INOVIQ
TECHNOLOGIES
Engineering Intelligent Industry

DIGITAL TRANSFORMATION IN DISCRETE, PROCESS & HYBRID INDUSTRIES

A CUSTOMER PRIMER

A vendor-neutral reference for new installations and legacy sites
Companion to the INOVIQ Digital Manufacturing Maturity Self-Assessment

Contents

1 Purpose of this primer
2 What digital transformation means in industry
3 Discrete, process and hybrid industries
4 Two starting points: new and legacy installations
5 Reference architecture
6 The ten capability dimensions
7 Modernizing legacy installations
8 Designing digital-ready new installations
9 Roadmap: from assessment to scale
10 Use cases matched to maturity
11 Cybersecurity and resilience
12 People, governance and change
13 Measuring value and avoiding pitfalls
14 Glossary and next steps

1 PURPOSE OF THIS PRIMER

Digital transformation pays off when it starts from a business problem, builds on a sound data foundation and grows one proven use case at a time. That holds for a car-parts line, a refinery or a food plant that mixes batches and then packs them, and whether the site opened last year or still runs control systems from the 1990s.

This primer is a vendor-neutral reference for plant owners, operations leaders, engineering managers and IT/OT teams in **discrete**, **process** and **hybrid** industries. It explains the vocabulary, a reference architecture, practical options for legacy and new installations, and a phased roadmap.

It is a companion to the **INOVIQ Digital Manufacturing Maturity Self-Assessment**. The assessment shows where a site stands across ten capability dimensions; this primer explains what each level looks like and how to move up.

How to use this primer

- Complete the self-assessment for each site: one per site, rating current, demonstrated capability only.
- Read Sections 2 to 5 for the shared language, your industry type and the reference architecture.
- Use Section 6 to compare your scores with what each maturity level looks like in practice.
- Read Section 7 if your site has significant legacy equipment, Section 8 if you are planning a new line or plant.
- Use Sections 9 to 14 to build, govern and measure your roadmap.

2 WHAT DIGITAL TRANSFORMATION MEANS IN INDUSTRY

In industrial operations, digital transformation is the use of connected data and software to make operations safer, more reliable, more efficient and more responsive. It is a change in how decisions are made, not a technology purchase.

- **Outcome first.** Every initiative traces to a measurable result: fewer unplanned stops, higher yield, lower energy per unit, faster changeovers, fewer quality escapes.
- **OT/IT convergence.** Operational technology (PLCs, DCS, SCADA, drives, instruments) and information technology (ERP, MES, analytics, cloud) stop working as islands. Data moves securely between them with clear ownership.
- **Continuous improvement, digitally enabled.** Digital tools strengthen proven disciplines such as Lean, TPM, Six Sigma and process safety management. They do not replace them.

Common misconceptions

Misconception	Reality
“We need to replace our control systems first.”	Most legacy assets can be connected non-invasively. Replacement is driven by obsolescence and risk, not by digital ambition alone.
“Buy a platform and the value follows.”	Platforms enable value; use cases, data quality and adoption deliver it.
“AI is the starting point.”	AI depends on reliable, contextualized data. Most sites gain more first from visibility and standard work.
“It is an IT project.”	It is an operations project with IT and OT as joint enablers. Plant leadership must own the outcomes.
“One playbook fits every plant.”	Discrete, process and hybrid operations have different control systems, data and value levers (Section 3).
“Small plants cannot afford it.”	Low-cost sensors, edge devices and subscription software make focused pilots affordable at almost any scale.

3 DISCRETE, PROCESS AND HYBRID INDUSTRIES

The principles in this primer apply to all three types of operation, but the starting systems, the data that matters and the first use cases differ. Identify which type describes each area of your site; many plants contain more than one.

	Discrete	Process	Hybrid
How product is made	Countable units assembled or machined from parts	Materials transformed by chemical or physical change, continuously or in batches	Process stage (mixing, reacting, forming) followed by discrete stage (filling, packing, assembly)
Typical sectors	Automotive, electronics, machinery, metal fabrication, aerospace, HVAC equipment	Oil and gas, petrochemicals, chemicals, cement, power, water, metals and mining	Food and beverage, pharmaceuticals, consumer goods, paint, tires, building materials
Typical control	PLCs, robots, CNC, machine HMIs, line-level SCADA	DCS, safety instrumented systems, analyzers, plant-wide SCADA	DCS or PLC for process; PLCs and packaging machines downstream
Data that matters most	Machine states, cycle times, counts, rejects, serial numbers	Continuous process values, lab results, alarms, energy and utilities	Batch records, recipes, lot genealogy, plus line performance
Common first use cases	OEE and downtime tracking, digital work instructions, serial traceability	Historian-based process monitoring, alarm rationalization, energy optimization, advanced process control	Electronic batch records, recipe management, end-to-end traceability, OEE on packing lines
Key standards	ISA-95, OPC UA companion specifications (e.g. machine tools, robotics)	ISA-95, ISA-18.2 (alarms), IEC 61511 (functional safety)	ISA-88 (batch), ISA-95, regulated record rules where applicable (e.g. FDA 21 CFR Part 11)

Why hybrid deserves particular attention

Hybrid sites are often where the largest gains are hiding: the process stage and the packing stage are frequently run, measured and improved as separate worlds. Connecting them gives one view of yield, quality and genealogy from raw material to finished goods.

4 TWO STARTING POINTS: NEW AND LEGACY INSTALLATIONS

New installations (greenfield) and established installations (brownfield) aim for the same connected, data-driven operation but take different routes. A new site designs connectivity in from day one; a legacy site layers it on carefully without disturbing production. Most real sites are a mix, such as a new packing line beside a decades-old process unit.

Aspect	New installation (greenfield)	Legacy installation (brownfield)
Typical starting maturity	L2 to L3 if specified well	L1 to L2, often uneven across areas
Main constraint	Specification discipline and integration effort across many suppliers	Uptime, obsolete hardware, undocumented logic, limited spares
Connectivity	Native Ethernet, OPC UA and MQTT specified in purchase orders	Serial fieldbuses, proprietary protocols, isolated HMIs, paper records
Data quality	Consistent tag naming and asset model from the start	Inconsistent names, missing context, manual logs
Biggest risk	Over-engineering, or locking into one vendor’s closed stack	Disrupting a running process; cyber exposure from new connections
Best first move	Write digital requirements into the design basis and FAT/SAT	Inventory assets and data, then connect read-only through an edge layer
Pace	Fast once commissioned	Incremental, aligned with shutdowns and budgets

The rest of this primer applies to both. Section 7 covers legacy-specific patterns and Section 8 covers new-build specifications.

5 REFERENCE ARCHITECTURE

A common architecture lets every new system plug into the same data foundation instead of adding another point-to-point link. It follows the ISA-95 levels most plants already recognize, plus two modern additions: an edge layer and a unified data layer. It applies equally to discrete, process and hybrid sites; only the systems at Levels 1 to 3 change.

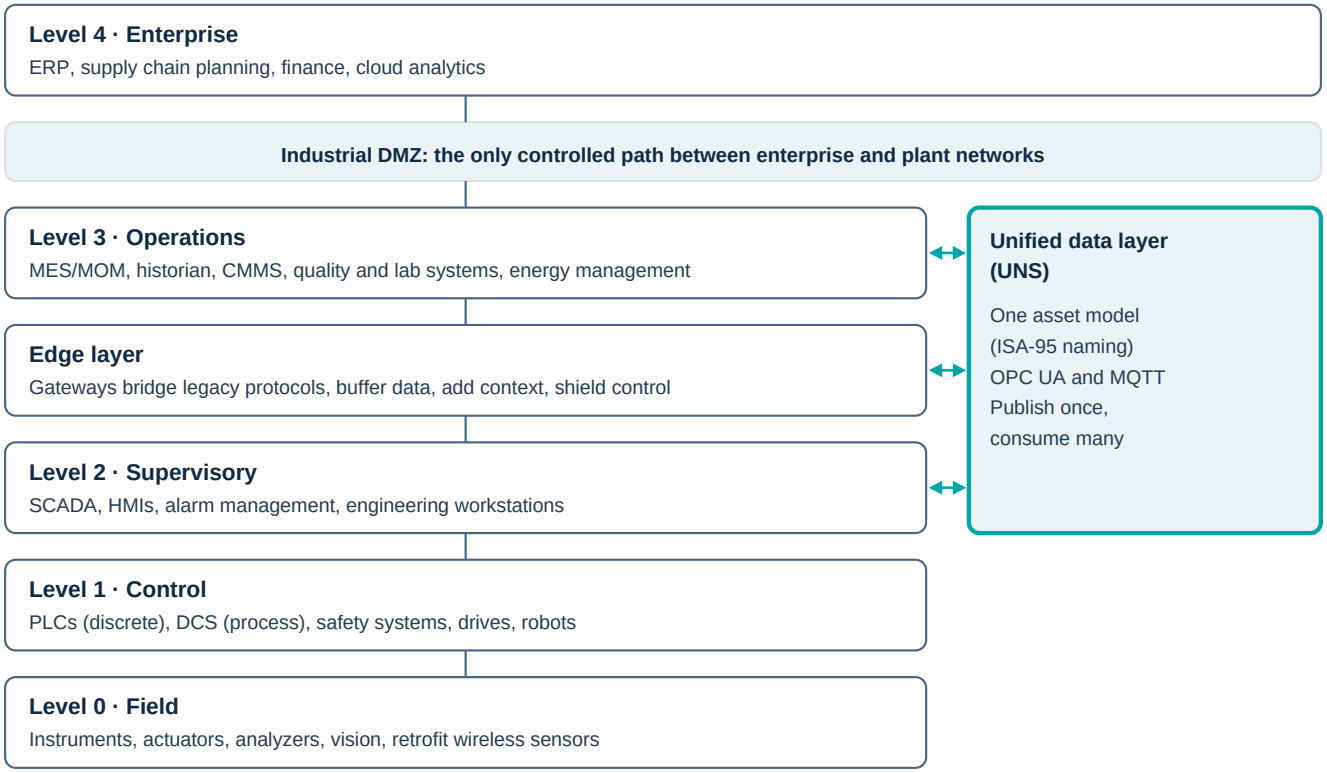

Figure. Every system shares plant data through one secured, structured layer. Control stays at Levels 0 to 2; data rises through the edge layer into the unified data layer, and the enterprise reaches it only through the industrial DMZ.

Design principles

- **Publish once, consume many.** Each source publishes its data once to the shared layer; MES, maintenance, quality and analytics subscribe to it. This replaces fragile point-to-point interfaces.
- **Context with the data.** Every value carries its asset, units, quality and timestamp, named by a consistent hierarchy (enterprise, site, area, line or unit, equipment).
- **Open standards.** OPC UA for structured machine and process data and MQTT for lightweight event messaging keep you vendor-neutral.
- **Edge before cloud.** Process data close to the equipment for speed, resilience and security; send summarized or contextualized data to the cloud where it adds value.
- **Security by zones.** Each level is a security zone; traffic between zones passes only through defined, monitored conduits (Section 11).

6 THE TEN CAPABILITY DIMENSIONS

Each dimension in the self-assessment is scored 0 to 4, giving a total out of 40 and an overall maturity level. The table below shows what low, middle and high capability typically look like, so you can check your scores and see the next step.

#	Dimension	Score 1: Initial	Score 2–3: Developing to Advanced	Score 4: Leading
1	Digital strategy & leadership	Isolated projects; no owner or budget line	Written roadmap, executive sponsor, business case per initiative	Strategy tied to business KPIs; portfolio reviewed quarterly; value tracked
2	Automation & process control	Manual operation, local controls, paper settings	PLC/DCS control with HMIs; key loops tuned; alarms rationalized	Advanced process control, model-based optimization, minimal manual intervention
3	Connected operations & systems	Islands of equipment; data copied by hand	Historian and MES connected to control; ERP interfaces for orders and stock	Unified data layer across plant and enterprise; events flow in near real time
4	Data, analytics & AI	Spreadsheets and end-of-shift reports	Dashboards, root-cause analysis, statistical process control	Predictive and prescriptive models in daily use, with governance
5	Asset reliability & maintenance	Run-to-failure; breakdown work orders	Preventive schedules in a CMMS; condition monitoring on critical assets	Predictive maintenance; reliability-centered strategy; spares optimized
6	Quality & traceability	Final inspection; paper batch or lot records	Digital quality checks, SPC, lot genealogy	In-line quality prediction; closed-loop correction; full digital batch or unit record
7	Planning & supply chain	Static plans in spreadsheets	Planning tool linked to ERP; inventory visibility	Dynamic scheduling that responds to plant status, demand and supply signals
8	People, skills & adoption	Few trained users; resistance to tools	Role-based training; digital champions in each area	Data-literate workforce; tools embedded in standard work
9	Cybersecurity & resilience	Flat networks; shared passwords; no OT backups	Segmented networks, asset inventory, tested backups	Risk-based program aligned to IEC 62443; monitored; incident drills run
10	Performance, energy & sustainability	Monthly manual KPIs; utility bills only	OEE and energy tracked per line or unit; targets set	Real-time KPIs at asset level; energy and emissions optimized continuously

Maturity levels

Total score	Level	What it typically means
0–8	L1 Foundational	Mostly manual and reactive; data is scattered or on paper
9–16	L2 Emerging	Pockets of digital capability; partial adoption, limited integration
17–24	L3 Established	Standardized systems and practices; key areas connected
25–32	L4 Integrated	Plant and enterprise integrated; analytics drive daily decisions
33–40	L5 Intelligent	Predictive and optimized operations; continuous, data-led improvement

Reading your results

A balanced profile is healthier than a high total with deep gaps. A score of 0 or 1 in cybersecurity (dimension 9), or any safety-related automation gap, needs action regardless of the overall level.

7 MODERNIZING LEGACY INSTALLATIONS

Old plants rarely need a rip-and-replace to become data-driven. The proven approach is to connect what exists read-only, add sensing where data is missing, and replace control hardware only where obsolescence, safety or performance demand it.

Step 1: Know what you have

- Build an asset and network inventory: controllers, firmware versions, HMIs, drives, protocols, PCs and their operating systems.
- Classify each system by criticality and obsolescence risk: spares availability, vendor support and in-house skills.
- Recover documentation: back up PLC and DCS programs, mark up P&IDs and loop diagrams, and record undocumented changes.

Step 2: Choose a modernization pattern per asset

Pattern	What it means	When to use it
Wrap	Leave control untouched; read data through a gateway or edge device	Control works well; you only need visibility
Retrofit sensing	Add wireless or clamp-on sensors for vibration, temperature, power, flow	Data was never instrumented, such as motor health or energy per machine
Bridge	Translate legacy protocols (Modbus, Profibus, serial, proprietary) to OPC UA or MQTT	Systems must share data but cannot be changed
Migrate	Replace HMI, SCADA, DCS or controllers in phases, reusing field wiring where possible	Hardware is obsolete, unsupported or a cyber risk
Retire	Decommission and consolidate	Duplicate or unused systems add cost and risk

Step 3: Connect safely and incrementally

- Start read-only. Do not write setpoints from new systems to legacy controllers until the integration is proven and change-managed.
- Place an edge layer between the control network and anything above it. It buffers data, normalizes tags and limits exposure.
- Digitize paper first where it hurts most: shift logs, maintenance rounds, quality checklists and batch records.
- Align intrusive work with planned shutdowns or turnarounds, with tested rollback plans. In continuous process plants these windows may be years apart, so plan early.

Typical legacy pitfalls

- Polling old controllers too fast and overloading their communication ports.
- Connecting unpatchable Windows XP or Windows 7 HMIs directly to the corporate network.
- Losing knowledge when long-serving technicians retire. Capture it while you modernize.

8 DESIGNING DIGITAL-READY NEW INSTALLATIONS

The cheapest time to make a plant digital is before it is built. Requirements written into the design basis and purchase orders cost little; retrofitting them after handover costs much more.

Specify in the design basis and purchase orders

- **Open interfaces.** Every machine, skid and package unit exposes data over OPC UA (or MQTT where suitable), with a documented information model. Avoid closed, license-locked gateways.
- **Naming and asset model.** A site-wide tag and asset naming standard based on the ISA-95 hierarchy, applied by all suppliers. Batch and hybrid sites add ISA-88 recipe and equipment models.
- **Data scope.** States, alarms, counts, rejects, energy use and key process values for every machine or unit, so OEE, quality and energy can be computed without later instrumentation.
- **Cybersecurity by design.** Zones and conduits per IEC 62443, hardened devices, no default passwords, remote access only through a managed gateway.
- **Documentation as data.** As-built drawings, I/O lists, control narratives and equipment data handed over in digital, searchable form, ideally structured for a digital twin.

Build in verification

- Include data and interface checks in factory and site acceptance tests (FAT/SAT), not only functional checks.
- Commission the historian, MES links and dashboards with the process, so day-one data is trusted.
- Size compute, storage and network for the next phase of use cases, not only today's.

Avoid the greenfield traps

- Specifying the most advanced option everywhere. Match technology to process risk and the team's ability to sustain it.
- Accepting each supplier's own dashboard as "the digital solution". Insist that data flows into the site's common layer.
- Leaving operators and maintainers out of design reviews. They are the long-term users.

9 ROADMAP: FROM ASSESSMENT TO SCALE

A phased roadmap with stage gates keeps investment tied to proven value. Durations are typical for a single site and vary with scope, size and shutdown windows.

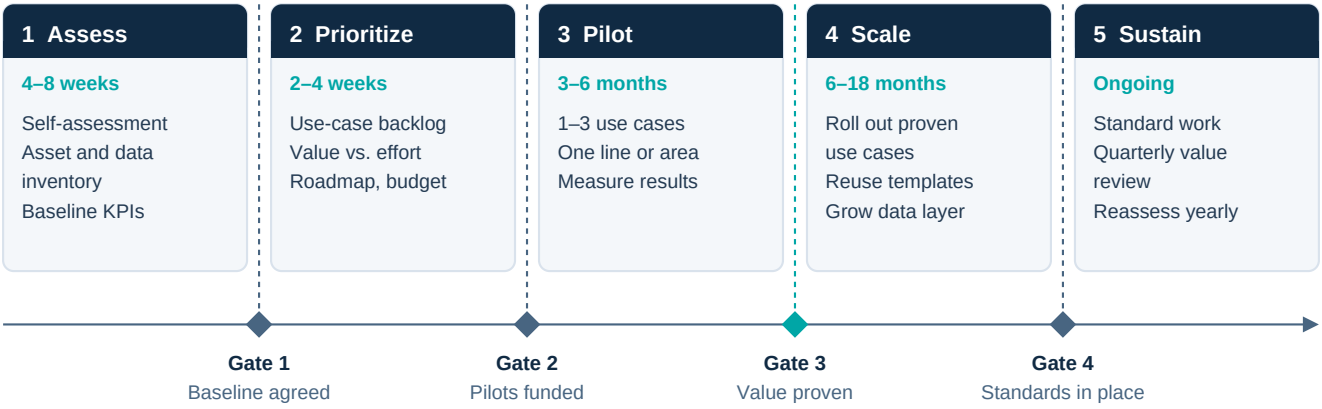

Figure. Scale only what a pilot has proven. Each gate is a go/no-go decision by the steering group; Gate 3 is where most programs stall.

Phase	Key activities	Output
1 Assess	Run the self-assessment; inventory assets, networks and data; walk the floor with operators; record baseline KPIs	Maturity profile, gap list, baseline
2 Prioritize	Build a use-case backlog; score value against effort and readiness; identify foundation work (connectivity, security, data)	Prioritized roadmap and budget
3 Pilot	Deliver one to three use cases on one line or unit, with operators involved; measure against baseline	Proven value and lessons learned
4 Scale	Replicate proven use cases with standard templates; extend the data layer and security controls site-wide, then to other sites	Site-wide capability
5 Sustain	Embed in standard work; review value quarterly; reassess maturity yearly and refresh the roadmap	Continuous improvement

A pilot that misses its target is redesigned or stopped, not quietly extended. Legacy sites usually spend longer in phases 1 and 4, where inventory and safe connection take most effort. New installations can enter at phase 3 for many use cases if digital requirements were written into the design.

10 USE CASES MATCHED TO MATURITY

Pick use cases your current foundation can support. A predictive model on unreliable data fails; a simple downtime tracker on a well-connected line pays back quickly and builds the data the predictive model will later need.

Use case	Value lever	Readiness	Best fit
Digital shift logs and checklists	Fewer missed checks, searchable history	L1–L2	All; quick win for legacy sites
Real-time OEE and downtime tracking	Throughput, loss visibility	L2	Discrete; hybrid packing lines
Energy monitoring per asset or unit	Lower energy intensity and cost	L2	All; often via retrofit meters
Alarm rationalization (ISA-18.2)	Safer, calmer operation; fewer upsets	L2	Process; hybrid process stage
SPC and digital quality checks	Yield, fewer defects	L2–L3	All
Condition monitoring on critical rotating equipment	Fewer unplanned stops	L2–L3	All: pumps, compressors, fans, conveyors
Electronic batch records and genealogy	Compliance, faster release, recall readiness	L3	Hybrid and batch process
Digital work instructions and connected workers	Faster training, consistent execution	L3	Discrete assembly; maintenance everywhere
Advanced process control and optimization	Throughput, yield, energy	L3–L4	Continuous process
Predictive maintenance models	Downtime and spares reduction	L4	Assets with failure history and sensors
Digital twin for simulation and training	Faster changes, safer start-ups	L4–L5	New lines and units; complex processes
AI-assisted scheduling and quality prediction	Responsiveness, right-first-time	L4–L5	High-mix discrete; variable-feed process

Score each candidate on business value and on effort or readiness. Start with high-value, high-readiness use cases, and fund foundation work (connectivity, data quality, security) alongside them.

11 CYBERSECURITY AND RESILIENCE

Every new connection is a new path for an attacker, so security must grow with connectivity, never after it. In operational technology the priorities differ from office IT: safety and availability come first, then integrity, then confidentiality.

Baseline controls every site should have

- An up-to-date inventory of OT assets, software versions and network connections.
- Network segmentation into zones and conduits, with a DMZ between plant and enterprise networks. No direct internet access from control networks.
- Managed, logged, multi-factor remote access for staff and vendors. No unmanaged remote-desktop tools or modems.
- Offline, tested backups of PLC and DCS programs, HMI projects and server images.
- Named accounts, no shared or default passwords, and removal of unused accounts.
- Removable media control and malware scanning stations.
- An OT incident response plan, practiced through tabletop exercises with operations, IT and key vendors.

> **Legacy-specific measures**
> Where systems cannot be patched, compensate: isolate them, allow only the traffic they need, and monitor passively for anomalies. Plan replacement of unsupported operating systems as part of the roadmap. Safety instrumented systems stay independent of business networks in every case.

Frameworks to align with. IEC 62443 is the main standard for industrial automation security. NIST CSF and ISO/IEC 27001 cover the wider organization. National and sector rules also apply in many countries, especially for critical infrastructure such as energy, water and utilities; confirm the obligations in each country where you operate.

12 PEOPLE, GOVERNANCE AND CHANGE

Technology is rarely what stalls transformation; adoption is. Tools that operators and maintainers do not trust, or were not involved in shaping, quietly fall out of use.

Governance that works

Role	Responsibility
Executive sponsor	Owns the strategy, removes barriers, protects funding
Digital steering group (operations, engineering, IT, OT, quality, HSE, finance)	Prioritizes the portfolio, approves stage gates, reviews value quarterly
Site digital lead	Runs the roadmap at plant level; single point of coordination
Use-case owner (from operations)	Accountable for the business result of each use case
IT/OT architecture and security	Sets standards for integration, data and cybersecurity
Digital champions	Front-line users who test, train peers and feed back issues

Change practices

- Involve operators in design from the first workshop and test with them on the shop floor or in the control room.
- Train by role, with hands-on sessions, and refresh training as tools change.
- Build digital tools into standard operating procedures, shift handovers and performance reviews.
- Communicate early wins with real numbers to build momentum.
- Apply formal management of change to any modification of control systems or safety functions.
- Build in-house capability over time so the site does not depend entirely on external suppliers.

13 MEASURING VALUE AND AVOIDING PITFALLS

Define a baseline before any pilot starts, so benefits are measured rather than estimated afterwards. Choose the KPIs that match your industry type: OEE suits discrete and packing lines, while process units often track yield, throughput against nameplate capacity and energy per tonne.

Area	Example KPIs
Productivity	OEE (availability × performance × quality), throughput, changeover or grade-change time
Reliability	Unplanned downtime hours, MTBF, MTTR, planned-to-reactive maintenance ratio
Quality	First-pass yield, scrap and rework rate, customer complaints, batch release time
Energy and sustainability	Energy per unit or tonne produced, water per unit, waste, Scope 1 and 2 emissions
Safety and security	Process safety events, alarms per operator per hour, OT security incidents
Adoption	Active users, use of digital checklists, share of decisions made from live data
Financial	Payback period, cost avoided, working capital released

Ten pitfalls to avoid

1 Starting with technology rather than a business problem.

2 Running endless pilots that never scale (“pilot purgatory”).

3 Ignoring data quality and context.

4 Connecting OT systems before securing them.

5 Building point-to-point integrations that become unmanageable.

6 Locking into proprietary formats that trap your data.

7 Leaving operators and maintainers out of design.

8 Under-funding training and change management.

9 Measuring activity (dashboards built) instead of outcomes (downtime reduced).

10 Treating the program as a one-off project rather than a continuing capability.

14 GLOSSARY AND NEXT STEPS

Term	Meaning
OT	Operational technology: hardware and software that monitor and control physical processes
Discrete / process / hybrid	Making countable units / transforming materials continuously or in batches / a process stage followed by a discrete stage
PLC / DCS	Programmable logic controller / distributed control system
SCADA	Supervisory control and data acquisition
MES / MOM	Manufacturing execution system / manufacturing operations management
Historian	Database optimized for time-series process data
ISA-95 / ISA-88	Standards for integrating enterprise and control systems / for batch control and recipes
OPC UA	Open, secure, vendor-neutral industrial communication standard with information modeling
MQTT	Lightweight publish/subscribe messaging protocol widely used for IIoT
Unified namespace (UNS)	A single, structured, event-driven hub where systems publish and consume plant data
Edge computing	Processing data close to the equipment, before it reaches central systems
Digital twin	A digital representation of an asset or process, kept in sync with real data
OEE	Overall equipment effectiveness
IEC 62443	Series of standards for industrial automation and control system security

Next steps

- ☐ Complete the INOVIQ maturity self-assessment for each site
- ☐ Classify each area of the site as discrete, process or hybrid
- ☐ Identify your strongest capability, biggest gap and top three priorities
- ☐ Inventory assets, data and networks, starting with critical areas
- ☐ Shortlist two or three use cases with clear value and readiness
- ☐ Agree sponsor, site lead and governance

Important: This primer is general guidance, not an audit, certification or design specification. For a facilitated assessment or a site-specific roadmap, contact INOVIQ Technologies at www.inoviqtech.com.