STRAT & IOT

Think Smart, Act Connected !

Future-ready industry



L'industrie du futur, ensemble

STRAT & IOT

From industrial needs to the right technology

EDITORIAL

When we meet plant directors in **Europe, India, the Middle East or Africa**, they rarely ask for "AI" or "digital twins". They ask for **six things**:

Predictive maintenance
Machines that do not stop without warning

Continuity
Production that keeps running, whatever happens

Traceability
Goods and spare parts they can trace end to end

Energy efficiency
Plants that use less energy, and can prove it

Reactivity
Teams that react in minutes, not hours

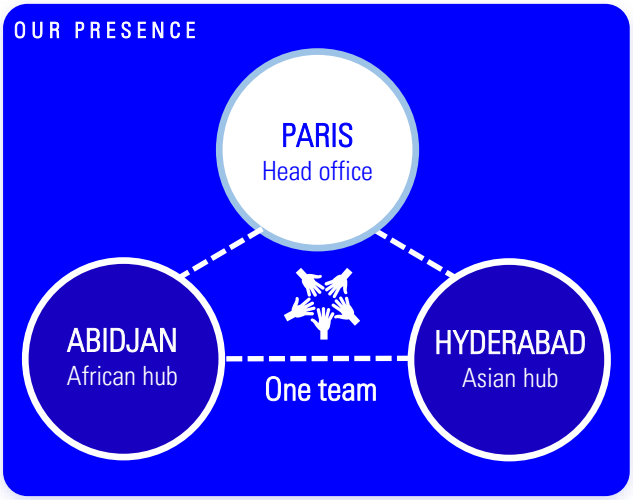
International development
The ability to grow into new countries

Technology only creates **value** when it serves **your plant**. A sensor nobody reads or a model built on **poor data** only adds **cost**. We start from your **industrial need**, then choose the **right tool**: a better alarm, a data platform or AI. **Let's talk about your plants.**

Aurélien Pallavisini, CEO, Strat & IoT Group

WHO WE ARE

Strat & IoT is a consulting and engineering group in **industrial IoT**, **energy** and **digital transformation**. Our Paris head office steers and supports every subsidiary: **one team across three continents**.



Paris *Head office · all subsidiaries*
Steers the group and supports every subsidiary with strategy, consulting and governance.

Hyderabad *Asian hub · group IT expertise*
Project delivery in India and Asia, and IT and OT expertise for all subsidiaries.

Abidjan *African hub · implementation*
Implementation capacity and financing partnerships for projects across the group.

OUR DIFFERENCE

- ✓ Business strategy + hands-on field delivery
- ✓ 20 years of senior OT and IT field experience
- ✓ Projects in Europe, India, Middle East and Africa
- ✓ Vendor-neutral: we specify for your interest

STRAT & IOT

Three activities, one value chain

Strat & IoT works across three connected activities, **Consulting**, **Software** and **Hardware**, forming one value chain. Unlike pure vendors or advisory firms, we stay with industrial clients from **field device selection**, through **platform integration**, to **strategic transformation**.



Strategy and innovation

- ✓ Industrial digital roadmap
- ✓ Industry 4.0 maturity assessment
- ✓ Business case and ROI
- ✓ Market entry and new-site strategy

Industrial data platforms

- ✓ SCADA and HMI (AVEVA, Ignition, Siemens)
- ✓ Unified namespace (ISA-95, OPC UA, MQTT)
- ✓ Production and quality: MES, QMS, LIMS.
- ✓ Maintenance and assets: CMMS, EAM.
- ✓ Logistics and supply chain: WMS, TMS.

Field devices and sensors

- ✓ Vibration, temperature and current sensors
- ✓ Energy meters and power quality analysers
- ✓ RFID and barcode readers
- ✓ Environmental sensors

Digital and operational transformation

- ✓ OT/IT convergence programmes
- ✓ Asset management (ISO 55000)
- ✓ Change management and operator training
- ✓ Cybersecurity advisory (ISA/IEC 62443)

Building and utilities software

- ✓ Building management systems (BMS)
- ✓ Energy management systems
- ✓ Maintenance system (CMMS) integration
- ✓ Carbon and ESG reporting

Control and connectivity

- ✓ PLCs and RTUs
- ✓ Industrial gateways and edge computing
- ✓ Industrial Ethernet, 4G/5G, LoRaWAN
- ✓ OT firewalls

Standards and compliance

- ✓ ISO 50001 energy management
- ✓ ISA/IEC 62443 security
- ✓ ESG and carbon reporting readiness
- ✓ Investment justification

Advisory on software

- ✓ Vendor-neutral platform selection and RFP
- ✓ Integration architecture
- ✓ Reusable engineering templates
- ✓ Custom development advisory

Advisory on hardware

- ✓ Vendor-agnostic selection
- ✓ Factory and site acceptance tests (FAT/SAT)
- ✓ BIS, IEC and CE compliance
- ✓ Obsolescence and spare-parts planning

STRAT & IOT
Our positioning

In a market where **generalist consultancies** bring business vision but lack **field reality**, and where **IT integrators** deliver technical execution but lack **strategic depth** and **vendor neutrality**, Strat & IoT combines both: embedded IoT and OT expertise, strategic vision and field execution, built on projects across **Europe, the Middle East, India and Africa**.

Generalist consultancies

- ✓ Business vision
- ✓ Sector benchmarking
- ✗ No hands-on OT or IoT delivery
- ✗ Out of touch on the plant floor

IT services and IoT integrators

- ✓ Technical expertise
- ✓ Project delivery
- ✗ No business vision
- ✗ Platform bias and vendor lock-in

STRAT & IOT

- ✓ Embedded IoT and OT expertise
- ✓ Strategic vision
- ✓ Vendor-neutral by design
- ✓ Field execution
- ✓ Practitioner, not theorist
- ✓ Hardware-to-platform fluency
- ✓ Large-scale deployment experience
- ✓ Multi-site, multi-country delivery
- ✓ Scoping in days, first results in weeks
- ✓ French and English, Paris and Hyderabad

The only partner who speaks technology in the morning and business model in the afternoon.

THE STANDARDS WE WORK TO

ISA-95 | ISA-88 | ISA/IEC 62443 | ISA-18.2 | ISA-101 | ISO 50001

ISO 55000 | OPC UA | MQTT | BACnet | Modbus | GS1 / EPCIS

ISO 14001 | ISO 9001 | ISO 28000

STRAT & IOT
Why industry, why now?

Production is moving
Supply chains diversify; new plants open in India and Africa, often steered from Europe.

Energy and carbon cost
Rising tariffs, customer ESG demands and EU carbon border reporting for exporters.

Plants are connected
OT and IT converge: downtime risk and cyber risk now grow together.

KEY RISKS

Unplanned downtime: one compressor, chiller or PLC failure stops a whole line.

Cyber incidents reaching production: in 2025 a cyberattack halted Jaguar Land Rover's UK plants for more than a month (est. £1.9 billion impact on the UK economy).

Ageing control systems: Siemens' SIMATIC S7-300 PLC family reached type discontinuation on 1 October 2025.

Energy cost and carbon exposure: utilities are often a plant's largest controllable cost.

Skills gap: new systems arrive faster than operators are trained.

OPERATIONAL CHALLENGES

Siloed data: across PLCs, SCADA, ERP and spreadsheets.

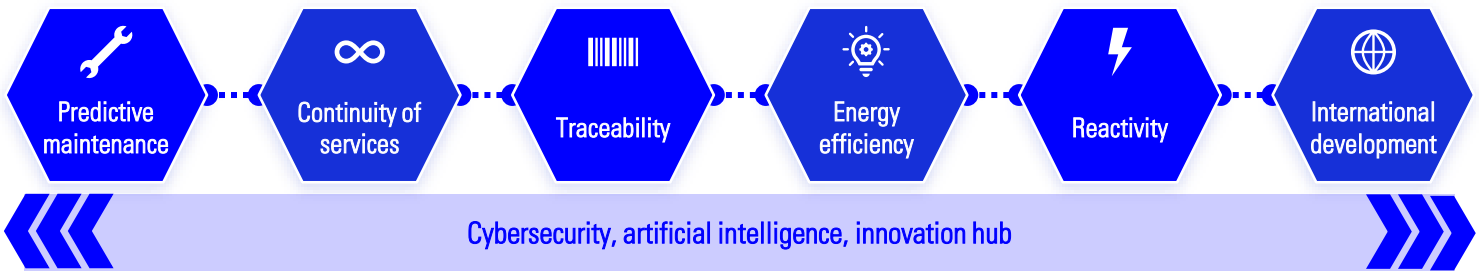
Alarm floods: and no single view of the plant.

Traceability gaps: for products and spare parts.

Vendor lock-in: on proprietary platforms.

Remote steering: of projects across time zones and languages.

WHAT INDUSTRY EXPECTS · PAGES FROM 6 TO 14

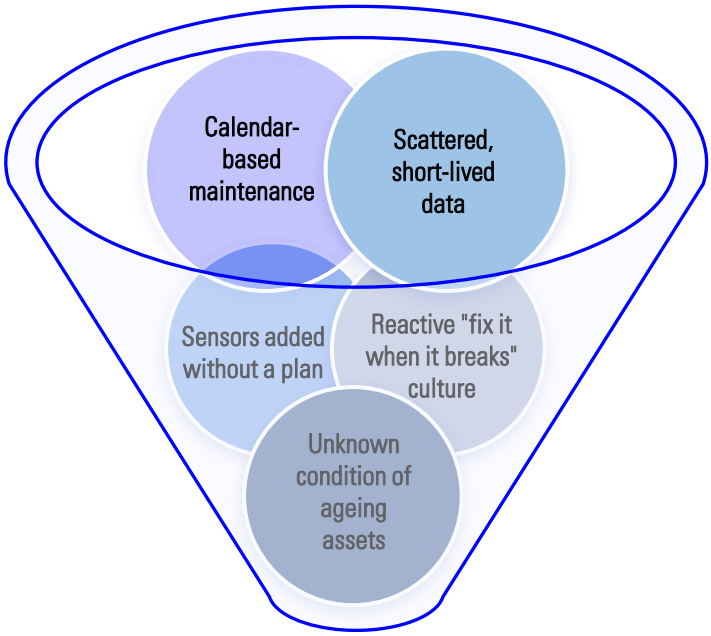


Sources: Computing (JLR results, 2025); Cyber Monitoring Centre via The National CIO Review; Eichler Service (Siemens S7-300 discontinuation).

Predictive maintenance

From calendar-based to condition-based

CHALLENGES



- ☐ Critical-asset register scored by impact on production, safety and cost (ISO 55000 principles)
- ☐ Condition-monitoring specification: which sensor, where, sampling rate and thresholds
- ☐ Historian set-up and baselines learned over about 90 days of normal running
- ☐ Predictive analytics experience on AVEVA and OSIsoft PI in power, refining and pharma
- ☐ Vendor-neutral CMMS selection, set-up or upgrade (SAP PM, IBM Maximo, Infor EAM or a lighter cloud tool), sized to your plant.
- ☐ Clean asset hierarchy, failure codes and spare-part links in the CMMS, so every intervention feeds the reliability analysis.

APPLICATIONS

ADDED VALUE

Technical layer

Sensing
- ✓ Electrical assets
- ✓ Rotating machines, beyond vibration
- ✓ Utilities, beyond chillers
- ✓ Process and machine data

Data
- ✓ Historian retention
- ✓ OPC UA and MQTT collection
- ✓ Asset data model (ISA-95)

Analytics
- ✓ Statistical baselines and drift
- ✓ Anomaly detection
- ✓ Machine learning once history allows

Strategic layer

Criticality
- ✓ Asset ranking
- ✓ Failure modes (FMEA)
- ✓ Spare-part priority

Business case
- ✓ Cost of downtime
- ✓ Shift of maintenance budget
- ✓ Payback per asset class

Roadmap
- ✓ Pilot on 10 critical assets
- ✓ Scale by asset class
- ✓ Multi-site template

Operational layer

Workflow
- ✓ Alert to work order
- ✓ CMMS integration
- ✓ Mobile access for technicians

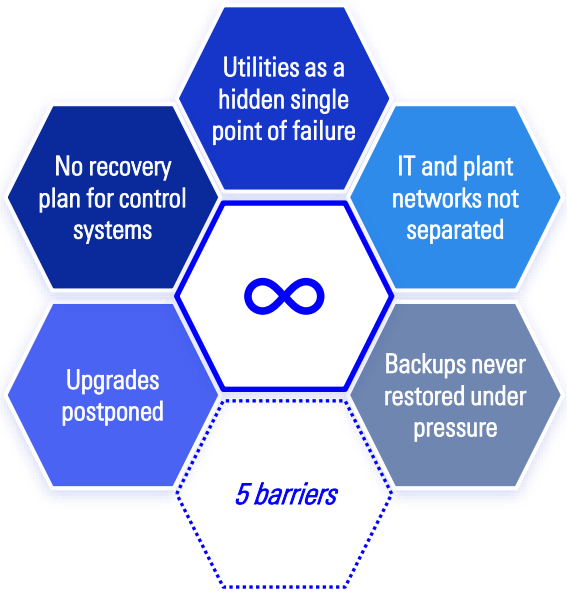
Performance
- ✓ MTBF and MTTR
- ✓ Share of unplanned work
- ✓ OEE availability

Practices
- ✓ Lead/lag rotation
- ✓ Run-hour equalisation
- ✓ Review of false alarms

Continuity of services

Keep running, whatever happens

CHALLENGES



1. Business impact analysis of utilities, control systems and networks
2. N+1 redundancy and automatic sequencing with permissive checks before each start
3. OT security architecture to ISA/IEC 62443: zones, conduits, controlled remote access
4. Backup and restore tests for PLC and SCADA programs
5. Phased upgrades without stopping production: chillers replaced in a live shopping complex with zero disruption

APPLICATIONS ↓

ADDED VALUE ↑

	Utilities	Control systems	Networks
Technical layer	✓ N+1 chillers, compressors and pumps ✓ Automatic sequencing ✓ UPS and generator monitoring	✓ Redundant SCADA servers ✓ Versioned PLC and HMI backups ✓ Migration of obsolete controllers	✓ Zones and conduits ✓ IT/OT demilitarised zone (DMZ) ✓ Secure remote access
	Risk	**Resilience plan**	**Investment**
Strategic layer	✓ Business impact analysis ✓ Map of single points of failure ✓ Customer and insurer requirements	✓ Recovery time objectives ✓ Spares and stock strategy ✓ Vendor service levels	✓ Prioritised CAPEX ✓ Phased upgrade plan ✓ Value of avoided downtime
	Readiness	**Monitoring**	**Change**
Operational layer	✓ Recovery drills ✓ Operator runbooks ✓ On-call escalation	✓ Health of utilities and networks ✓ Backup success ✓ Patch and vulnerability status	✓ Planned maintenance windows ✓ Offline logic validation ✓ Parallel commissioning

Traceability

Goods, spare parts and plant configuration

CHALLENGES

1. Separate systems, different codes
2. Data breaks at every partner handover
3. Spare parts tracked in spreadsheets
4. Obsolete controllers still in service
5. Records that can be altered

- ☐ Protocol benchmark and one standard for your product data: GS1, EPCIS, RFID, EDI, APIs
- ☐ Track-and-trace architecture linking batch, machine, operator and shipment
- ☐ Spare-parts registry by criticality, with an obsolescence and migration plan
- ☐ Versioned PLC and SCADA backups: your plant's own configuration is traceable too
- ☐ Industrialisation experience: 1,000,000 smart meters traced from factory test to field
- ☐ Spare parts linked to CMMS work orders: every part consumed is traced to the asset, the intervention and the technician.
- ☐ Full maintenance history per asset in the CMMS (serial numbers, interventions, replacements), ready for audits, insurers and GxP inspections.

APPLICATIONS

ADDED VALUE

TECHNICAL LAYER

1 Identification

GS1 identifiers · Barcode and RFID tags · Reader placement and read-rate tests

2 Events

EPCIS event model · Batch and genealogy records (ISA-88) · Machine and operator context

3 Integration

MES and ERP links · Data contracts with partners · APIs and EDI

STRATEGIC LAYER

1 Standards

One product data standard · Partner onboarding · Audit and compliance needs

2 Recall and quality

Smaller recall scope · Faster complaint root cause · Customer reporting

3 Obsolescence

Installed-base audit · Migration roadmap · Last-time buys

OPERATIONAL LAYER

1 Spare parts

Critical spares registry · Minimum and maximum stock · Authorised sources only

2 Records

Full audit trail · Role-based access · Tamper-proof storage

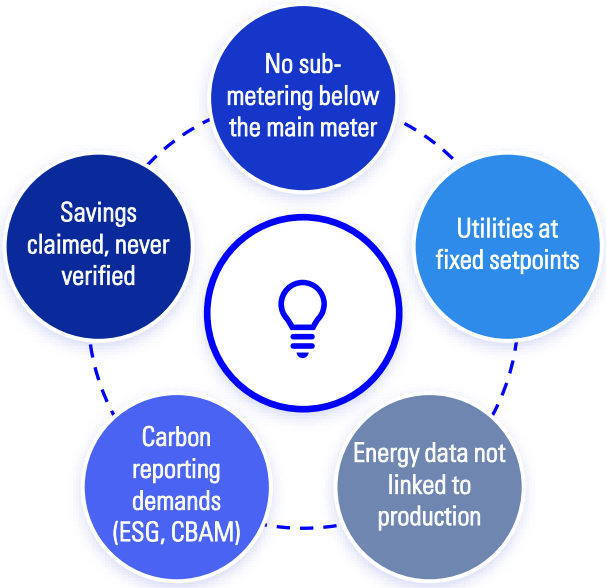
3 KPIs

Time to trace a batch · Critical-spares availability · Obsolete components in service

Energy efficiency

Energy you can measure is energy you can cut

CHALLENGES



1. Field survey of every consumption point, with a kWh, cost and CO2 baseline
2. Sub-metering plan with measurement and verification to IPMVP
3. Utilities optimisation: chiller plant, compressed air, HVAC sequencing and setpoints
4. ISO 50001-ready energy management system and KPI dashboards
5. Costed CO2 reduction roadmap, ready for ESG reporting

APPLICATIONS

ADDED VALUE

	Metering	Utilities control	Platform
Technical layer	✓ Sub-meters per line and utility ✓ Power quality analysers ✓ Compressed-air and steam flow	✓ Chiller plant optimisation ✓ Compressor sequencing and leak detection ✓ HVAC and lighting schedules	✓ EMS and BMS integration ✓ Energy historian ✓ Automated reports
	Baseline	**Business case**	**Decarbonisation**
Strategic layer	✓ Energy review (ISO 50001) ✓ Significant energy uses ✓ Cost and carbon baseline	✓ Savings per measure ✓ Payback and financing ✓ Tariff and demand charges	✓ Solar and storage options ✓ Carbon accounting ✓ CBAM and ESG reporting
	KPIs	**Routines**	**Verification**
Operational layer	✓ kWh per unit produced ✓ Chiller efficiency (kW per ton) ✓ Peak demand	✓ Energy team and monthly review ✓ Alarms on drift ✓ Shift-level targets	✓ Savings measured to IPMVP ✓ Tracking against baseline ✓ Continual improvement

Reactivity

The right information, to the right person, in minutes

CHALLENGES

- Alarm floods
- One screen per system, no single view
- Information stuck in the control room
- No agreed escalation rules
- Root cause takes hours

- ☐ Alarm rationalisation to ISA-18.2: around 150 alarms per operator per day is the benchmark
- ☐ High-performance operator screens to ISA-101: grey by default, colour means "act now"
- ☐ Unified control room across BMS, utilities, energy and production systems
- ☐ Tiered escalation by SMS or email, with a trend snapshot attached
- ☐ Experience: 1,000,000+ data points from 53 buildings unified in one control room
- ☐ Response and repair times tracked in the CMMS, so every incident feeds the improvement loop and the escalation rules.

APPLICATIONS

ADDED VALUE

TECHNICAL LAYER

1 Integration

Siemens, Schneider Electric, Honeywell, Johnson Controls · OPC UA, BACnet, Modbus · Unified namespace

2 Displays

ISA-101 screens · Situation dashboards · Secure mobile and web access

3 Alarms

Priorities and shelving · Flood suppression · Voice announcements on the shop floor

STRATEGIC LAYER

1 Governance

Escalation matrix · Roles and responsibilities · Response-time targets

2 Control room design

What to centralise · Shift organisation · Remote support model

3 Roadmap

Alarm audit · Rationalisation in waves · Roll-out site by site

OPERATIONAL LAYER

1 Response

Operator, shift engineer, plant head · On-call rotation · Incident log

2 Improvement

Review of "bad actor" alarms · Root-cause support · Lessons learned

3 KPIs

Alarms per operator per hour · Time to acknowledge · Time to resolve

International development

Build once, replicate everywhere

CHALLENGES



1. Site set-up: needs assessment, vendor-neutral specification and tender package
2. Integrator selection and commissioning governance: FAT/SAT, loop checks, snag lists
3. Reusable templates: engineering time cut by 38%, deployment from 14 to 6 weeks
4. Operator training with competency sign-off before handover
5. One group across Paris, Hyderabad and Abidjan, working in French and English

APPLICATIONS

ADDED VALUE

Technical layer

Templates

- ✓ Equipment object library
- ✓ Tag naming standard
- ✓ Standard screens and reports

Architecture

- ✓ Common data model
- ✓ One security baseline
- ✓ Open protocols

Commissioning

- ✓ FAT/SAT protocols
- ✓ Loop checks
- ✓ As-built documentation

Strategic layer

Market entry

- ✓ Site and supplier assessment
- ✓ Local standards (BIS, IEC, CE)
- ✓ Partner selection

Specification

- ✓ Vendor-neutral RFP
- ✓ Scoring grid
- ✓ Integrator shortlist

Governance

- ✓ Head office–site reporting
- ✓ Replication playbook
- ✓ Multi-site benchmarking

Operational layer

Handover

- ✓ Structured handover
- ✓ Operating and maintenance manuals
- ✓ Defect liability follow-up

People

- ✓ Hands-on operator training
- ✓ Competency sign-off
- ✓ Local champions

Performance

- ✓ Order to start of production
- ✓ Engineering hours per site
- ✓ Operators certified

Cybersecurity

Protect the process, protect the business

CHALLENGES



- ☐ OT security assessment and zoning to ISA/IEC 62443
- ☐ Secure-by-design specifications for new plants and every vendor
- ☐ Vendor onboarding playbook: device lifecycle from purchase to decommissioning
- ☐ SCADA design experience for critical oil and gas infrastructure, with cybersecurity built in
- ☐ Backup, recovery and incident playbooks, tested with operators
- ☐ The CMMS as the single OT asset inventory: firmware versions, network connections and vulnerabilities tracked for every controller.

APPLICATIONS

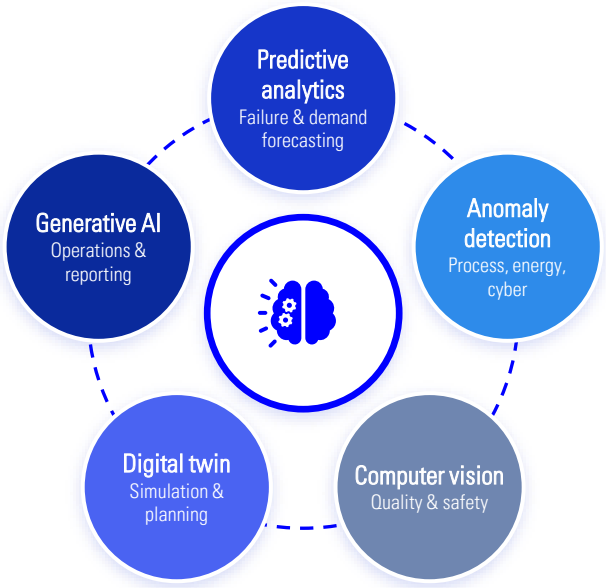
ADDED VALUE

PRODUCTION	UTILITIES & BUILDINGS	SUPPLY CHAIN & QUALITY
1 Threats Ransomware spreading from office IT · Unauthorised PLC changes · Infected vendor laptops and USB keys	**1 Threats** BMS exposed to the internet · Default passwords on controllers · Tampering with clean-room or HVAC conditions	**1 Threats** Compromised suppliers · Altered traceability records · MES or ERP outage that stops shipping
2 Defence Zones and conduits · PLC change detection and backups · Secure remote access	**2 Defence** BMS segmentation · Hardening and password policy · Monitored BACnet and Modbus gateways	**2 Defence** IT/OT DMZ for MES · Data contracts and access control · Full audit trail
3 AI-assisted security OT network behaviour baselines · Detection of unusual commands · Alert triage	**3 AI-assisted security** Sensor data integrity checks · Unusual setpoint changes · Energy and occupancy anomalies	**3 AI-assisted security** Tamper detection in records · Unusual access patterns · Automated compliance checks

Artificial Intelligence

From plant data to plant decisions

CHALLENGES



1. Data-readiness check before any AI investment: no model learns from data never recorded
2. Use cases chosen by business value, not by trend
3. AI built on your historian and SCADA data, with AVEVA and OSIsoft PI experience
4. Human in the loop: AI assists, operators decide
5. Vendor-neutral benchmark of AI and IoT platforms

APPLICATIONS ↓

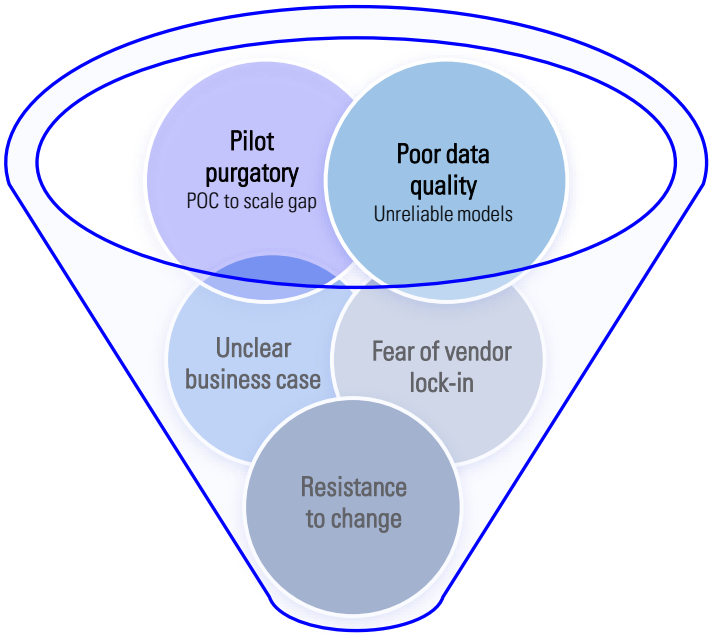
ADDED VALUE ↑

Production	**Predictive maintenance** ✓ Failure probability on motors, pumps, compressors ✓ Remaining useful life ✓ Spare-part forecasting	**Process** ✓ Drift detection ✓ Setpoint recommendations ✓ OEE loss analysis	**Operator support** ✓ Suggested root causes for alarms ✓ Automatic shift reports ✓ Multilingual operator assistant
Utilities & buildings	**Forecasting** ✓ Load and demand ✓ Peak shaving ✓ Tariff optimisation	**Optimisation** ✓ Chiller and compressor sequencing ✓ HVAC setpoints ✓ Compressed-air leak detection	**Reporting** ✓ Automated energy and carbon reports ✓ Savings verification ✓ Anomaly alerts
Supply chain & quality	**Quality** ✓ Vision inspection ✓ Defect prediction ✓ Batch release support	**Traceability** ✓ Matching and cleaning part records ✓ Tamper detection ✓ Recall impact analysis	**Planning** ✓ Demand forecasting ✓ Inventory optimisation ✓ Supplier delay prediction

Innovation hub

Prove it once, roll it out everywhere

CHALLENGES



- ☐ Innovation roadmap tied to the six industry expectations
- ☐ Digital-twin reference architecture on a unified namespace (ISA-95)
- ☐ Pilot design with KPIs and clear go/no-go criteria
- ☐ Ecosystem scouting: start-ups, universities and technology partners in Europe, India and Africa
- ☐ Replication playbook to roll out what works across sites
- ☐ CMMS failure and repair history used as training data for predictive models and the digital twin: no pilot starts from zero.

APPLICATIONS ↓

ADDED VALUE ↑

Digital twin & simulation

- ✓ Live model of assets and utilities
- ✓ "What if" scenarios: loss of a chiller, new line
- ✓ Energy and capacity simulation
- ✓ Operator training on the twin

AI & machine learning

- ✓ Failure prediction
- ✓ Process optimisation
- ✓ Vision inspection
- ✓ Assistants for operators and engineers

Green & energy technologies

- ✓ Rooftop solar and storage
- ✓ Heat recovery
- ✓ Efficient chillers and compressors
- ✓ Carbon accounting

IoT & edge computing

- ✓ Wireless sensors (LoRaWAN, private 5G)
- ✓ Edge analytics
- ✓ Retrofit of legacy machines
- ✓ Secure gateways

Emerging business models

- ✓ Energy-as-a-service
- ✓ Equipment-as-a-service
- ✓ Performance contracts
- ✓ Data sharing with partners

Open innovation & ecosystem

- ✓ Start-up scouting
- ✓ Pilot-to-scale governance
- ✓ Co-development and IP models
- ✓ Academic partnerships

Our differentiate know-how

What we do differently, end to end

Most industrial projects fail **between the steps**: a strategy never implemented, a specification written for one vendor, a system handed over to operators who were never trained. One senior team covers **every step**, from the first site visit to the next plant.

1 Assess

Usually: a generic audit report

With us: site visit, data and asset review, KPI baseline between 2 and 4 weeks

2 Design

Usually: an architecture tied to one platform

With us: vendor-neutral design on open standards (ISA-95, OPC UA, MQTT)

3 Specify & select

Usually: the vendor writes the tender

With us: tender package, scoring grid and integrator shortlist written for you

END TO END

4 Commission

Usually: sign-off on paper

With us: FAT/SAT, loop checks, snag lists and operator competency sign-off

5 Operate & improve

Usually: savings claimed, never checked

With us: KPIs tracked against the baseline; savings verified to IPMVP

6 Replicate

Usually: every site starts from zero

With us: templates and a playbook reused for each new site

OUR CORE ENABLERS

Six industry expectations · measurable results

Strategy

Business case per site: downtime, energy and carbon baselines before any spend

Data

One unified namespace (ISA-95); asset baselines from about 90 days of normal running

Cybersecurity

ISA/IEC 62443 zones and conduits; backups restored and tested, not assumed

AI

Only on clean, contextualised data; operators keep the decision

Operational excellence

ISA-18.2: ~150 alarms per operator per day; ISO 50001 and ISO 55000 practice

One senior team · vendor-neutral · Paris · Hyderabad · Abidjan

STRAT & IOT