

ARG

Industrial Digital Twin OT Data Integration

معماری اتصال همزاد دیجیتال در پالایشگاه‌ها و پتروشیمی‌ها

Refineries and Petrochemical Plants / Reference Architecture

Plant equipment, control and ARG

داده از تجهیزات و ابزار دقیق به سامانه کنترل می‌رسد و از مسیر مصوب امنیتی در اختیار همزاد دیجیتال قرار می‌گیرد.

PROCESS EQUIPMENT



CONTROL SYSTEM



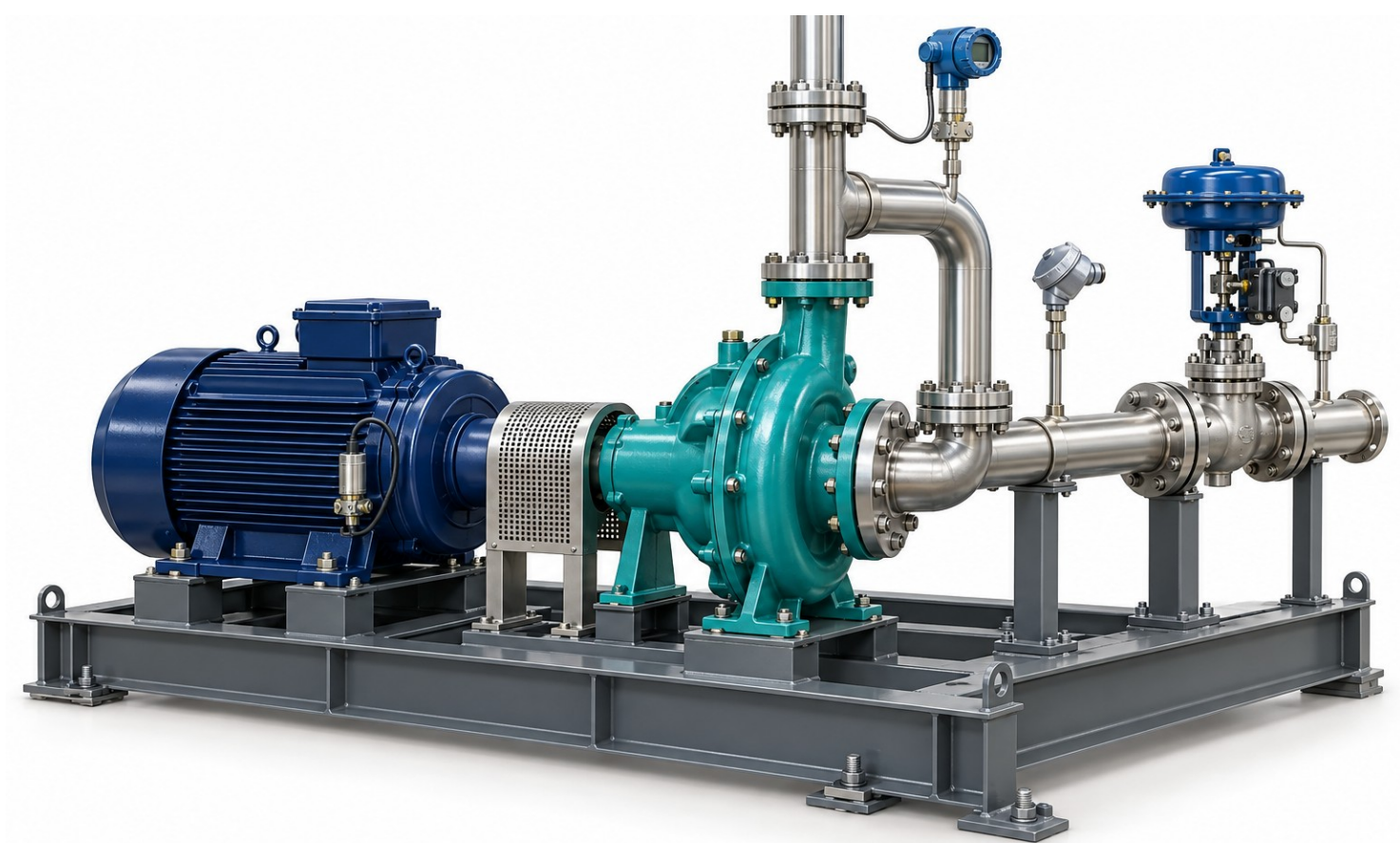
ARG DIGITAL TWIN



Illustrative equipment and screen. Approved telemetry flow; process control remains within the DCS.

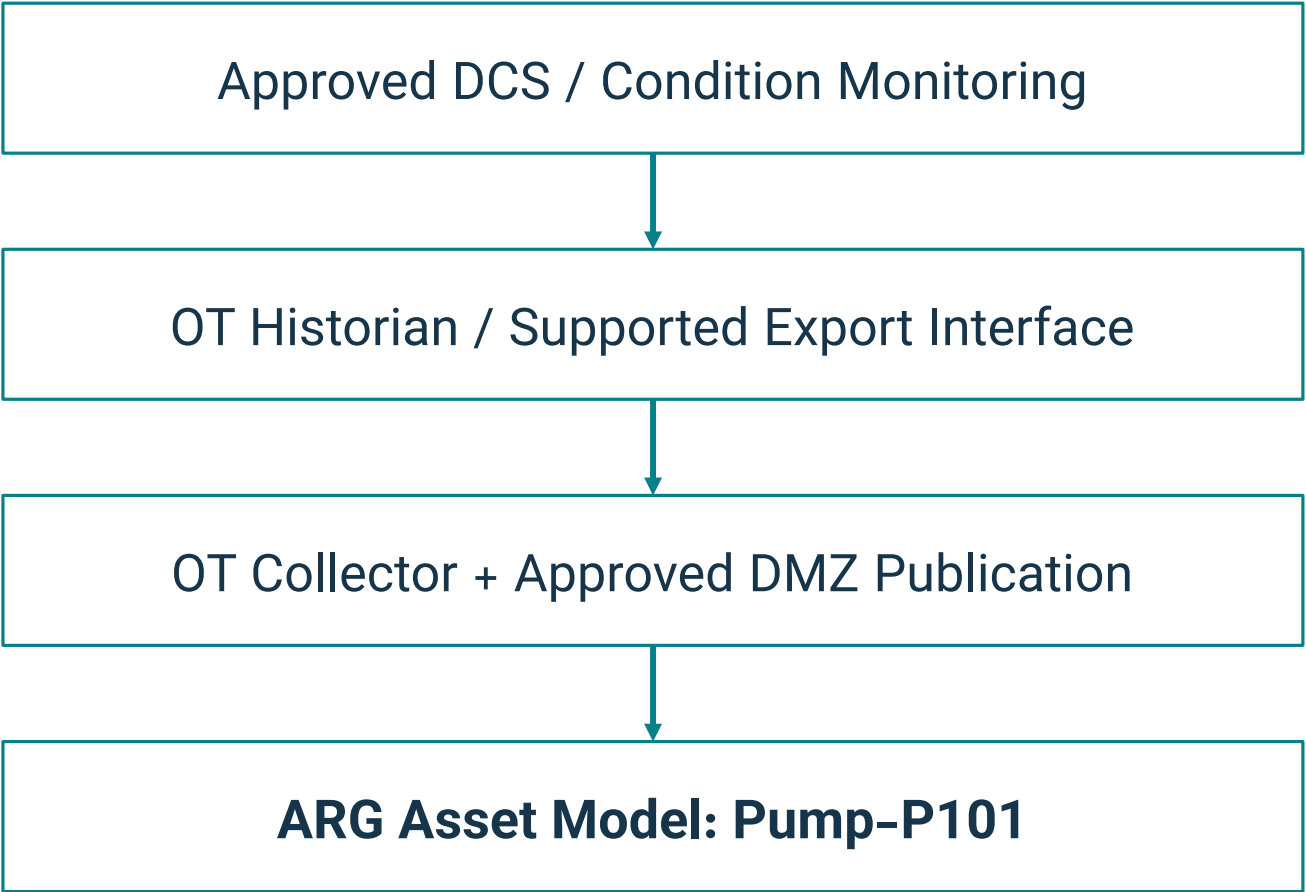
Pump data and the digital twin

نمونه یک پمپ نشان می‌دهد که مقدار اندازه‌گیری شده چگونه همراه زمان و کیفیت، به ویژگی تجهیز در نرم‌افزار ارگ تبدیل می‌شود.



PUMP P-101

Pressure / Temperature / Condition data



value + unit + timestamp + quality

Twin properties and analytics

Integration design basis

پیشنهاد ما یک مسیر مشخص برای اخذ داده است که مالک شبکه کنترل آن را تأیید و آزمون می‌کند.

- 01** Process control remains within the existing DCS / PLC domain.
- 02** The asset owner selects the approved data source and conduit.
- 03** The integration identity permits approved telemetry reads only.
- 04** FAT / SAT verifies load, quality, recovery and control independence.

این الزامات در طراحی و آزمون پذیرش ثبت می‌شوند؛ تأیید آن‌ها صرفاً با نمایش داشبورد انجام نمی‌شود.

Established industrial integration patterns

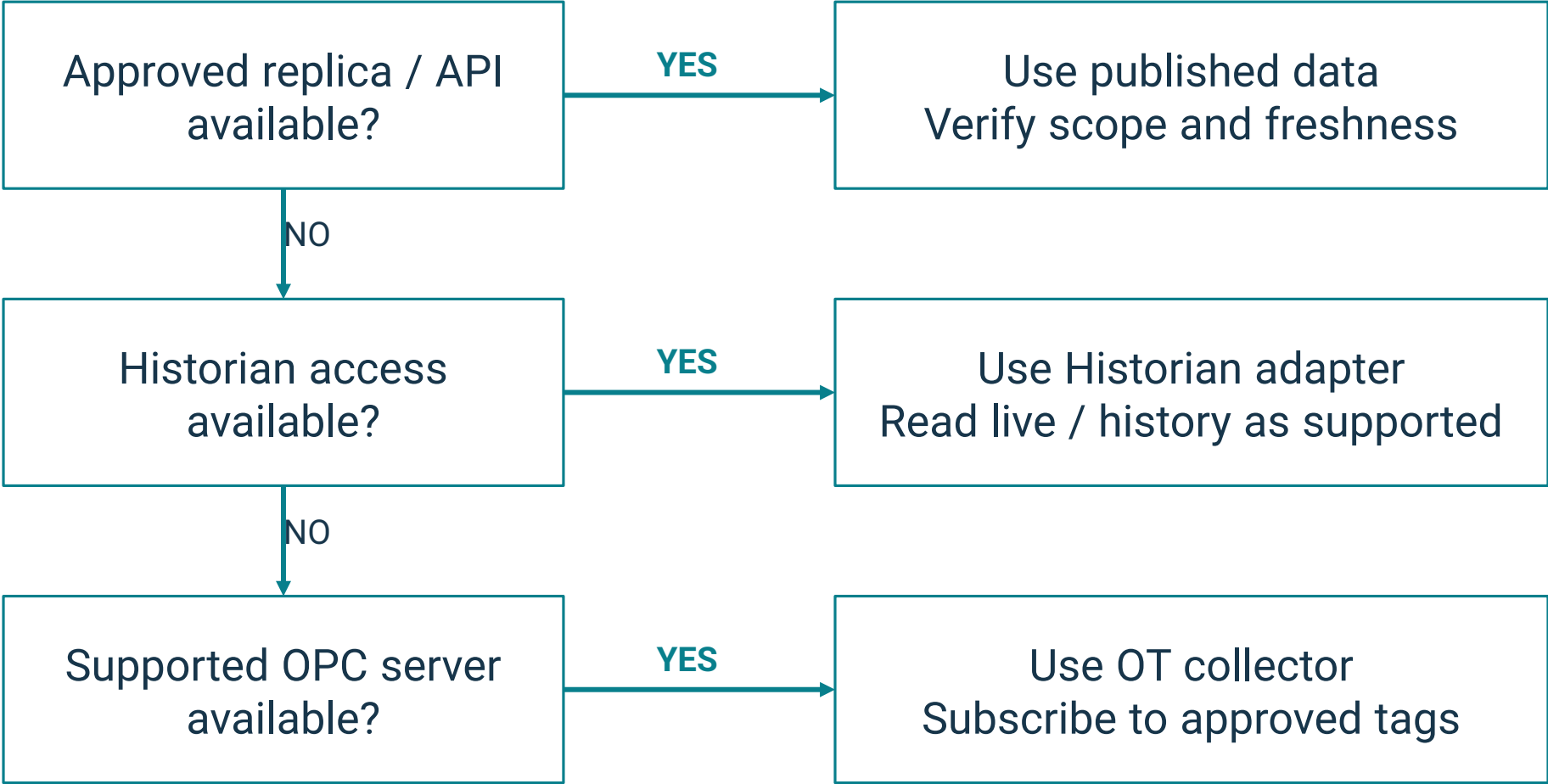
نمونه‌های رسمی سازندگان و راهنماهای امنیت صنعتی، مسیر جمع‌آوری محلی و انتشار کنترل‌شده داده را نشان می‌دهند.

Evidence	Documented pattern	Meaning for ARG
AWS IoT SiteWise	Onsite gateway reads Historian / industrial server	Collector at the plant, analytics downstream
AWS Industrial Digital Twin	Edge acquisition feeds an industrial twin	Acquisition and twin services have separate roles
Linde / GE, 2009 case	Historian infrastructure for 350+ sites	Historical evidence of enterprise data integration
NIST SP 800-82r3	DMZ services between OT and Enterprise	Explicit security boundaries and monitored conduits

Cloud deployment is optional. The same integration boundary can support an on-premises ARG platform.

Data source selection

اولویت انتخاب با مسیر داده‌ای است که در سایت موجود، پشتیبانی شده و مجاز باشد.

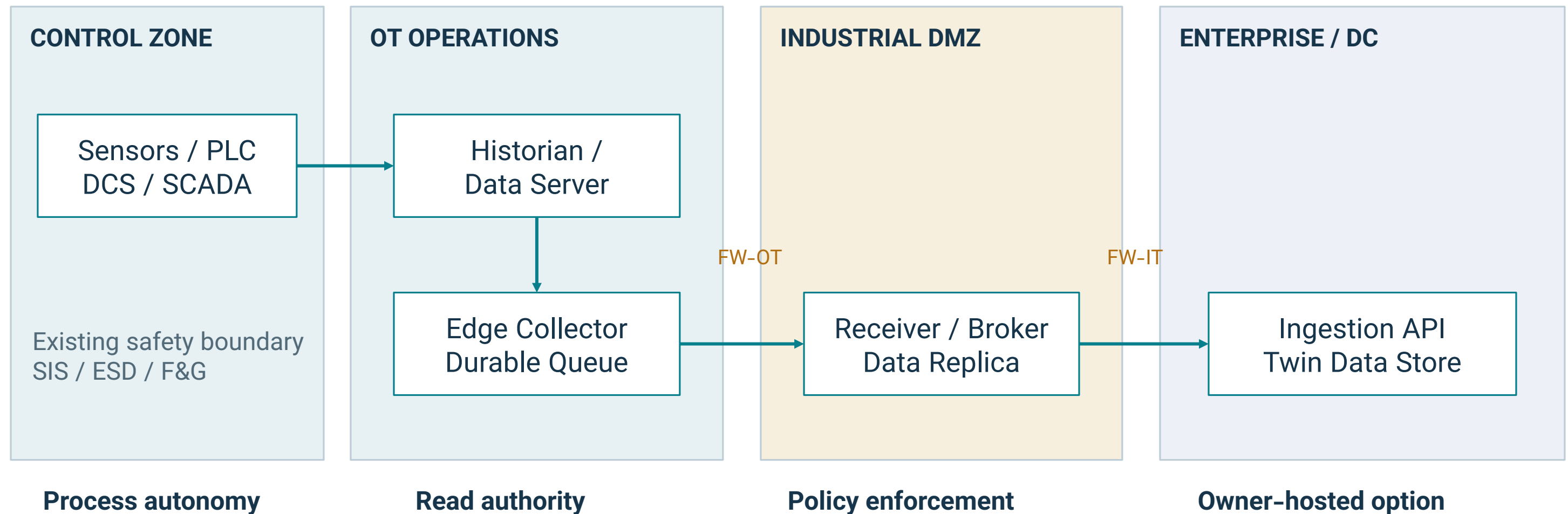


If all routes are unavailable

Interface engineering
Vendor option / license
MOC and risk review
Offline export if approved

Reference architecture and trust boundaries

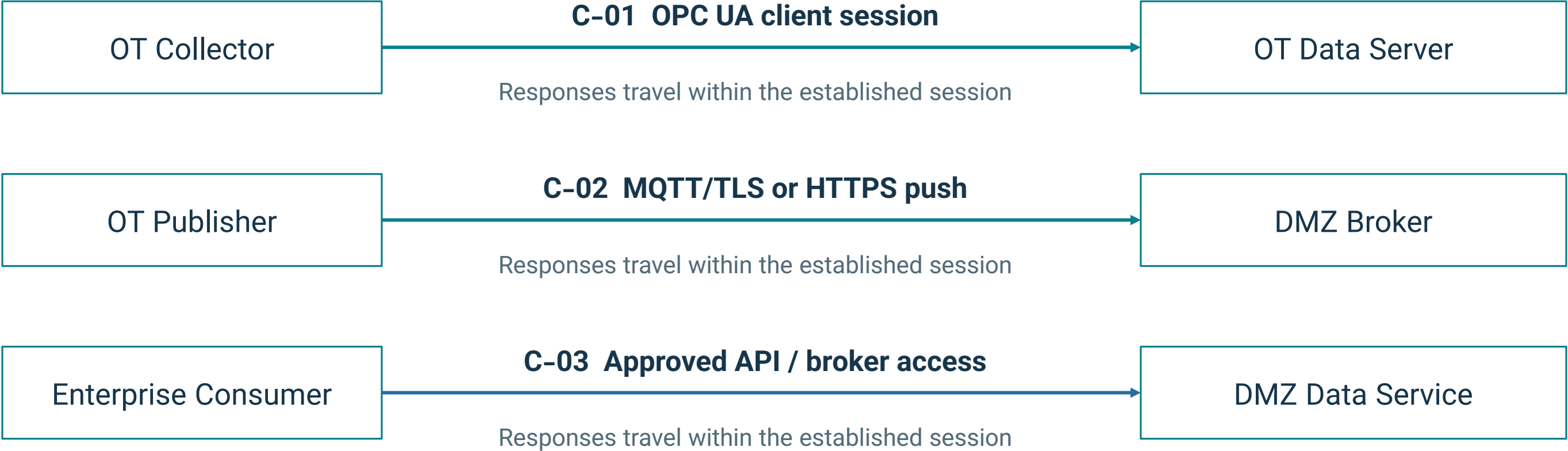
فلش‌ها در این اسلاید جریان منطقی داده را نشان می‌دهند؛ جهت آغاز نشست شبکه در اسلاید بعد مشخص است.



محل نصب و تعداد سرورها پس از بررسی شبکه تعیین می‌شود؛ این معماری وابسته به اتصال اینترنت نیست.

Session initiation and data flow

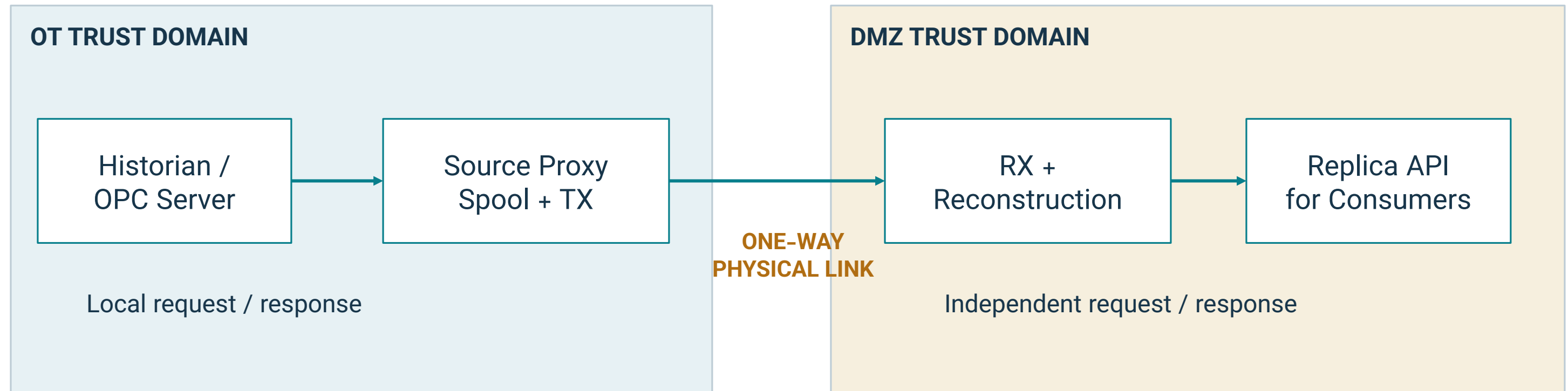
فقط خواندنی بودن حساب، به معنی یک طرفه بودن ارتباط شبکه نیست.



هر جریان به میزبان، مقصد، پورت واقعی، هویت سرویس و نرخ مجاز محدود می شود؛ ارتباط مستقیم از بک اند به کنترلر تعریف نمی شود.

Unidirectional transfer option

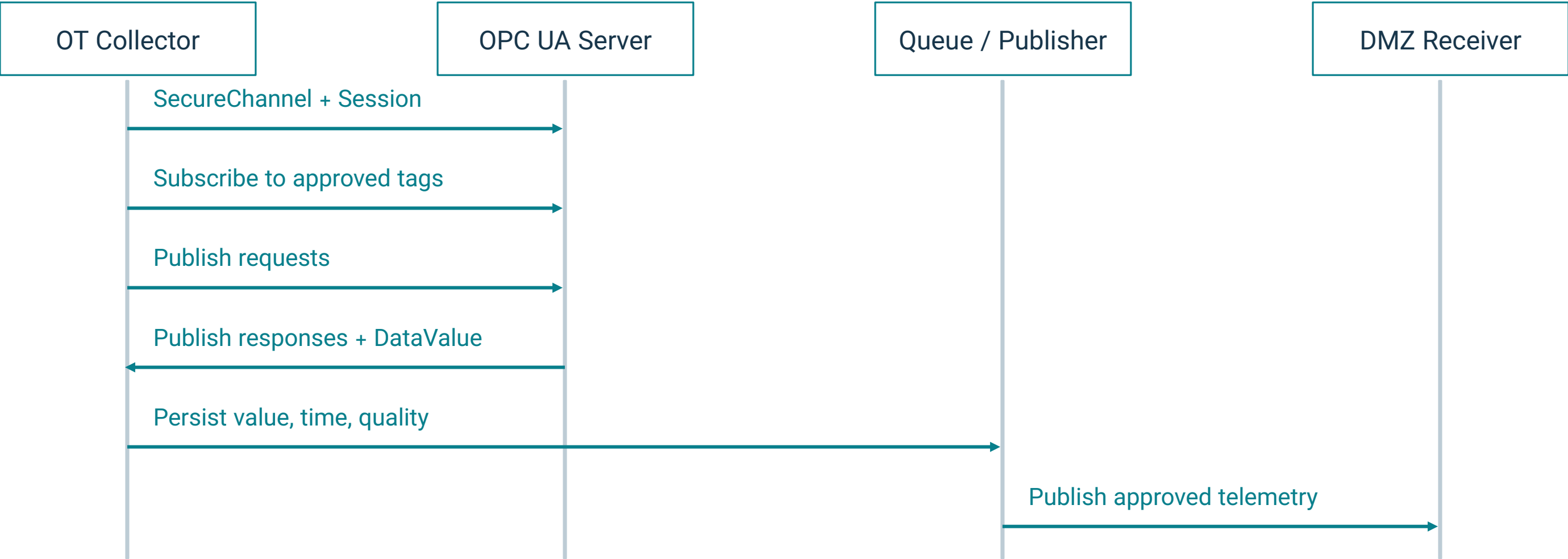
در سایت‌هایی که سیاست امنیتی انتقال فیزیکی یک‌طرفه می‌خواهد، پروتکل در دو سمت پایان می‌یابد و بازسازی می‌شود.



- 01** Validate loss detection, replay, backlog and integrity at the receiver.
- 02** Design certificate renewal and maintenance without an implicit return path.

OPC UA acquisition sequence

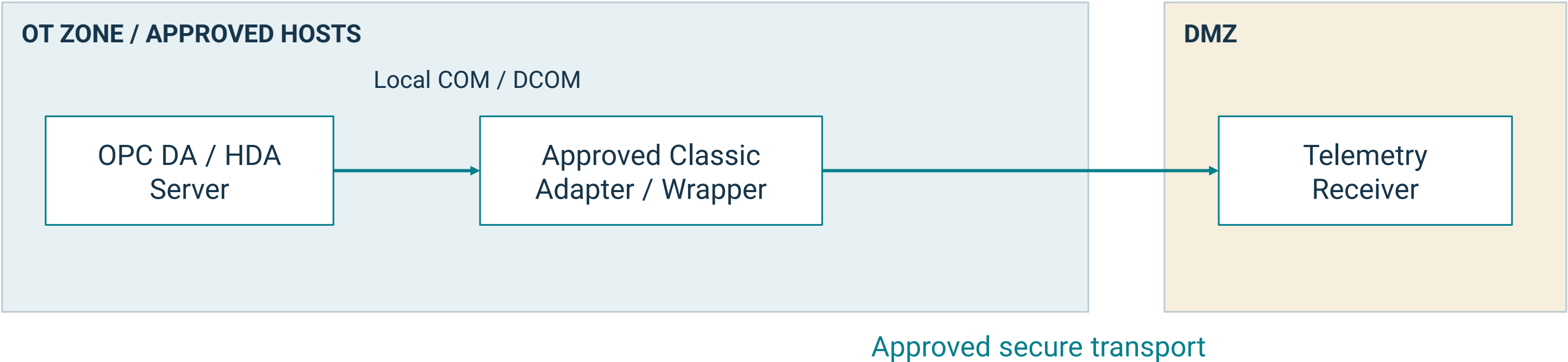
هویت برنامه، مجوز کاربر و روش خواندن داده باید جداگانه تنظیم و آزمون شوند.



بازیابی تاریخچه مسیر جداگانه و محدودشده دارد؛ بازسازی داده‌های از دست‌رفته به پشتیبانی و مدت نگهداری منبع وابسته است.

Legacy OPC Classic integration

وجود سامانه قدیمی، مسیر اتصال را عوض می کند و لزوماً به معنی تعویض کنترلرها نیست.

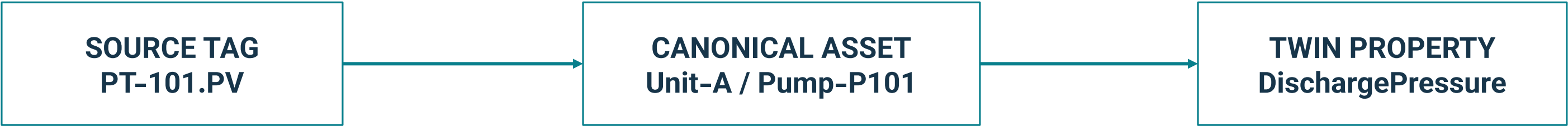


Compatibility checklist

OS / patch level	Vendor support	License
DA / HDA / A&E	Service identity	Capacity

Tag semantics and the twin model

ارزش داده زمانی حفظ می‌شود که شناسه تجهیز، زمان، کیفیت و واحد اندازه‌گیری همراه مقدار منتقل شود.



Field	Example / treatment
value / unit	12.4 bar, retain raw unit and conversion rule
sourceTime / ingestTime	UTC timestamps, distinguish age from transport delay
quality / status	Preserve raw StatusCode, flag stale / bad data
source / mappingVersion	Endpoint ID + tag key + versioned asset mapping

Illustrative record. Event IDs, sequence numbers and correction rules depend on the source interface.

Resilience and process independence

قطعی پلتفرم تحلیلی باید به توقف تحلیل محدود شود و استقلال کنترل در آزمون اثبات شود.

Failure	Expected behavior	Acceptance evidence
Twin backend unavailable	Queue within limit, then defined retention policy	Replay test + duplicate detection
Collector restart	Resume from durable checkpoint	Restart and sequence audit
Historian unavailable	Mark stale, reconnect with backoff	No uncontrolled polling burst
Source data gap	Backfill only if source history supports it	Gap ledger + recovery report
Integration disabled	Existing control operations continue	OT baseline comparison + operator sign-off

Buffering only protects data already acquired. Upstream loss needs source history or a separate recovery mechanism.

Primary DCS families

انتخاب کانکتور بر اساس خانواده و نسخه انجام می‌شود؛ نام برند به‌تنهایی کافی نیست.

Installed family	Documented interface candidate	Site verification
Honeywell Experion PKS	OPC UA on PKS Server from R510 History support depends on release	Release / updates, entitlement, access scope
ABB System 800xA	800xA History OPC UA Live / historical / events per product	History installation, endpoint and limits
ABB Freelance / AC 800F	Freelance OPC Server Classic adapter if required	Exact generation, OPC package, host support
Siemens PCS 7	Process Historian OPC UA option OS / WinCC route for live if supported	PH vs live service, installed option and license

وجود این قابلیت‌ها در هر سایت باید با فهرست دارایی، نسخه نصب‌شده و آزمون نمونه تأیید شود.

Additional DCS and SCADA families

پروتکل مشترک دریافت داده را ساده می کند؛ کنترل ظرفیت و مجوزها همچنان مخصوص هر محصول است.

Family	Interface candidate	Condition
Yokogawa CENTUM	Exaopc Classic / UA package	Model and release compatibility
Emerson DeltaV	Application Station DA / UA Continuous Historian HDA	Live, history and alarms verified separately
Schneider Foxboro	DCS OPC UA Server PSS 41S-6OPCUA	Server option installed and supported
Rockwell FactoryTalk	FactoryTalk Linx Gateway UA	Activation, tag access and capacity
Proficy iFIX / CIMPLICITY	Historian REST API for extraction	Historian version, API deployment and identity

Historian platforms such as AVEVA PI may aggregate several DCS families before ARG integration.

Plant interface survey

در هر سایت، مسیر مصوب خروج داده و مسئول فنی آن بر اساس بررسی شبکه و دارایی‌ها تعیین می‌شود.

- 01** Unit and use case: equipment scope, decisions, required freshness.
- 02** Source inventory: DCS family, release, Historian, export option.
- 03** Security path: zones, approved DMZ service or diode, hosting policy.
- 04** Interface contract: tags, time, quality, license and access owner.
- 05** Change authority: vendor support, MOC window, test and rollback.

خروجی این بررسی یک سند رابط و نقشه اتصال قابل تأیید است؛ آدرس‌ها و پورت‌ها از روی حدس تعیین نمی‌شوند.

Required equipment and services

اولویت با استفاده از زیرساخت موجود و مصوب است؛ تعداد نهایی میزبان‌ها پس از بررسی سایت و ظرفیت تعیین می‌شود.

Component	Deployment zone	Provisioning basis	Required check
Field instruments + DCS / PLC	Existing control zone	Reuse installed equipment	Approved measurements and tag ownership
Supported data export	OT server zone	Existing Historian / OPC / API; vendor option if absent	Release, license, service scope and capacity
Edge collector host	Approved OT zone	1 VM or industrial PC for a basic deployment*	Supported OS, durable queue, no IP forwarding
DMZ data service	Industrial DMZ	1 logical receiver / broker / replica service*	TLS, scoped publication and data retention
ARG application + data store	Enterprise / private DC	Reuse or provision the ARG hosting environment	Ingestion capacity, asset mapping and backup

* Design baseline, not a purchase quantity. Separate hosts or redundancy depend on the approved architecture.

Security infrastructure and optional equipment

اقدام امنیتی بر اساس سیاست سایت انتخاب می‌شوند؛ ارتباط یک‌طرفه و افزودنی برای همه پروژه‌ها الزام یکسان ندارند.

Component	Location	Provisioning basis	Required check
Firewall enforcement	OT / DMZ and DMZ / IT	Reuse approved boundary controls where available	Exact source, destination, port and initiator
Network ports + segmentation	Each approved zone	Existing managed switching / VLAN infrastructure	No uncontrolled bridge or dual-homed bypass
Identity, time and audit services	Approved local services	Service accounts, certificates and time source	Trust lifecycle, clock quality and audit export
Backup + queue storage	OT / DMZ / application	Capacity derived from retention and outage budget	Restore test, disk limits and overflow policy
Data diode + source/sink proxies	OT-to-DMZ boundary	Conditional: one supported unidirectional system	Protocol reconstruction, loss detection and maintenance
Redundant hosts / power	Per availability design	Conditional: size to the agreed recovery target	Vendor-supported failover and duplicate handling

A data diode replaces the approved transfer conduit. Its adapters and licenses form part of the equipment scope.

Installation procedure: OT preparation

نصب پس از تصویب سند رابط و مجوز تغییر انجام می شود؛ جزئیات هر محصول باید با نسخه نصب شده تطبیق داده شود.

Step	Action	Configuration / prerequisite	Evidence / owner
01 Survey + approval	Freeze the Interface Control Document	Endpoint, release, tag scope, rates, conduit and MOC approval	Approved ICD / asset owner
02 Prepare hosts	Provision in the approved OT / DMZ zones	Supported OS, host hardening, storage, local time, default-deny rules	Host baseline / OT and security
03 Install services	Install the approved collector and receiver	Approved package and checksum, service identity, backup, startup policy	Install record / integration team
04 Configure access	Set endpoint trust and telemetry permissions	Certificate trust + restricted account; deny process writes and control methods	Safe permission test / automation
05 Register data	Configure tag mapping and acquisition	Stable tag IDs, units, quality, timestamps, revised sampling and queue limits	Tag contract / integration team

Do not install on an operator or engineering workstation unless the vendor and asset owner explicitly approve it.

Commissioning procedure and rollback

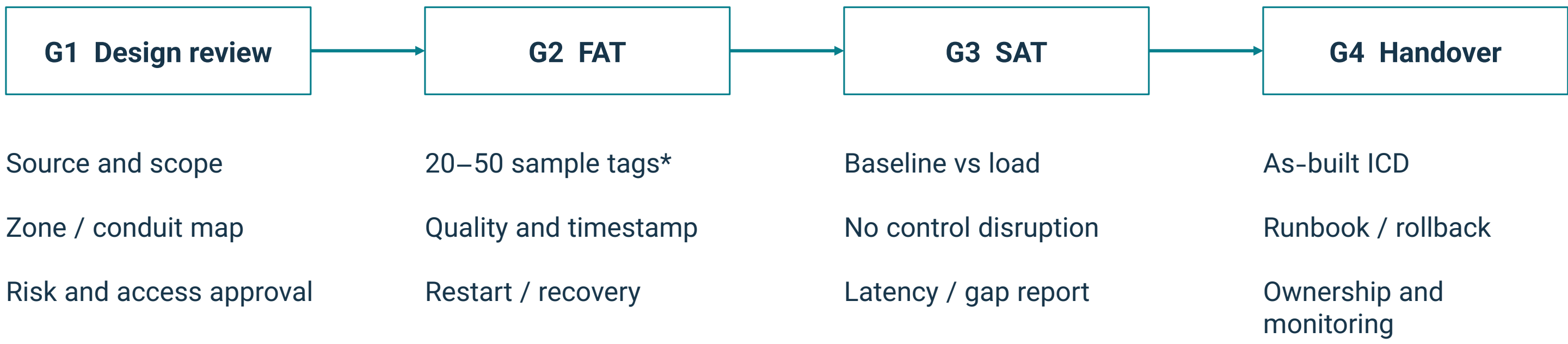
راهاندازی با آزمون محدود آغاز می‌شود و توسعه دامنه پس از تأیید کیفیت داده، بار و استقلال کنترل انجام می‌گیرد.

Step	Action	Configuration / test	Evidence / owner
06 Publish to DMZ	Enable the approved transfer service	TLS and destination allowlist; publish-only ACL; diode proxies if selected	Conduit test / security
07 Connect ARG	Read the published DMZ dataset	Scoped consumer identity, versioned asset mapping and duplicate handling	End-to-end record trace / ARG
08 FAT	Test representative tags and failures	Value / unit / time / quality; restart, downstream outage, replay and overflow	FAT report / joint team
09 SAT + ramp-up	Compare baseline and staged acquisition	CPU / network / service load, data age, gaps and control independence	Approved thresholds / operations
10 Handover + rollback	Release runbook and recovery plan	Stop integration services, revoke its access, restore approved configuration	Sign-off, backup and owners / joint team

Rollback removes the integration path only. Existing control, safety and historian services remain under plant change control.

Validation gates and acceptance evidence

شروع محدود برای اعتبارسنجی اتصال است؛ دامنه تجاری محصول به این آزمون محدود نمی شود.



Acceptance criteria

Approved read scope Data fidelity Bounded load Proven recovery

* Proposed test scope. Thresholds and observation duration require asset-owner approval.

Project responsibilities and deliverables

برای هر پروژه، مالک تصمیم، حدود مسئولیت و خروجی قابل تحویل مشخص می شود.

Owner	Decision / deliverable
Asset owner	Selected unit, approved data scope and export policy
Automation team	Supported interface, sample tags and vendor constraints
OT security	Conduit, hosting zone and authentication requirements
ARG	Interface design, adapter configuration and acceptance protocol

Design deliverable: Interface Control Document (ICD)

Appendix A Honeywell and ABB connection recipes

این مراحل برای تهیه تنظیمات اجرایی هستند؛ نام منوها و بسته‌ها باید با نسخه نصب‌شده تطبیق داده شوند.

Recipe	Engineering steps	Evidence to retain
Experion PKS	Identify server release and updates Verify UA option and read identity Validate live/history independently Test redundancy and session recovery	Endpoint export License / permissions Tag and failover results
800xA History	Verify History service and UA endpoint Map stable namespace URI + NodeId Test values, history and events as supported Measure subscription and query load	History configuration Service support matrix Capacity baseline
Freelance / AC 800F	Confirm generation and OPC Server Use vendor-supported host / adapter Keep Classic traffic inside approved OT zone Verify DA / HDA / A&E separately	Product/version record Adapter entitlement Classic compatibility test

Appendix B Siemens and Yokogawa recipes

مسیر داده زنده و مسیر تاریخچه می‌توانند سرویس‌ها و مجوزهای متفاوت داشته باشند.

Recipe	Engineering steps	Evidence to retain
Siemens PCS 7	Identify OS / WinCC and Process Historian Verify PH OPC UA module and license Choose live source separately if required Test retrieval range and redundancy	OS / PH release matrix UA service list Live vs history test
Yokogawa CENTUM	Identify CENTUM and Exaopc release Verify Exaopc UA Interface Package Use supported Classic path if required Check Exaquantum history export separately	CENTUM / Exaopc matrix Tag / alarm scope History access evidence

OPC UA Server capability, OPC UA Client capability and HistoryRead capability are separate checks.

Appendix C Other vendor connection recipes

تنظیمات هر خانواده در یک سند رابط مستقل ثبت می شود تا تغییرات نسخه قابل مدیریت باشند.

System	Preferred engineering entry point	Key check
DeltaV	Application Station for supported live access Continuous Historian HDA for history	UA option / DA host, historian scope, licenses
Foxboro	OPC UA Server package 41S-6OPCUA	Do not substitute FDC OPC UA Client driver
FactoryTalk	Linx Gateway UA endpoint and read identity	Activation, tag permissions, endpoint trust
Proficy	Historian REST API for raw / calculated values	API version, authentication, paging, time range

Appendix D Firewall and conduit schedule

هر ردیف باید قبل از اجرا با میزبان‌ها و پورت‌های واقعی تکمیل و توسط تیم امنیت تصویب شود.

ID / Initiator	Destination	Transport / purpose	Control
C-01 OT collector	Approved OT server	OPC UA / vendor API Telemetry read	Exact host + endpoint Least privilege
C-02 OT publisher	DMZ receiver	Approved TLS transport Data publication	Destination allowlist Publish-only topic ACL
C-03 IT consumer	DMZ data service	HTTPS / broker client Published data access	Read / subscribe rights Rate limit
M-01 OT admin	Managed OT host	Approved maintenance Separate from data path	Time bound access Audit and rollback

Data diode deployments replace C-02 with the validated one-way product path.

Appendix E Security and operational controls

حساب فقط خواندنی تنها یکی از کنترل هاست؛ اثر بار، مدیریت تغییر و استقلال سامانه نیز بررسی می شود.

- 01 Identity: application certificate + restricted service account.
- 02 Transport: approved encryption policy, trust list, certificate rotation.
- 03 Boundary: allowlisted conduits, no host bridging, separate admin path.
- 04 Safety: preserve SIS / ESD boundary, no process write or alarm acknowledge.
- 05 Operations: resource limits, patch review, backup and tested rollback.

A read-only connection still consumes server resources. Load and availability require measured acceptance.

Appendix F Capacity calculation example

این محاسبه روش برآورد را نشان می‌دهد و ادعای ظرفیت سامانه ارگ یا تجهیزات سایت نیست.

Assumption / result	Value	Qualification
Tag count / sample interval	10,000 / 5 s	Illustrative fixed-rate stream
Base acquisition rate	2,000 records/s	Excludes alarms and metadata
Serialized record size	160 bytes/record	Must measure actual encoding
Base payload throughput	0.32 MB/s = 2.56 Mb/s	Before TLS / protocol overhead
2-hour acquired-data buffer	2.304 GB	Before indexes, replication and margin
Catch-up at 6,000 records/s total	1 hour for a 2-hour backlog	4,000/s spare capacity while live continues

Source outages require upstream retention. Local buffering covers downstream outages after acquisition.

Appendix G Standards traceability

مراجع زیر مبنای طراحی‌اند؛ سطح امنیت هدف و انطباق نهایی با ارزیابی پروژه تعیین می‌شود.

Design topic	Reference	Verification artifact
Zones / conduits / target level	IEC 62443-3-2:2020	Risk assessment and approved topology
System security requirements	IEC 62443-3-3:2013	Allocated requirements and test evidence
DCS / IIoT boundary architecture	NIST 800-82r3 §5.4.1–5.4.2, Figs 18–19	Firewall and DMZ design review
Functional integration hierarchy	ISA-95	OT / enterprise function mapping
UA security and data access	OPC UA Parts 2, 4 §5.13, 11 §4	Endpoint, identity, data and recovery tests
UA PubSub over MQTT, if selected	OPC UA Part 14 §7.3.4	Profile, broker and payload validation

Appendix H Integration questions and answers

پاسخ کوتاه باید روی مسیر فنی، حدود مسئولیت و مدرک قابل آزمون متمرکز باشد.

Question	Engineering answer
Is internet connectivity required?	No. An owner-hosted deployment can consume DMZ data locally.
Must we change the PLC program?	Prefer an existing supported export interface. Any required change needs MOC.
Can read access affect production?	Yes, through load or failure propagation. Limit it and verify independence.
Can you guarantee zero data loss?	Only within an agreed failure envelope and proven source / buffer retention.
What if there is no OPC UA?	Use approved Historian API, Classic adapter or vendor export path.
What is the first deliverable?	An ICD with a supported endpoint, conduit, data contract and test criteria.

References Standards and architecture

لینک کامل مراجع در یادداشت هر اسلاید مرتبط نیز درج شده است.

- S01** [NIST SP 800-82 Rev. 3](#) §5.4.1–5.4.3, Figures 18–21
- S02** [IEC 62443-3-2:2020](#) System risk assessment, zones, conduits and SL-T
- S03** [IEC 62443-3-3:2013](#) System security requirements and capability levels
- S04** [ISA-95](#) Enterprise-control functional integration
- S05** [OPC UA Part 2](#) §4 Security Model and §9 Certificate Management
- S06** [OPC UA Part 4](#) §5.13 MonitoredItem Service Set
- S07** [OPC UA Part 11](#) §4 Historical Access concepts
- S08** [OPC UA Part 14](#) §7.3.4 MQTT transport mapping

References Vendor and deployment evidence

قابلیت محصول به نسخه و مجوز وابسته است؛ وضعیت نصب باید برای هر سایت جداگانه بررسی شود.

V01	<u>Honeywell System HINTS</u> October 2021, Experion PKS R510 / R520 interfaces	V08	<u>Schneider Electric Foxboro</u> PSS 41S-6OPCUA, OPC UA Server, January 2025
V02	<u>ABB System 800xA 6.2</u> System Guide Summary, 7PAA007862 en C	V09	<u>Rockwell FactoryTalk Linx Gateway 6.60</u> OPC UA Server quick start and security
V03	<u>ABB Freelance 9.2 SP1</u> Getting Started, 3BDD012560R05	V10	<u>Proficy Historian 9.1</u> REST APIs reference manual, raw data access
V04	<u>Siemens SIMATIC PCS 7</u> Process Historian OPC UA Server option and license	V11	<u>AVEVA PI System</u> PI Web API developer technologies
V05	<u>Yokogawa Exaopc</u> CENTUM OPC Server and OPC UA Interface Package	E01	<u>AWS IoT SiteWise</u> Onsite gateway collecting from Historian / industrial server
V06	<u>Emerson DeltaV OPC HDA</u> Read-only access to DeltaV Continuous Historian	E02	<u>AWS Industrial Digital Twin guidance</u> Reference implementation using SiteWise Edge
V07	<u>Emerson DeltaV Application Station</u> Application Station Software Suite data sheet	E03	<u>GE Linde deployment report</u> 2009 historical case, more than 350 sites