The Connected Factory's Data Spine: Valuing Industrial Digital Twins

An M&A framework for testing data coverage, model fidelity, workflow adoption, validated savings and buyer-specific synergies

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

An industrial digital twin can be a valuable operating asset, a collection of disconnected models or an expensive interface that few people use. The distinction matters in M&A. A buyer can pay for projected availability, yield, energy and maintenance benefits that depend on incomplete sensor coverage, stale asset identities, unvalidated models, vendor-controlled interfaces or workflows that never changed. Reported savings can also combine avoided downtime, recovered output and lower unit cost in ways that count the same operational event more than once.

This paper develops a Digital-Twin Acquisition Value Framework for connected factories. It tests six linked propositions: the physical asset graph is complete; data are available and governed at the required frequency; models reproduce material plant behaviour within documented tolerances; operators and engineers use outputs in controlled workflows; claimed savings reconcile to operational and financial evidence; and the buyer can retain, integrate and improve the capability after closing. The framework connects those tests to stand-alone value, buyer-specific synergy, purchase-price protection and a one-hundred-day integration programme.

A wholly hypothetical case covers eight plants, forty-two production lines and thirty-one lines described as twin-enabled. Only twenty-four lines show active workflow use during the latest ninety days and nineteen have at least twelve months of comparable evidence. Management initially identifies USD 6.6 million of annual gross benefit. After removing baseline changes, overlapping benefits, unverified capacity value and recurring platform cost, the central case retains USD 3.8 million of annual validated benefit. A separate buyer-synergy bridge adds integration benefits only where rights, interfaces, accountable owners, cost and timing are evidenced. Every amount, percentage, asset count and valuation input in the case is a hypothetical management assumption created solely to demonstrate the method. It is not observed company data, a benchmark, a forecast or a valuation opinion.

The analysis draws on the ISO 23247 manufacturing digital-twin framework, NIST work on trustworthy manufacturing digital twins and their economics, ISO asset-management and data-quality standards, NIST operational-technology security guidance, CISA asset-inventory guidance, IFRS valuation and intangible-asset requirements, and the EU Data Act's treatment of connected-product data. The conclusion is practical: a buyer should value the evidenced chain from asset identity to governed data, validated model, adopted decision, verified outcome and durable cash flow. A broken link reduces value even when the visual twin appears sophisticated.

JEL Classification: G32, G34, L23, L60, M15, O32, O33

Keywords: industrial M&A, digital twins, connected factories, industrial data, model fidelity, workflow adoption, operational technology, synergy valuation, post-merger integration

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE ACQUISITION DECISION

The acquisition decision is how much stand-alone and buyer-specific value can be attributed to the target's industrial digital twins, which evidence supports that value, which dependencies can survive closing and which risks require price or contractual protection. The buyer should decide what the target owns, what it licenses, what it can modify, which data it may retain, who can validate changes and how the capability behaves after a supplier, employee, network or ownership change.

The decision is narrower than whether the target will use digital-twin software. A factory can display a sophisticated virtual model while depending on the technology vendor for every material update, fault investigation and optimisation. It can also hold large volumes of operating data that it cannot combine, interpret or reuse. Conversely, a broad transfer may expose the technology provider's background intellectual property, global model improvements or trade secrets beyond the agreed field, territory and duration.

The framework therefore tests six conditions. The asset graph must cover the material production perimeter. Data must be available, timely, attributable and usable. Models must be verified, validated and fit for their stated decisions. Users must incorporate outputs into controlled workflows. Benefits must reconcile to finance and operations without double counting. Rights, security, people and architecture must allow the buyer to operate and integrate the capability after closing.

Table 1. Digital-twin rights stack for an industrial target

Rights layer	Typical subject matter	Core transaction question	Minimum evidence
Background technology	Pre-existing process models, libraries, algorithms and source code	What remains owned by each party and what licence reaches the target?	IP schedule, provenance, registration and licence scope
Manufacturing configuration	Plant-specific asset hierarchy, parameters, recipes and engineering rules	Who controls the configured twin and modifications created for the plant?	Configuration baseline, change history and acceptance record
Operating data	Sensor, event, quality, maintenance and production records	Who may collect, combine, export, retain and reuse the records?	Data inventory, classification, purpose and access matrix
Derived outputs	Features, simulations, model weights, alerts and optimisation recommendations	Does the target own outputs or receive a limited use right?	Derivation logic, version record and permitted-use schedule
Local know-how	Work instructions, tuning practices, failure libraries and trained capability	What capability must remain in the jurisdictions in which the target operates without continuing external intervention?	Competency matrix, witnessed tests and operating records
Improvements	New methods, code, models and inventions developed during target ownership or collaboration	How are improvements owned, licensed and commercialised?	Invention disclosure, contributor record and improvement policy

Each layer requires a defined owner, permitted use, accountable decision maker and exit treatment.

2. DISTINGUISH THE DIGITAL TWIN FROM ITS COMPONENTS

A digital twin is not one indivisible asset. The ISO 23247 series describes a manufacturing digital-twin framework that links observable manufacturing elements, data collection, device control, models and user applications [1-2]. In a transaction, the twin usually consists of several assets and services with different owners and restrictions. It may include mechanical and process models, control logic, equipment master data, interfaces, data pipelines, vendor software, cloud services, simulation tools, maintenance rules, operator judgement and evidence created after commissioning.

This distinction matters because delivery of one component does not establish operating independence. A target may receive a plant model but lack the live interfaces needed to update it. It may receive executable software but not source code or rights to modify it. It may own site data but rely on a vendor-held ontology or calibration method. A trained local team may operate the system during normal production but remain unable to recover it after a major upgrade or cyber incident.

The transaction documents should therefore define the governed capability, not merely the platform name. The capability is the ability to maintain an authoritative plant representation, connect approved operating evidence, run agreed analyses, validate outputs, manage changes and recover service. Rights, people, systems and operating procedures must work together. The absence of one critical element can make another contribution economically stranded.

3. ESTABLISH THE ACQUISITION THESIS

The buyer should state why the target's data spine changes value. The thesis may depend on higher availability, shorter changeovers, lower scrap, improved energy intensity, lower maintenance cost, faster product introduction, more reliable capacity or a scalable service proposition. Each claimed source of value needs a baseline, causal mechanism, evidence owner, implementation cost and route to cash.

The thesis should identify the relevant operating decisions. These may include production scheduling, recipe approval, energy optimisation, quality release, predictive maintenance, debottlenecking and engineering change. Each decision requires a defined evidence chain and a named accountable owner. Broad digital-transformation language has limited valuation meaning when the investment case depends on a small number of high-value decisions.

The thesis should separate current value from future option value. Current value rests on adopted workflows and benefits that reconcile to comparable operating periods. Option value can reflect new lines, plants, products or buyer datasets when technical feasibility, rights, investment and commercial consequences are explicit. A platform label, pilot or three-dimensional model does not establish either category by itself.

4. MAP THE OBSERVABLE MANUFACTURING PERIMETER

The digital-twin perimeter should begin with the physical production system. The parties should identify the plant, line, cell, machine, tool, utility, material flow, product family and quality stage represented by the twin. Each observable manufacturing element needs a persistent identity and relationship to drawings, bills of material, sensors, controls, work orders and operating limits. The map should distinguish equipment owned by the target from leased assets, vendor-controlled systems and shared infrastructure.

The data perimeter should then identify every source used to initialise, calibrate, update or validate the twin. Typical sources include engineering design files, programmable-controller tags, historians, manufacturing execution systems, laboratory systems, maintenance systems, operator logs, energy meters, inspection records and original-equipment-manufacturer portals. For each source, the map should record ownership, legal control, security classification, location, retention, export capability, format, quality and dependency.

The model perimeter should identify the representations used for geometry, physics, process behaviour, controls, statistics and machine learning. A model may be reliable only within specified products, loads, ambient conditions or equipment configurations. The parties should record intended use, calibration evidence, validation population, limitations and change authority. A twin that lacks a controlled perimeter can produce plausible outputs that refer to an obsolete configuration or an operating state outside the validated range.

5. BUILD THE RIGHTS ARCHITECTURE

The rights architecture should separate ownership from access, use, modification, commercialisation and control. Ownership may remain with a party while the target receives a durable, paid-up licence

for a defined field and territory. A licence can be exclusive or non-exclusive, transferable or personal, perpetual or time-limited, and capable or incapable of surviving termination. These dimensions should be negotiated independently.

The architecture should also distinguish background technology from foreground improvements. Background technology exists before the transaction or is developed independently outside it. Foreground improvements arise through target-funded work, plant operation or collaboration. A simple rule that all improvements belong to one party can create disputes when employees, contractors, operating data and pre-existing code contribute together. The agreement should define contribution records, invention disclosure, ownership tests, licence-backs and rights to general learning.

Source-code access requires particular care. Full assignment may be unnecessary if continuity can be protected through escrow, step-in rights, documented interfaces, local build capability and a licence that activates on defined events. Escrow alone is weak when the deposited code is incomplete, cannot be compiled or excludes required dependencies. A verification plan should test build instructions, third-party components, credentials, update cadence and release triggers.

6. BUILD THE ASSET AND DATA COVERAGE FUNNEL

The diligence team should reconcile the population from physical assets to economically active workflows. The starting population includes plants, lines, cells, critical assets, sensors, control tags and operating states. Each level should show what is identified, connected, quality-controlled, modelled, used and seasoned. Coverage measured as connected tags can mislead when the missing tags govern the constraint, product quality or failure mode that creates value.

The asset graph should connect persistent identifiers to location, hierarchy, equipment class, configuration, product, bill of material, process step, sensor, controller, historian, work order and financial consequence. Duplicate identities, reused tag names, undocumented bypasses and stale configurations weaken the link between model output and physical reality. The buyer should sample critical paths and trace them in both directions.

Data quality requires dimensions suited to the decision: completeness, accuracy, consistency, timeliness, uniqueness, provenance and contextual validity. A monthly energy model may tolerate a frequency that is unusable for cycle-level quality control. A predictive-maintenance model may fail when maintenance actions are recorded as free text or when failure labels reflect inspection practice rather than actual condition. ISO 8000 and ISO/IEC 25012 provide useful data-quality concepts, while NIST's digital-thread work emphasises trusted information flows across the lifecycle [8][9][24].

7. CREATE AN OPERATIONAL-CAPABILITY AND ADOPTION SCORECARD

A useful scorecard measures whether the target can perform defined tasks without fragile dependence on one vendor or employee. Capability can be assessed across people, process, data, tooling, authority and evidence. The buyer should identify the level required at closing and the evidence that an independent reviewer can inspect.

The scorecard should avoid equating attendance with competence. Training hours show exposure, not performance. A stronger test requires local personnel to complete a task using controlled procedures and evidence, under defined operating conditions and escalation rules. Examples include restoring a model from an approved baseline, adding an asset, validating a parameter change, investigating a quality deviation, executing a simulation and reconciling the result to plant evidence.

Table 2. Illustrative digital-twin capability and adoption scorecard

Capability	Initial state	Milestone test	Acceptance evidence	Governance consequence
Plant model administration	Provider-operated	local team updates asset hierarchy and rolls back a change	Change ticket, validation report and recovery log	Routine administration delegated locally
Data engineering	Shared support	Local team connects and quality-checks an approved source	Lineage record, quality metrics and access approval	New approved sources can be onboarded locally
Model validation	Provider-led	Joint team validates a defined use case on local evidence	Test set, error analysis, limits and approval	Model release authority becomes shared
Maintenance analytics	Advisory use	Local engineers investigate alerts and close the evidence loop	Alert, inspection, action and outcome record	Routine decisions move to plant governance
Cyber recovery	Provider-dependent	Local team restores service from a clean baseline	Recovery exercise and security sign-off	Continuity step-in right becomes operational
Improvement development	Limited	Local team develops an approved plant-specific enhancement	Contributor record, code review and benefit evidence	Improvement ownership rule is applied

Capability is accepted through witnessed performance and controlled evidence rather than platform access alone.

8. GOVERN DATA CLASSIFICATION AND PERMITTED USE

Industrial data can contain several legal and commercial interests at once. A production event may reveal process know-how, customer demand, employee activity, equipment performance and supplier quality. The target should classify data by sensitivity, owner or controller, permitted purpose, territory, retention and access role. Classification should travel with exports, backups and derived datasets.

The buyer should separate industrial operating data, personal data, customer data, supplier information and trade secrets. Employee identifiers, biometric access records, video, shift histories and detailed operator-performance records can require specific handling even when the main purpose is industrial optimisation. The EU Data Act is also relevant to connected-product data in its scope because it gives users rights to access and share certain data generated by connected products and related services [10]. Applicable privacy, employment, sector and data-access rules require jurisdiction-specific review.

Permitted use should be described precisely. The technology provider may need access to diagnose faults and improve the licensed service. The target may need the right to retain records, benchmark

assets and continue local models after termination. The parties should define whether provider learning may be used for other customers, whether data must be aggregated or anonymised, and whether the target receives benefits from global improvements. Cross-border transfers and remote support require a current legal and security assessment.

9. USE A CONTROLLED DIGITAL-TWIN ARCHITECTURE

The architecture should create a traceable path from the physical plant to the decision. ISO 23247 provides a manufacturing digital-twin framework with observable manufacturing elements, data-collection and device-control entities, core entities and user entities [1]. For a target, the architecture should add transaction controls: rights metadata, provenance, version history, jurisdiction, approval state, access role and exit treatment.

The authoritative configuration should be identifiable at any time. Plant changes, software releases, sensor replacements and model updates can create divergence between the physical system and its virtual representation. The change process should show who proposed the change, what evidence supported it, which tests were run, who approved release and how the prior state can be restored. Safety and production controls should remain independent where appropriate.

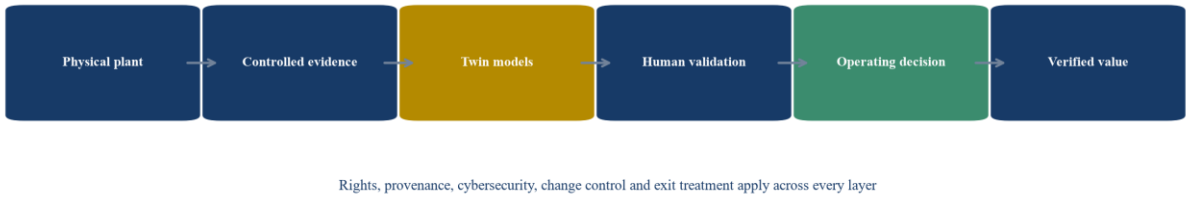

Figure 1. Digital-twin acquisition governance architecture

The architecture connects the physical plant, controlled evidence, models, human decisions and transaction rights.

10. PROTECT INTELLECTUAL PROPERTY AND TRADE SECRETS

The intellectual-property schedule should identify patents, software, copyright works, databases, designs, confidential know-how, trademarks and contractual rights used by the target. The buyer should confirm ownership, contributor chains, open-source obligations, licence restrictions, assignment requirements and any formalities needed to preserve rights after closing. IAS 38's identifiability framework helps distinguish contractual or separable intangible assets from broader operating capability, while transaction value still depends on enforceable rights and economic utility [12].

Trade-secret protection depends on behaviour as well as drafting. Access should follow role, purpose and need. Repositories should separate target-specific material from the provider's broader libraries. Download, export and administrative actions should be logged. Contractors should receive only the information required for their tasks and should return or destroy it at the end of access. Sensitive design and process information should not move through unmanaged collaboration tools.

The agreement should address reverse engineering, benchmarking, publication, patent filing, employee inventions and third-party claims. It should also define the response when plant data reveals an improvement to background technology. The parties may agree that the inventor owns the improvement while the target receives a permanent plant-use licence, or that specified classes of plant-specific improvements belong to the target. The rule should follow the economic bargain and remain workable after exit.

11. DESIGN KNOWLEDGE TRANSFER AS OPERATING CAPABILITY

Technology transfer becomes durable when the recipient can perform the required operating and engineering tasks. Documents and classroom sessions support that outcome but do not prove it. The plan should identify the decisions, tasks and failure situations that local teams must handle. It should define prerequisite skills, supervised practice, independent performance, assessment criteria, refresher requirements and escalation limits.

Tacit knowledge deserves explicit attention. Experienced engineers often recognise abnormal behaviour through context that is absent from a formal manual. The transfer plan can capture this knowledge through paired investigations, structured failure reviews, annotated operating cases, decision journals and witnessed shutdown or commissioning work. A failure library should record symptoms, conditions, diagnosis, action, outcome and lessons without turning one local event into a universal rule.

Retention also matters. A target can meet a training milestone and lose the capability when key personnel leave. The operating model should identify critical roles, succession, minimum staffing, protected learning time and a method for maintaining competence. Incentives for the technology partner can be linked to capability outcomes that remain valid after a defined period, rather than completion of training inputs.

12. CONTROL CROSS-BORDER ACCESS AND PERSONAL DATA

Remote support can improve speed and provide scarce expertise, but it changes the data and security perimeter. The target should identify which users outside the jurisdictions in which the target operates can access systems, which data are visible, whether sessions are recorded, where support logs are retained and whether files can be downloaded. Privileged access should be time-limited, approved, monitored and capable of rapid revocation.

The personal-data assessment should focus on identifiable people in industrial records. Maintenance work orders may name technicians. Video analytics may show employees. Access-control logs and shift records can reveal attendance and behaviour. The parties should establish a lawful purpose, limit collection, provide required information, manage retention and rights, and apply appropriate technical and organisational safeguards under applicable law.

The operating-data assessment should also cover national data classifications, sector restrictions, customer confidentiality and critical-infrastructure requirements. A dataset that is not personal can still be highly sensitive. The data-sharing schedule should define approved purposes, recipients, environments, aggregation and return or destruction. Any proposed secondary use for product

development, global model training or commercial benchmarking should have a separate approval path.

13. SECURE OPERATIONAL TECHNOLOGY

NIST SP 800-82 addresses operational-technology security while recognising performance, reliability and safety requirements [15]. CISA's operational-technology asset-inventory guidance describes the inventory and taxonomy as foundations for defensible architecture, risk management and incident response [16]. IEC 62443 provides an additional industrial-automation and control-system security framework [17]. A digital-twin architecture that connects operating technology to enterprise, cloud or remote environments should be assessed against applicable control sets and plant-safety constraints.

The transaction should identify every new connection, service account, gateway, historian interface, cloud component and remote-support path. It should record data direction, protocol, authentication, encryption, logging and failure behaviour. The architecture should preserve safe local operation when analytics or remote services are unavailable. Models and recommendations should not bypass established safety interlocks or authorised control procedures.

Cybersecurity responsibilities should be reflected in the acquisition governance model. The technology provider may control software development and vulnerability remediation. The target may control plant networks and identities. A managed-service provider may operate monitoring. The agreement should allocate patching, incident notice, evidence preservation, recovery, regulatory engagement, audit and cost. Shared responsibility should not become unassigned responsibility.

14. GOVERN MODELS AND HUMAN ACCOUNTABILITY

A model can support a decision without owning it. The target should assign accountable people for model approval, engineering interpretation, operating action and financial recognition. Model documentation should state intended use, prohibited use, inputs, assumptions, training or calibration population, performance measures, limitations, monitoring and override procedures.

The OECD AI Principles and NIST AI Risk Management Framework emphasise transparency, traceability, robustness and accountability across the AI lifecycle [21][22]. These principles are relevant when a twin incorporates predictive models, optimisation or generative interfaces. The parties should retain sufficient records to reconstruct important outputs and subsequent decisions. They should also provide a safe method to override, repair or withdraw a model that behaves outside expectations.

Joint ownership of a model does not automatically create joint accountability. The governance schedule should identify who can propose, validate and approve changes. A provider should not be able to push a material update into production without plant approval. A local team should not be able to alter safety-relevant parameters outside the validated process. Independent challenge is useful for high-consequence use cases and for disputes over whether a milestone has been met.

15. ALIGN ACQUISITION CONTROL AND DIGITAL DECISION RIGHTS

IFRS 3 treats an acquisition as a transaction in which an acquirer obtains control of one or more businesses [13]. The legal transfer of control does not automatically deliver practical control of a digital twin. A vendor can retain administrative credentials, model registries, deployment pipelines, cryptographic keys or interfaces that the target cannot replace. A former owner can also retain rights over site configurations or derived improvements.

The buyer should map corporate authority to system privileges and operating procedures. Relevant decisions include annual budgets, production plans, model releases, licensing, material data sharing, cybersecurity architecture and appointment of accountable technical leaders. Routine plant decisions need defined delegation. Material changes require evidence, independent challenge, approval and rollback.

The closing plan should identify every credential, key, repository, tenant, service account, certificate, domain, escrow deposit and vendor consent required for continuity. Practical control should be tested through an access rehearsal and a controlled recovery exercise before the buyer attributes full continuity value.

Table 3. Digital-twin acquisition decision-rights matrix

Decision	Proposer	Independent challenge	Approver	Required record
Background-technology release	Technology owner	IP and security review	Deal steering committee	Licence schedule, provenance and dependency assessment
Plant-specific configuration	Engineering team	Process-safety and quality review	Target technical director	Change request, tests and rollback plan
New data source or cross-border access	Data owner	Privacy and cybersecurity review	Data-governance committee	Purpose, classification, lineage and access decision
Model release	Model owner	Independent validation	Engineering and AI governance owner	Test report, limitations and monitoring plan
Operating action	Plant function	Discipline specialist where required	Authorised plant manager	Evidence, decision, action and outcome
External commercialisation	Rights owner	Competition, IP and valuation review	Deal steering committee	Market scope, licence economics and conflict assessment

Corporate authority, technical privilege and operating accountability should point to the same decision owner.

16. SELECT THE VALUATION APPROACH

The value of the digital-twin contribution depends on the rights and capabilities transferred. A relief-from-royalty approach can estimate the present value of avoided licence payments for a legally protectable technology right. A cost approach can estimate the cost to recreate documented software, models, data preparation and engineering knowledge, adjusted for obsolescence and economic

utility. An incremental cash-flow approach can estimate buyer-specific operating benefits after implementation, recurring cost, ramp time and risk.

The methods answer different questions. Replacement cost does not prove that the capability will produce cash benefits. A royalty benchmark may not reflect the restricted field, territory, exclusivity or dependence in the actual transaction. Incremental cash flow can capture operating value but is sensitive to the baseline, attribution and execution assumptions. A robust analysis uses the method appropriate to the right being valued and reconciles differences.

Accounting recognition should remain separate from transaction value. IAS 38 defines an intangible asset through identifiability and requires probable future economic benefits and reliable measurement for recognition [12]. A contractually protected licence may be recognisable while a broader operating capability is not a separate accounting asset. Conversely, a target can derive economic value from integrated know-how and data even when no separate asset appears on the balance sheet. Accounting specialists should assess the specific facts.

17. BUILD THE OPERATING BASELINE

The valuation should begin with expected performance without the digital-twin contribution or incremental operating capability programme. The baseline should cover availability, throughput, yield, energy, maintenance cost, spare-parts use, quality loss and service risk. It should reflect the planned plant design and operating ramp, not a mature benchmark imported from another country or factory.

The evidence should separate technical loss from commercial loss. A production interruption has economic value only when it constrains saleable output, causes incremental cost or changes customer outcomes. Spare labour or inventory may absorb some events. A quality improvement may reduce scrap, rework, claims or lost contribution, but these effects should not be counted several times. Energy benefit should be measured against production mix and operating conditions.

The baseline should also show what existing systems and people would achieve. A digital twin may accelerate diagnosis but not replace sound maintenance, process control or competent engineering. Benefits created by the broader factory ramp should not be attributed to the twin. Finance, engineering and operations should agree the evidence ledger before benefits are included in the investment case.

18. LINK MILESTONES TO CONTRIBUTION VALUE

Contribution value should vest as the target receives usable rights and capability. A single contribution value at signing can overstate delivery when material elements depend on later integration, training or validation. Staged recognition can link value, royalties, equity credit, earn-out or other economics to defined milestones.

Milestones should be objective enough to test. Examples include delivery of an approved configuration baseline, verified data interfaces, successful recovery, local administration, validated use cases and sustained performance over an agreed period. A milestone should identify the

acceptance authority, evidence, cure period and consequence of failure. It should also distinguish a provider delay from a plant-access or data-quality delay controlled by the target.

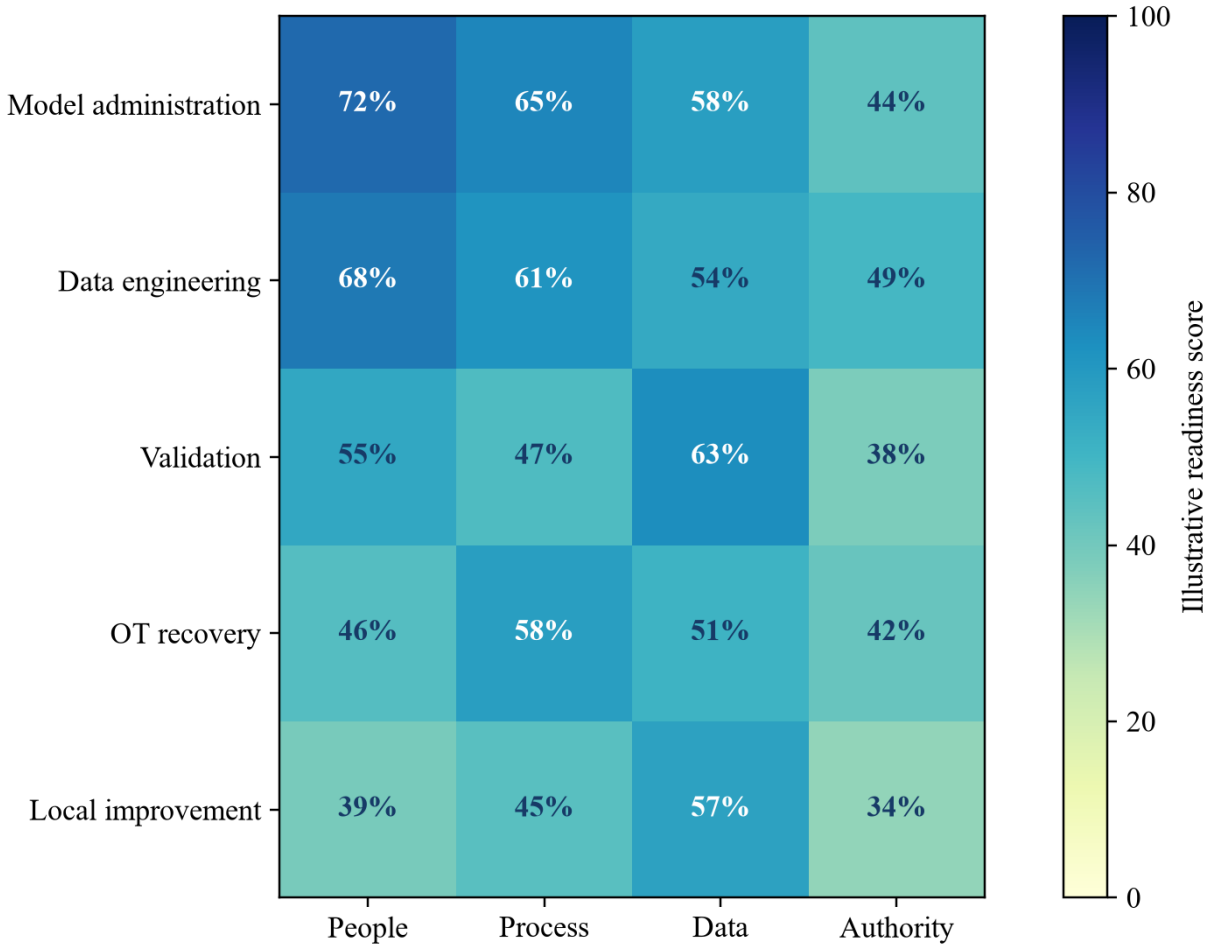

Figure 2. Illustrative operating capability-readiness heat map

Management-assumed readiness scores identify capabilities that require evidence before economic value can vest.

19. DEMONSTRATE THE HYPOTHETICAL CASE

The illustrative target operates eight plants and forty-two production lines. Management describes thirty-one lines as twin-enabled. Diligence finds that twenty-seven lines meet the required data-completeness threshold, twenty-four show active workflow use during the latest ninety days and nineteen have at least twelve months of comparable evidence. The funnel matters because a benefit extrapolated from nineteen seasoned lines to all forty-two lines would assume adoption, fidelity and economic conditions that have not been demonstrated.

Management identifies USD 6.6 million of annual gross benefit: USD 2.7 million from availability and recovered output, USD 1.6 million from yield and quality, USD 1.1 million from energy optimisation and USD 1.2 million from maintenance and spares. The diligence bridge removes USD 0.7 million associated with production-volume and product-mix changes, USD 0.5 million of overlap between recovered output and avoided downtime, USD 0.4 million of unverified capacity value and USD 1.2 million of recurring software, support, data-engineering, security and validation cost. The central case retains USD 3.8 million of annual validated benefit.

The stand-alone case assumes USD 4.5 million of completion and remediation cost across data mapping, model validation, interfaces, security and training. Benefit ramps from USD 2.1 million in year one to USD 3.8 million in year two and USD 4.2 million in years three to five. A management-assumed thirteen-percent discount rate produces an illustrative value range that remains sensitive to benefit persistence, capital requirements and the buyer's tax and financing position. The model excludes terminal value and treats buyer-specific synergy separately.

Table 4. Hypothetical connected-factory valuation case

Item	Timing	Management assumption	Valuation treatment
Completion and remediation	Completion and year 1	4.5	Initial and year-one cash outflow
Validated operating benefit	Year 1	2.1	Discounted inflow
Validated operating benefit	Year 2	3.8	Discounted inflow
Validated operating benefit	Year 3	4.2	Discounted inflow
Validated operating benefit	Year 4	4.2	Discounted inflow
Validated operating benefit	Year 5	4.2	Discounted inflow
Illustrative discount rate	Five-year model	13 percent	Management assumption
Terminal value	Excluded	0.0	Requires separate support

All figures are management assumptions in USD millions and demonstrate the framework only.

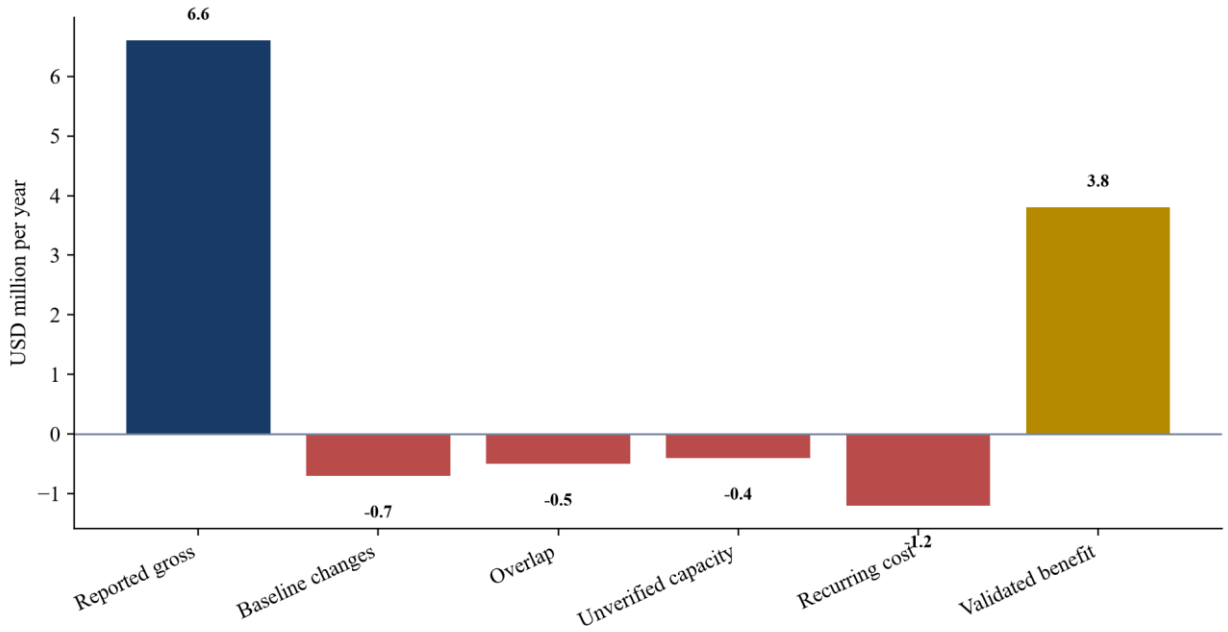

Figure 3. Hypothetical annual savings-validation bridge

Management assumptions show how reported gross benefit becomes validated recurring benefit.

20. ALLOCATE ECONOMICS WITHOUT DOUBLE COUNTING

The valuation should distinguish the value of licensed technology, plant-specific configuration, knowledge transfer and future services. A royalty can compensate ongoing use of background technology. A contribution value can recognise rights committed at formation. Service fees can compensate continuing support. Milestone payments can reward completed operating capability.

Using all four mechanisms without reconciliation can charge the target several times for the same economic benefit.

The parties should maintain a value bridge from each payment to a defined right or service. The bridge should show whether the consideration is fixed, usage-based, performance-linked or cost-plus. It should identify related-party pricing, withholding, tax and accounting implications for specialist advice. It should also show the effect of termination and step-in rights.

The operating-benefit model should avoid double counting. Availability and throughput may describe the same recovered production. Yield improvement and lower material cost can overlap. Reduced emergency maintenance may lower overtime and contractors without reducing salaried headcount. Energy benefit may partly arise from a separate equipment upgrade. Each benefit should appear once, with a baseline, owner, evidence source and attribution rule.

21. DESIGN RESERVED MATTERS AND DELEGATIONS

Reserved matters should protect decisions that can alter the target's strategic rights, risk or value. Digital-twin reserved matters may include assignment or material amendment of core licences, use outside the agreed field, export of sensitive data, changes to cybersecurity architecture, external commercialisation, disposal of source code, abandonment of a material model and approval of large related-party technology contracts.

Routine operations require delegation. A plant should be able to replace an approved sensor, correct a mapping, tune a model within validated bounds and perform ordinary maintenance without repeated board approval. Delegations should specify thresholds, accountable roles, evidence and reporting. The technology partner may retain consent for changes that expose background intellectual property, while the plant retains authority over safety and production.

System privileges should follow the governance map. Administrative rights, signing keys, deployment pipelines and model registries can create practical control. The target should maintain dual control for sensitive actions, emergency procedures for continuity and periodic review of access. A constitutional veto has limited value if one party can disable operations through an unmanaged technical dependency.

22. PREPARE FOR DEADLOCK AND CONTINUITY

Digital-twin disputes can stop production or delay operating capability. The agreement should define escalation paths for disagreements over model release, data access, milestone acceptance, security remediation, licence fees and improvements. A technical dispute may require an independent expert with the right discipline and access to the underlying evidence. A commercial deadlock may require executive escalation, mediation, buy-sell mechanisms or another agreed remedy.

Continuity measures should operate while the dispute is resolved. The target may need a right to continue the last approved version, obtain critical support, access escrow materials or appoint an alternate provider. The technology partner may need protection against unauthorised copying, non-payment or use beyond scope. Interim rights should be limited to preserving safe operation and should not determine the final merits.

The deadlock matrix should distinguish safety-critical issues from commercial disputes. Safety, cybersecurity and legal compliance should have immediate protective procedures. A pricing disagreement should not automatically permit a shutdown. The agreement should also address what happens when a regulator, customer or insurer requires a change that one party has not anticipated.

23. BUILD TRANSACTION PROTECTIONS AROUND EVIDENCE

Representations and warranties should address ownership or authority, disclosed third-party components, infringement claims, licences, material interfaces, cybersecurity incidents, data provenance, export capability and compliance with agreed development practices. They should be tailored to the actual contribution. A broad statement that the technology is fit for purpose may create uncertainty when intended uses and plant conditions are undefined.

Conditions precedent can require delivery of agreed licences, approvals, baseline documentation, data inventories, security assessments and escrow arrangements. Milestone conditions can govern staged contribution value or payments. Indemnities may address specific known risks such as a third-party licence gap or undisclosed infringement claim. Caps, exclusions, survival and remedies should reflect the negotiated risk allocation and local legal advice.

Acceptance testing should reproduce critical tasks. The target should test installation, interfaces, model outputs, failure recovery, access controls and documentation. Performance tests should use agreed conditions and tolerances. A test that proves functionality on sample data does not establish plant performance. The acceptance record should distinguish software delivery from operating benefit, which requires evidence over time.

24. PROTECT COMPETITION AND CLEAN-TEAM BOUNDARIES

An acquisition can require competitors, suppliers or customers to share sensitive information before closing. The clean-team protocol should restrict competitively sensitive plant, customer, pricing, capacity and cost data to approved recipients and defined purposes. Competition counsel should determine filing, gun-jumping, control and information-exchange requirements for the relevant jurisdictions.

Before approval and closing, clean-team controls can limit access to competitively sensitive information. Production costs, customer demand, pricing, future capacity, bids and strategic plans may require aggregation or specialist review. Technical diligence should receive the information needed to assess the digital twin without giving operating teams unnecessary visibility into competitive strategy.

Post-close information sharing should remain tied to a legitimate operating purpose. The data-governance schedule should identify recipients, aggregation, delay and purpose. External commercialisation of combined models or benchmarks can require additional competition, confidentiality and data-rights review.

25. EXECUTE THE FIRST HUNDRED DAYS

The first thirty days should preserve evidence and establish authority. The target confirms licence schedules, IP provenance, data classifications, system owners, privileged access, approved baselines,

security responsibilities and milestone evidence. It freezes undocumented changes to critical models and interfaces while allowing safe production. It also confirms training cohorts and the initial capability assessment.

Days thirty-one to sixty should establish controlled transfer. The team maps observable manufacturing elements, confirms data lineage, tests interfaces, validates recovery materials and runs the first witnessed capability tasks. It closes critical security gaps and identifies any third-party rights that prevent intended use. Finance establishes the operating-benefit baseline and evidence ledger.

Days sixty-one to one hundred should release limited use cases through the approved governance process. The target validates outputs on local evidence, tests human review and rollback, measures early operating effects and records exceptions. The board receives a rights, capability, security and value report. Further economic credit or rollout depends on the evidence gates agreed in the transaction.

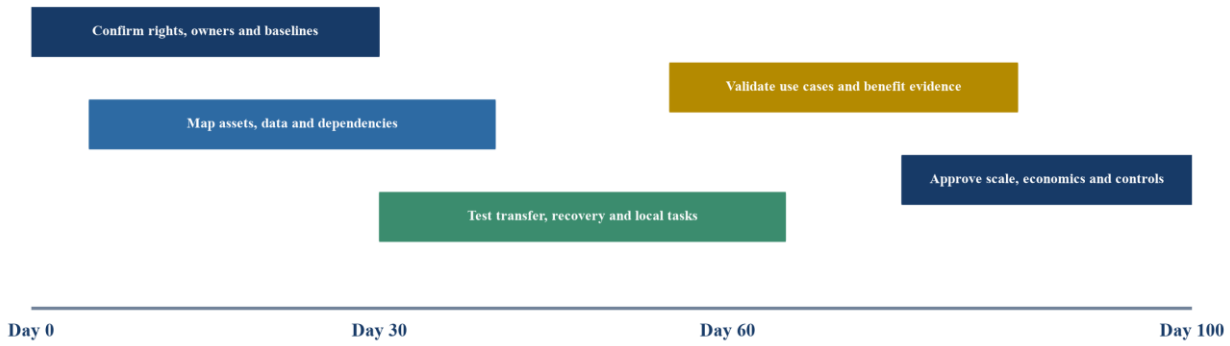

Figure 4. First hundred day digital-twin governance roadmap

The roadmap moves from rights and evidence preservation to controlled transfer, local validation and board-approved scaling.

26. GOVERN EXIT, TERMINATION AND CHANGE OF CONTROL

Exit should be designed when the rights architecture is agreed. A target may end through sale, listing, partner buyout, insolvency, expiry or termination for breach. The continuing business needs clarity on plant data, configured models, interfaces, documentation, source code, licences, trained capability and support. The technology provider needs protection against use beyond the surviving scope.

The agreement should define licences that survive each exit path. A buyer of the target may need consent or may inherit defined rights. A competing buyer may create legitimate restrictions. A technology-provider change of control may introduce a competitor, sanctions issue or security concern. Step-in, escrow or transition rights can protect continuity while the parties implement the agreed remedy.

Data exit should include format, metadata, lineage, credentials, derived outputs, retention and verified deletion. The target should be able to reconstruct the last approved configuration and continue agreed operations. The provider should be able to separate its background technology and

confidential information without deleting target-owned records. A tested exit rehearsal is stronger evidence than a contractual promise that has never been operationalised.

27. RECOGNISE LIMITATIONS

The framework cannot determine the legal effect of a specific local acquisition agreement, licence, data transfer or intellectual-property arrangement. Applicable requirements depend on the parties, sector, data, technology, transaction structure and current law. local legal, tax, accounting, competition, intellectual-property, cybersecurity and sector specialists should review the actual arrangement.

Digital-twin performance is context-dependent. A model validated on another plant may not transfer to local equipment, materials, climate, workforce, suppliers or operating practices. Documentation can be incomplete. Source code can depend on undisclosed libraries or services. Data may be biased toward stable operation and contain too few abnormal events. Cybersecurity or safety constraints can limit connectivity and automation.

The hypothetical case uses management assumptions and excludes terminal value, tax, financing, working capital, transfer pricing, grants, incentives and negotiated value sharing. It does not predict the value of any project. Commercial demand for a particular structure remains unverified until supported by project-specific evidence and agreed transaction terms.

28. DRAW THE INVESTMENT CONCLUSION

A digital twin supports technology transfer and operating capability when the target receives a governed operating capability. The capability combines durable rights, plant-specific configuration, controlled data, validated models, trained people, change authority, cybersecurity, continuity and evidence of economic effect. Delivery of software or documents alone does not establish that result.

The investment case should define high-value decisions, map every component and dependency, separate background technology from target improvements, and make operating capability milestones independently testable. Reserved matters, technical privileges and operating delegations should align. Valuation should follow the rights actually transferred and use incremental cash flow after implementation, recurring cost, ramp time and risk.

The strongest transaction structure links economics to evidence. It rewards the technology provider for valuable rights and successful transfer, gives the target operating team the capability required for resilient local operation, and preserves accountability for safety, security and investment decisions. The resulting governance system can convert operating capability from an aspiration into a measurable operating asset.

REFERENCES

[1] [1] International Organization for Standardization, ISO 23247-1:2021 Automation systems and integration: Digital twin framework for manufacturing, Part 1 https://www.iso.org/standard/75066.html

[2] [2] International Organization for Standardization, ISO 23247-2:2021 Reference architecture https://www.iso.org/standard/78743.html

[3] [3] National Institute of Standards and Technology, Digital Twins for Advanced Manufacturing https://www.nist.gov/programs-projects/digital-twins-advanced-manufacturing

[4] [4] National Institute of Standards and Technology, Digital Twins https://www.nist.gov/digital-twins

[5] [5] National Institute of Standards and Technology, Economics of Digital Twins: Costs, Benefits, and Economic Decision Making https://www.nist.gov/publications/economics-digital-twins-costs-benefits-and-economic-decision-making

[6] [6] International Organization for Standardization, ISO 55000:2024 Asset management, vocabulary, overview and principles https://www.iso.org/standard/83053.html

[7] [7] International Organization for Standardization, ISO 55013:2024 Guidance on the management of data assets https://www.iso.org/standard/82455.html

[8] [8] International Organization for Standardization, ISO 8000 data quality standards https://www.iso.org/committee/54158/x/catalogue/

[9] [9] International Organization for Standardization, ISO/IEC 25012 data quality model https://www.iso.org/standard/35736.html

[10] [10] European Commission, EU Data Act gives users control over data from connected devices https://digital-strategy.ec.europa.eu/en/news/eu-data-act-gives-users-control-over-data-connected-devices

[11] [11] IFRS Foundation, IFRS 13 Fair Value Measurement https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

[12] [12] IFRS Foundation, IAS 38 Intangible Assets https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

[13] [13] IFRS Foundation, IFRS 3 Business Combinations https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[14] [14] IFRS Foundation, IAS 36 Impairment of Assets https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/

[15] [15] National Institute of Standards and Technology, SP 800-82 Rev. 3 Guide to Operational Technology Security https://csrc.nist.gov/pubs/sp/800/82/r3/final

[16] [16] Cybersecurity and Infrastructure Security Agency, Foundations for OT Cybersecurity: Asset Inventory Guidance https://www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf

[17] [17] International Electrotechnical Commission, IEC 62443 industrial automation and control systems security https://www.iec.ch/cyber-security

[18] [18] OPC Foundation, OPC UA for Asset Administration Shell https://reference.opcfoundation.org/specs/OPC-30270/full

[19] [19] Digital Twin Consortium, Digital Twin System Interoperability Framework https://www.digitaltwinconsortium.org/wp-content/uploads/sites/3/2022/06/Digital-Twin-System-Interoperability-Framework-12072021.pdf

[20] [20] National Institute of Standards and Technology, Cybersecurity Framework 2.0 https://www.nist.gov/cyberframework

[21] [21] Organisation for Economic Co-operation and Development, OECD AI Principles https://www.oecd.org/en/topics/ai-principles.html

[22] [22] National Institute of Standards and Technology, AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework

[23] [23] International Organization for Standardization, ISO/IEC 30173:2023 Digital twin concepts and terminology https://www.iso.org/standard/81442.html

[24] [24] National Institute of Standards and Technology, Digital Thread for Manufacturing https://www.nist.gov/programs-projects/digital-thread-manufacturing

ABOUT THE AUTHOR

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.