

Site Assessment & Implementation Plan

فرم برداشت و برنامه اجرا برای استقرار Digital Twin، سامانه مستقل ARG_AI، ML، RAG و LLM در پالایشگاه، پتروشیمی یا کارخانه.

Document control	Entry
Site / organization	_____
Plant / process area	_____
Assessment date / revision	_____
Client IT / OT / process focal points	_____
ARG lead and team	_____
Site confidentiality class	_____

این سند فرم قابل تکمیل است؛ خانه‌های خالی، ظرفیت‌ها و مسیرهای شبکه باید با اطلاعات و مجوز همان سایت تکمیل شوند. وجود ML و RAG در ARG_AI بنا بر اعلام مالک محصول مبناست؛ جزئیات نسخه سرور در بازدید فنی ثبت می‌شود.

Deliverable	Gate
Site baseline	Signed OT topology, source systems, inventory and use cases
Implementation package	ICD, qualified BOM, schedule, RACI and FAT/SAT plan
Go-live	Production as-built, evidence, rollback and operations handover

1. Assessment boundaries and use cases

نخست دامنه فرایند و تصمیم عملیاتی مشخص می شود؛ پاسخ هر ردیف باید صاحب، داده واقعی و معیار پذیرش داشته باشد.

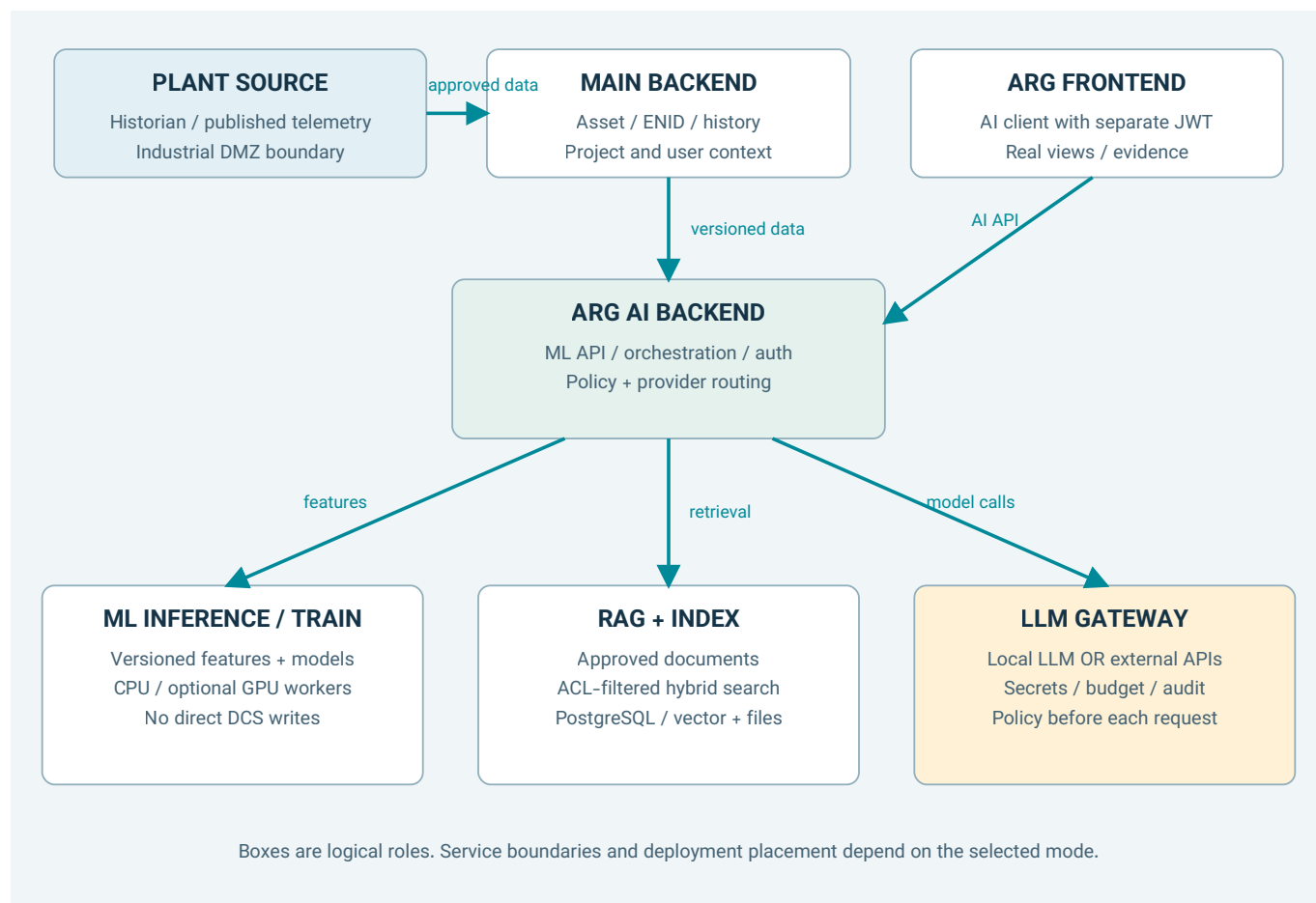
ID	Unit / asset / ENID	Use case & decision	Owner / priority	Baseline / KPI
UC-01	_____	Anomaly / failure triage	_____	_____
UC-02	_____	Energy / consumption forecast	_____	_____
UC-03	_____	SOP / manual answer with citations	_____	_____
UC-04	_____	Scenario / what-if	_____	_____

Question to resolve	Site answer
Will the deployment be site-only, WAN-assisted or hybrid?	_____
Are these advisory outputs or inputs to a separately approved workflow?	_____
What is the operator response to stale, missing or bad-quality data?	_____
Which languages, shifts and engineering teams use the system?	_____

برای هر مورد: **asset boundary**، افق زمانی، تصمیم قابل پشتیبانی، تعریف خطا، معیار اقتصادی و خط پایه ثبت شود.
هیچ مسیر نوشتن مستقیم از AI به DCS یا SIS در این طرح پیش فرض نیست.

2. Site topology and system inventory

نقشه واقعی شبکه را مالک OT تأیید می‌کند. این شکل نقش‌های منطقی را نشان می‌دهد و جای نقشه As-Is سایت را نمی‌گیرد.



System	Vendor / version	Zone & owner	Read interface / export	Evidence
DCS / PLC / SCADA				
Historian / OPC server				
Main Backend / asset registry				
ARG_AI existing ML & RAG				

پیوست بازدید: topology نسخه‌دار، VLAN/subnet، firewall/DMZ، نقاط جمع‌آوری داده و مالک تغییرات.
اطلاعات حساس IP و حساب‌ها فقط در پیوست کنترل‌شده سایت ثبت شوند.

3. OT data publication survey

برای هر منبع، مسیر خواندن تأییدشده، نرخ و کیفیت داده را ثبت کنید تا ICD بدون حدس تهیه شود.

Source ID / tag	Asset / ENID	Unit / time / quality	Protocol & server	Rate / retention / owner
T-001				
T-002				
T-003				
T-004				
T-005				

Check	Required evidence
History access	Sample time series, timezone, gaps, status and sampling policy
Naming	Tag-to-asset-to-ENID reconciliation and unit normalization
Conduit	Source initiator, direction, firewall change, TLS, ACL and rate cap
Failure	Historian outage, stale state, buffer/queue and recovery test

داده لازم را از Historian یا انتشار تأییدشده Industrial DMZ بگیرید؛ دسترسی به شبکه کنترل فقط طبق طراحی مصوب OT انجام می‌شود.

4. ML and RAG current-state discovery

در این صفحه قابلیت موجود ثبت می‌شود تا استقرار بر اجزای واقعی ARG_AI تکیه کند.

ARG_AI function	Version / actual implementation	Input and storage	Owner / evidence
ML train / async train	_____	_____	_____
ML analyze / drift / health	_____	_____	_____
RAG ingest / OCR / indexing	_____	_____	_____
RAG retrieve / citation / ACL	_____	_____	_____
Chat / provider settings	_____	_____	_____
Digital twin simulation	_____	_____	_____

Verification	Evidence artifact
Released build	Binary/source ref, dependencies, config schema and OpenAPI
ML lineage	Real dataset → features → labels → job → model artifact → inference
RAG lineage	Approved source → parse → chunk → index → permitted retrieval → citation
Isolation	Tenant, project, role and document revocation tests

5. Knowledge and document survey

اسناد پیش از ورود به RAG باید صاحب، نسخه، طبقه‌بندی و سطح دسترسی داشته باشند.

Collection	Format / count / OCR	Owner & revision	Classification / ACL	Refresh / expiry
SOP / operating instruction	_____	_____	_____	_____
Manual / datasheet	_____	_____	_____	_____
P&ID / engineering drawing	_____	_____	_____	_____
Maintenance / incident report	_____	_____	_____	_____

Question	Answer
Are scanned Persian documents searchable after OCR?	_____
How are superseded drawings removed from retrieval?	_____
Are diagram images required in answers?	_____
What is the approved review set of 100 Persian/English questions?	_____

ارزیابی RAG شامل صحت‌بازیابی، استناد دقیق، رد پاسخ بی‌مدرک و جلوگیری از بازیابی اسناد خارج از دسترسی است.

6. AI deployment and egress decision

نوع استقرار با سیاست داده، اتصال WAN و بار واقعی تعیین می‌شود.

Decision	Site answer / gate
Local-only, API-led or hybrid	_____
Permitted model and embedding providers	_____
Data classes allowed to leave site	_____
Concurrent sessions / context / p95 goal	_____
Expected training frequency and inference volume	_____
API budget, rate limits and outage policy	_____
GPU candidate, model license and offline asset staging	_____

Control	Approval evidence
Local LLM	Version-pinned model, driver/runtime, VRAM/KV benchmark at target load
External API	Egress proxy allowlist, key vault, classification routing, audit and billing
Agents	Read-only tool allowlist, user scope, bounded calls and human review

مقدار GPU و سرور از اندازه مدل به تنهایی تعیین نمی‌شود؛ بارسنجی با طول متن و تعداد کاربران همزمان شرط خرید قطعی است.

7. Infrastructure and prerequisites

واحد IT این فرم را قبل از نصب تکمیل می کند؛ تجهیزات قطعی در BOM جداگانه پس از بارسنجی قفل می شوند.

Role	Host / OS / compute	Storage / backup	Network / DNS / TLS	Owner / ready
ARG_AI application				
Existing ML worker / model registry				
Existing RAG DB / index / source docs				
Local LLM host (if selected)				
Provider gateway / outbound proxy				
Monitoring / logs / secrets				

Prerequisite	Status / ticket
Virtual or physical host and OS hardening	
NTP, DNS, certificate issuance and service identity	
Firewall/DMZ flows and signed port register	
Storage, snapshot, backup schedule and restore location	
Staging and rollback of released ARG_AI build	

دسترسی عملیاتی با حساب خدماتی کم دسترسی، تفکیک محیط آزمایشی و تولید، و مسیر تغییرات مصوب سایت انجام شود.

8. Interface register for the ICD

هر ردیف این فرم باید به قرارداد رابط نسخه‌دار و آزمون end-to-end تبدیل شود.

ID / initiator	Destination / endpoint	Transport & port	Data / auth / direction	Rate / error handling / approver
I-01 Historian export				
I-02 ARG Main Backend				
I-03 Browser → ARG_AI				
I-04 ARG_AI → ML				
I-05 ARG_AI → RAG				
I-06 ARG_AI → local LLM				
I-07 Gateway → external API				

ICD بعدی payload/schema, time semantics, retries, timeout, pagination, idempotency, rate limit, versioning و mapping خطا را برای هر ردیف اضافه می‌کند.

9. Step-by-step implementation schedule

ترتیب اجرا به صورت gate است؛ زمان‌بندی نهایی پس از پاسخ سایت و دسترسی به نسخه واقعی نرم‌افزار تثبیت می‌شود.

Phase	Work and tangible output	Exit gate / sign-off
P0 Scope	2–3 use cases; stakeholder and KPI baseline	Process owner approves scope
P1 Survey	OT topology, historian sample, ARG_AI release and document inventory	OT + IT sign site baseline
P2 Detailed design	ICD, ACL/data policy, deployment mode, sizing benchmark and BOM	Architecture + security approve
P3 Platform	Servers, network/TLS, backup, secrets, ARG_AI release and monitoring	Infrastructure smoke and restore test
P4 Data & models	Real features to existing ML; docs into existing RAG; LLM routing	Lineage, retrieval and prohibited-route tests
P5 Integrated FAT	End-to-end scenario, failure, performance, permission and rollback	Joint FAT report
P6 Site SAT	Controlled data ramp, operators, as-built and acceptance	Site SAT and operations handover

وابستگی مهم: تا تأیید مسیر داده و نمونه واقعی Historian، آموزش مدل و صحت سناریوی صنعتی قابل پذیرش نیست.

10. Responsibility matrix

برای هر فعالیت، R انجام‌دهنده، A تأییدکننده، C مشاور و I دریافت‌کننده اطلاع تعیین می‌شود.

Activity	Plant OT	Plant IT/security	Process owner	ARG platform / AI
Historian publication	A/R	C	C	I
Firewall and external egress	C	A/R	C	C
Asset mapping and label definition	C	I	A/R	R
ARG_AI installation and integration	I	C	C	A/R
RAG document release and ACL	I	C	A/R	R
FAT/SAT evidence and approval	C	C	A	R
Backup and incident response	I	A/R	I	R

نمونه اولیه RACI است؛ نام اشخاص، حق تصویب و قرارداد پشتیبانی در جلسه آغاز پروژه تکمیل و امضا می‌شود.

11. FAT / SAT and operational handover

پذیرش با شواهد ثبت شده انجام می شود؛ ستون نتیجه تا زمان اجرای آزمون خالی می ماند.

Test ID	Method / required evidence	Target agreed by	Result / defect
AT-01	Trace 10 real tags: OT source → feature → ML result → UI	_____	_____
AT-02	Stale, bad-quality, missing and shifted timestamps	_____	_____
AT-03	100 reviewed RAG questions, citations and denied-role access	_____	_____
AT-04	LLM route by data class, API 429/ outage, no forbidden egress	_____	_____
AT-05	Target load p95/p99, concurrency and GPU/CPU/storage trend	_____	_____
AT-06	Backup restore, index rebuild, model rollback and key rotation	_____	_____
AT-07	Packet evidence of approved DMZ flows and no AI→controller write	_____	_____

Handover pack	Owner / status
As-built topology, ICD and configuration baseline	_____
Runbooks, accounts, certificates and rotation ownership	_____
Training, monitoring dashboard, drift review and support escalation	_____
Signed defects, exceptions and site acceptance	_____

12. Open items and sign-off

این برگه تصمیم‌های باز و مسئول رفع آنها را به سند اجرایی بعدی منتقل می‌کند.

ID	Open item / required artifact	Owner	Due / decision
O-01	ARG_AI release, API specification and exact ML/RAG persistence	_____	_____
O-02	Approved OT publication and historian sample	_____	_____
O-03	Document repository ownership and ACL matrix	_____	_____
O-04	WAN/provider policy and model candidate	_____	_____
O-05	Measured capacity and final procurement BOM	_____	_____

Approval	Name / date / signature
Plant OT	_____
Plant IT and security	_____
Process owner	_____
ARG engineering / AI	_____

این سند یک **baseline** قابل تکمیل برای سایت است؛ هیچ مقدار خالی یا نمونه‌ای به‌عنوان مشخصات تأییدشده مشتری تلقی نمی‌شود.

References: [NIST SP 800-82 Rev. 3](#) · [NIST AI RMF](#) · ARG client API paths at pinned revisions in the prior ARG_AI infrastructure document.