A Capability Framework and Certification System for Industrial Robot Service Professionals

Six Capability Domains	
Domain 1	*Service Lifecycle Management*
Domain 2	*Fault Diagnosis & Technical Support*
Domain 3	*Remote Service & Digital Operations*
Domain 4	*SLA Design & Service Commitment*
Domain 5	*Cross-Platform Service Procedures*
Domain 6	*AI/ML System Service Methods*

Robotics Service Framework

White Paper

Version 1.0

Initiated and published by

RobotToday.com

About This Document

Document Name	RSF Robotics Service Framework — White Paper
Version	v1.0 (Initial Public Release)
Publication Date	2026
Initiating Organization	RSF Initiative, with RobotToday.com as the initiating platform
Initial Public Release	Chapter 1 + Chapter 2 with Appendices
Target Audience	Robotics service professionals (including field service engineers and service leads)
Language	English (primary)
Supporting Resources	Certification inquiries · ATC partnership · Framework feedback: framework@robottoday.com
Copyright Notice	Copyright belongs to RSF Initiative. No part of this document may be reproduced in full without written authorization. Citations must acknowledge the source (RSF Robotics Service Framework v1.0, RobotToday.com) and obtain written permission.

RSF Positioning **The Robotics Service Framework (RSF)** is the world's first professional capability framework to systematically cover the full service lifecycle of industrial robots. Built upon the compliance foundation of the ISO/IEC standards landscape, RSF establishes dedicated systems for service-engineer competence certification, service-quality commitment, and cross-platform service procedures — addressing capability-layer needs that sit, by design, outside the scope of existing standards.

RSF takes the six capability domains as its content backbone, the four-tier certification system (Professional · Specialist · Expert · Master) as the capability-development pathway, and the ATC Authorized Training Center network as its implementation vehicle, establishing a common professional vocabulary and capability standard for the robotics service industry.

Standards Reference Notice *International standards cited in this document (ISO, IEC, ANSI/RIA series) are referenced for descriptive purposes only. For any technical limits, parameters or specifications related to cited standards, the official published text of the respective standard organization shall be the authoritative source. This document does not replace any international standard and does not constitute a compliance certification document.*

Table of Contents

Table of Contents

Key Terms Glossary (Selected)

Abbreviation / Term	English Full Name	Definition
RSF	*Robotics Service Framework*	Robotics Service Framework — the professional capability framework system defined in this document
6D	*Six Capability Domains*	The six core capability modules of the RSF framework (Domain 1 – Domain 6)
Professional	*RSF Professional*	Entry tier of the RSF four-level certification; masters execution-layer service capability (Know-How)
Specialist	*RSF Specialist*	Second tier of the RSF four-level certification; masters independent handling of complex faults (Know-Why)
Expert	*RSF Expert*	Third tier of the RSF four-level certification; capable of service-system design and cross-domain integration (Know-Across)
Master	*RSF master*	Highest tier of the RSF four-level certification; capable of industry-standard formulation and technology-roadmap decisions (Know-Beyond)
ATC	*Authorized Training Center*	RSF Authorized Training Center — responsible for course delivery and certification-exam execution
SLA	*Service Level Agreement*	Service Level Agreement — contractual document that quantifies service-quality commitments
OEE	*Overall Equipment Effectiveness*	Overall Equipment Effectiveness = Availability × Performance × Quality
MTTR	*Mean Time to Repair*	Mean Time To Repair — average time from work-order opening to equipment return to normal operation
RUL	*Remaining Useful Life*	Remaining Useful Life — predicted remaining service time of a critical component before maintenance threshold
RDT	*Robot Digital Twin*	Robot Digital Twin — physical-digital virtual mirror system synchronized in real time
UCSP	*Unified Cross-Platform Service Procedures*	Unified Cross-Platform Service Procedure framework
PSC	*Platform Service Card*	Platform Service Card — standardized document format for platform-specific service procedures
MLOps	*Machine Learning Operations*	Machine Learning Operations — methodology for full-lifecycle management of AI models
RaaS	*Robots as a Service*	Robot-as-a-Service — subscription deployment model in which the service provider retains equipment ownership
RAG	*Retrieval-Augmented Generation*	Retrieval-Augmented Generation — AI technique combining knowledge-base retrieval with large language models
CPD	*Continuing Professional Development*	Continuing Professional Development — RSF certification's continuous-learning credit system
OTA	*Over-The-Air*	Over-The-Air update — remote deployment of equipment firmware or software via network
LOTO	*Lockout/Tagout*	Lock-Out Tag-Out — operating procedure for safely isolating

		energy sources during mechanical maintenance
FTFR	*First-Time Fix Rate*	First-Time Fix Rate — share of work orders whose root cause is correctly identified on the first visit
KFL	*Known Fault Library*	Known-Failure-Mode Library — organizational knowledge asset that stores diagnostic experience in structured form
VDA 5050	*VDA 5050 Interface Specification*	Industry-standard communication protocol for AMR (Autonomous Mobile Robot) fleets
PINN	*Physics-Informed Neural Network*	Physics-Informed Neural Network — AI model fusing physical equations with data-driven learning

Full Glossary in Appendix D · Bilingual (English / Chinese)

Chapter 1

RSF Framework — General Overview

The large-scale industrial deployment of robotics is advancing far faster than expected. The installed base of industrial arms, collaborative robots, autonomous mobile robots, and now humanoid robots is growing rapidly, generating an unprecedented scale of demand for maintenance, upgrade, fault handling, and end-of-life management of these systems. Yet the capability system that should support this demand — who performs the service, how their competence is assessed, and how service quality is quantitatively committed — still lacks systematic framework support.

This chapter builds the general overview of RSF from three progressive perspectives. Section 1.1 analyses the existing international-standards landscape to reveal the five key gaps in robotics service and explains why they fall outside the design scope of those standards. Section 1.2 establishes the precise structural relationship between RSF and the existing landscape through a three-layer nesting model that defines what RSF is, what it co-exists with, and what it fills. Section 1.3 defines the scope and usage of RSF, identifying which scenarios this framework applies to and how readers should use each chapter in practice.

1.1 Five Capability-Layer Needs in Robot Service

International standardisation has been at work in the robotics field for decades, and the results are undeniable. ISO 10218-1/-2 (2025) establishes strict technical boundaries for the safety design and integration of industrial robots; IEC 61508 provides the mathematical framework for quantitative argumentation of safety functions; ISO 9001 and ISO 55001 set management baselines for service organisations from the perspectives of quality management and asset-lifecycle management respectively. Together, these standards form the compliance floor of robotics service operations, and they are the starting point and outer boundary of everything RSF contains.

Understanding a standard's value precisely also requires understanding its boundaries precisely. ISO 10218-2, in its clauses on operational management and information for use, explicitly requires maintenance personnel to be "competent persons," but the standard neither defines competence tiers nor prescribes assessment methods, nor offers a certification pathway — the specification of competence requirements is left entirely to the user organisation. This is by design: a safety standard's job is to set the floor; constructing a competence-certification system is outside its scope. ISO 55001 is similar: it requires the organisation to establish a maintenance strategy and track asset status, but it does not prescribe who executes that strategy or how their competence is assessed.

What is, by design, a reasonable empty space has — under today's rapid evolution of robotics technology — become a systemic industry gap. Robot systems have evolved from purely mechanical devices to mechatronic systems, and now to intelligent systems carrying AI perception and decision layers; the resulting service complexity far exceeds the coverage of any single existing framework. The following five key gaps constitute the fundamental rationale for RSF's existence.

Capability Layer 1 — Building a Service-Engineer Competence Certification System

ISO 10218 calls for "competent persons," but no current robot-specific ISO/IEC technical standard anywhere defines competence tiers, assessment dimensions, or certification pathways for robot-service engineers. The automotive industry has the ASE certification system; aviation maintenance has the FAA/EASA licensing regime; IT services have the ITIL certification tiers — the robotics-service industry has no equivalent. The direct consequences are several: employers cannot objectively assess engineer competence, customers cannot compare service providers' professional credentials, and the market cannot form effective quality-signalling. The gap leaves the robotics-service market in a state of competence invisibility, which in turn suppresses providers' incentives to invest in professional development.

Capability Layer 2 — Building a Cross-Platform Service Lifecycle Framework

Existing safety standards are highly product-typed: ISO 10218 covers industrial arms, ISO/TS 15066 covers cobots, ISO 3691-4 covers mobile robots, and ISO 13482 covers service robots. This product-type-based structure is technically sound for safety design, but creates fundamental difficulties in service management. In practice, robot application scenarios are almost always heterogeneous — a typical modern manufacturing plant may operate six-axis industrial arms, cobots, and AMRs simultaneously, the three platform classes falling under three separate standards regimes, with no existing standard providing a unified cross-platform service lifecycle framework. There is no normative basis for unifying escalation paths, designing consistent maintenance strategy, or managing engineers' authorisation across platforms.

Capability Layer 3 — Building Service Procedures for AI/ML-Integrated Systems

ISO 10218:2025 made important updates in functional safety, but the logical foundation of its safety framework remains deterministic control systems. Modern robots integrate deep-learning perception layers, reinforcement-learning policy layers, and adaptive control layers — their failure modes are probabilistic: model drift, out-of-distribution inputs, and reward-function misalignment cannot be fully captured by traditional FMEA or fault-tree analysis, nor mapped to deterministic fault codes and troubleshooting trees. ISO/IEC 42001 (2023) establishes a governance framework for AI management systems, but does not reach the operational-layer procedures that field engineers need for diagnosing, recording, and judging AI-layer faults. As commercial deployment of AI-enabled robots accelerates, this gap is widening at a noticeable rate.

Capability Layer 4 — Building an SLA Framework for Robotics Service

Across the entire ISO/IEC standards corpus, no document defines response-time tiers, availability-commitment metrics, escalation triggers, or SLA-performance assessment methods for robotics service. IT has ITIL's SLA design framework and the certifiable ISO/IEC 20000-1 implementation standard; aviation MRO has MEL (minimum equipment list) and AOG (aircraft-on-ground) response protocols — the robotics-service field has no equivalent normative language. Service-contract negotiations are conducted on each side's non-standard understanding of the terms, which protects neither the customer nor the provider's ability to build a quantifiable quality-commitment system.

Capability Layer 5 — Building Specifications for Remote Service and Service-Data Management

ISO 27001 provides a robust management-system framework for information security, and IEC 62443 covers industrial control-system cybersecurity — neither addresses the operational specifications of robotic remote diagnostics: who is authorised to initiate a remote connection, how diagnostic data is classified for storage and access, how update authority is allocated for digital-twin models, what the service-verification procedure is for OTA firmware push. ISO 23247 provides a reference architecture for digital-twin manufacturing but again does not descend to the service-procedure layer. Remote service has become one of the principal delivery modalities of robotics service, yet its operational boundaries remain in a standards vacuum.

Table 1.1-1 RSF Five Capability Layers and the Division of Responsibilities with Existing Standards

Gap No.	Gap Area	Capability-Layer Content and RSF's Contribution
Layer 1	**Service-Engineer Competence Certification**	ISO 10218 calls for "competent persons," but no current robot-specific ISO/IEC technical standard defines competence tiers, assessment dimensions, or certification pathways for robot-service engineers. Direct consequence: competence invisibility and market-signal failure.
Layer 2	**Cross-Platform Service Lifecycle Management**	Existing standards are organised by product type (industrial arm / cobot / AMR / service robot); no unified cross-platform service lifecycle framework exists. Direct consequence: fragmented procedures in heterogeneous fleets, and an inability to standardise escalation paths.
Layer 3	**AI/ML System Service Procedures**	ISO 10218:2025 is built on a deterministic-systems framework and cannot cover probabilistic failure diagnosis of AI perception and policy layers. ISO/IEC 42001 stops at the governance level and does not reach field operational procedures.
Layer 4	**Robotics Service SLA Framework**	No ISO/IEC standard defines response-time tiers, availability commitments, or SLA-performance metrics for robotics service. Direct consequence: no common language in service-contract negotiation, and no objective basis for accepting quality commitments.
Layer 5	**Remote Service and Data-Management Specifications**	ISO 27001 / IEC 62443 do not cover remote-diagnostic operational procedures, digital-twin access-authority allocation, or OTA service-verification procedures. Direct consequence: remote-service operational boundaries sit in a standards vacuum.

Structural conclusion These five capability-layer needs share a defining characteristic: each sits, by design, outside the scope of the existing standards landscape. Existing standards precisely answer "what is a safe robot system" — and do so with rigour and authority. The complementary set of questions — "who maintains it, how is competence assessed, how is service quality committed" — lies, from the outset, in the service-capability layer above the compliance baseline. This is a sound and intentional division of responsibilities among standards bodies; it is also precisely where RSF makes its contribution. RSF builds that service-capability layer on top of the compliance baseline, forming an inheritance-and-supplement relationship with the existing landscape — not a replacement, but a purposeful continuation.

1.2 Three-Layer Nesting Model — RSF and Existing Standards

Understanding the relationship between RSF and the existing standards landscape requires a precise structural model. Saying simply that RSF "is based on" or "references" existing standards invites two misreadings: first, that RSF is merely a repackaging of those standards; second, that RSF is in competition with them. Neither is accurate. The relationship is a three-layer nesting structure — an outer layer of compliance baseline, a middle layer of RSF framework content, and an inner layer of operational pattern reference. Each layer has explicit boundaries of responsibility, with no intrusion across them, and together they form the complete robotics-service competence system.

Table 1.2-1 RSF Three-Layer Nesting Model

Tier	Name	Source Authority	Core Responsibilities
Outer Layer	**Compliance Baseline**	ISO/IEC international standards (some legally binding)	Sets the floor. Defines the statutory boundaries for robot-system design and field operations; all RSF content is conditional on conformance with this outer layer.
Middle Layer	**RSF Framework**	RSF Initiative — original framework content	Fills the gaps. Defines service-engineer competence tiers, assessment dimensions, certification pathways, and service procedures — answering "who does it, how it is done, and how the quality is assessed."
Inner Layer	**Operational Pattern Reference**	Automotive 4S system, ITIL (operational patterns reinterpreted for robotics)	Provides patterns. Operational practices validated at large market scale, integrated into RSF's operational design in a translated, robotics-specific form.

1.2.1 Outer Layer · Compliance Baseline

The outer layer consists of ISO/IEC international standards and constitutes the statutory boundary of the whole system. Its defining feature is that these standards are mandatory: ISO 10218-1/-2 has de facto legal force under the EU Machinery Directive (2006/42/EC); IEC 61508's SIL-level assessment is unavoidable in functional-safety certification; ISO 45001 has been incorporated into occupational-health-and-safety regulations in many countries.

The outer layer's job is to set the floor. Any service engineer performing any on-site robot operation must first operate within the outer compliance baseline. All RSF course content and certification requirements are conditional on conformance with the outer-layer standards; RSF does not modify, bypass, or replace any outer-layer standard. The outer layer also has the property of stability — ISO standards are typically revised on a five-year systematic cycle. RSF takes the currently-valid version of each outer-layer standard as its baseline and synchronously revises related training content when a standard is updated. Citations in this document are based on the current valid version of each referenced standard, with the ISO 10218 series in its 2025 edition.

1.2.2 Middle Layer · RSF Framework

The middle layer is RSF's core contribution and the direct response to the five capability-layer needs described in §1.1. The outer compliance baseline answers "what safety requirements should the robot system satisfy"; the middle RSF framework answers a different set of questions: what competence the service engineer should possess, how that competence is tiered and assessed, what procedures the service process should follow, and how service quality is defined and committed.

The middle-layer framework is built from four core components: a competence-tier system (Professional, Specialist, Expert, Master, organised by deepening cognitive dimension — see §2.3); definitions of the six capability domains (Service Lifecycle Management, Fault Diagnosis & Technical Support, Remote Service & Digital Operations, SLA Design & Service Commitment, Cross-Platform Service Procedures, AI/ML System Service Methods — see Chapters 3–8); the RSF Service Maturity Model (RSF-MM, Levels 0–5, covering an organisation's service-capability evolution path; planned for release in v2.0); and a certification-and-authorisation mechanism that links competence certification with the engineer's authorised scope of work — making certification an authorisation, not just a credential.

The four-tier system organises engineer development along a deepening cognitive dimension — Professional (Know-How), Specialist (Know-Why), Expert (Know-Across), and Master (Know-Beyond) — with parallel Engineer and Service Manager tracks at every tier. Professional covers SOP execution and routine maintenance; Specialist handles complex cross-layer faults and initial team management; Expert leads cross-domain integration, complex-customer operations and ATC-system design; Master sets technology roadmaps, contributes to industry standards, and shapes global service strategy. The complete tier-by-tier definitions — including responsibilities for both tracks — are given in Table 9.2-1 (§9.2).

1.2.3 Inner Layer · Operational Pattern Reference

The inner layer is drawn from the automotive 4S service system and ITIL's structural design of service management. Placing them in the inner layer reflects an important RSF design judgement: these systems supply operational thinking validated at large market scale; their value lies in practical maturity rather than regulatory authority.

The automotive 4S system offers direct reference value to RSF along four dimensions: the structural logic of tiered-technician certification linked to authorised work scope (the ASE system — adopted in its entirety by RSF's four-tier certification); the closed-loop service process "appointment → reception → diagnosis → repair → delivery → follow-up" (translated into RSF's eight-step on-site service procedure); CSI/NPS-based customer-satisfaction tracking (applied to quality assessment of the RSF training system and to ATC reviews); and the ABC parts-inventory model (applied to RSF Domain 1's spare-parts procedure). Each adoption is conditional on a clearly drawn transformation boundary — AI-layer fault diagnosis, software/firmware service procedures, and multi-brand fleet management cannot be ported from the 4S system and require original RSF design (see Appendix B for the full adoption logic and transformation boundary).

Table 1.2-2 Three-Layer Nesting — Division of Responsibilities and Inter-Layer Logic

Tier	Core Question Answered	Source of Authority	RSF's Relationship
Outer Layer — Compliance Baseline	What safety requirements should the robot system satisfy?	Mandatory ISO/IEC standards	RSF takes this as a precondition; it conforms but does not modify
Middle Layer — RSF Framework	Who maintains the system? How is competence assessed? How is service quality committed?	RSF Initiative (original framework content)	RSF's core contribution, filling the five gaps that sit above the outer layer
Inner Layer — Operational Pattern Reference	How should service operations be organised and executed?	Automotive 4S system / ITIL (translated)	RSF's operational reference, integrated after explicit transformation

The overall logic of the three-layer structure is: the outer layer sets the boundary, the middle layer fills the gaps, and the inner layer provides patterns. Together they constitute a complete robotics-service competence system; each layer has its own source of authority and scope of responsibility; the inter-layer relationships are clear, with no overlap and no conflict.

1.3 Scope and Usage of the RSF Framework

RSF is a competence framework and operational reference system aimed at robot-service engineers and service managers. Making the scope and usage of RSF explicit helps readers from different backgrounds use this document in the most effective way and avoids over-interpretation or mis-application.

1.3.1 Robot Platform Types in Scope

The RSF framework applies to service activities for the following types of robot system:

Robot Type	Typical Representatives	RSF Framework Notes
Industrial Arm **Industrial Robot Arm**	Six- or seven-axis industrial robots (Fanuc, ABB, KUKA, Yaskawa)	All six RSF capability domains apply fully; Domains 1–5 form the main framework layer, and Domain 6 applies selectively depending on the degree of AI integration
Cobot **Collaborative Robot (Cobot)**	UR series, FANUC, KUKA Yaskawa、Doosan Robotics、Franka	All RSF framework content applies; force-and-torque verification per ISO/TS 15066 has dedicated procedures in Domains 1 and 5
Autonomous Mobile Robot (AMR)	MiR, Locus Robotics, Amazon/KIVA, Addverb, Geek+, Standard Robots	RSF framework applies; SLAM navigation and path-planning layers receive dedicated treatment in Domains 2 and 6
Service Robot	Commercial service robots, delivery robots, inspection robots	RSF framework applies; ISO 31101:2023 provides the scenario risk-assessment basis for Domain 4 (SLA Design)
Humanoid Robot **Humanoid Robot**	Boston Dynamics Atlas, Unitree H1/G1, UBTECH Walker	RSF framework applies; multi-modal perception and embodied-AI components receive a dedicated service methodology in Domain 6, updated as the technology evolves

1.3.2 Applicable Service Scenarios

RSF covers service activities across the full robot lifecycle from delivery to decommissioning, including:

On-Site Service

Service activities performed by engineers at the customer site — installation and commissioning, preventive maintenance, fault response and repair, end-of-life equipment disposition. This is the most central application scenario of the RSF framework, with direct coverage across all six capability domains.

Remote Service

Diagnostic, monitoring, and service-delivery activities conducted via remote connection, digital twins, and predictive-maintenance platforms. Covered specifically by Domain 3 (Remote Service & Digital Operations).

Service Management

Internal service-strategy formulation, SLA design and performance management, team-competence assessment, training-system construction, and service-quality improvement. Covered specifically by Domain 4 (SLA Design) and the Certification System chapter.

Service-Competence Assessment

Assessment of an individual service engineer's or an entire service organisation's competence level — used for hiring, training planning, certification, or service-provider qualification verification. The four-tier certification system is designed specifically for this scenario, with the RSF-MM maturity model (planned for release in v2.0) to extend it to organisation-level assessment.

> **Scope boundary (out-of-scope scenarios) RSF does not apply to:** (1) the R&D and manufacturing stages of a robot system; (2) mechanical design or electrical schematic design of a robot; (3) functional-safety certification (SIL/PL assessment must be performed by qualified functional-safety engineers under IEC 61508 / ISO 13849, outside RSF's scope); (4) industrial-automation system integration (the principal business of system integrators, which partially intersects with — but does not overlap — the RSF service-competence framework). For competence frameworks applicable to the above scenarios, RSF recommends consulting the relevant domain-specific standards or certification systems.

1.3.3 Primary Reader Groups and Usage Modes

The principal reader groups for this framework are four, each with a different usage emphasis:

Reader Group	Typical Role / Background	Recommended Usage Emphasis
Robot Service Engineer	Field service engineer, maintenance engineer, service manager	Use Chapters 3–8 (the six domains) as a daily technical reference; use the certification system in Chapter 2 as a personal development pathway; use the appendix's standards-mapping matrix as a compliance-boundary check tool
Service-Organisation Manager	Director of Service, Regional Service Manager, Director of Operations	Use §1.2 as the basis for explaining the service-system positioning to customers and partners; use Domain 4 (Chapter 6) as a framework reference for SLA-system design; use Chapter 9's certification system as a tool for team-competence assessment and talent planning
Customer / End User	Plant operations manager, equipment-procurement lead, maintenance-contract negotiator	Use Chapter 1 to understand the framework as a whole; use the six-capability-domain definitions in Chapter 2 as the reference standard for service-provider qualification; use Domain 4 (SLA) chapter as a reference for contract-negotiation metrics
Training and Certification Institutions	ATC-authorised training centres, university engineering schools, vocational training institutions	Use the full document as the content basis for course development; use Chapter 9 (the certification system) as the alignment reference for course design and assessment methods; use the Appendix glossary as the unified basis for teaching terminology

1.3.4 Document Versioning and Update Mechanism

This document is RSF Framework v1.0, released by the RSF Initiative with RobotToday.com as the initiating platform. The continuing validity of the RSF framework depends on a regular content-update mechanism, driven by three categories of trigger:

■ **ISO/IEC standards updates: when a relevant outer-layer standard (especially the ISO 10218 series) publishes a new version, RSF will complete the corresponding chapter synchronisation**

within a reasonable period after the standard takes effect.

■ **Robotics technology evolution: AI/ML service methodology (Domain 6) and digital-twin / remote-service procedures (Domain 3) are fast-evolving areas; content review and updates are planned at a defined cadence.**

■ **Certification-data feedback: based on actual RSF examination data and curriculum feedback from authorised ATCs, the framework content will undergo routine detail revisions; revisions without structural change are released under v1.x numbering.**

> **Chapter Summary** RSF's existence rests on five evidence-backed industry gaps (§1.1) that are not deficiencies of standards quality but competence-layer needs sitting outside the design scope of existing standards. RSF establishes a precise collaborative relationship with the existing landscape through the three-layer nesting structure (§1.2): building the middle-layer framework content on top of the outer compliance baseline, with the inner operational-pattern layer as practical reference. RSF applies to on-site service, remote service, service management, and competence-assessment scenarios for industrial arms, cobots, AMRs, service robots, and humanoid robots; it does not extend to R&D and manufacturing or to functional-safety certification (§1.3). Chapter 2 will establish the structural panorama of the six capability domains, providing the navigational basis for the deep treatments of each domain in Chapters 3–8.

Chapter 2

Six Capability Domains — Overview and Relationship Map

RSF organises the core competencies of a robot-service engineer into six interrelated Capability Domains, which constitute the main body of the RSF framework. These six domains are not a simple knowledge taxonomy — they are a systematic mapping of how robotics service actually operates: they cover the complete lifecycle from delivery to decommissioning, span both the technical-execution and service-management dimensions, and take the robot system's four-layer technical architecture (physical — electrical — software — intelligent) as their internal logical axis.

This chapter, in turn, explains the definitions and boundaries of the six domains (§2.1), the structural relationships among them together with their mapping to typical service scenarios (§2.2), and the capability-growth framework of the RSF four-tier certification system (§2.3). Together these three sections form RSF's structural panorama and provide the navigation basis for the deep treatments of each domain in Chapters 3–8.

2.1 Domain Definitions and Boundaries

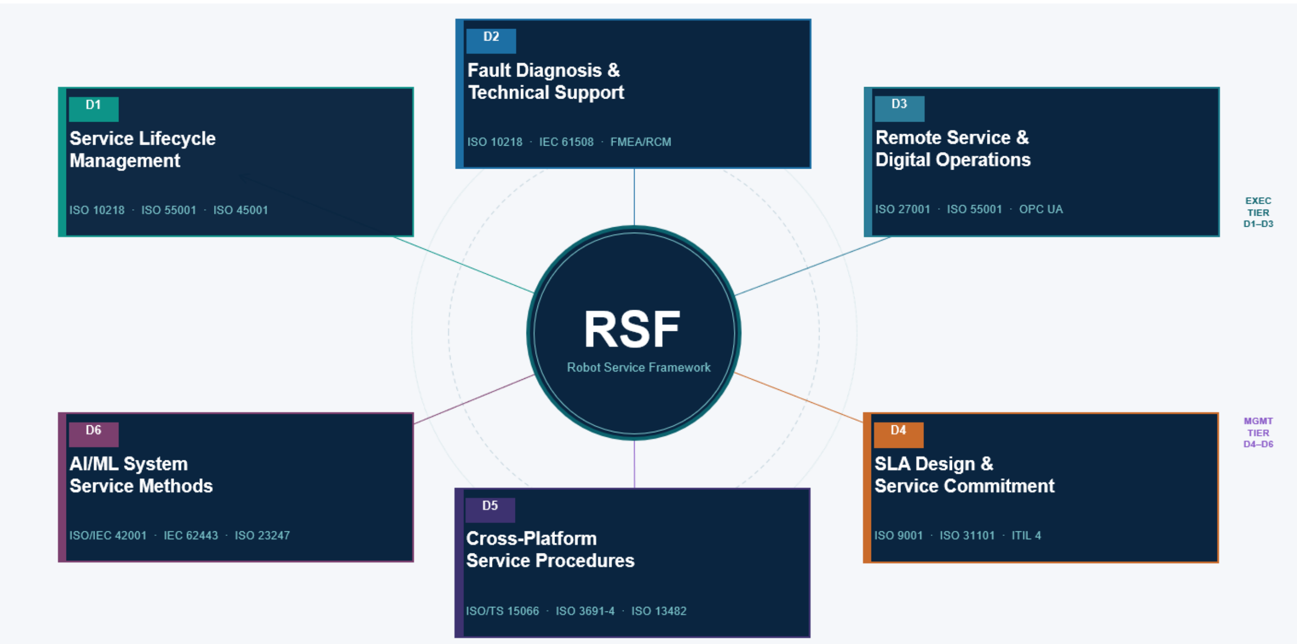
The six RSF capability domains are structurally divided into two tiers. The Service-Execution Tier (Domains 1–3) concerns the engineer's technical capabilities acting directly on robot systems in field and remote environments. The Management-Architecture Tier (Domains 4–6) concerns service-quality commitment, multi-platform service procedures, and AI/ML service methodology — the systematic expression and continuous-optimisation mechanism for service competence. The two tiers are not sequential but cooperative: without the execution tier, management-tier design lacks an implementation foundation; without the management tier, execution-tier action lacks systematic direction.

Table 2.1-1 RSF Six Capability Domains — Overview

Capability Domain	English Name	Core Definition	Tier
Domain 1 Service Lifecycle Management	Service Lifecycle Management	The capability to plan, execute, record, and continuously improve service activities at every phase of a robot system's full lifecycle, from delivery and installation through operation and maintenance to decommissioning.	**Service-Execution Tier**
Domain 2 Fault Diagnosis & Technical Support	Fault Diagnosis & Technical Support	The capability to systematically identify and localise the root causes of faults in a robot system's mechanical, electrical, software, and AI layers through a stratified diagnostic method, and to deliver effective technical solutions.	**Service-Execution Tier**

Domain 3 Remote Service & Digital Operations	Remote Service & Digital Operations	The capability to perform diagnostics, monitoring, and service delivery on robot systems off-site through remote connection, digital twins, predictive maintenance, and OTA updates.	**Service-Execution Tier**
Domain 4 SLA Design & Service Commitment	SLA Design & Service Commitment	The capability to design, negotiate, execute, and track robotic service-level agreements, covering response time, availability commitments, escalation processes, performance-indicator definitions, and contractual expression.	**Management-Architecture Tier**
Domain 5 Cross-Platform Service Procedures	Cross-Platform Service Procedures	The capability to formulate and apply unified service procedures across multiple robot platforms (industrial arms, cobots, AMRs, humanoid robots), achieving consistency and portability of service delivery while maintaining safety and regulatory compliance.	**Management-Architecture Tier**
Domain 6 AI/ML System Service Methods	AI/ML System Service Methods	The capability to apply dedicated diagnostic logic, model-performance evaluation methods, and data-driven maintenance procedures to robot systems incorporating AI perception, machine-learning decisioning, or reinforcement-learning policies.	**Management-Architecture Tier**

> **Boundary note: the partition of the six capability domains follows the functional logic of service work rather than disciplinary boundaries of knowledge. There are areas of content overlap among domains — for example, fault diagnosis (Domain 2) involves judging the service-lifecycle phase state (Domain 1), and AI/ML service methods (Domain 6) share data-acquisition infrastructure with remote monitoring (Domain 3). The framework's partition principle maximises practical utility: domains are assigned by the engineer's primary work task, not by a search for logical mutual exclusivity.**



2.1.1 Service Execution Tier: Domains 1–3

The three capability domains in the service-execution tier correspond to the most frequent and most direct work content of the robot-service engineer.

Domain 1 Service Lifecycle Management

Service demand on a robot system is not evenly distributed across its useful life — it shows structural differences across phases: delivery-phase installation and commissioning, operating-phase preventive maintenance and incident response, decommissioning-phase asset disposition. The service objectives, risk priorities, and documentation requirements of each phase differ in nature. Domain 1 requires the engineer to have a systematic understanding of these phase differences, to take the right service action at the right phase, and to maintain complete records spanning the full cycle.

The reference standards for Domain 1 include ISO 55001 (asset lifecycle management), ISO 10218 (on-site operations safety), and ISO 45001 (occupational health and safety). On top of these standards' compliance framework, RSF establishes dedicated service-phase models, key-document specifications, and milestone-assessment mechanisms for the robotics service context.

Domain 2 Fault Diagnosis & Technical Support

A modern robot system integrates the mechanical, electrical, software, and AI layers, and an anomaly in any one layer can trigger cross-layer fault propagation. Traditional single-layer diagnostic experience — analysing problems only from the angle of mechanical wear or electrical short — fails systemically when faced with AI-perception failure or reinforcement-learning policy drift. Domain 2 establishes a stratified diagnostic methodology: first localise the fault layer (mechanical / electrical / software / AI), then apply the layer's appropriate diagnostic logic, and finally identify the root cause and select the remediation path.

Domain 2 has a significant intersection with Domain 6 (AI/ML System Service Methods): Domain 2 handles the general fault-diagnosis framework for all robot systems, while Domain 6 focuses on the special diagnostic logic for AI components. The division line: when the fault phenomenon stems primarily from AI-model behaviour (such as perception-accuracy degradation or decision-policy drift), enter Domain 6's specialised methods; when the root cause lies in the mechanical, electrical, or classical software layer, Domain 2's framework applies.

Domain 3 Remote Service & Digital Operations

Industrial-robot service delivery is undergoing a structural shift: from reactive response based on on-site dispatch to proactive prediction based on data. The technical foundations of this shift — remote-connection protocols, digital-twin modelling, continuous sensor-data acquisition, and OTA firmware management — form the core of Domain 3. Domain 3 requires engineers not only to use remote-service tools but also to understand the interpretation logic of digital-twin data and the trigger mechanisms behind predictive-maintenance decisions.

On information security, Domain 3 is governed by ISO 27001 — remote-connection authorisation, tiered access permissions for diagnostic data, and third-party-provider access control all operate within the ISO 27001 framework. On top of this baseline, RSF adds a dedicated data-authorisation framework for the robotic-remote-service context.

2.1.2 Management Architecture Tier: Domains 4–6

The three capability domains of the management-architecture tier address service-system-level systematisation — the precondition for execution-tier capabilities to scale, standardise, and continuously improve.

Domain 4 SLA Design & Service Commitment

In the existing international-standards landscape, no ISO/IEC standard defines response time, availability commitment, or escalation processes for robotics service. This gap has left the robotics-service market without a common language for quality commitment: providers cannot make explicit commitments to customers, and customers cannot perform quantitative acceptance of service quality. Domain 4 fills this gap, establishing structured methods for contractual expression, KPI-system design, and performance tracking in robotics service.

The SLA-metrics framework for robotics service differs fundamentally from that of IT service. IT service centres on RTO (recovery time objective) and RPO (recovery point objective), addressing logical faults that are fully remotely fixable; robotics service addresses physical-system faults, and its metrics should centre on OEE (Overall Equipment Effectiveness), MTTR (mean time to repair), and equipment availability — with response-time definitions distinguishing remote-response and on-site arrival as two separate dimensions.

Domain 5 Cross-Platform Service Procedures

Existing international standards set norms type by type: ISO 10218 for industrial arms, ISO/TS 15066 for cobots, ISO 31101 for service robots — a type-by-type structure that works well in plants with a single platform type, but creates fragmented service procedures in modern manufacturing and logistics scenarios where multiple platform types are deployed together.

Domain 5's core contribution is to establish a unified framework for cross-platform service procedures: it identifies what is shared across platforms (safety-verification workflow, work-order record format, delivery-acceptance standards) and systematically catalogues each platform's differentiated requirements (force-torque sensor verification for cobots, map-consistency verification for AMRs, proprioception calibration for humanoid robots), so that engineers switching between platforms can systematically invoke the right procedure instead of relying on scattered experience.

Domain 6 AI/ML System Service Methods

AI/ML penetration in robot systems has expanded from peripheral perception modules into the core decision layer: motion planning, grasping policy, spatial perception, and task generalisation are increasingly executed by trained neural networks rather than deterministic algorithms. This architectural evolution places entirely new demands on service engineers — the traditional "measure → compare to spec → replace part" diagnostic logic is essentially ineffective against AI-failure categories such as model degradation, distribution shift, and adversarial interference.

Domain 6 establishes a dedicated service methodology for AI/ML systems, covering AI-layer fault-symptom recognition (distinguishing the surface differences between AI faults and hardware faults), model-performance evaluation protocols (benchmark-test design, performance-metric interpretation), model-update and rollback procedures, and AI-service compliance foundations (the service-engineer-applicable clauses of the ISO/IEC 42001 AI-management system).

2.2 Inter-Domain Relationships and Service Scenario Mapping

In actual service work the six capability domains do not operate independently — they form a structured cooperative relationship. Understanding these relationships has direct operational meaning for correctly judging which capability domains a specific service task needs to invoke, and in what order.

2.2.1 Principal Inter-Domain Relationships

The relationship structure among the six domains can be understood along three dimensions:

Domain 1 ↔ Domain 2 — Phase-and-Diagnosis Relationship

Service Lifecycle Management (Domain 1) provides context to Fault Diagnosis (Domain 2): in judging a fault phenomenon, the engineer must first confirm the equipment's lifecycle phase — the same vibration anomaly has completely different diagnostic paths during commissioning (likely a parameter issue) versus during stable operation (likely mechanical wear).

Domain 2 ↔ Domain 3 — Field-and-Remote Cooperation

Fault Diagnosis (Domain 2) and Remote Service (Domain 3) form a dual-track structure of diagnostic capability: remote diagnostics is the preferred path (faster response, lower cost), while on-site diagnostics is the necessary supplement (when physical inspection, part replacement, or safety-procedure execution cannot be skipped). Domain 3's digital-twin and predictive-maintenance data give Domain 2's on-site diagnosis a historical baseline that significantly shortens diagnostic time after arrival.

Domain 4 ↔ Domains 1–3 — Commitment-and-Execution Relationship

The SLA (Domain 4) is the quality-framework constraint on the service-execution tier (Domains

1–3): Domain 4 defines what "fast enough" response time and "good enough" availability mean, and the execution quality of Domains 1–3 determines whether those commitments are met. Root-cause tracing of an SLA breach must traverse from Domain 4 back to the specific execution touchpoints in Domains 1–3.

Domain 5 ↔ All Domains — Procedure-Standardisation Relationship

Cross-Platform Service Procedures (Domain 5) is the multi-platform adaptation of execution methods from Domains 1–3: Domain 5 does not independently define diagnostic logic; instead, it systematically catalogues each platform's commonalities and differences in Domain 1 (maintenance phases), Domain 2 (diagnostic methods), and Domain 3 (remote-access protocols), so that the service procedures become switchable between platforms.

Domain 6 ↔ Domains 2 & 3 — AI-Specific Relationship

AI/ML Service Methods (Domain 6) is the deepening extension of Domain 2 (Fault Diagnosis) in the direction of AI components, and it shares data-acquisition infrastructure with Domain 3 (Remote Service). When Domain 2's stratified diagnostic locates a fault to the AI layer, Domain 6 supplies the further specialised analysis tools; Domain 3's continuous-monitoring data stream is the main data source for Domain 6's model-performance evaluation.

2.2.2 Typical Service Scenarios and Capability-Domain Invocation Matrix

The table below maps eight of the most common service scenarios for a robot-service engineer to the combinations of capability domains they principally invoke. The matrix is not a complete operations manual but a reference tool to help readers build the "scenario → domain" mapping intuition.

Table 2.2-1 Typical Service Scenarios and Capability-Domain Invocation Matrix

Service Scenario	Primary Domains Invoked	Trigger Mechanism and Key Tasks
New-Equipment Delivery and Commissioning	Domain 1 (primary), Domain 2 (supporting)	Customer procurement and on-site arrival → unpacking acceptance, mechanical mounting, electrical wiring, parameter configuration, safety-function verification, operator training delivery
Preventive Maintenance Execution	Domain 1 (primary), Domain 3 (data support)	PM cycle due or predictive-maintenance trigger → checklist inspection, lubrication, consumable replacement, performance verification, record update
Fault Response and Repair (On-Site)	Domain 2 (primary), Domain 1 (context), Domain 5 (platform procedures)	Customer reports downtime or performance anomaly → symptom record, stratified diagnosis, root-cause localisation, repair operation, verification test, work-order closure
Fault Response and Repair (Remote)	Domain 3 (primary), Domain 2 (diagnostic logic), Domain 4 (SLA tracking)	Monitoring alarm or remote customer report → remote-connection authorisation, data extraction, remote parameter adjustment or firmware push, disposition record

AI-Component Performance Degradation	Domain 6 (primary), Domain 2 (stratified localisation), Domain 3 (data acquisition)	Vision recognition rate drop, abnormal policy behaviour, generalisation failure → AI-layer fault recognition, model evaluation, data-annotation audit, model rollback or update
SLA Performance Monitoring and Customer Communication	Domain 4 (primary), Domains 1/2/3 (data sources)	Monthly / quarterly SLA review cycle → KPI data aggregation, MTTR / availability calculation, reporting to customer, variance analysis, improvement plan
Mixed-Platform Service Environment	Domain 5 (primary), Domain 2 (diagnosis), Domain 1 (lifecycle)	Plant simultaneously operates industrial arms + cobots + AMRs → procedure-switching recognition, platform-specific safety verification, unified work-order format execution
OTA Firmware Update and Version Management	Domain 3 (primary), Domain 1 (change records), Domain 2 (verification testing)	Manufacturer firmware release → update-package validation, current-version backup, staged rollout testing, function verification, rollback contingency

2.2.3 Mapping Between the Four-Layer Technical Architecture and the Capability Domains

The design of RSF's capability domains takes the robot system's four-layer technical architecture as its inner logical axis. These four layers — Mechanical Body, Electrical Control, Software Middleware, AI Decision — provide a systematic analytical framework for fault diagnosis and maintenance decisions. The mapping below explains the correspondence between the four layers and the six capability domains, and is the structural premise for understanding each domain's technical content.

Table 2.2-2 Mapping Between the Robot Four-Layer Technical Architecture and the RSF Capability Domains

Technical Layer	Layer Content	Principal Associated Domains	Typical Service Tasks
L1 Mechanical Body Layer	Joints, transmission systems (harmonic and RV reducers), end-effectors, chassis structure	Domain 1 (install / maintain), Domain 2 (mechanical-layer diagnosis), Domain 5 (platform procedures)	Lubrication, backlash measurement, TCP-accuracy verification, joint replacement, mechanical-wear assessment
L2 Electrical Control Layer	Servo drives, safety controllers (PLC), power systems, sensors (torque / position / vision), communication interfaces	Domain 1 (safety procedures), Domain 2 (electrical-layer diagnosis), Domain 3 (remote I/O monitoring)	Servo-parameter tuning, safety-circuit testing, LOTO operations, sensor calibration, communication-anomaly troubleshooting
L3 Software Middleware Layer	Robot operating system (ROS / ROS2), motion-controller firmware, coordinate-system management, communication protocols (EtherCAT / OPC UA)	Domain 2 (software-layer diagnosis), Domain 3 (OTA / remote debug), Domain 5 (cross-platform procedures)	Firmware updates, parameter backup / restore, log analysis, communication-cycle inspection, coordinate-system calibration verification

L4 AI Decision Layer	Vision-perception models, motion-planning networks, reinforcement-learning policies, natural-language command parsing, multi-modal fusion inference	Domain 6 (AI/ML methods), Domain 2 (AI-layer localisation), Domain 3 (model-monitoring data)	Perception-accuracy benchmark testing, model-performance evaluation, distribution-shift detection, model rollback, data-annotation quality audit

2.3 Four-Tier Certification and Capability Growth Pathway

The RSF certification system uses a four-tier progressive structure, with deepening cognitive dimension as its core logical axis: from Professional (Know-How — knows how to do it) to Specialist (Know-Why — knows why it works), then to Expert (Know-Across — knows how to integrate across domains), and finally to Master (Know-Beyond — knows how to define the future). Advancement between tiers is not merely an accumulation of knowledge but a systematic transformation of cognitive mode and work perspective.

The design logic of this certification architecture references the structure of the automotive ASE certification system (tier linked to authorised scope) and the ITIL certification framework (balanced emphasis on knowledge and practical capability), but the content is reconstructed entirely around the specific needs of robotics service — neither is replaceable by the other.

The four-tier system organises engineer development along a deepening cognitive dimension — Professional (Know-How), Specialist (Know-Why), Expert (Know-Across), Master (Know-Beyond) — with parallel Engineer and Service Manager tracks at every tier. The complete tier-by-tier definitions, including responsibilities for both tracks and coverage across the six capability domains, are given in Table 9.2-1 (§9.2).

2.3.1 Depth of Six-Domain Coverage Across Certification Tiers

The four certification tiers do not correspond to different capability domains; rather, they progress within the same six-capability-domain system, with continuously deepening cognitive depth and expanding scope of application. The table below sets out the core competence requirements of each capability domain at each tier, clarifying the assessment focus and the expected competence boundary at each level.

Table 2.3-2 Coverage Depth of the Six Capability Domains Across the Four Certification Tiers

Capability Domain	Professional	Specialist	Expert	Master
Domain 1 Service Lifecycle	Execute standard SOP, complete service tasks of the designated phase, fill in work-order records	Design phase-based maintenance strategies, assess decommissioning timing, optimise the service-process closed	Build a cross-organisation service-lifecycle management system that	Define the best-practice standard for robotics-industry service lifecycle

		loop	integrates ISO 55001 requirements	
Domain 2 Fault Diagnosis	Recognise common fault phenomena, execute stratified diagnostics per the decision tree, invoke standard remediation procedures	Independently handle cross-layer complex faults, lead root-cause analysis, deliver improvement recommendations	Design diagnostic-methodology frameworks, build platform-specific fault databases	Define industry-level diagnostic standards and assessment specifications for AI-assisted diagnostics
Domain 3 Remote Service	Use authorised remote tools to execute designated operations, report diagnostic data	Independently manage digital-twin data interpretation, formulate predictive-maintenance trigger rules	Design remote-service-platform architecture, integrate OTA and digital-twin systems	Define industry specifications for robotics-remote-service data governance and secure access
Domain 4 SLA Design	Understand and execute existing SLA terms, record and report SLA-related performance data	Participate in SLA negotiations, design KPI systems, manage SLA-violation handling processes	Lead SLA-contract-system design, establish service-pricing and cost models	Define industry-benchmark indicators and standard-clause frameworks for robotics-service SLAs
Domain 5 Cross-Platform Procedures	Recognise the procedural differences across robot platforms, execute operations per the designated procedure	Formulate unified service procedures for multi-platform environments, manage procedural version updates	Design cross-platform service-capability assessment matrices and authorisation-procedure systems	Participate in formulating international standards for cross-platform service procedures
Domain 6 AI/ML Service	Recognise AI-layer fault symptoms, distinguish AI faults from hardware faults, escalate per procedure	Execute model-performance evaluation, participate in data-annotation audits, manage model-update workflows	Design AI-service methodology frameworks, establish model-service-capability benchmark-test systems	Define industry-governance frameworks and ethics-compliance standards for AI-robot service

2.3.2 Advancement Requirements and Authorization Mechanism

RSF certification is directly linked to the engineer's authorised scope of work: the certification tier determines which types of service tasks the engineer is authorised to perform independently. This design references the authorisation logic of the ASE certification system — certification is not only proof of knowledge, but also a definition of the work boundary.

Table 2.3-3 RSF Four-Tier Certification — Advancement Requirements and Authorisation Boundaries

Advancement Path	Prerequisites	Assessment Method	Scope of Authorisation
Entry → Professional	No prior certification required; basic electromechanical	Written examination (specific pass	May execute standard preventive-maintenance tasks

	background or relevant work experience is recommended	threshold per the ATC Examination Guide)	under supervision; may independently complete basic work-order records; may participate in fault response under Specialist supervision
Professional → Specialist	Professional certification held for the prescribed period, plus sufficient independently completed work-order records (specifics per the ATC Examination Guide)	Written examination, practical assessment, and submission of a real service-improvement case (DMAIC format)	May independently handle complex faults without supervision; may lead SLA communication with customers; may audit and mentor Professional-level operations
Specialist → Expert	Specialist certification held for the prescribed period, plus leadership of multiple service-improvement projects with quantifiable outcomes (specifics per the ATC Examination Guide)	Submission of a white-paper-level case, plus oral defence before the RSF peer-review committee	May design service-system solutions; may serve as an ATC trainer; may submit revision recommendations for the RSF framework
Expert → Master	Expert certification held for the prescribed period, plus verifiable industry-level contribution (standards participation, peer-reviewed publication, or systemic innovation)	Nomination by RSF Board of Trustees, review of contribution dossier, plus peer review	Represents RSF in industry-standards formulation; may serve on the RSF Certification Committee; authorised to publish revision recommendations for the RSF framework

Note: this table summarises prerequisites, assessment method and authorised scope at a glance. Quantitative work-experience windows, performance evidence requirements and special-case notes for each advancement step are detailed in Table 9.2-2 (§9.2.2).

> **Chapter Summary** **RSF's six capability domains** form an internally coherent service-competence system: the service-execution tier (Domains 1–3) provides the technical capabilities that act directly on robot systems, and the management-architecture tier (Domains 4–6) provides the systemic framework that allows execution capabilities to scale and standardise. The six domains have explicit cooperative relationships rather than being independent knowledge modules.
>
> The four-tier certification system (Professional → Specialist → Expert → Master), with deepening cognitive dimension as its core logical axis, achieves tiered competence assessment and authorisation management within the same six-domain framework. Chapters 3–8 deepen the treatment of each domain in turn.

Appendices

Appendix A

Standards-to-Six Capability Domains Mapping Matrix

This matrix systematically presents the correspondence between the existing international standards system and the six RSF capability domains: what each standard covers, which RSF capability domain it primarily relates to, and what specialized content RSF supplements in that domain beyond the standard's scope. Reading guide: the domain listed under "Primary Associated Domain" is where the standard contributes most directly to RSF; the "RSF Supplementary Content" column shows content that existing standards cannot cover and that has been filled in originally by RSF.

A.1 Safety and Compliance Standards

Table A-1 Mapping of Safety and Compliance Standards

Standard No.	Scope	Primary Associated Domain	Standard Coverage	RSF Supplementary Content (beyond the standard)
ISO 10218-1/-2 :2025	Industrial robot-arm safety requirements (design layer + system-integration layer)	Domain 1 (Lifecycle), Domain 2 (Diagnosis), Domain 5 (Platform Procedures)	Robot design safety requirements; system-integration safety specifications; safety-guard design; emergency-stop requirements; safety-function classification (STO / SS1 / SS2)	Tiered competency assessment of service engineers; on-site maintenance SOPs; step-by-step safety-state verification procedures during the maintenance phase; service-operation safety procedures for cobot scenarios
ISO/TS 15066 :2016	Collaborative-robot (cobot) safety requirements	Domain 2 (Diagnosis), Domain 5 (cobot-specific)	Power and Force Limiting (PFL) human-contact limits; Speed and Separation Monitoring (SSM); Hand Guiding (HG); Safety-Rated Monitored Stop (SRMS)	Torque-sensor temperature-compensation management procedure; quarterly torque-compliance verification method; standardized procedure for establishing torque baselines; early-warning mechanism for cobot safety-parameter degradation
IEC 61508 (SIL assessment)	Functional safety of electrical / electronic / programmable safety systems	Domain 1 (Installation Verification), Domain 2 (Safety-Circuit Diagnosis)	Quantitative SIL evaluation method; functional-safety lifecycle; failure-rate calculation for safety functions	Safety-function test procedure for robot service engineers; step-by-step re-verification checklist for safety functions after repair; SIL applicability guide for service scenarios
ISO 45001 :2018	Occupational health and safety management system	Domain 1 (Full Lifecycle), Domain 5 (Universal	Occupational health-and-safety risk assessment; LOTO (energy-isolation)	Dedicated LOTO procedure for robot field service; pre-condition checklist for safe service operations; SVP-1

		Safety Procedures)	management requirements; safety-training record management	Universal Safety Verification Procedure (a core component of UCSP)
IEC 62443 :2024	Industrial control-system cybersecurity	Domain 3 (Remote-Service Security Architecture)	OT-network Zone / Conduit segmentation model; Security Level (SL 1–4) definitions; organizational cybersecurity-program requirements (added in the 2024 edition)	DMZ architecture specification for robot remote service; zero-trust remote-access implementation for robot service scenarios; six-step remote-session management procedure; IEC 62443 compliance path for OTA updates
ISO/IEC 42001 :2023	AI management system	Domain 6 (AI / ML Service)	AI-system lifecycle management requirements; AI risk-assessment framework; organizational governance requirements for AI systems	Model performance-evaluation procedure for robot AI components; four-quadrant classification framework for AI-layer faults; engineer-applicable MLOps clauses for robot-service scenarios; compliance boundaries of Agentic AI maintenance workflows

A.2 Asset and Quality Management Standards

Table A-2 Mapping of Asset and Quality Management Standards

Standard No.	Scope	Primary Associated Domain	Standard Coverage	RSF Supplementary Content
ISO 55001 :2014	Full-lifecycle asset management	Domain 1 (Lifecycle Management — main axis)	Asset-management objectives and planning; asset-performance monitoring; asset-retirement decision framework; maintenance-strategy requirements	Five-phase robot service-lifecycle model; phase-transition Stage Gate criteria; four-dimensional retirement-assessment matrix; Equipment Configuration Baseline system
ISO 9001 :2015	Quality management system	Domain 1 (Service-Documentation System), Domain 4 (SLA Compliance)	Process control and documentation requirements (Clause 8.5); customer-satisfaction management; non-conformance management; continual improvement (PDCA)	Five-field standard for robot work-order records; work-order closure standard (dual-signature regime); service-improvement closed loop (fault response → root cause → controlled change); format standard for monthly SLA reports
ISO 31101 :2023	Safety management for service-	Domain 1 (Lifecycle), Domain 4 (SLA Design)	Operating-environment risk assessment for service robots;	Risk-adjusted SLA design for service robots; on-site service safety-assessment steps for

	robot application scenarios		personnel-protection requirements for operating sites; incident-reporting and analysis framework	service robots; adaptation of service procedures to non-manufacturing environments (hospitals / retail / home)
ISO 3691-4 :2023	Mobile-robot (AMR) safety requirements	Domain 5 (AMR-specific procedures)	AMR navigation-safety requirements; emergency-stop specification; geofencing requirements; speed limits when co-existing with personnel	AMR map-management procedure (mapping requirements / validity period / version control); AMR battery-health management procedure; VDA 5050 interface-compatibility verification; service-engineer operating standards for AMR fleet coordination
ISO 13482 :2014	Personal-care robot (service-robot) safety	Domain 5 (Humanoid-Robot Reference)	Safety requirements for personal-care robots; contact-force limits; personnel-detection requirements	Starting-point framework for humanoid-robot service (extending the spirit of ISO 13482); SVP-1 specialized safety-verification steps for humanoid robots; fall-risk assessment procedure for humanoid robots

A.3 Information Security and Digital-Operations Standards

Standard No.	Scope	Primary Associated Domain	Standard Coverage	RSF Supplementary Content
ISO 27001 :2022	Information-security management system	Domain 3 (Remote-Service Data Security), Domain 6 (AI Data Governance)	Information-asset classification and access control; remote-access security requirements (Clause A.6.7, added in the 2022 edition); audit-log requirements; supplier-relationship management	Six-step management procedure for robot remote-diagnostic sessions; remote-access data-classification framework (L1–L4); compliance path for cross-border data transfer in robot service; authorization standard for use of AI training data
ISO 23247 (Digital Twin)	Manufacturing digital-twin reference architecture	Domain 3 (Digital Twin)	Reference architecture for manufacturing digital twins; data-acquisition interface specification; model-update mechanism	Service-function definitions for the four-layer Robot Digital Twin (RDT) system architecture; four mechanisms of physical-digital synchronization; digital-twin-based AI maintenance-agent workflows; RDT Health Index (HI) calculation and alerting rules

VDA 5050 (AMR Communication)	AGV / AMR fleet-communication protocol (industry standard)	Domain 5 (AMR Fleet Management), Domain 3 (Remote Service)	Communication-interface definition between AGV / AMR and fleet-management systems; order management; status-report format; error classification	Multi-brand AMR service-data aggregation method based on VDA 5050; VDA 5050 version-compatibility verification procedure; migration-path guide between ISO 21423 (in development) and VDA 5050

A.4 Summary of Standards Coverage Density Across the Six Capability Domains

Table A-4 Standards Coverage Density and RSF Contribution Weight by Capability Domain

Capability Domain	Existing Standards Coverage Density	Primary Covering Standards	RSF Contribution Weight
Domain 1 Service Lifecycle Management	★★★★ (High)	ISO 55001 (Asset Management), ISO 9001 (Quality Management), ISO 45001 (Safety Management), ISO 10218 (On-Site Operational Safety)	Medium: standards provide the principle framework; RSF provides the five-phase model, Stage-Gate criteria, and operational procedures
Domain 2 Fault Diagnosis & Technical Support	★★☆ (Low–Medium)	ISO 10218 (Safety-Function Verification), IEC 61508 (Functional-Safety Assessment)	High: four-layer stratified diagnostic framework, diagnostic-funnel model, seven-category tool-capability framework, case library — all RSF originals
Domain 3 Remote Service & Digital Operations	★☆ (Low)	IEC 62443 (OT Cybersecurity), ISO 27001 (Information Security), ISO 23247 (Digital-Twin Reference Architecture)	Very high: S1–S4 evolution model, four-layer RDT architecture, predictive-maintenance system, OTA management procedures — all RSF originals
Domain 4 SLA Design & Service Commitment	☆ (Very Low)	No ISO / IEC standard directly applicable	Very high: robot SLA-metrics framework, four-tier SLA product system, SLA strategies for emerging companies, compensation mechanisms — all RSF originals
Domain 5 Cross-Platform Service Procedures	★★ (Low–Medium)	ISO 10218 (industrial arms), ISO/TS 15066 (cobots), ISO 3691-4 (AMR), ISO 13482 (service robots)	High: standards are platform-isolated; RSF provides a unified cross-platform framework (UCSP), the PSC platform-card system, and a heterogeneous-fleet management architecture
Domain 6 AI/ML System Service Methods	★☆ (Very Low)	ISO/IEC 42001 (AI Management System, governance level only)	Very high: AI four-quadrant fault classification, model-performance evaluation, MLOps service-engineer applicability framework, Agentic AI service platform — all RSF originals

Matrix Pattern Existing standards cover Domain 1 (Service Lifecycle Management) most densely, and RSF's relative contribution there is lowest (mainly operational procedures). Domain 4 (SLA Design) and Domain 6 (AI / ML Service) have almost no existing-standard coverage, and RSF's contribution in those two domains is almost entirely original. This distribution maps directly onto the five capability-layer needs described in §1.1 — technical evidence of where RSF's contribution is most needed.

Appendix B

Automotive 4S System — Adoption Logic and Transformation Boundaries

The inner layer of the RSF three-tier nested model — the Operational-Pattern Reference layer — is drawn primarily from the automotive 4S service system. This appendix systematically explains what RSF adopts from the 4S system, why, and where the boundaries lie. Both questions matter equally: the first establishes the legitimacy of the adoption; the second prevents distortion from mechanical transplantation.

B.1 Premise of Adoption: Structural Isomorphism of Business Models

The fundamental reason the automotive 4S system serves as a core reference for RSF is the high structural isomorphism of the business model. In service economics, an industrial robot and an automobile are very similar: both are high-unit-cost hardware products (complex purchase decision, service life of 10+ years), both have maintenance costs that represent a significant share of total lifecycle cost, and both customers lack self-repair capability. These shared properties give rise to the same commercial demands: a specialized service network, authorized-technician certification, spare-parts supply-chain management, and quantifiable service-quality assessment. The automotive industry spent decades validating and iterating a service-operations system that meets those demands across millions of service touchpoints worldwide — and that is exactly where the 4S system's core value to RSF lies.

B.2 Four Core Items Adopted

Item 1 — Tiered Technician Certification Structure (ASE Certification Logic)

The core design of ASE (Automotive Service Excellence) certification is: classification by specialty, tiering by capability level, and a mandatory link between certification status and authorized scope of work. Holding a specific ASE certificate means the holder is authorized to independently perform the corresponding type of repair — certification is permission, not merely a credential. RSF's four-tier certification system (Professional / Specialist / Expert / Master) adopts this structural logic directly: the four tiers correspond to a progression in cognitive dimension; the six capability domains replace the specialty-direction classification used in automotive repair; each certification tier maps to a clearly defined authorized scope of work. The design principle of "linking certification to authorization" is transferred intact from the ASE system.

Item 2 — Service Closed-Loop Process Architecture

The 4S service blueprint standardizes a single repair as a reproducible end-to-end workflow: appointment registration → vehicle reception → fault diagnosis → repair authorization → repair execution → quality inspection → customer delivery → service follow-up. RSF converts this closed-loop logic into the basic architecture of robot field service (see §3.5): on-site assessment → fault diagnosis → work-authorization confirmation → maintenance execution → functional verification → service-record archiving → customer confirmation → remote follow-up. The conversion preserves the closed-loop logic and the data-accumulation principle while replacing the technical content of each node.

Item 3 — Quantified Customer-Satisfaction Tracking Mechanism

The automotive industry's CSI (Customer Satisfaction Index) and NPS (Net Promoter Score) systems provide quantifiable, geographically comparable, and decision-actionable service-quality measures. RSF brings the CSI / NPS mechanism into two layers: the annual review of ATC certification training centers (student-satisfaction NPS ≥ 8.0 / 10 is one of the pass criteria), and the customer-satisfaction metric (CSAT) within the SLA performance-tracking system (see §6.8).

Item 4 — Parts-Inventory Management Model (ABC Classification)

The automotive 4S system's ABC classification for parts inventory: Class A — high-frequency, high-value parts (high safety stock, highest priority); Class B — medium-frequency, medium-value parts (standard safety stock); Class C — low-frequency, low-value parts (order-triggered procurement). The parts-strategy design in RSF Domain 1 (Service Lifecycle Management) adopts this classification framework, applying differentiated safety-stock policies to common robot consumables (reducer grease, batteries, encoders, driver boards) under the ABC principle.

B.3 Transformation Boundaries: Three Non-Transferable Areas

There are clear technical boundaries on how far the 4S system can be adopted. Crossing these boundaries distorts the framework, because the technical assumptions of automotive service differ fundamentally from those of robot service:

Non-Transferable Area	4S System Assumption	Reality of Robot Service and RSF Handling
Fault-Diagnosis Logic	Standard OBD-II interface; fault modes discrete, finite, and deterministic; clear mapping from fault codes to troubleshooting trees	Robot fault modes (especially in AI-integrated systems) are probabilistic — vision-perception distribution shift and RL policy drift cannot be mapped to deterministic fault codes. RSF Domain 2 establishes the four-layer stratified diagnostic framework (original); Domain 6 establishes the AI four-quadrant fault classification (original).
Software and Firmware Service Procedures	ECU flashing is relatively simple; vehicle-model update cycles are measured in years; a clear rollback procedure exists for failed software updates	Robot software service is far more complex than automotive: ROS-node dependency management, AI-model version control, multi-system firmware-compatibility verification, safe rollback after a failed OTA push — none of which has any counterpart in the 4S system. The OTA-management section of RSF Domain 3 is entirely original.
Multi-Brand Mixed-Fleet	A 4S dealership serves a single brand; technician training,	Robot service providers typically manage mixed fleets of industrial arms, AMRs, and cobots — cross-brand service

Management	tooling, and spare-parts supply chains are all optimized for that brand	coordination has no precedent in the 4S system. The Unified Cross-Platform Service Procedure (UCSP) framework in RSF Domain 5 draws its reference from service-integration methodology (the spirit of the SIAM framework) rather than from the 4S system.

B.4 Summary Table of Adoption Items

Table B-1 Summary of 4S Adoption Items and Transformation Boundaries

Adoption Dimension	Source in the 4S / Automotive System	RSF-Transformed Content	Transferability
Tiered Technician Certification	ASE certification tier linked to authorized scope of work	Four-tier Professional / Specialist / Expert / Master certification linked to authorized domain scope	Structure transferred intact, content replaced
Service Closed-Loop Process	Seven-step 4S service-blueprint closed loop	Eight-step robot field-service procedure	Logic transferred, node content rewritten
Lean Site Management	Toyota TPS · 5S · SOW standardized work	Service-SOP documentation · standardized tool carts	Methodology applied directly
Quantified Customer Satisfaction	CSI / NPS linked to authorization status	Training NPS · ATC review system · SLA CSAT metric	Mechanism transferred, metrics localized
Parts-Inventory Management	ABC classification · safety-stock model	Tiered high-frequency robot-parts inventory and stock baseline	Model transferred, categories redefined
Fault-Diagnosis Logic (❌)	OBD-II · deterministic fault tree	Not transferable; Domain 2 and Domain 6 are entirely original	Not transferable
Software / Firmware Service Procedures (❌)	Standard ECU-flashing workflow	Not transferable; Domain 3 OTA management is entirely original	Not transferable
Multi-Brand Mixed-Fleet Management (❌)	Single-brand 4S exclusive-dealership model	Adopts the spirit of the SIAM framework, not the 4S system	Not transferable; reference frame replaced

Appendix C

RSF Innovation Contribution and Competitive Positioning

Formal Innovation Statement

Using the ISO / IEC compliance system as its outer boundary and the operational maturity of the automotive 4S service system as a reference, RSF is the first framework to construct a professional service-capability certification covering the full range of modern robotic systems (including AI / ML integration), filling the systemic industry gaps in service-personnel assessment, AI-layer service procedures, and robot SLA design.

C.1 Technical Evidence for "First-Constructed"

"First-constructed" is a factual statement, not a value claim. Across the following three dimensions, no public framework with equivalent coverage existed prior to RSF:

Dimension	Industry State before RSF	RSF First Contribution
Service-Engineer Competence Certification	ISO 10218 calls for "competent persons" but does not define capability levels; no ISO / IEC standard provides a tiered assessment framework for robot service engineers; no comparable international certification system exists	Established the Professional / Specialist / Expert / Master four-tier certification framework; defined knowledge requirements, practical-skill standards, and authorized work scope for each tier; established certification-linked continuing professional development (CPD)
AI / ML Component Service Procedures	ISO 10218:2025 covers deterministic control systems; ISO/IEC 42001 stops at the governance layer; no standard or framework defines field-diagnosis methods for AI-layer faults, model-performance evaluation procedures, or MLOps procedures applicable to service engineers	Established the four-quadrant AI-layer fault classification framework (Q1–Q4); defined the standard benchmark-suite specification for model-performance evaluation; established the four-agent architecture for Agentic AI maintenance workflows; first to systematize the dual role of AI as service platform (Role B) and AI as service object (Role A)
Robotics Service SLA Framework	No ISO / IEC standard defines availability targets, response-time tiers, SLA performance metrics, or breach-compensation mechanisms for robot service; service contracts rely mainly on non-quantified "reasonable efforts" clauses	Established an OEE-centered robot SLA-metrics system (separating outcome, process, and data metrics); designed a four-tier SLA product system (L1–L4); proposed eight SLA strategies for emerging robotics companies; defined the structural restructuring of the SLA system under the RaaS model

C.2 Three Historical Precedents and Their Relationship to RSF

RSF was not established in a vacuum; it follows the historical path of three industries that produced service-management frameworks after technology reached scale. Understanding these three precedents clarifies RSF's positioning and boundaries. They are design references for RSF, not substitutes — the particularities of robot service (statutory physical-safety requirements, AI uncertainty, cross-platform complexity) make none of the existing frameworks directly transferable.

Table C-1 Three Historical Precedents: Core Insights and RSF Design Conversion

Precedent	Historical Context	Core Contribution and Conversion into RSF Design	Key Differences between RSF and the Precedent
ASE Certification + Automotive 4S	1970s–2000s: as automotive ECUs became widespread, traditional mechanics lacked electronic-diagnostic capability; customers could not judge the skill level of dealership technicians	◦ ASE established tiered certification across 8+ specialties, turning capability into verifiable qualification ◦ The closed-loop structure "certification → authorized scope of work → customer trust" is fully adopted by RSF ◦ The closed-loop logic of the 4S service blueprint is converted into RSF's eight-step field-service procedure	RSF must additionally handle probabilistic AI-layer diagnosis, heterogeneous cross-platform fleets, and AI-model version management — none of which has any parallel in automotive service
CMMI (Software Capability Maturity)	1990s: software projects were widely over schedule or failing, but process capability could not be assessed in advance; the industry lacked a common language for capability maturity	◦ Defined organizational process-capability levels 1–5, letting organizations know "where they stand" ◦ RSF adopts the tiering mindset and will establish the Robot Service Maturity Model (RSF-MM Level 0–5, planned for release in v2.0) ◦ The logic "capability can be tiered → assessed → improved" is transferred directly	CMMI targets pure software processes with no physical-safety requirements; RSF must coexist with statutory baselines such as IEC 61508; robot-service "processes" include physical operations, so CMMI's metric system must be rebuilt from scratch
ITIL (IT Service Management)	1980s: IT service was chaotic; the UK government commissioned a service-management framework that later became the de facto global standard for IT service management	◦ ITIL's evolution from industry initiative → framework document → certification system → international influence serves as a development reference for RSF ◦ ITIL's three-layer closed loop — incident management → problem management → change	ITIL targets IT systems (logical failures, fully remote-recoverable); robot service targets physical systems (physical intervention required); ITIL's SLA system is based on RTO / RPO, while robot SLAs must be based on MTTR / OEE — the metric system must be rebuilt from scratch

		management — is converted by RSF into a three-tier closed loop of fault response → root-cause analysis → service improvement ◦ The full-lifecycle perspective of Service Value (Value Co-creation) shapes the value orientation of RSF's lifecycle-management chapter	

C.3 RSF's Contemporary Value: Avoiding ITIL's Late-Arrival Mistake

It took the IT industry roughly twenty years to establish ITIL — a service-management framework that arrived only after technology had been deployed at scale. During those twenty years, the IT service industry endured large amounts of avoidable disorder: no capability standard, no quality commitment, no incident procedure. In 2025 the robotics industry is going through the technology-scaling inflection point that the IT industry went through around 1985.

RSF's strategic significance is to move the establishment of a service-capability framework forward — from "10–20 years after technology deployment" to "contemporaneous with deployment." This is not only an efficiency issue but a safety issue: deploying robots at scale without a standardized service-capability framework would mean tens of thousands of engineers maintaining industrial equipment capable of real physical harm, without standard training, without capability assessment, and without safety procedures. RSF's emergence is the industry's systemic response to that risk.

Appendix D

Glossary of Terms

This glossary collects the core professional terms used in the RSF framework, grouped by capability domain and topic. Each entry includes: abbreviation (if any), English full name, and a concise definition. This glossary is the standard terminology reference for RSF certification examinations and ATC training courses.

D.1 Framework and Certification System

Abbreviation	English Term	Definition
RSF	Robotics Service Framework	The professional capability framework and certification system for industrial-robot service defined in this document
6D	Six Capability Domains	The six core capability modules (Domain 1 – Domain 6) of the RSF framework, covering both the service-execution layer and the management-architecture layer
RSF-MM	RSF Maturity Model	A Level 0–5 maturity assessment model for service organizations, similar in logic to CMMI; planned for release in v2.0
ATC	Authorized Training Center	An institution authorized by RSF to deliver certification training courses and administer examinations
CPD	Continuing Specialist Development	Credit-based continuing-learning system required to maintain RSF certification (30 credits every 3 years)
T3	Train-the-Trainer	Authorized training program for ATC trainers, qualifying them to deliver RSF certification courses
PSC	Platform Service Card	A standardized one-page reference document for platform-specific service requirements, used alongside the UCSP universal procedure
UCSP	Unified Cross-Platform Service Procedures	RSF's two-layer framework for cross-platform service management (common layer + platform-specific layer)

D.2 Domain 1 — Service Lifecycle Management

Abbreviation	English Term	Definition
—	Service Lifecycle	The full process of a robot system from delivery and installation to controlled decommissioning; RSF divides it into five phases
PM	Preventive Maintenance	Scheduled maintenance performed before failures occur, aimed at maintaining high equipment availability
LOTO	Lockout/Tagout	Safety procedure that physically isolates and labels all energy sources before maintenance work begins
TCP	Tool Center Point	Reference point of the robot end-effector and the core measurement baseline for accuracy verification
OEE	Overall Equipment Effectiveness	Availability × Performance × Quality — composite performance metric for manufacturing equipment (world-class benchmark ≥ 85%)
MTTR	Mean Time to Repair	Average time from work-order opening to equipment return to normal operation
MTBF	Mean Time Between	Average time during which equipment operates normally between

	Failures	two failures
EOL	End of Life	OEM announces that a part is no longer produced; spare-parts strategy and equipment-retirement schedule must be reassessed
DAC	Delivery Acceptance Certificate	Gate document for Phase 2 → Phase 3 transition; must be co-signed by the service provider and the customer
KFL	Known Fault Library	Organizational knowledge asset that stores past successful diagnoses in structured form
SVP	Safety Verification Procedure	Four-step standardized safety pre-check that must be performed before any service operation on any platform (a component of UCSP)

D.3 Domain 2 — Fault Diagnosis and Technical Support

Abbreviation	English Term	Definition
L1	Mechanical Layer	First layer of the four-layer diagnostic architecture: joint mechanisms, reducers, bearings, end-effectors, and other physical mechanical components
L2	Electrical Control Layer	Second layer of the four-layer diagnostic architecture: servo drives, safety controllers, sensors, communication interfaces
L3	Software Middleware Layer	Third layer of the four-layer diagnostic architecture: controller firmware, ROS, communication protocols, coordinate-frame management
L4	AI Decision Layer	Fourth layer of the four-layer diagnostic architecture: perception models, planning networks, reinforcement-learning policies
FTFR	First-Time Fix Rate	Share of work orders whose root cause is correctly identified on the first visit (target ≥ 75 %)
MTDA	Mean Time to Diagnose (Accurately)	Average time from diagnosis start to root-cause confirmation
RCA	Root Cause Analysis	Systematic analytical method for identifying the root cause of a fault (rather than its surface symptoms), including 5-Why, Ishikawa, and FTA
MCSA	Motor Current Signature Analysis	Diagnostic method that analyzes the motor-current spectrum to detect winding and bearing faults
OSCE	Objective Structured Clinical Examination	Multi-station standardized scoring framework used in the RSF practical-skills assessment

D.4 Domain 3 — Remote Service and Digital Operations

Abbreviation	Chinese Term	English Term	Definition
RDT	**Robot Digital Twin**	Robot Digital Twin	Virtual digital model synchronized in real time with the physical robot system, supporting state assessment, simulation, and prediction
RUL	**Remaining Useful Life**	Remaining Useful Life	Predicted remaining normal-operation time of a critical component before its maintenance threshold is reached
HI	**Health Index**	Health Index	Composite equipment-state metric that fuses multi-dimensional sensor data into a single value in the 0–100 range

OTA	**Over-The-Air Update**	Over-The-Air	Technology for remotely deploying equipment firmware, control software, or AI models via network
CBM	**Condition-Based Maintenance**	Condition-Based Maintenance	Proactive maintenance strategy triggered when sensor data or diagnostic indicators exceed defined thresholds
PdM	**Predictive Maintenance**	Predictive Maintenance	Maintenance approach that uses machine-learning models to predict failure timing and intervene in advance
PsM	**Prescriptive Maintenance**	Prescriptive Maintenance	Extension of predictive maintenance that automatically prescribes the optimal maintenance action (when, where, and what to do)
LSTM	**Long Short-Term Memory network**	Long Short-Term Memory	Deep-learning model that excels at time-series data and is well suited to equipment degradation-trend prediction
PINN	**Physics-Informed Neural Network**	Physics-Informed Neural Network	AI model that embeds physical-equation constraints into a neural network — currently the state-of-the-art approach for RUL prediction
ZTA	**Zero-Trust Architecture**	Zero Trust Architecture	Cybersecurity architectural principle of "never trust, always verify," applicable to robot remote-access scenarios
DMZ	**Industrial DMZ**	Industrial Demilitarized Zone	Isolated buffer zone between the OT network and the IT / Internet network through which all remote access must be relayed
SOH	**State of Health**	State of Health	Battery's current full-charge capacity as a percentage of its rated capacity — a measure of battery aging
TSN	**Time-Sensitive Networking**	Time-Sensitive Networking	Industrial-Ethernet protocol providing deterministic low latency; the network infrastructure for real-time robot control
MFA	**Multi-Factor Authentication**	Multi-Factor Authentication	Authentication mechanism requiring two or more verification factors — a baseline requirement for RSF remote access
PSI	**Population Stability Index**	Population Stability Index	Statistical measure of data-distribution shift (> 0.25 marks the major-drift warning threshold)

D.5 Domain 4 — SLA Design and Service Commitment

Abbreviation	English Term	Definition
SLA	Service Level Agreement	Contract document that quantifies service-quality commitments, including metric definitions, target values, and breach-compensation clauses
KPI	Key Performance Indicator	Quantifiable indicators used to measure service performance (e.g., availability, MTTR, PM compliance rate)
RaaS	Robots as a Service	Subscription deployment model in which the service provider retains equipment ownership — the strongest incentive structure for SLA fulfillment
CSAT	Customer Satisfaction	Survey-based metric of customers' subjective evaluation of service

	Score	quality (RSF target ≥ 7.5 / 10)
NPS	Net Promoter Score	Metric of customers' likelihood to recommend; used in ATC training-quality assessment (target ≥ 8.0 / 10)
P&L	Profit and Loss	Revenue and cost management of service operations; the core financial responsibility of Specialist-tier Service Managers
TCO	Total Cost of Ownership	Complete cost over the equipment's full lifecycle, including acquisition, maintenance, energy, and end-of-life disposal

D.6 Domain 5 — Cross-Platform Service Procedures

Abbreviation	English Term	Definition
AMR	Autonomous Mobile Robot	Mobile robot that uses SLAM or other navigation technology to autonomously plan paths
Cobot	Collaborative Robot	Robot designed for safe collaboration with humans in a shared workspace; governed by ISO/TS 15066
SLAM	Simultaneous Localization and Mapping	Algorithm by which a mobile robot simultaneously builds an environment map and localizes itself within it
SEA	Series Elastic Actuator	Joint design with an elastic element placed in series between motor and load, used for force control and collision compliance
VLA	Vision-Language-Action Model	Core AI architecture for humanoid robots fusing visual perception, natural-language understanding, and action generation
FMS	Fleet Management System	Software platform that uniformly dispatches and monitors multiple AMRs, typically using the VDA 5050 protocol for communication
STO	Safe Torque Off	Robot safety function that immediately removes all motor torque without waiting for deceleration
SS1	Safe Stop 1	Controlled stop: decelerate to halt, then activate STO (Category 1 stop)
SS2	Safe Stop 2	Controlled stop: decelerate to halt and maintain the stopped position (motor continues to apply holding torque)

D.7 Domain 6 — AI / ML System Service Methods

Abbreviation	English Term	Definition
MLOps	Machine Learning Operations	Methodology for full-lifecycle management of AI models, from training to deployment, monitoring, and updating
RAG	Retrieval-Augmented Generation	AI technique combining knowledge-base semantic search with large-language-model generation, used for intelligent diagnostic assistants
LLM	Large Language Model	General-purpose language AI model trained on large-scale text (e.g., GPT-4, Claude), applicable to service-knowledge assistance
mAP	Mean Average Precision	Composite performance-evaluation metric for object-detection models (typically expressed as mAP@0.5)
Q1–Q4	Four-Quadrant AI Fault Classification	RSF-defined AI-layer fault classification framework: Q1 distribution shift / Q2 model drift / Q3 policy drift / Q4 data-quality failure
AMDM	Adaptive Multi-Dimensional Monitoring	Agentic AI monitoring framework that reduces anomaly-detection latency to 5.6 seconds

KFL	Known Fault Library	Organizational asset that stores diagnostic experience in structured form; the core data source for RAG knowledge systems

D.8 General Technical Terms

Abbreviation	English Term	Definition
EOAT	End of Arm Tooling	Tool mounted at the wrist of a robot (gripper, suction cup, welding torch, vision system, etc.)
TCP	Tool Center Point	Reference point of the robot end-effector and the core measurement baseline for accuracy verification
EtherCAT	EtherCAT	Real-time industrial bus protocol based on Ethernet, widely used for servo-drive communication
PROFINET	PROFINET	Industrial-Ethernet communication protocol promoted by Siemens and other vendors
OPC UA	OPC Unified Architecture	Cross-platform data-exchange standard for the Industrial IoT, supporting robot-to-cloud integration
MQTT	Message Queuing Telemetry Transport	Lightweight IoT messaging protocol, suitable for low-bandwidth transmission of high-volume sensor data
ROS	Robot Operating System	Mainstream middleware framework for robot software development (ROS / ROS2), widely used in AMRs and research robots
FTA	Fault Tree Analysis	Top-down logic analysis method that traces all possible root causes of a top-level failure event
FMEA	Failure Mode and Effects Analysis	Preventive analysis tool that systematically identifies potential failure modes and their effects
PPE	Personal Protective Equipment	Safety protective equipment required during robot field service (safety shoes, safety glasses, gloves, etc.)
BOM	Bill of Materials	Complete list of all parts and materials required for a product or maintenance task
CMMS	Computerized Maintenance Management System	Software platform for managing work orders, PM schedules, spare-parts inventory, and service performance