DIGITAL STRATEGY

genabyte.

The Unified Namespace: more than a broker

A structured approach to connecting every system in your industrial enterprise - not a product you buy. Producers publish once; any authorised consumer subscribes.

THE CORE IDEA

A UNS is a real-time single source of truth for your industrial business.

The MQTT broker is one component of the UNS, not the UNS itself. Buying a broker does not give you a Unified Namespace any more than buying bricks gives you a house. The value is in the approach and the data structure around it: a shared, organised view of the business that any authorised system or person can reach in real time.

Walker Reynolds, who popularised the concept, described it as living "everywhere and nowhere". It is a **real-time single source of truth** - a place where producers publish their data once and any authorised consumer subscribes to what it needs, from PLC to ERP to analytics platform.

WHAT IS THE PROBLEM?	→ HOW UNS SOLVES IT
✗ Every new app needs **its own connection** to every source	→ ✓ **Publish once**; any consumer subscribes, no new integration needed
✗ Changing a source means **updating every consumer** individually	→ ✓ Consumers are **decoupled**; change the source once
✗ Current state **scattered** across dozens of disconnected systems	→ ✓ **One real-time view** of the business, always current
✗ OT-to-IT data requires **custom translation** for each use case	→ ✓ Data in **shared context**; any system reads it directly

WHY IT IS MORE THAN JUST A BROKER

DATA STORAGE AND DATA OPERATIONS

The broker holds a **real-time snapshot** - it is not a database. For long-term storage you still need a historian or data lake to collect and retain values over time. On top of that, not all brokers include data operations such as calculations, aggregations, or transformations - those typically require additional tooling alongside the UNS.

DATA QUALITY: GOLD IN, GOLD OUT

Gold in, gold out - but equally, garbage in, garbage out. The most important foundation is a good data model. Your ERP or CMMS is a solid starting point. Do not get pinned down trying to fix every inconsistency before you begin - do the data validation your use cases actually need, and keep the scope tied to the problem you are solving.

NETWORK SEGMENTATION AND CYBERSECURITY

The **Purdue model, IEC 62443 zones and conduits, and NIS2 compliance** all remain in force. Flattening data access raises the security stakes, it does not lower them.

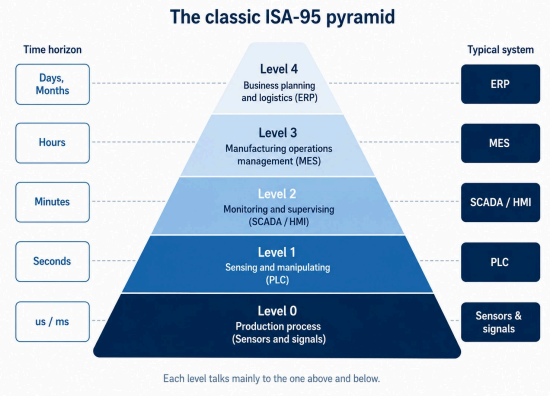
ISA-95 AND DIRECT CONTROL-LAYER CONNECTIONS

ISA-95 remains the structural foundation. For availability-critical loops, **the direct SCADA/DCS-to-PLC connection typically stays.** The UNS runs alongside it.

HOW DID WE GET HERE

ISA-95 is the international standard that describes how to structure and connect the systems inside an industrial company - from sensors and PLCs on the factory floor up to ERP in the boardroom. Published in the early 2000s, it became the universal reference model for organising OT and IT together.

It organises the enterprise into a clear hierarchy where each layer operates on its own time horizon and communicates mainly with the level directly above and below it. That discipline kept scope clean and systems manageable. The layered architecture maps directly onto the **Purdue network segmentation model**: traffic between zones is limited and controlled via defined conduits, which constrains the blast radius of any cyber incident. ISA-95 and the Purdue model together remain the cybersecurity foundation for most OT environments today - and become more important, not less, as IT and OT converge.

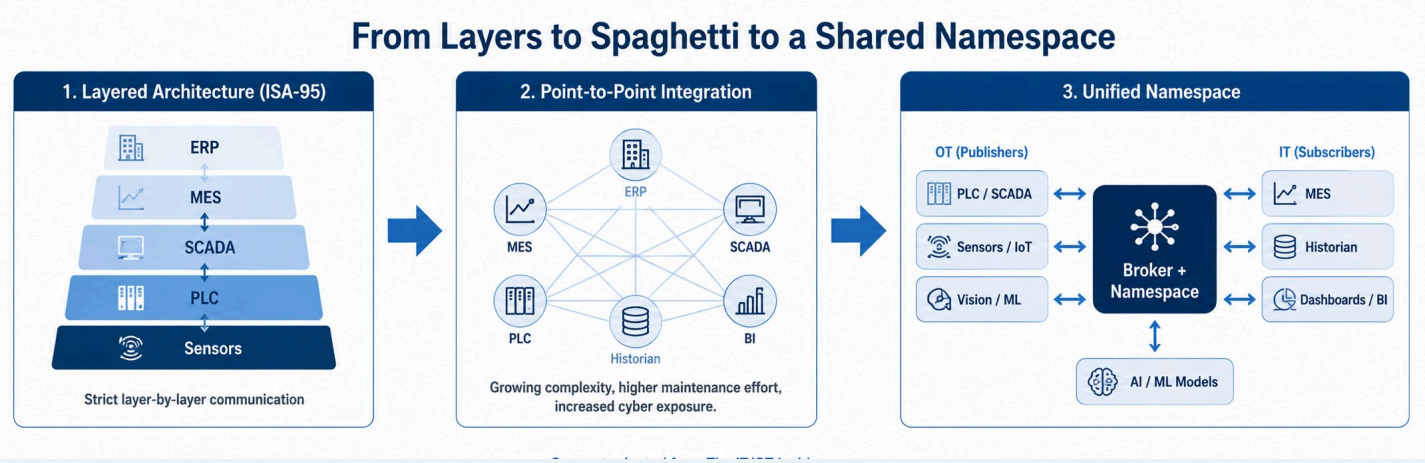


THE SPAGHETTIFICATION PROBLEM

Over time, plants added layer upon layer of new tools: MES, historians, visualisation platforms, reporting solutions, advanced process control, and more. Each new tool was wired directly to the systems it needed data from. The result is a growing web of point-to-point connections - **"spaghettification"**. On top of that, suppliers increasingly deploy their own edge devices to read out machine data, each with its own interface, credentials, and network footprint. Every new link adds load, maintenance cost, and a potential cyber exposure.

WHAT SPAGHETTIFICATION CREATES

- ✗ **Duplicate pipelines**
  Multiple tools pull the same source in different formats, creating redundant load.
- ✗ **Data silos**
  Each tool holds its own copy with its own context - no shared truth.
- ✗ **Diverging reports**
  Dashboards and KPIs calculated from different copies produce different answers.
- ✗ **Uncontrolled cyber exposure**
  Supplier edge devices multiply entry points with little governance or oversight.
- ✗ **Integration maintenance burden**
  IT and OT teams spend time keeping connections alive instead of delivering value.

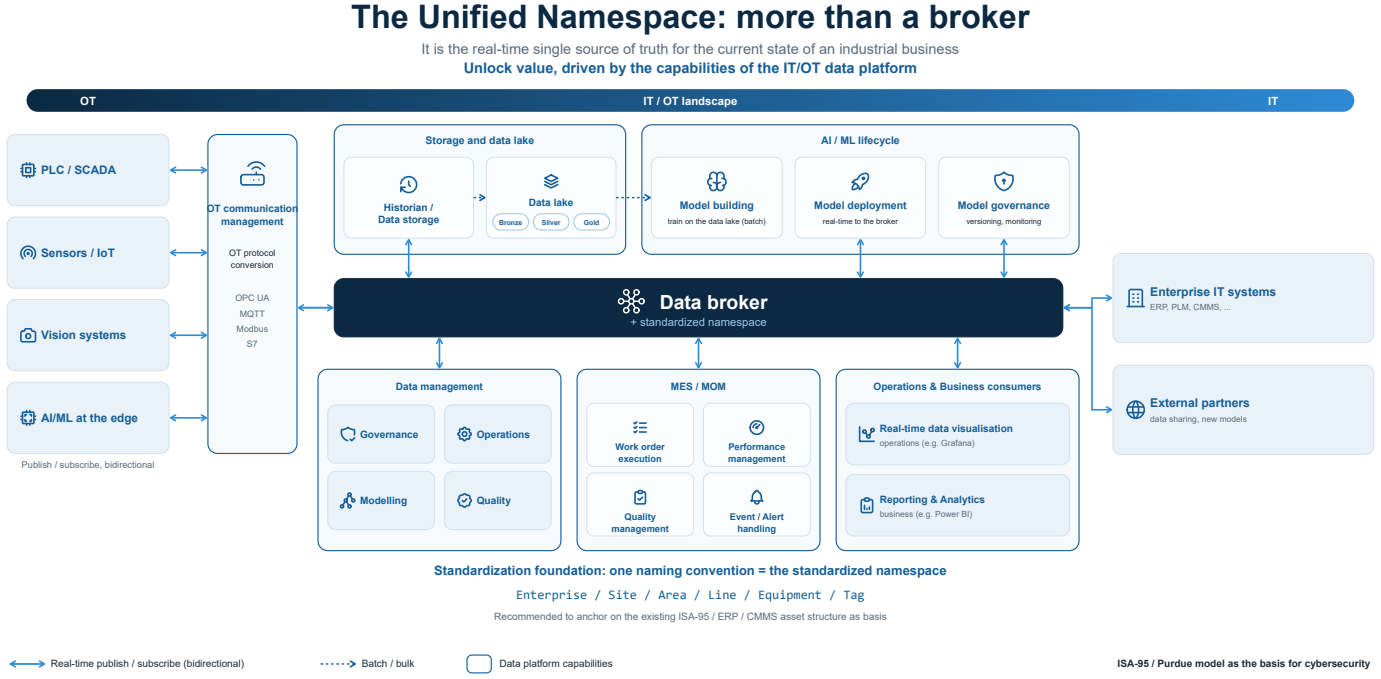


THE UNIFIED NAMESPACE AS THE ANSWER

Instead of every system connecting to every other system, each participant connects once to the broker: publish the data you have, subscribe to the data you need. The broker holds the latest value for every topic in real time. Adding a new consumer no longer requires a new integration - it requires a subscription.

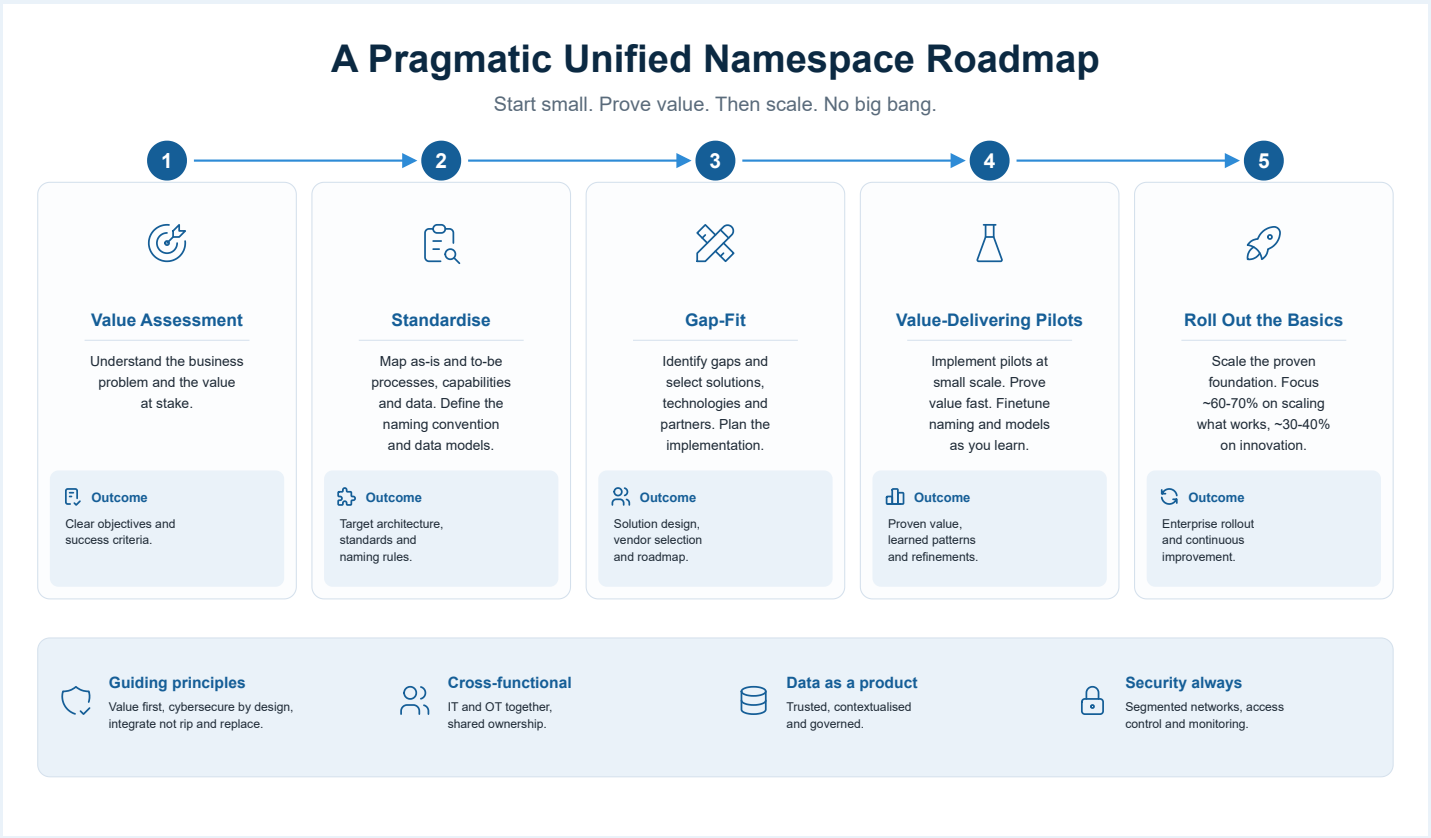
The UNS is the structured namespace around the broker. Any authorised system or person - from PLC to ERP to an analytics platform - can reach the data it needs through one common, contextualised structure.

Note: ISA-95 is not replaced. Critical point-to-point connections such as PLC to SCADA/DCS are kept for availability and determinism - the control path stays direct, the data path becomes shared. ISA-95 and the UNS coexist.



THE TYPICAL ADOPTION ROADMAP

The industrial data platform around the broker encompasses the full IT and OT capability landscape: data acquisition from PLCs and sensors, operational systems such as SCADA and MES, storage in historians and data lakes, visualisation, analytics, and the AI models that are increasingly embedded in the OT environment. The broker bridges and organises the data flow between them.



DATA MODEL

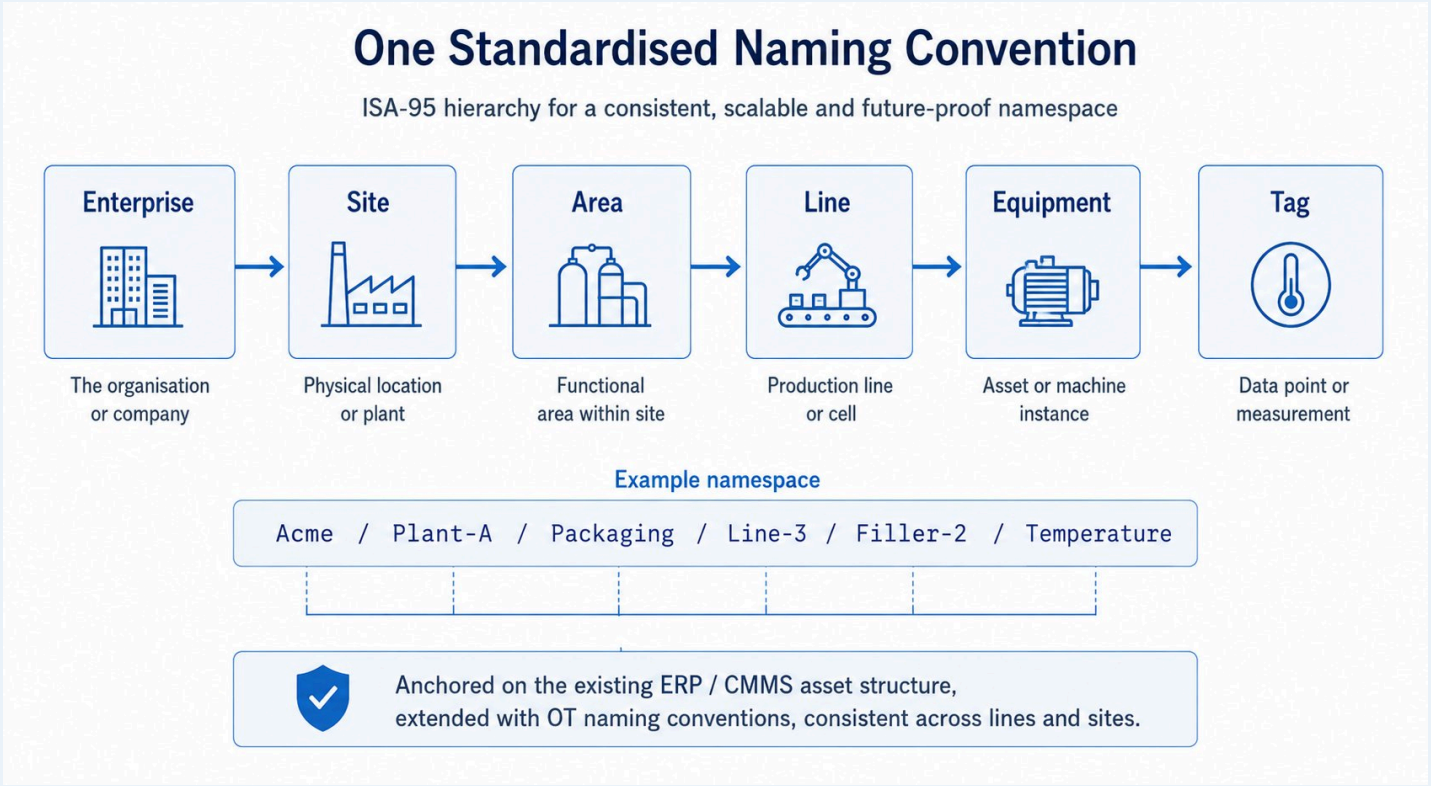
A naming convention is not just a technical detail - it is what makes the UNS useful at scale. A well-designed data model builds a standardised representation of factory reality: which assets exist, where they sit in the hierarchy, and what data points they expose.

The industry term is **digital twin**, but in practice what most organisations build first is a **digital shadow**: a read-only, real-time reflection of physical reality, not yet a full bidirectional model. That is already enough to unlock significant value.

ISA-95 remains the structural foundation here. Anchor the naming convention on the site / area / line / cell hierarchy you already use in ERP or your maintenance system, then extend it with OT sensor conventions.

WHY IT MATTERS IN PRACTICE

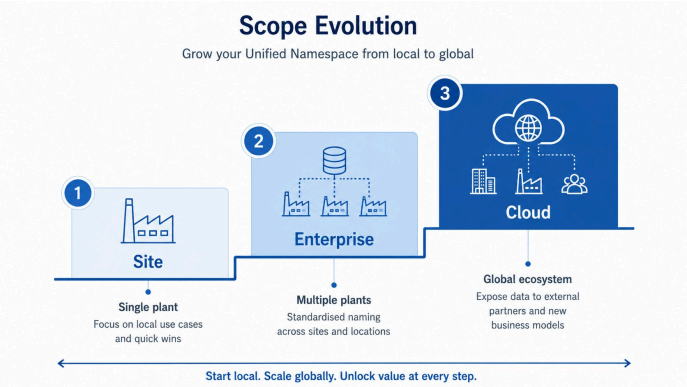
- Reports and dashboards built once work across all lines and sites that follow the same model
- Deployment speed shifts from **weeks or months** per site to **hours or minutes** once the model is proven
- New consumers (analytics, AI, external tools) subscribe to well-named topics without custom mapping work
- Focus on the use cases you are delivering - clean up only the data those use cases need, not everything at once



SCOPE EVOLUTION

A UNS can start at a single production line or a single site. As use cases are proven and the naming convention matures, scope expands: multiple sites, integration with a group ERP solution, and eventually a cloud layer for cross-site analytics and reporting.

It is normal for more than one namespace or model to coexist while the approach develops. The guiding principle is to integrate rather than rip and replace, and to let proven use cases drive the next increment.



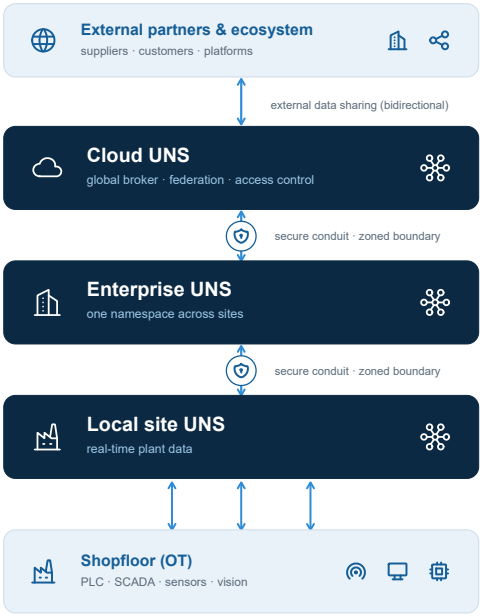
EXTERNAL DATA SHARING

Today many IoT vendors arrive with their own interface device to read out machine data. Each device adds a new network connection, new credentials, and a new cybersecurity exposure to manage. Multiplied across vendors, this becomes a governance headache.

A cloud UNS layer solves this: you publish the data you choose to share on your own cloud broker and grant your suppliers access - bidirectional if needed. You control what is exposed and to whom. Suppliers can offer managed versions of this as well, but it is an important building block to design for from the start.

A multi-tier Unified Namespace

Federated brokers from shopfloor to cloud: share data externally, securely, without outbound edge devices on the floor



What the tiering gives you

Share data externally, both ways
Partners and customers exchange data at the cloud tier. The namespace travels up; nothing reaches uninvited down into the plant.

Cybersecure by design
Every tier is a zoned boundary with controlled, authenticated conduits (Purdue / IEC 62443). Data flows up, access stays governed.

No outbound edge devices on the floor
Suppliers no longer run their own boxes phoning home from the shopfloor network. The floor stays inbound-only, so the plant's attack surface does not grow with every new external integration.

WHAT TO KEEP IN MIND

ISA-95 stays

A UNS builds on ISA-95 rather than replacing it. It removes the rigid layer-by-layer data flow but uses the ISA-95 hierarchy as the backbone of its naming convention. ERP, MES, SCADA and PLCs all remain in place.

Roughly 80% organisational, 20% technology

The hard part of a UNS is not the broker. It is defining a naming convention that will hold, aligning teams across IT and OT, and governing how the namespace evolves. Technology is the smaller share of the effort.

Cybersecurity: the stakes rise, not fall

Flattening data access does not reduce security obligations. The Purdue network zoning and the IEC 62443 zones-and-conduits model continue to apply. As more systems gain connectivity and AI models enter the OT landscape, the governance and security bar rises further. Enterprise requirements such as ISO 27001 and the NIS2 directive remain in scope.

ACRONYM LEGEND

UNS	Unified Namespace
MQTT	lightweight publish/subscribe messaging protocol
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology
IT	Information Technology
ISA-95 / IEC 62264	enterprise-control integration standard
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
MES / MOM	Manufacturing Execution System / Manufacturing Operations Management
ERP	Enterprise Resource Planning
OEE	Overall Equipment Effectiveness
IEC 62443	industrial automation and control system security standard
ISO 27001 / NIS2	enterprise information security standard and EU directive
CMMS	Computerised Maintenance Management System
APC	Advanced Process Control

SOURCES AND ATTRIBUTION

The IT/OT Insider — David Ariens and Willem van Lammeren, "The Unified Namespace (UNS) Explained". This article builds further on that reference.

HiveMQ, "What is Unified Namespace (UNS) in IIoT / Industry 4.0?". Note: we do not fully agree with all positions in this article, but a number of the underlying principles remain relevant.

Litmus, "Embracing the Unified Namespace Architecture".

Reference standards: ISA-95 / IEC 62264, the Purdue model, IEC 62443, ISO 27001 / NIS2.

genabyte.

genabyte.be