The National Grid Digital Twin

Investment Opportunities from Real-Time Power Intelligence

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

Electricity systems are becoming harder to observe and plan. Variable generation, power-electronic equipment, distributed resources, electric transport, large computing loads and more severe operating conditions create interactions that static network studies cannot represent continuously. Grid operators are therefore joining network models, asset records, measurements, forecasts and simulations into digital twins that can support decisions across planning, operation and maintenance.

This paper develops an investment and execution framework for a national grid digital twin. It defines the minimum operating capability, separates asset, network, market and scenario twins, and explains why a federated system of independently governed twins is often more realistic than one central model. It maps the technology and service value chain from sensors and communications through data spaces, model orchestration, real-time simulation, cyber assurance and operator workflows.

The evidence base spans Great Britain's Virtual Energy System, the European Union's TwinEU initiative and ENTSO-E's federated approach, Singapore's national Grid Digital Twin, United States Department of Energy and national-laboratory research, and Dubai Electricity and Water Authority's distribution-grid work. These programmes have different mandates and maturity. Together, they show that interoperability, data quality, model validation, decision ownership and cyber-physical safety determine whether a digital twin produces enduring value.

Six figures present the capability stack, federated architecture, use-case portfolio, evidence chain, commercial ecosystem and delivery roadmap. Six tables provide a decision register, international comparison, data and model controls, procurement structure, hypothetical investment case and 180-day execution plan. Every price, cost, saving, probability, duration and financial result in the worked example is a hypothetical management assumption created solely to demonstrate the method.

Power-system modelling, operational technology, protection, communications, cyber security, licensing, market design, procurement, accounting, tax, valuation, credit and investment decisions require qualified professional review. This paper provides general information for professional audiences and does not provide engineering, operational, legal, regulatory, cyber-security, tax, accounting, valuation, credit or investment advice.

JEL Classification: G31, G32, L94, O31, O33, Q40, Q48

Keywords: grid digital twin, electricity networks, real-time power intelligence, grid observability, energy data, digital infrastructure, predictive maintenance, grid investment, interoperability, power-system resilience

1. Define the decision before the twin

A digital twin should improve a specified decision. The starting point can be a connection study, an asset-renewal programme, a stability assessment, an outage-restoration plan, a maintenance intervention or a long-term network investment. Each decision has an owner, time horizon, evidence threshold and consequence of error.

The phrase digital twin is used for several different systems. A static three-dimensional asset model, a network simulation, a live operational replica and a federation of sector models can all carry the label. Investment committees need a stricter definition: a governed virtual representation that is updated from its physical counterpart and used within an accountable decision process.

Great Britain's National Energy System Operator describes the Virtual Energy System as an ecosystem of interconnected digital twins operating alongside the physical energy system. Singapore's Energy Market Authority separates a Network Twin, used to analyse new loads and distributed resources, from an Asset Twin, used to improve asset planning, operation and maintenance.[1][7] These distinctions matter because every component has a different data cadence, model fidelity and control risk.

The first investment document should name the decision, present the existing baseline and specify the expected improvement. Measures can include study time, connection capacity identified, outage minutes, inspection cost, false alarms, forecast error, maintenance deferral or capital avoided. The twin becomes an investable programme when its value can be tested through decisions.

Figure 1. National grid digital-twin capability stack

Author framework. Decision ownership sits above technology and determines the required evidence.

2. Separate the twin families

An asset twin represents an individual transformer, cable, line, breaker, inverter or generating unit. It can combine design data, as-built records, sensor readings, inspections, maintenance and failure models. Its value lies in asset health, remaining life, intervention and renewal.

A network twin represents topology, electrical parameters, operating state and constraints. It supports power-flow, voltage, fault, stability, congestion, hosting-capacity and restoration analysis. A market twin represents bids, schedules, prices, reserves, settlement and participant behaviour. A scenario twin supports longer-term demand, generation, storage, climate and network pathways.

These twins should share identifiers and controlled interfaces while retaining their purpose. An asset-health score should not automatically change an operational limit. A market forecast should not overwrite a protection setting. A planning model should not be treated as a real-time operational model without validation.

The United States Department of Energy describes grid control as the real-time matching of electricity supply and demand, supported by visibility, situational awareness and control.[9] National Renewable Energy Laboratory research on dynamic state estimation highlights the value of estimating system variables that cannot be measured directly, while recognising data-quality, model-uncertainty and scaling challenges.[12]

Investment scope should therefore describe the twin family, target fidelity, update frequency, geographic boundary and decision rights. A programme that attempts to build every twin simultaneously is difficult to validate and govern.

3. Choose federation over forced centralisation

A national electricity system contains organisations with different statutory duties, technologies, security boundaries and commercial interests. Transmission and distribution operators, generators, storage owners, retailers, market operators, regulators and large users rarely share one technology estate or one data owner.

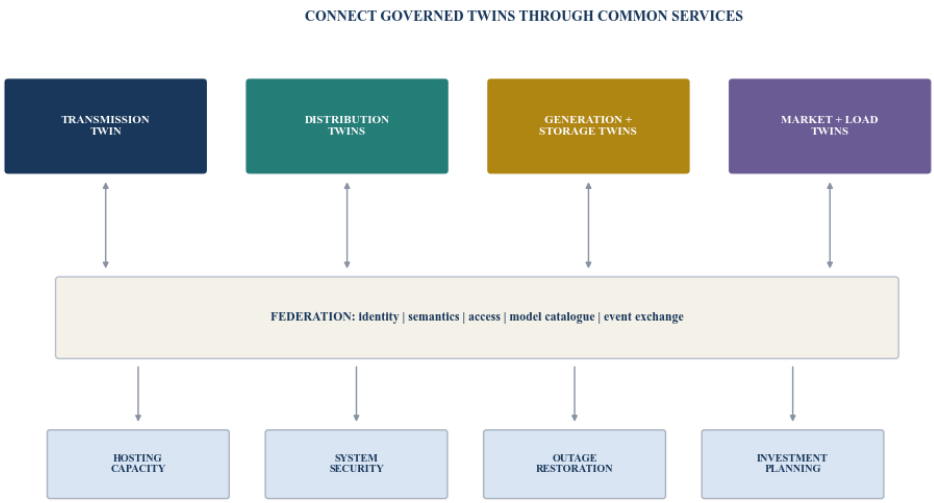
A federated architecture connects independently operated twins through agreed identities, semantics, interfaces and governance. The underlying data can remain with its responsible owner. The federation requests the information, model result or service needed for an authorised use case.

ENTSO-E's 2026 report describes federation as connecting independently operated twins through shared semantics, open standards and common governance without requiring centralisation or loss of data sovereignty.[4] Europe's TwinEU project is developing a federation of local electricity-system twins across eight demonstrations and 11 countries, supported by a data-space layer and a service workbench.[3][5]

Great Britain's Virtual Energy System follows a comparable ecosystem logic. NESO states that participating twins contribute to and access real-time data from other elements of the system through an interoperable framework.[1]

Federation does not remove integration effort. It moves investment into data contracts, common identifiers, model catalogues, access control, interface testing, version management and cross-organisation governance. These functions create a durable commercial market for neutral infrastructure, assurance and managed services.

Figure 2. Federated national grid digital-twin architecture



Author framework. Local control is preserved while authorised services cross organisational boundaries.

4. Build observability before intelligence

The digital twin needs a current view of the grid. Data can come from supervisory control and data acquisition, phasor measurement units, intelligent electronic devices, smart meters, weather systems, equipment sensors, geographic information systems, outage management, maintenance records and market platforms.

Availability does not establish fitness. Time alignment, measurement accuracy, topology, units, naming, calibration, completeness and latency determine whether data can support a specific decision. A current measurement mapped to the wrong asset can be more dangerous than a clearly missing value.

Observability investment includes sensors, communications, time synchronisation, secure gateways, streaming, quality rules, identity resolution and state estimation. It also includes field work to correct drawings, asset registers and connectivity. These tasks can carry more value than a sophisticated analytical layer built on weak foundations.

Singapore's Network Twin models how additional loads and distributed resources affect the grid. Its Asset Twin supports condition analysis for transformers, switchgear and cables.[7][8] NREL's SMART-DS platform provides realistic synthetic distribution systems and scenarios for testing algorithms and technologies without exposing actual utility networks.[11]

The investment committee should fund data readiness as a measured workstream. Readiness metrics can include critical assets with verified identifiers, network elements with current parameters, measurements within quality thresholds, time-synchronised feeds, resolved topology conflicts and authorised data contracts.

5. Establish a common identity and semantic layer

Systems cannot cooperate reliably when the same substation, feeder, transformer or connection is represented by incompatible names and structures. A national twin requires controlled identifiers, reference data, electrical semantics, geographic relationships and lifecycle status.

The semantic layer should describe equipment, terminals, connectivity, measurements, limits, events, market resources and organisations. It should also record source, owner, effective date, confidence, version and permitted use. Standards can accelerate integration, though local profiles and legacy systems still require mapping.

Model exchange should be tested on real workflows. A successful file transfer does not prove that phase designation, units, equipment status, operating limits or connectivity mean the same thing at both ends. Conformance tests should compare the resulting network and calculations.

Vendor-neutral identifiers and export rights preserve future competition. The owner should retain a complete machine-readable model catalogue, lineage and interface specification. Proprietary algorithms can remain protected while input, output and performance obligations remain inspectable.

Table 1. Digital-twin decision and evidence register

Decision	Twin component	Required evidence	Baseline measure	Acceptance test
Connection capacity	network and scenario twin	topology, limits, demand and generation scenarios	study time and capacity identified	independent study reaches an agreed result range
Asset renewal	asset and network twin	condition, criticality, failure and consequence	inspection cost and replacement plan	intervention ranking is reproducible and reviewed
Stability assessment	dynamic network twin	synchronised measurements and validated device models	analysis time and missed phenomena	known events are replayed within tolerance
Outage restoration	network and weather twin	switching state, faults, crews and access	restoration time and customer minutes	exercise produces safe feasible sequences
Predictive maintenance	asset twin	sensor history, work orders and failure modes	unplanned failures and maintenance cost	prospective trial shows useful precision and recall
Hosting capacity	distribution twin	feeder model, voltage, protection and DER profiles	manual study throughput	published capacity range survives sample engineering review
Market and flexibility	network and market twins	constraints, forecasts, bids and dispatch	curtailment and balancing cost	settlement-grade test reconciles physical and market outputs
Long-term planning	scenario and network twins	demand, supply, climate and project pathways	capital plan and forecast error	scenario decisions remain traceable to assumptions

Every use case requires an accountable decision owner and a measurable baseline.

6. Match fidelity to consequence

Model fidelity describes how closely the twin represents the physical system for a stated purpose. More detail can increase computational cost, data requirements and validation burden. The correct fidelity depends on the decision and time available.

A long-term expansion study can use hourly or representative-period scenarios. A voltage assessment needs network detail at the affected location. Protection and inverter-driven stability can require electromagnetic-transient models and much shorter time steps. A maintenance twin needs component condition and degradation rather than a full national dynamic model.

The twin should support multiple resolutions connected by controlled boundaries. High-fidelity local models can be embedded within a wider lower-resolution system. Operators should know which phenomena are represented, simplified or excluded.

ENTSO-E's 2026 research plan identifies high-fidelity models, wide-area measurements and enhanced observability as inputs to real-time stability assessment, fault localisation, weather response, reconfiguration and cascading-failure mitigation.[6] The cited plan is a research and innovation proposal rather than evidence that every capability is operational.

Fidelity should be accepted through tests tied to consequence. A planning model can be judged on investment decisions. An operational model needs stricter accuracy, availability, latency, fail-safe behaviour and human oversight.

7. Validate through replay and parallel operation

Validation compares model outputs with physical observations and known outcomes. It should cover steady state, dynamics, contingencies, asset behaviour, forecasts and workflow decisions. A twin validated on ordinary conditions can still fail during extreme or changing events.

Historical replay uses measured disturbances, outages, weather and load changes. The team compares simulated voltages, flows, frequency, protection actions or asset signals with recorded behaviour. Prospective parallel operation runs the twin alongside current processes before any operational reliance.

Tests should record input version, model version, tolerances, exceptions and approval. Performance can drift as assets, firmware, topology, operating practices and loads change. Validation therefore becomes a lifecycle control rather than a one-time commissioning exercise.

The model-risk register should classify decisions by consequence. A recommendation that schedules an inspection has a different risk from a command that changes system operation. Human review, independent calculation and technical limits should scale with consequence.

Figure 3. Evidence chain from measurement to authorised action

Author framework. Higher-consequence actions require stronger validation and independent control.

8. Build a portfolio of bounded use cases

The programme should sequence use cases by value, readiness, safety and reuse. An early use case needs a clear owner, accessible data, measurable baseline and contained operational consequence. It should also create assets that support later applications.

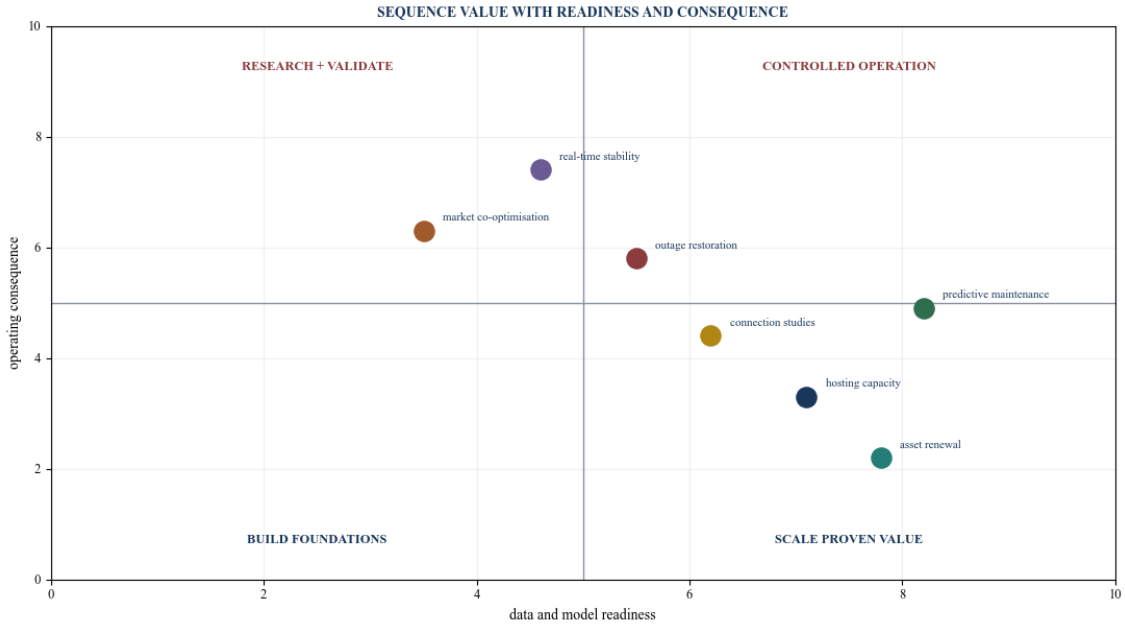
Connection and hosting-capacity analysis can reuse network topology, demand forecasts and constraint models. Asset-health work creates verified identifiers, sensor histories and maintenance data. Outage replay improves topology and event records. These foundational assets then support broader planning and operations.

Singapore's two-part programme demonstrates this portfolio logic. The Network Twin assesses the effect of electric-vehicle demand and distributed resources. The Asset Twin addresses health, criticality, degradation, monitoring and cable insulation.[7][8]

TwinEU's 2026 pan-European scenarios include hosting-capacity maps, energy and balancing-market co-optimisation, forecasting, flexibility, system security and line monitoring.[5] These are programme scenarios that require local validation before commercial reliance.

The portfolio should avoid counting the same benefit twice. Faster studies can reduce staff effort and accelerate a connection. The model should not add both benefits at full value when the same time saving causes both. Capital deferral and increased network utilisation should be reconciled at asset level.

Figure 4. Use-case portfolio by readiness and operating consequence



Author framework. Placement is illustrative and should be rebuilt from current programme evidence.

9. Map the commercial opportunity stack

Digital-twin investment creates several markets. The physical layer includes sensors, intelligent devices, communications, timing and edge computing. The data layer includes integration, quality, streaming, storage, identity, semantic mapping and governed data spaces.

The modelling layer includes network analysis, dynamic simulation, asset physics, forecasting, optimisation, synthetic data and model orchestration. The workflow layer includes planning, control-room decision support, maintenance, connection management, market operations and regulatory reporting.

Cyber security, assurance, systems integration, training and managed operations cross every layer. Public research, test facilities and standards support the ecosystem. Specialist advisers can define investment cases, procure platforms, structure partnerships and assure benefits.

Commercial attractiveness depends on recurring need, switching cost, data access, integration burden, liability and procurement. Sensor deployment can create hardware revenue and maintenance. A model platform can create subscriptions, though vendor concentration can reduce owner flexibility. Managed services can create recurring cash while transferring operational dependency to the provider.

Investors should distinguish products from project work. Reusable software and reference models can scale across networks. Custom integration, field verification and change management remain labour-intensive. A credible plan should disclose the expected mix.

Figure 5. Commercial ecosystem for national grid digital twins

Author framework. Opportunity value depends on evidence, repeatability and contractual allocation.

10. Treat cyber security as a design constraint

A grid digital twin joins operational technology, information technology, cloud or high-performance computing, external data and multiple organisations. It can expose network topology, asset condition, vulnerabilities, operating constraints and prospective actions. Its compromise can affect confidentiality, integrity and availability.

Security design should classify data, systems, models and actions by consequence. It should segment networks, authenticate users and services, apply least privilege, protect keys, sign software and model releases, monitor activity, control remote access and preserve reliable local operation during loss of the twin.

Model integrity deserves explicit control. An attacker or accidental change can alter topology, limits, forecasts or equipment parameters while leaving the platform available. The programme needs version control, provenance, approvals, comparison tests and independent operational safeguards.

NREL's control-room research describes digital twins as a possible environment for checking AI-supported decisions and producing physics-aware data.[10] This remains a research direction. Any AI recommendation in a critical workflow needs defined limits, validation, operator authority and auditability.

Cyber procurement should cover incident reporting, vulnerability management, software components, patching, access logs, data residency, subcontractors, recovery, exit assistance and evidence rights. Insurance and liability should match the service provided.

11. Govern data rights and confidentiality

Data can carry national-security, operational, personal, commercial and market sensitivity. A national programme needs a legal and governance basis for each exchange. Purpose, ownership, controller, processor, retention, location, onward use and deletion should be recorded.

Federation can reduce central copying while still revealing results. A hosting-capacity output can expose local constraints. A model query can reveal asset state. Access controls therefore need to apply to derived information as well as raw data.

Commercial contributors should know whether their data can train models, support other customers or create products. Public bodies should preserve rights to continuity, audit, export and public-interest use. Research access can use synthetic, masked or aggregated data when appropriate.

The data catalogue should state quality, lineage, cadence and permitted decisions. A dataset suitable for planning may be prohibited for real-time operation. Retention should support incident investigation and model validation without collecting information indefinitely.

Table 2. Data and model control framework

Control area	Minimum evidence	Principal failure	Owner test
Identity	authoritative asset and organisation identifiers	conflicting or duplicate objects	sample traces resolve to the physical asset
Topology	current connectivity and switching state	calculation on an obsolete network	operating and model views reconcile
Measurement	source, calibration, time and quality flags	false precision or stale data	quality thresholds are visible to the decision
Model	purpose, equations, parameters and exclusions	use outside validated scope	model card states accepted decisions
Version	immutable release, change and approval records	untraceable output change	result can be reproduced from archived inputs
Access	role, purpose, duration and authentication	excessive or orphaned privilege	access review matches current duties
Interface	schema, units, semantics and conformance tests	technically valid but incorrect exchange	independent systems reach equivalent meaning
Cyber	segmentation, monitoring, recovery and incident plan	compromise spreads into operations	exercises show containment and recovery
Exit	export, documentation, transition and deletion	vendor lock-in or lost history	replacement supplier can receive usable assets

Controls should be calibrated to current law, system criticality and contractual duties.

12. Contract for interoperable outcomes

Procurement should begin with use cases and acceptance tests. A request for a national digital twin can attract broad platforms that are difficult to compare. A request for a validated hosting-capacity service across specified feeders, with defined interfaces and performance, creates a testable obligation.

The contract should separate foundation, configuration, integration, validation, operation and expansion. Milestones can require verified identifiers, data connections, model acceptance, historical replay, parallel operation, user adoption and measured benefit.

Intellectual-property terms should preserve the supplier's reusable product while granting the owner durable rights to data, configurations, interfaces, derived operational records and exit materials. The owner should receive current documentation, model catalogues, schemas and test

packs.

Performance measures should address availability, latency, calculation success, data quality, model accuracy, incident response, defect correction and workflow outcomes. Credits alone may be insufficient for critical failure. Step-in, cure, transition and termination rights require careful design.

Procurement can use modular lots when the owner has strong integration capability. A prime contractor can simplify accountability while increasing concentration. An independent integrator or assurance function can test interfaces and reduce platform bias.

Table 3. Procurement structure and acceptance gates

Package	Supplier obligation	Acceptance evidence	Payment gate	Exit requirement
Foundation	identities, catalogue, security and environments	reconciled samples and control test	accepted baseline	complete machine-readable export
Data integration	governed live and historical feeds	quality, latency and lineage report	feed-by-feed acceptance	connectors and mapping documentation
Model services	defined calculations and scenarios	benchmark, replay and sensitivity tests	model acceptance	parameters, interfaces and test pack
Workflow application	decision screens, cases and approvals	user acceptance and process audit	operational-readiness gate	cases and audit history export
Federation	cross-organisation exchange and orchestration	conformance and failure-mode tests	interoperable service accepted	open interface and transition assistance
Managed operation	monitoring, updates, support and incident response	service report and exercise	recurring service payment	knowledge transfer and orderly handover
Expansion	new geography, assets or decisions	agreed reuse and benefit evidence	outcome milestone	additions inherit the same export rights

Commercial terms require project-specific legal, technical, cyber and procurement review.

13. Value decisions rather than data volume

Digital programmes often report connected assets, data points, model runs and users. These measures describe activity. The investment case needs financial and operational outcomes linked to controlled decisions.

Connection value can come from faster studies, more capacity found within existing assets or earlier energisation. Maintenance value can come from avoided inspection, better intervention timing, fewer failures and longer asset life. Operational value can come from lower congestion, curtailment, reserve cost or restoration time. Planning value can come from better sequencing and capital deferral.

Each benefit requires a counterfactual. The baseline should state what would happen without the twin, including existing systems and planned improvements. Benefits should be counted only when the decision changes and the resulting cash, cost or service outcome can be evidenced.

Financial models should distinguish cash, accounting cost, risk exposure and public-service value. Avoided outage loss is uncertain and should remain a scenario unless an enforceable payment or saving mechanism exists. Capital deferral should account for the revised timing and any later cost.

Benefits can decay if users return to manual processes, models drift or data feeds fail. Operating expenditure for data, licences, computing, cyber, support and validation should continue through the full life of the capability.

14. Examine international programme evidence

Great Britain's Virtual Energy System is an industry-wide mission to create an ecosystem of connected twins and common data infrastructure.[1][2] The programme highlights interoperability and sector coordination rather than a single central platform.

The European Commission reports that TwinEU began in January 2024 with a budget of EUR 25.2 million, including EUR 20 million in EU funding. It aims to federate local twins across the European electricity system.[3] ENTSO-E's 2026 work places common data foundations, lifecycle-aligned models, cyber security, functional safety, open standards and ontologies at the centre of federation.[4]

Singapore's programme combines a Network Twin and Asset Twin. EMA reports that the Network Twin assesses additional demand and distributed resources while the Asset Twin supports remote condition analysis and asset planning.[7][8]

United States programmes provide research and test infrastructure rather than one national operational twin. DOE's grid-control programme addresses visibility, situational awareness and controls. NREL provides dynamic state estimation, realistic synthetic distribution systems and a control-room research concept linking digital twins and AI.[9][10][11][12]

DEWA has conducted distribution-grid digital-twin work using real-time simulation and describes a smart-grid strategy organised around foundational capabilities, automation, AI and value-added services.[13][14] Programme maturity and scope should be verified directly before any procurement or investment decision.

Table 4. Selected international grid digital-twin programmes

Geography	Programme	Publicly stated focus	Architecture lesson	Investment question
Great Britain	NESO Virtual Energy System	interconnected twins and open data infrastructure	common framework across sector participants	who operates identity, access and orchestration?
European Union	TwinEU and ENTSO-E federation	federation of local twins, data spaces and reusable services	preserve local control through shared semantics	which services can scale across borders and operators?
Singapore	EMA Grid Digital Twin	network impacts and asset-health applications	separate network and asset twins with shared evidence	which use case produces the first measured decision value?
United States	DOE and national-laboratory research	grid control, dynamic estimation, synthetic networks and testing	combine operational research with safe test environments	how does a prototype cross into utility-grade operation?
Dubai	DEWA distribution-grid and smart-grid work	real-time simulation, automation and intelligent networks	link digital-twin capability to wider grid modernisation	which foundation and operational interfaces already exist?

The programmes have different mandates and maturity; comparison identifies design questions rather than performance rankings.

15. Structure the investment perimeter

The programme perimeter can include field sensors, communications, edge gateways, data platforms, model services, computing, cyber controls, applications, integration, validation, training and managed operation. Omitting a layer can leave a model unable to reach the decision it was funded to improve.

Existing assets should be inventoried before new procurement. Utilities may already hold geographic information, network management, outage management, asset performance, metering, weather and planning systems. The digital-twin programme should integrate or improve these capabilities rather than duplicate them.

Capital and operating expenditure should be classified consistently. Sensors and computing can require refresh. Software licences, cloud consumption, communications, data services, cyber monitoring, support and model maintenance recur. Validation and field reconciliation remain ongoing.

The owner should also fund organisational change. Engineers and operators need time to define models, resolve data, test recommendations, revise procedures and learn the system. Benefits can depend more on workflow adoption than model performance.

Investment phasing should retain optionality. Shared identity, security and data foundations can support several uses. Each later phase should pass a benefit and control gate before more geography, model fidelity or operational authority is added.

16. Finance suppliers and platforms carefully

Technology suppliers can offer licences, subscriptions, transaction fees, managed services, equipment sales or outcome-based contracts. Investors should test revenue quality, customer concentration, procurement cycles, implementation obligations, liability and renewal drivers.

Recurring software revenue can be attractive when the product remains essential to repeated workflows. Extensive bespoke integration can reduce gross margin and slow deployment. A vendor may report contracted value before acceptance, while cash depends on milestones and utility procurement.

Technical diligence should examine architecture, code and model release practices, cyber controls, interoperability, reference deployments, implementation capacity, support, key personnel, subcontractors and product roadmap. Commercial diligence should separate reusable product revenue from services and pass-through cloud or hardware.

Customer value evidence should include baseline, accepted output, actual workflow adoption and realised benefit. A pilot that produced an accurate result may still fail to convert into recurring revenue if the operator cannot rely on it or procurement remains unresolved.

Financing structures should match cash. Venture or growth equity can fund product expansion. Project finance is difficult where cash depends on software acceptance or uncertain benefits. Vendor finance, milestone payments and strategic partnerships can bridge deployment when obligations and remedies are clear.

17. Test a hypothetical national programme

Consider a hypothetical electricity-system operator that selects three first-wave uses: connection studies, transformer-renewal prioritisation and outage replay. Management assumes existing data platforms can be integrated, while additional sensing and topology correction are required in selected regions.

Management assumes a staged 30-month programme with foundation, pilot, parallel operation and scale phases. Every cost, timing, benefit, adoption rate and financial result in this demonstration is a hypothetical management assumption. It does not represent an actual grid, supplier quotation, procurement, tariff, forecast or realised saving.

The model includes field work, integration, licences, computing, cyber controls, validation, internal staff, training and contingency. Benefits include reduced external study effort, maintenance targeting and selected capital deferral. Outage-loss value is reported separately and does not support the base financial case.

Table 5. Hypothetical national grid digital-twin investment case

Item	Hypothetical assumption	Model treatment	Principal caveat
Programme scope	three bounded use cases across selected regions	phased before national scale	final system and geography undefined
Foundation and integration	USD 18.0m	identity, data, cyber and interfaces	existing-system condition unverified
Sensors and field reconciliation	USD 11.5m	targeted observability upgrade	field quantities and access unverified
Models and workflow applications	USD 13.0m	configuration, validation and rollout	supplier and acceptance terms unverified
Internal change and assurance	USD 5.5m	staff, training, audit and independent testing	organisational capacity unverified
Annual operating cost after scale	USD 8.4m	licences, compute, communications and support	consumption and pricing unverified
Annual cash-cost reduction at scale	USD 10.2m	study, inspection and process savings	requires measured adoption and avoided spend
Capital deferral present value	USD 19.0m	asset-specific decisions only	timing and counterfactual unverified
Connection-value benefit	reported separately	customer and system scenario	payment mechanism absent
Avoided outage loss	reported separately	risk scenario	no certain cash receipt

Every value is a hypothetical management assumption for method demonstration; USD-equivalent amounts are not current market evidence.

18. Stress the programme

The base case should survive lower adoption, delayed data access, weak topology, integration overruns, higher computing cost, vendor failure and model underperformance. Benefits should fall when the affected workflow remains manual.

Cyber or operational restrictions can delay a cloud architecture or limit data exchange. The programme should retain a secure local-operating path and alternative deployment options. Data-residency, national-security and critical-infrastructure duties need current review.

Vendor lock-in can increase renewal cost and delay replacement. Exit tests should be run before dependency becomes critical. The owner should demonstrate model, data, configuration, workflow and audit export into a controlled environment.

Capital deferral should be reversed in downside cases when evidence is inadequate. Avoided loss should remain outside debt or committed funding decisions. A programme that depends on unmeasured system risk to justify recurring cost has a weak financial foundation.

19. Govern the operating capability

The board or designated committee should receive measures across service, evidence, value and risk. Service measures include availability, latency, data-feed health, model runs and incident resolution. Evidence measures include verified assets, quality thresholds, model validation and drift.

Value measures should track decisions changed, cash saved, capital deferred and benefits realised against baseline. Risk measures include cyber events, unauthorised access, model exceptions, stale topology, manual overrides, failed interfaces and unresolved high-consequence recommendations.

Every operational use should have a responsible engineer or function. The system should record recommendation, evidence, reviewer, decision, action and outcome. This history supports learning and accountability.

Change control should cover data sources, equipment parameters, topology, algorithms, software, interfaces and user roles. Emergency change needs later review. Material changes should trigger targeted revalidation before the affected use returns to service.

Independent assurance can review model governance, cyber controls, benefit measurement and procurement compliance. Its scope should remain proportionate to consequence and public duty.

20. Execute through six gates

The first 30 days define decisions, owners, baselines and constraints. Days 31 to 60 reconcile current systems, data, identity, cyber and legal rights. Days 61 to 90 complete architecture, procurement packages and validation design.

Days 91 to 120 build the bounded services and correct field or data gaps. Days 121 to 150 run replay, independent tests and parallel operation. Days 151 to 180 decide whether each service scales, changes or stops.

Figure 6. 180-day national grid digital-twin delivery roadmap

Author framework. Timing should be adapted to current procurement, security, engineering and regulatory requirements.

Table 6. 180-day execution plan

Days	Workstream	Required output	Gate
0 to 15	decision scope	accountable owners, use cases and decision consequences	bounded services approved
16 to 30	baseline	current process, cost, time, quality and risk	measurable counterfactual accepted
31 to 45	estate and data	systems, assets, feeds, gaps and reuse plan	current capability reconciled
46 to 60	rights and security	data authority, classification, access and recovery	lawful secure route confirmed
61 to 75	architecture	federation, interfaces, identity and environments	target design approved
76 to 90	procurement and tests	packages, acceptance, IP, exit and validation	comparable obligations issued
91 to 105	foundation build	identifiers, catalogue, feeds and controls	data-readiness threshold passed
106 to 120	service build	models, workflows, audit and user procedures	service ready for controlled test
121 to 135	historical replay	benchmark events, exceptions and remediation	model tolerance approved
136 to 150	parallel operation	live comparison, operator review and failure modes	operational readiness accepted
151 to 165	value assurance	adoption, cash, capital and service evidence	benefits independently reconciled
166 to 180	scale decision	scope, funding, contracts, controls and roadmap	scale, revise or stop decision

Timing is an author framework and should be revised for the programme's current approvals and delivery conditions.

21. Set the investment decision

The investment committee should approve the named decisions, system boundary, operating owners, evidence thresholds, cyber classification, data rights, target architecture, supplier structure, capital, recurring cost and benefit-measurement plan.

Conditions should cover current regulatory and security review, data agreements, interface rights, model validation, independent testing, operator procedures, business continuity, insurance, acceptance, documentation and exit. Higher operational authority should require a separate decision after parallel operation.

Funding should follow verified gates. Foundation investment can proceed when several valuable uses share the same identity, security and data assets. A use case should scale when it changes real decisions and produces evidence of service or financial value.

The programme should pause or resize when the decision owner is absent, topology cannot be reconciled, data rights remain unresolved, operational safety cannot be protected, model performance falls outside tolerance or supplier exit cannot be demonstrated.

22. Limitations and conclusion

Digital-twin technology, electricity systems, cyber threats, standards, market rules, procurement, computing, communications and regulatory duties can change. Programme decisions require current evidence from system operators, network owners, regulators, equipment suppliers, cyber specialists, model developers, independent engineers, procurement teams, insurers and qualified advisers.

The cited programmes describe their own mandates and stages. Great Britain, European Union, Singapore, United States and Dubai evidence cannot establish performance, legality or economics in another electricity system. Public programme descriptions do not replace technical diligence, source-system access, validation or contractual evidence.

Every cost, saving, schedule, adoption rate, probability, capital-deferral value and financial result in the worked example is a hypothetical management assumption. No actual grid programme, supplier price, contract, operating result or investment return is claimed.

A national grid digital twin can become valuable infrastructure when it improves a bounded, accountable decision. The investable asset includes observability, identity, data rights, models, validation, workflows, cyber controls, people and continuous governance.

Federation provides a practical architecture for a multi-organisation electricity system. Commercial value develops across sensing, communications, data, models, applications, assurance and managed operations. Durable value depends on interoperability, measurable decisions and a credible exit from every critical supplier.

References

[1] National Energy System Operator, Virtual Energy System, official programme page accessed 13 August 2026. https://www.neso.energy/about/our-projects/virtual-energy-system

[2] National Energy System Operator, Introducing the Virtual Energy System, 5 November 2021. https://www.neso.energy/news/introducing-virtual-energy-system

[3] European Commission, Key Actions for Digitalising Energy, official programme page accessed 13 August 2026. https://energy.ec.europa.eu/topics/eus-energy-system/digitalisation-energy-system/key-actions-digitalising-energy_en

[4] ENTSO-E, Digital Twins: Towards a Federated Approach, 20 February 2026. https://www.entsoe.eu/news/2026/02/20/entso-e-publishes-a-report-on-the-benefits-of-a-coordinated-approach-to-digital-twins-for-the-european-power-system/

[5] TwinEU, Building Pan-EU Scenarios of Local Digital Twins, 2026. https://twineu.net/building-pan-eu-scenarios-of-local-digital-twins/

[6] ENTSO-E, Research, Development and Innovation Implementation Plan 2026-2030, consultation draft, 20 March 2026. https://consultations.entsoe.eu/r-i/innovation-implementation-plan-2026-2030/

[7] Energy Market Authority of Singapore, Grid Digital Twin, official programme page updated 21 February 2024. https://www.ema.gov.sg/our-energy-story/energy-grid/grid-digital-twin

[8] Energy Market Authority of Singapore, Leveraging Digital Solutions to Future-Proof Singapore's Energy Grid, 24 October 2023. https://www.ema.gov.sg/news-events/news/media-releases/2023/leveraging-digital-solutions-to-future-proof-singapore-energy-grid

[9] United States Department of Energy, Grid Control and Data Science, official programme page accessed 13 August 2026. https://www.energy.gov/oe/grid-control-and-data-science

[10] National Renewable Energy Laboratory, Digital Twin and AI: Control Room of the Future, 2024. https://www.nrel.gov/docs/fy25osti/89725.pdf

[11] National Renewable Energy Laboratory, SMART-DS: Synthetic Models for Advanced, Realistic Testing, official programme page accessed 13 August 2026. https://www.nrel.gov/grid/smart-ds

[12] National Renewable Energy Laboratory, Dynamic State Estimation, official programme page accessed 13 August 2026. https://www.nrel.gov/grid/dynamic-state-estimation

[13] Dubai Electricity and Water Authority, R&D Centre Workshop on Digital Twin Development of the Distribution Grid, 1 January 2024. https://www.dewa.gov.ae/en/about-us/media-publications/latest-news/2024/01/dewas-r-and-d-centre-organises-a-workshop

[14] Dubai Electricity and Water Authority, Smart Grid, official programme page accessed 13 August 2026. https://www.dewa.gov.ae/en/about-us/strategic-initiatives/smart-grid

About the Author

Chennakeshav Adya is an independent researcher and Managing Partner of Matchpoint Partners. His research focuses on investment strategy, capital formation, transaction execution, governance and operating-model design across international markets.