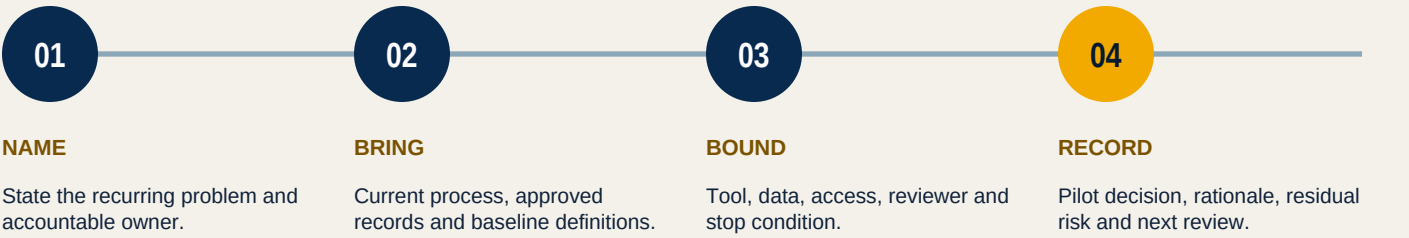
BRING TO THE FIRST SESSION

- The current process and accountable owner
- Approved source records and baseline definitions
- Qualified reviewers for operational and control boundaries
- A specific stop condition and decision date

DOES NOT AUTHORIZE

Unsafe deployment, autonomous process control, final safety or quality decisions, or unapproved data use.

FIRST WORKING SESSION - 60 MINUTES



SESSION OUTPUT

A named workflow, current-process record, approved boundary, qualified reviewer, stop condition and scheduled decision gate.

RISK MAP

MATCH CONTROLS TO CONSEQUENCES

Risk depends on the tool, data, user, workflow, integration, audience and consequence of error - not on the word AI alone.

01	BEGIN HERE Draft support using approved, nonconfidential information	EXAMPLES Agendas, shift summaries, training outlines and plain-language explanations	CONTROL Human review before use
02	CONTROLLED USE Work that can influence an operating process	EXAMPLES Draft work instructions, maintenance summaries, inventory analysis and internal briefings	CONTROL Qualified review plus retained evidence
03	DO NOT DELEGATE Consequential decisions or direct control	EXAMPLES Safety approval, equipment control, product disposition, emergency response or sole-basis employment decisions	CONTROL Authorized person decides; automation stops

THE BOUNDARY-CHANGE TEST			
Before a workflow moves to another band, record exactly what changed and who accepts the new consequence.			
DATA	ACCESS	CONSEQUENCE	REVIEW
Did sensitivity, retention or sharing change?	Did the tool gain connectors, autonomy or OT reach?	Can an error affect people, product, process or rights?	Can a qualified person verify and reverse the output?

RECLASSIFY	If any answer changes, stop the current use and obtain a new boundary decision before the next run.
-------------------	---

SELECTION GATE

CHOOSE ONE WORKFLOW THAT CAN TEACH YOU SOMETHING

A pilot is a controlled learning exercise. Favor a stable, recurring task with evidence that a qualified reviewer can check.

FOUR QUESTIONS BEFORE APPROVAL

01

PROBLEM

What recurring delay, error, rework burden or learning need are we solving?

02

OWNER

Who owns the current process and accepts or rejects every result?

03

EVIDENCE

What current record proves the baseline and lets us verify each output?

04

BOUNDARY

What data, access, action or consequence forces escalation or stop?

USE-CASE SCREEN		
	A STRONG FIRST PILOT	ESCALATE OR REJECT
Process	Stable, recurring and owned	Unmapped, changing or unowned
Information	Approved, minimal and traceable	Sensitive, controlled or unclear
Output	Draft or analysis with qualified review	Autonomous action or final disposition
Measurement	Baseline and review burden are observable	Success is only a plausible answer

GOOD FIRST CANDIDATES

SHIFT HANDOFF

Format approved notes; supervisor verifies against source records.

TRAINING OUTLINE

Draft from a current approved procedure; qualified trainer verifies every step.

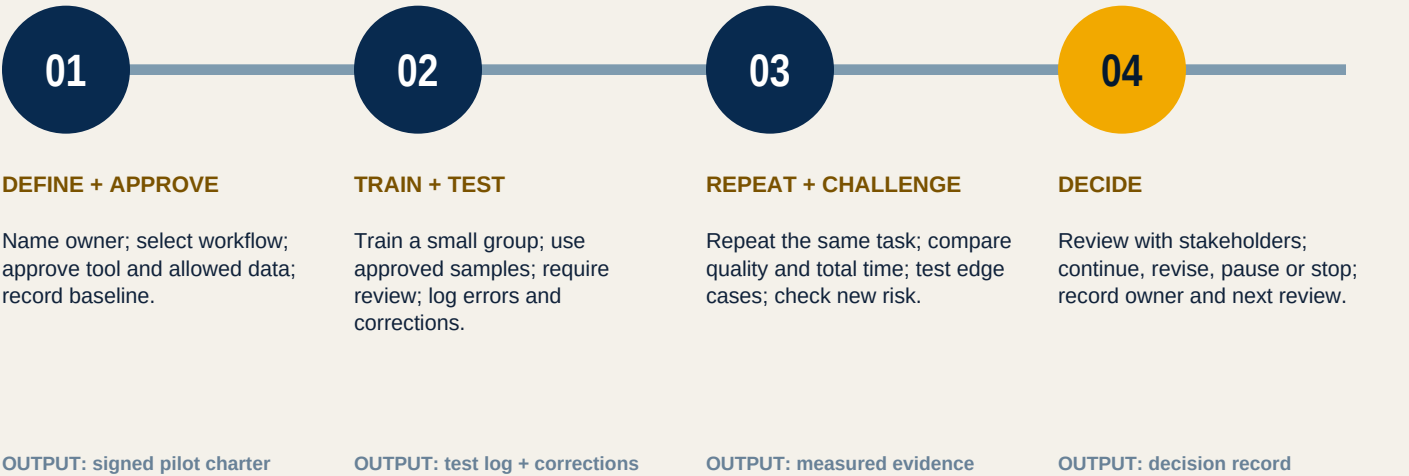
WORK-ORDER TRENDS

Organize de-identified records; maintenance experts diagnose and decide.

OPERATING SEQUENCE

MAKE THE PILOT A MEASURABLE LINE

Four weeks. One bounded workflow. Evidence retained at every gate. Scope does not expand automatically.



EVIDENCE RETAINED AT EVERY GATE

QUALITY Accuracy, corrections and reviewer acceptance	TOTAL TIME Draft, checking, correction and handoff time	REPEATABILITY Variation across users, records and edge cases	RISK Data, access, safety, quality, workforce and legal effects
---	---	--	---

CONTROLLED DECISION

CONTINUE / REVISE / PAUSE / STOP

GOVERNANCE

PUT A NAMED PERSON AT EVERY CONTROL POINT

A vendor, model or prompt does not own the decision. The pilot owner coordinates qualified review and retains the record.

ACCOUNTABLE ROLE	OPERATING RESPONSIBILITY	DECISION RIGHT
PILOT OWNER	Defines the problem, scope, baseline, evidence and decision meeting.	Can pause the pilot at any time.
PROCESS REVIEWER	Checks every output against source records, procedure and operational context.	Accepts, corrects or rejects each output.
CONTROL REVIEWERS	IT/OT, cybersecurity, privacy, safety, quality, HR, legal or procurement review the boundaries that apply.	Approve controls within their authority.
EXECUTIVE SPONSOR	Ensures resources, resolves conflicts and owns expansion beyond the pilot.	Cannot waive legal, safety or security requirements.

STOP AUTHORITY Any named owner or qualified reviewer may pause work for sensitive-data exposure, unsafe output, unauthorized access or action, missing evidence, or review burden above the approved limit.

ILLUSTRATIVE EXAMPLE - REPLACE WITH LOCAL EVIDENCE

SHIFT-HANDOFF SUMMARY

A production team tests draft assistance for a consistent handoff. The tool does not change settings, issue instructions, make safety decisions or replace supervisor review.

- 01

SOURCE

Approved shift notes and current handoff form
- 02

DRAFT

AI formats a concise summary inside the approved environment
- 03

VERIFY

Outgoing supervisor checks every event, quantity, hold and owner
- 04

RETAIN

Source references, corrections, reviewer, final summary and decision



CONTEXTUAL PHOTOGRAPH

EVIDENCE LEDGER

PROBLEM + OWNER	Recurring handoff burden; operations owner and supervisor named.
BASELINE + TARGET	Current preparation time, missing fields, corrections and reviewer effort measured before a local target is set.
DATA + SYSTEM	Approved, minimized shift information only; credentials, unrestricted personnel data and uncontrolled OT access excluded.
HUMAN REVIEW	Supervisor checks events, quantities, safety items, maintenance references, owners and unresolved conditions.
STOP	Pause for protected-data exposure, unsafe or fabricated instruction, missing evidence, unauthorized action or excessive review burden.
DECISION	Continue only when measured value is repeatable and residual risk remains inside the approved boundary.

COMPLETE WHEN

Every output is traceable; total employee time is counted; failures and corrections are logged; residual risk is explained; and the decision has an effective period and next review.

STARTER PATTERNS

FIVE MANUFACTURING AI WORKFLOWS

Replace bracketed placeholders, use only approved information, require the system to identify assumptions and missing data, and have a qualified person verify the result.

01 LOWER RISK Draft a shift-handoff summary		
USE WHEN	ASK	VERIFY
A supervisor needs a consistent format for production status, open issues and assigned follow-up.	Create a concise template for [LINE]. Include status, downtime, holds, safety events, shortages, open work orders, owners and next-shift priorities. Mark missing information as not provided.	Quantities, equipment status, holds, incidents, owners and source references.
BOUNDARY Draft only. No production action, safety decision or final instruction.		
02 CONTROLLED USE Create a training outline		
USE WHEN	ASK	VERIFY
A qualified trainer needs a draft lesson structure based only on a current approved procedure.	Using the approved procedure, draft a [LENGTH]-minute outline for [AUDIENCE] with objectives, prerequisites, demonstration points, practice, knowledge checks and trainer sign-off.	Every step against the controlled document, PPE, site rules and current revision.
BOUNDARY The approved procedure remains controlling; the trainer verifies and signs off.		
ALWAYS RETAIN Prompt or instruction; approved inputs; tool/version; output; corrections; reviewer; accepted record; exception; and decision.		

STARTER PATTERNS

WORKFLOWS FOR MAINTENANCE, SUPPLY CHAIN AND QUALITY

AI may organize approved information and draft a review aid. Qualified people retain diagnostic, commercial, safety, engineering and disposition authority.

03		CONTROLLED USE	Summarize work-order trends	
USE WHEN		ASK		VERIFY
Maintenance leaders need help organizing approved, de-identified work-order data.		Group by equipment class, failure description, downtime band and repeat occurrence. Identify patterns to investigate; do not diagnose root cause.		Classifications, counts, periods, missing records and apparent patterns.
BOUNDARY		Maintenance experts retain diagnosis and work authorization.		
04		CONTROLLED USE	Prepare a material-shortage response	
USE WHEN		ASK		VERIFY
Supply-chain and operations teams need a structured internal briefing.		Use confirmed inventory, delivery dates, affected orders, options, owners and open questions. Separate facts from assumptions.		Inventory, purchase orders, lead times, contracts and decision authority.
BOUNDARY		Qualified owners make customer and commercial commitments.		
05		CONTROLLED USE	Prepare a quality problem-solving meeting	
USE WHEN		ASK		VERIFY
A quality team needs a neutral structure for reviewing verified observations.		Organize facts, unknowns, containment, process stages, evidence to collect and questions. Do not determine root cause or disposition.		Lot, part, date, measurement, defect, containment and source records.
BOUNDARY		Quality authorities retain containment, disposition and corrective action.		
ALWAYS RETAIN		Prompt or instruction; approved inputs; tool/version; output; corrections; reviewer; accepted record; exception; and decision.		

CONTROL BOUNDARY

TREAT THE AI TOOL AS ANOTHER SYSTEM

Keep the information below out of unapproved tools. Any exception requires specific authorization for the system and data use, plus applicable legal, security and contractual controls.

BLOCK UNLESS SPECIFICALLY AUTHORIZED

- 01

Trade secrets and proprietary formulas
- 02

Customer drawings and technical specifications
- 03

Controlled, classified or export-controlled information
- 04

Source code, credentials, network diagrams or security details
- 05

Employee, applicant, customer or supplier personal information
- 06

Nonpublic quality, incident, contract, pricing or financial records

FIVE CONTROL GATES

- 01

IDENTITY
Organization-approved accounts, least privilege and MFA
- 02

CONNECTIONS
Disable unnecessary connectors, plug-ins and integrations
- 03

RETENTION
Confirm storage, deletion and model-training settings
- 04

INVENTORY
Record tool, owner, use, version, access and review date
- 05

INCIDENT
Route AI issues through the existing incident process

BEFORE PROCUREMENT OR PILOT USE

DATA FLOW

What enters, where it is processed, what is retained and who can retrieve it

ACCESS

Accounts, roles, connectors, APIs, logging and administrative rights

MODEL USE

Whether inputs or outputs train a shared or future model

EXIT

Export, deletion, revocation, incident support and vendor offboarding

PROCUREMENT AND CONTROL

REVIEW THE TOOL IN PROPORTION TO ITS REACH

The depth of review should match access, autonomy, integration, data sensitivity and potential consequences. A public chatbot and an OT-connected system do not receive the same review.

REVIEW AREA	REQUIRE BEFORE PILOT	ESCALATE OR STOP
OWNER + PURPOSE	Named owner; approved use; excluded uses	No accountable owner or vague enterprise-wide purpose
DATA	Allowed/prohibited data; retention; training; deletion	Unknown processing, reuse, location or deletion
IDENTITY + ACCESS	SSO/MFA; least privilege; admin and user roles	Shared accounts, excessive privilege or weak revocation
INTEGRATION	Connectors, APIs and permissions are necessary and bounded	Unneeded mail, file, code, network or OT reach
OUTPUT + REVIEW	Qualified reviewer, source traceability and correction path	Unverifiable output or automation bias
SECURITY	Logging, incident reporting, vulnerability handling and support	No usable logs, notification or response commitment
CONTRACT	Confidentiality, IP, audit, change notice and exit terms reviewed	Unclear ownership, unilateral change or lock-in
MEASUREMENT	Baseline, success criteria, burden and stop conditions recorded	Success defined only by adoption or plausible output

DECISION

APPROVE WITH BOUNDARY / RETURN FOR EVIDENCE / REJECT

EVIDENCE GATE

MEASURE THE RESULT AND THE BURDEN OF CONTROL

A pilot is not successful merely because the system produced an answer. Count verification, correction, exception handling and operator effort.

MEASURE	BASELINE	PILOT RESULT	DECISION QUESTION
QUALITY	Current error and revision level	Verified error and revision level	Did the reviewed output meet the defined standard?
TOTAL TIME	Current completion time	Draft + review + correction time	Did total time improve after review was included?
CONSISTENCY	Current variation	Observed variation	Was performance repeatable across users and examples?
RISK	Known process risks	New or changed risks	Did data, safety, cyber, quality or workforce concerns increase?
USEFULNESS	Current user experience	Participant feedback	Would trained users choose the controlled workflow again?

DECISION LOGIC

CONTINUE	REVISE	PAUSE	STOP
Measured value + controlled residual risk	Promising result; boundary or burden needs work	Evidence gap or correctable control failure	Value unproven or control is inadequate

IMMEDIATE STOP

Sensitive-data exposure; unauthorized access or action; deceptive or unsafe output; repeated material error; loss of evidence; or a new event affecting safety, quality, security, privacy, rights or customer commitments.

FROM PILOT TO OPERATING CONTROL

CONNECT THE WORKFLOW TO POLICY, TRAINING AND INCIDENT RESPONSE

A playbook does not replace organizational policy. Expansion requires a controlled operating model, not a successful demonstration.



OPERATING-CONTROL TEST

Expansion is permitted only when policy names the use, training prepares the roles, operations own the record, and the incident route is live.

EXPANSION RECORD



COMMON QUESTIONS

USE THE METHOD, NOT A SHORTCUT

The answers below preserve the human decision boundary while routing readers to the practical next step.

WHAT IS A MANUFACTURING AI PLAYBOOK?

A planning and operating resource for selecting a use case, protecting data, testing a workflow, requiring human review, measuring results and deciding whether a controlled pilot should continue.

CAN AI WRITE MANUFACTURING SOPS?

It may help draft a template, but qualified personnel must verify every instruction against approved procedures, equipment documentation, safety requirements, quality systems and applicable standards.

WHAT SHOULD NOT GO INTO A PUBLIC TOOL?

Trade secrets, customer drawings, controlled technical data, source code, credentials, security details, employee information, proprietary formulas or other nonpublic records without specific approval.

CAN AI MAKE SAFETY OR QUALITY DECISIONS?

It should not independently approve safety procedures, engineering changes, process parameters, equipment operation, product release or quality disposition. Authorized people retain responsibility.

WHERE SHOULD A MANUFACTURER BEGIN?

With one bounded, lower-risk workflow using approved, nonconfidential information; a named owner; a small pilot group; human review; and measures of quality, total time, repeatability, burden and risk.

NEXT

Record scope, owner, approved data and tool, baseline, reviewer, evidence, stop conditions and next review. Use the web pilot charter and decision record to capture the decision.

PUBLIC AUTHORITY + LOCAL EVIDENCE

GROUND THE METHOD IN AUTHORITATIVE SOURCES

MAIN developed the operating model, decision logic, examples and working tools in this publication. The public sources below support specific risk, safety, security, workforce and manufacturing boundaries.

01	NIST AI Risk Management Framework AI risk governance and lifecycle foundation
02	NIST AI RMF Playbook Suggested actions for operationalizing the framework
03	NIST MEP: AI implementation strategies Manufacturing-specific implementation considerations
04	NIST 2026 AI/ML roadmap for smart manufacturing Research and technical direction for smart manufacturing
05	NIST Trustworthy AI in Critical Infrastructure concept note Emerging critical-infrastructure risk context; not a final profile
06	NIST Generative AI Profile Generative-AI risks and actions extending the AI RMF
07	CISA artificial intelligence resources Cybersecurity and secure-use context
08	OSHA Recommended Practices for Safety and Health Programs Worker participation, hazard prevention and program improvement
09	EEOC resources on AI and the ADA Employment and disability-related compliance context
10	NIST Cybersecurity Framework 2.0 Cybersecurity governance and control context for connected systems

REVIEW RECORD

OWNER

Named local owner controls applicability, links and currency.

CHECK

Review when law, standards, vendor, model, data, access, policy or observed performance changes.

STOP

Do not rely on an expired, inaccessible or superseded source without qualified review.

Contextual photo: Freek Wolsink / Pexels. Not a MAIN facility or AI deployment.

PUBLIC AUTHORITY Sources reviewed September 5, 2026