CHAPTER

1

Digital Twins and Humans

A *digital twin* is a virtual, computational representation of a physical system, process, or organization that continuously reflects real-world state through data, models, and interaction. It links physical and digital environments into a single evolving system, providing visibility, simulation, and operational insight.

A twin may appear as a dashboard, map, 2D/3D model, mathematical construct, mesh, or even an AI agent. It can represent something simple—a small component or workflow—or a complex, multi-layered enterprise integrating technologies, human roles, and AI agents. Its core advantages are situational awareness, simulation capability, and operational efficiency.

Digital twins predate AI as static models and monitoring systems. AI shifts them from passive representations to active reasoning systems capable of simulation, optimization, and decision support in natural language (see Table 1.1). That power also expands risk, making engineering discipline and security foundational from the start.

Table 1.1 What Distinguishes an AI-powered Digital Twin from Its Predecessors

	Pre-AI Twin	Generic AI System	AI-powered Twin (this book)
Anchored to a real physical system	✓	✗	✓
Continuously updated from live data	✓	✗	✓
Reasons, simulates, acts	✗	✓	✓
Deterministic processing	✓	✗	✓ core
Probabilistic reasoning	✗	✓ ungoverned	✓ bounded
Auditable and traceable by design	✓	✗	✓
Governed—agents bounded, never sovereign	✗	✗	✓

The AI-powered twin combines physical anchoring with AI reasoning but uniquely adds a governance architecture that bounds probabilistic agents within a deterministic, auditable core.

Note. Terminology

Physical world: physical entities, processes, infrastructure, organizations—the real systems this book is about. Complex system: physical or digital entities connected by processes whose interactions produce behaviors no single component can predict alone. Digital world: computational representations, data, models—the parallel world the twin creates. Connecting layer: interaction, synchronization, workflows—how physical and digital stay aligned. Intelligence layer: AI, simulation, agents, and decision-making—what makes the twin active rather than passive, operating on the knowledge from the semantic layer and accountable through governance.

Critical Infrastructures and What's Worth Digital Twinning

Human population has nearly doubled since I was born. Humanity's core needs—energy, food, water, education, healthcare, security, moderate climates, and love—have not changed, but their scale and interdependence have intensified. Twice as many people now rely on infrastructures and supply chains that are deeply connected, data-driven, and regulated across multiple layers and geographic locations. These systems are sometimes too large and complex to manage through fragmented tools.

The strongest candidates for digital twinning are systems where physical, digital, and human components intersect. Digital twins' capabilities directly strengthen critical infrastructure sectors that anchor national security, economic stability, and public health—from energy, water, transportation, and communications to the defense industrial base, healthcare, finance, chemicals, and emergency services.

As physical systems merge with digital operations, critical infrastructures face escalating risks from natural disasters, cyberattacks, and cascading failures. Disruptions to these sectors already carry massive cost: the 2024 CrowdStrike outage caused ~$5.4B in losses across aviation, healthcare, and financial services; the 2025 Iberian power failure cost ~$3B and halted automotive, chemical, and food production across the region. In critical infrastructure, digital twins unify operational, cyber, and physical context, allowing operators to simulate decisions and evaluate consequences before acting on real systems.

Example: Before and After Digital Twin for a Large Energy Provider Company

A large energy provider company is usually a mature, regulated utility (usually cyber-regulated by NERC CIP). That is, energy providers are not starting from scratch when it comes to digital integration.

Existing operational technology (OT) security, monitoring, and compliance tools are necessary because they provide deterministic control, real-time visibility, and auditable safeguards required for safe grid operations and NERC CIP compliance. However, these tools are insufficient because they operate largely as siloed, alert-driven systems that cannot explain why behaviors change, distinguish faults from malicious manipulation, or reason across cyber, physical, and operational layers. AI-powered digital twins add this missing cognitive layer—providing explanation, context, and defensible decision support without necessarily touching live operations. In Chapter 3, we provide a roadmap of a fully agentic ecosystem where safety and security are more crucial than in *read-only* digital twins.

Regulations, Compliance, and Penalties: AI, Commodities, and Supply Chains

The race to deploy AI across interconnected systems—without governance, system context, or auditability—has moved faster than our ability to test, secure, or anticipate the full range of consequences. Governments and industries face growing pressure to meet regulatory mandates while maintaining operational efficiency. AI-powered digital twins provide traceability, testing, and accountability needed to operate responsibly at scale. Unlike healthcare, aviation, or construction, the digital world still lacks a true engineering standard of care, even as it governs systems capable of causing massive physical, financial, and societal harm. We aim to change that.

History shows what happens when fast-moving industries operate without oversight. The commodity trade world functioned in obscurity for decades—until regulators intervened. BNP Paribas paid nearly $9 billion in sanctions-related penalties, plus additional fines for benchmark manipulation and reporting failures, ultimately shutting down its Swiss commodity-trade finance operations. There is a lesson here for the AI industry: no one wants to be the first to face catastrophic penalties. Digital twins prevent such failures in AI-powered systems by enabling end-to-end visibility, risk modeling, and compliance before reputational and financial damage occur. This is particularly critical in supply chain mapping, where regulations now span product safety (FDA and CPSC), environmental and deforestation laws, labor and anti-slavery protections, privacy and data regulations (GDPR, CCPA, and HIPAA), international trade controls, and rigorous due-diligence mandates like the German Supply Chain Act. Table 1.2 shows the similarities between the AI industry and the commodity trade industry.

Table 1.2 Similarities Between the Commodity Trade Industry and the AI Industry

Dimension	Commodity Trade Industry	AI Industry
Information Asymmetry as Competitive Edge	Relies on real-time market, weather, and geopolitical data; superior information creates outsized advantage.	Data is the raw material; proprietary datasets and insights are the primary source of competitive edge.
Speculation and Volatility	Driven by fluctuating supply-demand, policy, and global events.	Subject to hype cycles and market speculation.
Infrastructure Requirements	Needs physical infrastructure like ports, pipelines, and storage.	Requires computing infrastructure—GPUs, cloud, data centers.
Global Interconnectedness	Operates through global markets with complex supply chains.	Talent, data, and compute are globally distributed.
Regulatory Oversight and Risk	Regulated for safety, trade practices, and environmental impact.	Scrutinized for bias, misuse, and national security risks.
Scalability and Arbitrage	Profit through geographic/temporal price differences and exploiting market inefficiencies.	Advantage through near-zero marginal cost of scaling and first-mover dominance in model deployment.
Concentration of Power	Dominated by a few major players (e.g. Glencore, Cargill).	Concentrated in tech giants with resources and compute power.

(*Continued*)

Table 1.2 (Continued)

Dimension	Commodity Trade Industry	AI Industry
Geopolitical Leverage and Supply Chain Vulnerability	OPEC and resource-rich nations use commodity supply as geopolitical leverage; disruptions cascade globally.	Export controls on advanced chips (e.g. U.S. restrictions on NVIDIA GPUs) weaponize the AI supply chain; access to compute is a strategic asset.
Talent and Expertise	Requires experienced traders, logisticians, and analysts.	Needs elite researchers, engineers, and scientists.
Ethical and Sustainability Concerns	Environmental damage, labor exploitation, and political concerns.	Risks include misinformation, surveillance, and job displacement.

Regulations for Operational Technology and Cybersecurity: Satcom Example

New cybersecurity rules from the Committee on National Security Systems (CNSS) now apply to U.S. national-security space systems and commercial satellite vendors, imposing real-time on-board intrusion detection and prevention, hardware root-of-trust for secure reboot, and mandatory patch management across both satellite and ground segments. These policies—incorporated into procurement contracts—aim to plug the longstanding "detection gap" in satellite telemetry by requiring embedded intrusion detection system tools and behavior-based indicators of compromise rather than post-fact anomaly logs.

Meanwhile, operational technology (OT; see Chapter 6 for full treatment) remains a security Wild West, where functionality ships first and risk analysis comes last. OT regulations are expanding across critical infrastructure sectors: new mandates now govern water, energy, transportation, manufacturing, and communications systems, demanding rigorous asset tagging, lifecycle monitoring, segmentation, and resilience engineering. Combined, these rules signal that digital connectivity amplifies physical-system risk. Digital twins serve as critical tools for cyber defense, incident response, and OT resilience. We can deploy digital twins of industrial control systems, power grids, manufacturing lines, and SCADA networks to bridge engineering, operational safety, cybersecurity, and AI.

How Asset Tagging and Digital Twins Enable Compliance

Hierarchical tagging offers a systematic path to compliance and operational security. By assigning every physical or digital asset—satellites, ground stations, OT devices, networks, firmware versions, human operators—a structured tag (e.g. sector, site, function, risk level, control plane, data sensitivity), organizations index the semantic map of the system. A digital twin then mirrors this map: the virtual replica tracks state changes, patch status, trust anchors, and threat indicators in real time.

When a new regulation mandates on-board IDS for a satellite class, for example, the twin flags all assets with tags like satellite.us-af.class-x.cnss-compliance.pending. It can simulate a patch-rollout scenario, validate root-of-trust activation, or run intrusion-response workflows across the fleet. For OT environments, tagging supply-chain components, manufacturing lines, and grid segments enables traceability, real-time anomaly detection, and audit trails aligned with regulatory regimes. Tagging integrates compliance directly into system operation, enabling continuous validation and traceability.

Technology Law, Liability, and a Career at the Frontier

As AI-powered digital twins move from prototypes to production, the legal questions multiply faster than the deployments. Who is liable when a twin's recommendation leads to a cascading grid failure—the model developer, the system integrator, the operator, or the cloud provider whose latency delayed the update? Today, the answer is: it depends—and often, nobody knows. That fuzziness is not a footnote; it is a structural risk to the entire ecosystem.

Traditional product liability was built for tangible goods with identifiable defects. AI breaks that framework: a model that performs correctly 99.7% of the time is not defective in the classical sense, yet that 0.3% can shut down a water treatment plant. Digital twins compound the problem by layering AI reasoning on physics models, real-time data, and human decisions, thereby creating causal chains so entangled that assigning fault becomes archaeology, not adjudication. The EU AI Act takes a first pass at risk-based classification, but enforcement is still forming. In the United States, AI liability remains a patchwork of state tort law, sector-specific rules, and executive orders that shift with administrations.

Every architecture decision in this book—governance layers, human-in-the-loop checkpoints, audit trails, explainability—is also a legal boundary. Engineers designing these systems are drawing the lines that future courts will use to assign responsibility.

That convergence is creating an entirely new career. Technology law—spanning AI liability, algorithmic accountability, data governance, and cybersecurity regulation—is one of the fastest-growing fields at the intersection of law and engineering. Law schools are already adding specialized tracks, and firms are hiring associates who can read both a contract and a system architecture diagram. For students entering college today: you do not have to choose between engineering and law. The systems this book describes need people who can do both. Five years ago, this was a niche specialization. It is now a career path, and demand is accelerating faster than the pipeline can fill it.

Real-world Deployments

Real-world deployments of digital twins span all domains, from an individual patient's heart to the entire planet. They provide a computational representation of real-world complexity; AI extends that representation into analysis, simulation, and action. The following examples are as of 2025 only and do not adopt the holistic approach for engineering AI-powered digital twins laid out in this book.

1. **Planetary and Climate-scale Digital Twins**
   High-fidelity climate and weather twins are among the most ambitious digital twins in existence. They are pushing the limits of high-performance computing, AI, and physics. These *multiscale*,

planetary-scale twins illustrate the future of infrastructure resilience and environmental forecasting within national digital twin ecosystems.

Destination Earth (DestinE). The European Union is building operational digital twins of the Earth system on EuroHPC supercomputers, capable of simulating extreme weather, hydrological cycles, climate-change scenarios, and disaster impacts at unprecedented resolution. These systems allow governments to test adaptation strategies decades into the future with physics-based accuracy.

NVIDIA's Earth-2. This platform combines GPU-accelerated physics models with AI surrogates to produce kilometer-scale climate simulations in seconds. It is already driving real-world deployments:

- Taiwan's Central Weather Administration uses Earth-2 for typhoon forecasting.
- The Weather Company uses AI-enhanced climate models for operational meteorology.

2. **Healthcare and Hospital Operations Twins**

Healthcare offers some of the clearest examples of digital twins directly improving human well-being.

Hospital Operations Management. The UK National Health Service and global health systems increasingly use digital twins for patient-flow optimization, bed forecasting, operating room scheduling, and surge planning. Twin platform continuously update based on sensor data, Electronic Health Record system events, and staffing availability. GE HealthCare Command Centers operate as digital twins of hospital operations, providing real-time situational awareness. Hospitals use these twins to reduce emergency department wait times, unify telemetry from multiple wards, anticipate bottlenecks, and coordinate transfers.

Patient and Organ Twins. Systems from Siemens Healthineers and academic medical centers extend the concept down to the patient level, using personalized models of organs, physiology, or treatment response. These twins are used in cardiac modeling, oncology treatment planning, and early forms of digital companions for chronic conditions.

3. **Industrial, Energy, and Manufacturing Twins**
   Industrial engineering remains one of the earliest and most mature domains for digital twins.

   Accelerated Development of a Manufacturing Facility. One engineering and design team used a virtual twin to compress the timeline of designing and constructing a major manufacturing facility—from the typical three to five years to under 22 months. AI-assisted design review, simulation, and scheduling replaced dozens of manual cycles.

   Global Energy Systems and Turbine Twins. Siemens, GE Digital, and utilities worldwide maintain turbine fleets, wind farms, and grid assets as digital twins, enabling predictive maintenance, anomaly detection, and performance tuning.

Note. Digital Twin for Asset Information Management

An information digital twin can unify fragmented industrial data into a semantically rich, secure platform that supports advanced analytics and AI. The twin captures operational telemetry and metadata from generation, grid, and renewable assets, compresses and archives it securely, and integrates it with design, commissioning, asset management, and financial data into a single contextual data model. This asset information model links real-world sources to their digital representations in a structured way, enabling consistent interpretation across applications and users.

Securely moving data from the edge to cloud and then contextualizing it is crucial: edge collectors ingest high-frequency signals from field devices, enforce validation and governance at the source, and stream this data over protected channels into centralized stores. Once centralized and enriched, the information twin becomes the substrate for predictive analytics, anomaly detection, and AI agents tasked with forecasting equipment health, suggesting maintenance actions, and optimizing operational parameters. Because the twin contextualizes both real-time and historical data against asset models, AI agents can correlate patterns across domains and time, turning raw signals into actionable insight while preserving auditability and compliance.

Process and Factory Twins. Systems from Dassault Systèmes, PTC, and Siemens manage complex production lines, robotics, quality control loops, and supply chains. These factories integrate OT telemetry, robotics, ERP data, and 3D models into unified operational twins.

U.S. Shipyards and Engineering Firms. U.S. shipyards and engineering firms such as Michael Baker International use Dassault's digital twin platforms to coordinate multistakeholder workflows, engineering requirements, asset specifications, and real-time construction updates, aligning thousands of components and contractors.

4. **Solving Science with AI-powered Digital Twins: The Genesis Mission Executive Order**
   On November 24, 2025, the White House launched Genesis Mission, a national effort to harness AI and vast scientific datasets to dramatically accelerate discovery. The initiative tasks the Department of Energy and its national laboratories to build a unified AI platform, called the American Science and Security Platform, which integrates supercomputers, data across agencies, AI agents, and automated research workflows. The goals span critical domains: advanced manufacturing, biotechnology, critical materials, nuclear fission and fusion, quantum information science, semiconductors, and other frontier challenges.

   My view of Genesis Mission is that we are building the infrastructure—if implemented correctly—to *solve science itself* through AI-powered digital twins of scientific systems: materials labs, fusion reactors, biology pipelines, and manufacturing floors alike. In Genesis Mission, digital twins become national instruments, fusing physical assets (labs, instruments, datasets) with virtual counterparts (models, agents, simulations) into a single adaptive research loop.

Semantic Twin— Ontology, Knowledge Graph, and Tagging Experiments, instruments, materials, processes, and datasets are tagged, structured, and linked across scientific domains.

Process Twin and Simulation Loop AI agents execute workflows, analyze results, design experiments, and guide real-world execution, creating closed-loop scientific discovery.

Execution and Infrastructure Layer High-performance compute, secure digital twin sandboxes, trusted data pipelines, and edge inference are orchestrated under rigorous security controls.

Deployed at scale, this stack compresses scientific timelines from years or decades to months or even weeks. It also demands digital twin architectures that support massive scale, deep specialization, secure collaboration, and agent-driven research. Engineers working on digital twins will recognize the pattern: the same architecture used to twin a manufacturing line can twin a national laboratory. The difference though is the scale, domain depth, and criticality. From where I stand, the Genesis Mission offers a blueprint and a call to arms for a new era of digital twinning at the frontier of human discovery.

5. **Logistics, Ports, Utilities, and Private 5G Twins**
   Digital twins flourish wherever physical infrastructure, supply chains, and real-time telemetry intersect.

   Port Operations and Logistics. Ports (e.g. Port of Virginia–style deployments) use private 5G, IoT networks, and digital twins to coordinate semi-autonomous cranes, routing optimization, container flow forecasting, and vessel turnaround scenarios.

   Utilities and Grid Resilience. Electric utilities build digital twins of their transmission lines, substations, and distributed energy resources. Combined with private LTE/5G networks, wearables, and robots, these twins support field operations, asset management, wildfire mitigation, and outage prediction.

   Smart Warehousing and Industrial Logistics. Logistics companies deploy twins to simulate demand, plan route optimizations, automate warehouse robotics, and track high-value assets in real time.

6. **Smart Cities, Public Safety, and Climate Infrastructure**
   Urban environments increasingly rely on digital twins to coordinate municipal services.

   Smart Cities. Cities are deploying twins for traffic flow prediction, zoning simulations, emergency response routing, water system optimization, and environmental monitoring.

Public Safety and Fire Departments. Fire departments use city building twins, sensor data, and incident-command models to plan evacuations, coordinate multi-agency response, and run training simulations.

Climate Adaptation. Cities use climate digital twins to explore extreme heat events, flooding patterns, infrastructure vulnerability, emergency evacuation routes. These simulations feed into long-term urban resilience planning.

7. **Digital Twin of the Enterprise**
   Most organizational dysfunction comes from misalignment between *mission*, *vision*, *strategy*, and the actual work that people perform. AI-powered organizational digital twins correct this by giving enterprises a precise, dynamic language for modeling work itself. With thousands of AI agents mapped to processes, roles, permissions, and systems, the twin becomes a living representation of how the organization actually functions. It provides every employee with an in-house consultant: instant visibility into workflows, data, bottlenecks, and outcomes. As people interact with the twin, they refine it, extend it into new corners of the organization, and quantify how their own work advances the mission.

Organizational twins can overhaul management and reporting. They are practical systems that harmonize people, processes, data, and decisions. This reshapes operations and culture simultaneously, guiding organizations toward transparency, efficiency, and a shared strategic reality. Unlike ERPs, CRMs, catalogs, and governance platforms—which take years to implement and rarely interoperate—an AI-powered digital twin binds these systems together and adapts to the organization at its current level of readiness. Twins for administrative functions can navigate spaghetti-like requirements, automate annual reports, and provide rapid cyber-incident response—mapping complex institutional logic into accessible AI workflows. The cultural shift emerges naturally: employees twin and automate the most painful parts of their jobs, freeing time for meaningful work, creativity, and collaboration. Some may even transition into "digital twinning" roles, shaping the organization's evolving cognitive architecture. All of this happens through natural language, eliminating arcane interfaces and reducing digital friction.

Human-centered Approach and the New Workforce

We build and advance new technologies not only for us, but for our children, their children, their children, and so on. Our children are the AI-native generation—the real intended users, as they are the ones who can carry technologies forward and innovate in ways that our generation, the makers, cannot fathom. We only need to reflect on the original forms and intentions of the first computer, the first network, the first penicillin, the first electric circuit, or the first nuclear reactor. Every generation wonders what a new technology will do to its workforce, the economy, and the global power structure. The honest and brutal reality is that there will be both casualties and opportunities. A human-centered approach keeps the focus and benefit for humans, accepting the technology's virtues, securing it, and educating about its reality, impact, and flaws.

Built by Humans for Humans: A New World with AI-powered Digital Twins

AI-powered digital twins succeed only when they reduce human cognitive load rather than increase it. Their purpose is improved decision-making, accountability, and operational clarity, which requires human participation throughout design, deployment, and operation. In simple terms, digital twins reduce *time*, *cost*, and *risk* (important for insurance). Disruptive technologies have always reshaped societies, and AI-powered digital twins are no different. The reasons AI is disruptive are simple:

- AI has the power to affect millions instantly.
- AI applies to all verticals and industries.
- There is an international race to win AI.
- There is an international race to dominate AI's supply chain.
- There are trillions of dollars invested into AI's development and wide-scale adoption.

As Yuval Harari argues in *Nexus* (Random House, 2024), disruptive technologies reorganize the deep structure of society, reshaping power, labor, communication and even human identity while creating new elites, vulnerabilities and dependencies. As he warns, AI, robotics, and ubiquitous surveillance can centralize power at unprecedented levels or democratize it, depending entirely on how societies architect their systems and values.

In this framing, AI-powered digital twins are equally capable of strengthening resilience, transparency, and human agency, or accelerating inequality when deployed without guardrails. Because a digital twin is bound to its physical counterpart, it needs a continuous feedback cycle involving human stakeholders throughout its lifetime. Humans and subject matter experts must be involved early in design and deployment and remain part of operational checkpoints. The goal is augmentation and reallocation of human work, not replacement.

The questions then are those of scalability:

- Do human subject matter experts have the time and resources to aid in the building of an AI-powered digital twin that ultimately will serve them? Why spend time and resources building something to ultimately save time and resources?
- Does every digital twin need to be custom built?

These questions have to be addressed early on to avoid disappointment, clashes, and loss of investment. A cost-benefit analysis removes fear of missing out and clarifies where AI and twinning are worthwhile and where they are not. In most organizations, only some processes should be twinned or completely revamped, while others should remain unchanged.

The answer to customization is that the subject being twinned may be unique, but the tools and principles used to build safe and secure twins can remain general. A successful platform provides humans with flexible tools while maintaining consistent governance, privacy, and access control. Identity and tagging solutions help enforce these boundaries. Engineering questions follow naturally: whether data and computation live in separate places, and whether the same “brain” can operate across different environments. AI enables such flexibility, but it also increases privacy and security responsibilities.

Humans Are Overwhelmed with Too Many Tools, Apps, Features, and Systems

In 2000, my cousin managed a large warehouse for a luxury products company. She repeatedly complained that the digital system was difficult to learn, inflexible where it needed flexibility, and full of unnecessary features. The system slowed operations and lowered morale. Decades later, organizations still face an overload of tools, systems, and integrations. Devices are connected, data migrates constantly to the cloud, and everyone is trying to integrate AI. How exactly to do this, which tools to use? My philosophy has always been to let needs guide tools rather than forcing humans to adapt to fragmented technologies. AI-powered digital twins organize technology around operational needs instead of forcing humans to adapt to fragmented tools.

Digital twins put technology in perspective—to maximize visibility, situational awareness, efficiency, and utility. When the need and utility guide tool selection, integration follows naturally. AI binds multiple technologies through natural language. It also accelerates learning the needed tools and their syntaxes to a degree that once seemed impossible. Is it perfect? Not anytime soon. Is it useful and worth it? Absolutely.

A recent example is a young CEO competing with large technology companies using a team of three student "developers" supported by generative AI. Humans are refocusing on goals while AI helps navigate the tools. I have noticed that it is the more advanced and well-versed developers that have an aversion to such approach. Ultimately, we all need their wisdom, but we can also acknowledge that technologies serve more generations that follow than those who built them.

Looking Ahead: Preserving Human Agency

A human-AI workforce must be grounded in fundamentals, ethics, and responsibility, anchored by empathy, communication, and care. As digital twins transform industries, our systems of learning must shift from rote tasks to systems thinking and critical reasoning.