

Swift-Autonomy Solution

End-to-End Information and Communications
Technology (ICT) for Unmanned Surface Vessels

Solution White Paper

INTEGRATE
COMMUNICATE
MONITOR
OPERATE
DELIVER



SECURE
COMMUNICATIONS



INTEGRATED
SYSTEMS



REAL-TIME
AWARENESS



SCALABLE
SOLUTIONS



MISSION
READY

PEOPLE | VESSELS | SOLUTIONS
A SAFER TOMORROW

AUTONOMY
TODAY.
A STRONGER
TOMORROW.

Table of Contents

1. Executive Summary3

2. The Operational Need.....3

3. Design Principles3

4. The Swift-Autonomy (SA-1) Solution.....4

 4.1 Five Key Elements.....4

 4.2 Software Baseline5

 4.3 Common, Scalable Communications Framework.....5

5. Capability by ICT Area.....5

 5.1 Classified Networks to Support USV Operations.....5

 5.2 Robust Cybersecurity.....6

 5.3 System and Payload Integration.....6

 5.4 Unmanned Operations, Health and Status, and Resilience6

 5.5 SATCOM Integration6

 5.6 Application Hosting, PNT, and SWaP.....6

6. Capability Maturity Matrix6

7. Verification Status and Performance8

9. Systems Engineering, Integration, and Test.....9

 9.1 Configuration Management and Interface Control9

 9.2 Integration and Test Approach.....9

10. Sustainment.....9

11. Export, Disclosure, and Co-Production9

Appendix A: Systems Architecture10

Appendix B: List of Acronyms.....11

1. Executive Summary

Navies and maritime security forces are moving unmanned surface vessels (USVs) into fleet service. The limiting factor is rarely the hull or the engine; it is the information and communications technology (ICT) that connects the vessel, its autonomy, and its payloads to command and control (C2) nodes ashore and afloat, securely, at the required classification level, and across contested or degraded communications environments. Swiftships answers that need with the Swift-Autonomy (SA-1) Solution: a platform-agnostic ICT and autonomy stack built around a Ground Control System (GCS), a multi-link transport layer, and standardized onboard interfaces. Every element operates today on our USV and is exercised daily through the SA-1 Simulator, which serves as the solution's digital twin. This white paper describes the operational need, the design principles we apply, the solution architecture, the capability delivered in each ICT area, an honest capability maturity matrix that distinguishes what is fielded today from what is tailored per program, verification status and measured performance, and our systems engineering, sustainment, and export approach; see *Appendix A*.

Key Discriminators: (1) A fielded, export-controlled autonomy and C2 software baseline with health monitoring, adaptive multi-link bandwidth management, emissions control, and zero-trust security controls built in. (2) A browser-based SA-1 Simulator that functions as a digital twin, allowing operators to rehearse missions and engineers to verify software integrity before deployment to afloat hardware. (3) Modular, plug-and-play payload bays with isolated power and data channels and auto-recognition, which allow a customer's own sensors and effectors to be integrated without redesign. (4) Vertical integration: Swiftships builds hulls, integrates electronics, trains operators, and sustains vessels from its own shipyard and regional facilities, which shortens the ICT-to-vessel integration path and de-risks delivery.

2. The Operational Need

Across our customer base the requirement is consistent. Fleets need an end-to-end ICT solution that enables C2 of multiple USVs and their modular payloads from several remote locations, ashore and afloat, in support of distributed maritime operations. The ICT must carry vessel C2, payload operations including off-board data, communication between onboard systems across security domains, and communication with government and third-party systems. It must operate at the classification level the mission demands, up to and including Secret, on platforms that have no crew to reset a radio or reload a key.

It must be a common framework that scales across vessel classes and payload types rather than a unique build per hull. It must be designed for unmanned operation, with zero-touch provisioning and self-healing so that a vessel returns to a mission-ready state after a disruption without anyone on board. It must control its own radio frequency emissions on command. It must keep working, at reduced rates if necessary, when communications are denied, degraded, intermittent, or limited (DDIL). And it must be built for security authorization from the outset, with approved cryptography, remote key management, zero-trust architecture, and defensive cyber capability. *Table 1* summarizes the attributes we design against, grouped by the priority our customers typically assign to them.

Priority	Attributes
Primary	System readiness and rapid deployment; integration with onboard autonomy and payloads; payload transport to control nodes; a common, scalable communications framework with standardized interfaces; reliable unmanned operation with remote control, zero-touch provisioning, and self-healing; RF emissions control on command; resilient communications in contested and degraded environments; classified information exchange up to Secret; tactical control interfaces to government and third-party systems ashore and afloat; health and status reporting to the autonomy and the C2 node; security designed for national cryptographic approval, including encryption at rest and in transit, remote rekey, and remote or automated zeroization.
Secondary	Security domain transfer; defensive cyber operations (protect, detect, mitigate, respond, report); zero-trust architecture per NIST SP 800-207; reliability and maintainability with predictive maintenance; remote patching while underway with automatic rollback on failure.
Tertiary	Scalable application hosting with a defined IT service model; assured positioning, navigation, and timing (PNT) distribution and inertial navigation integration; onboard access to classified network web services; size, weight, and power (SWaP) reduction and modularity for multiple space sizes.
Program	Demonstration in operationally relevant environments; use of a digital twin to verify software before deployment; robust configuration management with documented interface control documents (ICDs) and open architecture; a lifecycle sustainment plan covering hardware, software, supply chain security, training, and obsolescence.

Table 1: ICT Attributes for USVs

3. Design Principles

Seven principles govern the Swift-Autonomy Solution. Each is a lesson from building and operating SA-1 on its USVs and from working alongside fleet program offices on USV requirements. *Table 2* states each principle and how the solution implements it.

Principle	Implementation - Swift-Autonomy (SA-1) Solution
Platform-agnostic, end-to-end	SA-1 is both an autonomy/C2 system and an ICT integration layer. We can demonstrate end-to-end traffic between a controlling node and a vessel with our own autonomy from day one, and integrate a customer's or third party's autonomy, C2, or payload system through traffic generators and then live interfaces. Swiftships acts as lead systems integrator for the ICT and works with vessel and payload vendors to bring their data into the system.
Common, scalable architecture	A three-tier framework (transport, secure network core, application/ICD layer) scales across vessel classes by changing only the transport tier. The same framework serves small craft such as S-class, medium and large USVs, and can extend to other unmanned vehicle types.
Multi-orbit, hybrid transport	SATCOM is central to over-the-horizon USV operations, and multi-orbit or hybrid transport maximizes end-to-end connectivity in contested environments. The transport tier combines SATCOM, line-of-sight RF, LTE/5G, and vessel-to-vessel mesh under an adaptive link manager, with defined insertion points for a customer's military SATCOM terminals and program-of-record radios.
DDIL by design	Throughput will fall, and latency will rise under degraded or contested conditions. The ICT publishes a Link Quality Advisory so that autonomy, C2, and payload systems can adapt their data rates, and the autonomy can continue the mission, hold station, or return to base when links are lost.
Security for authorization	Security is built for the customer's national cryptographic approval process rather than added later. Where a commercial two-layer approved-cryptography approach is acceptable to the customer's authority, it is the fastest credible path to Secret operations; where Type 1 or national high-grade devices are required, the architecture accommodates them in the same enclave design.
Open standards, governed interfaces	Every exchange is governed by an ICD built on open standards: UMAA over DDS for the autonomy bus, STANAG 4586 and JAUS adapters for control traffic, NMEA 0183 for navigation sensors, STANAG 4607 for radar tracks, and RESTful APIs for management and health. Vendors integrate against this layer, not against the transport.
Verify in the twin first	The SA-1 Simulator is a digital twin used for mission rehearsal, operator training, and regression testing. Software is verified in the twin before it is deployed to afloat hardware.

Table 2: Design Principles and their Implementation

4. The Swift-Autonomy (SA-1) Solution

The SA-1 solution treats the USV as a secure, self-managing ICT enclave connected to remote C2 nodes over an adaptive multi-link transport, with a digital twin closing the verification loop. Figure 1 shows the end-to-end architecture.

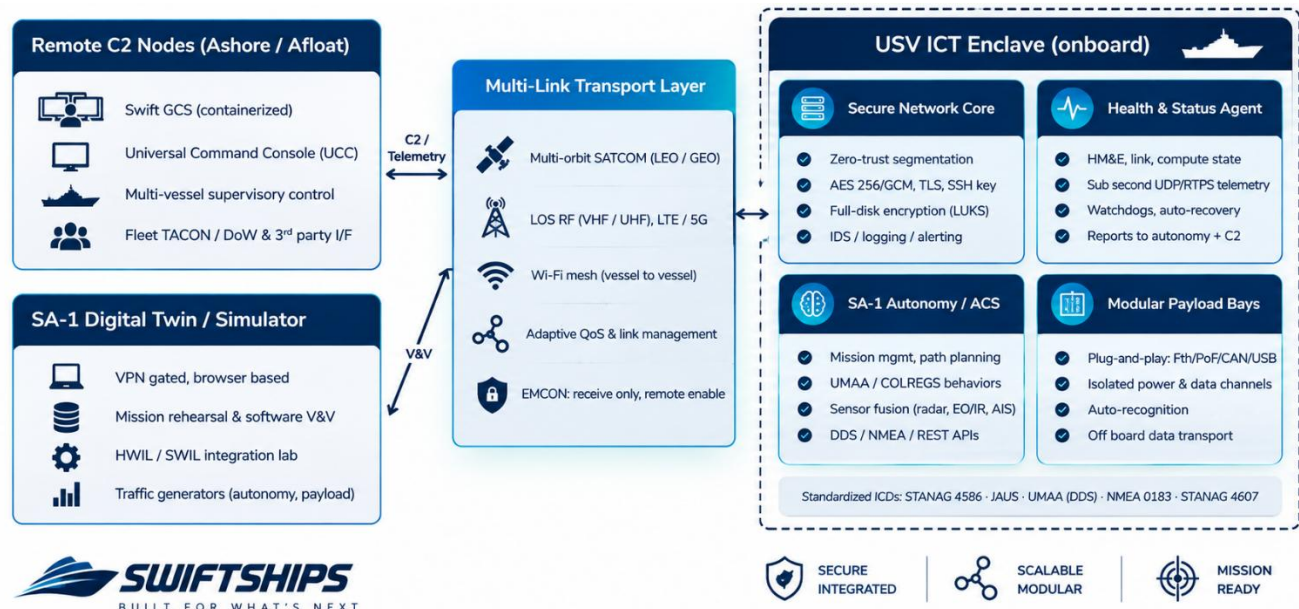


Figure 1: Swift-Autonomy Solution end-to-end architecture

4.1 Five Key Elements

Remote C2 nodes include the Swift GCS (containerized, deployable ashore or afloat) and the Universal Command Console (UCC), which provide multi-vessel supervisory control and serve as the interface point to government and third-party systems for tactical control. The multi-link transport layer combines multi-orbit SATCOM, line-of-sight RF, LTE/5G, and vessel-to-vessel mesh under an adaptive link manager with emissions control. The onboard secure network core enforces zero-trust segmentation, encryption in transit and at rest, and intrusion detection. The SA-1 autonomy and control system provides mission management, COLREGS-compliant navigation, sensor fusion, and health monitoring, and is the local data-exchange hub for

payloads. The SA-1 Simulator is the digital twin used for mission rehearsal, operator training, and software verification before deployment to afloat hardware.

4.2 Software Baseline

SA-1 is a next-generation Unmanned Maritime System (UMS) software that enables secure, scalable command and control of single or multiple USVs. It integrates sensing, navigation, communication, and mission execution for coastal security, port defense, anti-piracy, counter-terrorism, and swarming operations, enhancing maritime domain awareness while deterring conventional and asymmetric threats. SA-1 is classified as ITAR-controlled technical data under USML Category XI and is delivered only on AI/ML hardware with an anti-tamper-protected architecture in accordance with U.S. export and foreign disclosure requirements. *Table 3* summarizes the baseline.

Function	SA-1 capability (current baseline)
Autonomous controls	Real-time, high-fidelity control outputs to an Autonomy Baseline Layer (ABL) standard; PID plus ML-driven adaptive control; low-latency CAN bus engine/throttle/steering; automated fault detection and closed-loop assurance; watchdogs, emergency stop, and manual override.
Mission management	Plans, executes, and adapts missions in real time. Modes: man-in-the-loop (remote operator), man-on-the-loop (autonomy with oversight), fully autonomous (waypoint-driven with obstacle/collision avoidance). Route corridors, geofenced regions, station keeping, return to base, and in-mission route edits.
Communications and security	Optimized multi-link bandwidth with adaptive QoS for mission-critical traffic; EMCON for stealth; AES-256/GCM encryption with TLS authentication; zero-trust-based inference and privileged access; LUKS full-disk encryption; certificate-based remote access with hardened firewall policies and SSH-key-only authentication; intrusion detection with logging and automated alerting to the GCS.
Data links	RF (VHF/UHF), SATCOM (Iridium, Starlink), LTE/5G, and Wi-Fi mesh; sub-second UDP/RTPS telemetry for navigation and health.
Computing	Ruggedized industrial PC (OnLogic Karbon 800 class) with GPU for AI and parallel processing; ModBag and PCIe expansion; 2 x 32 GB DDR4; 1 TB NVMe rugged storage. Interfaces: WAN, USB, serial, PoE (2 x 2.5 GbE LAN), CAN bus.
Interoperability	NMEA 0183, DDS, and RESTful APIs; open architecture frameworks (UCI and/or JAUS); STANAG 4586 and STANAG 4607 (radar); UMAA and COLREGS-compliant path planning; sensor fusion middleware and data logging/analysis tools.
Situational awareness	Common operational picture with fused charts, traffic (AIS), weather, and history; radar (SIMRAD HALO 24), GNSS/INS (Vector Nav VN-300, RTK/PPK), FLIR EO/IR (M364C), 6 to 8 cameras for 360-degree coverage; FinBladeAI computer vision for imagery and pattern recognition; expandable to LiDAR, sonar, and EW sensors.

Table 3: SA-1 Baseline Capabilities Relevant to USV ICT

4.3 Common, Scalable Communications Framework

The framework has three tiers. Scaling across vessel classes is a matter of sizing Tier 1 (number and type of link modules) and Tier 2 (compute and switching) while holding Tier 3 constant, so that vessel and payload vendors integrate once.

- **Transport (Tier 1):** Interchangeable link modules (multi-orbit SATCOM, LOS RF, LTE/5G, mesh, and defined insertion points for customer military SATCOM and program-of-record radios) behind a common link-manager API. Each module reports availability, throughput, latency, and emission state. The link manager applies adaptive QoS, enforces EMCON directives from the C2 node, and publishes a Link Quality Advisory so autonomy, C2, and payload systems can throttle data rates in degraded or contested conditions.
- **Secure network core (Tier 2):** A zero-trust segmented onboard network with separate enclaves for vessel control, payload data, and management, encrypted in transit and at rest. The core is built from commercial components selected for eligibility under national approved-cryptography programs so that a classified enclave can be established early in a program, with the same enclave design accommodating national high-grade devices where required.
- **Application and ICD layer (Tier 3):** A single set of Interface Control Documents governs every exchange: UMAA over DDS for the autonomy bus, STANAG 4586/JAUS adapters for legacy control traffic, NMEA 0183 for navigation sensors, STANAG 4607 for radar tracks, and RESTful APIs for management and health.

5. Capability by ICT Area

5.1 Classified Networks to Support USV Operations

The onboard secure network core provides zero-trust segmentation, AES-256/GCM with TLS authentication, LUKS full-disk encryption, SSH-key-only certificate-based access, hardened firewall policies, and intrusion detection with logging and alerting to the GCS. These controls are the foundation for a classified enclave but are not by themselves a classified network. Our path to Secret operations is a two-layer approved-cryptography construct: two independent layers of encryption from products on

the customer's national approved-components list, configured to the applicable capability package, with a key management concept that supports remote rekey and remote or automated zeroization. Data at rest on the platform uses eligible full-disk encryption products in the same two-layer construct. Where the customer's authority requires national high-grade or Type 1 devices, SA-1 accommodates them in the same enclave design.

5.2 Robust Cybersecurity

SA-1 was designed with a zero-trust posture from the outset: continuous authentication and access control, privileged access management, per-user certificate authentication, hardened firewall policies, full-disk encryption, and intrusion detection with automated alerting. The GCS provides cybersecurity management (IDS and encryption) as a mission control function. For each program we map these controls to the NIST SP 800-207 zero-trust pillars (identity, device, network, application, data, visibility and analytics, automation and orchestration), document the security architecture to the customer's national policy set, and produce the authorization artifacts the customer's security authority requires. Defensive cyber operations (protect, detect, mitigate, respond, report) build on the existing IDS and logging pipeline with an onboard playbook engine that can isolate an enclave or force a safe state, and a reporting channel to the C2 node.

5.3 System and Payload Integration

Integration with onboard systems is the core of SA-1. Local data exchange uses CAN bus for the Glendinning remote control system and the autonomy controller; NMEA 0183 and 3.3-volt logic over CAN, Ethernet, RS-232, I2C, and SPI for sensors; and DDS, NMEA, and RESTful APIs for higher-level systems. Payload integration on S-class is by modular payload bays with quick-release mounts and a hot-swappable interface hub that provides plug-and-play Ethernet, USB, serial, CAN, and PoE connectivity, isolated power and data channels for performance and electrical safety, auto-recognition of installed payloads, and API-driven control and monitoring, including API-driven triggers for weapon or effector payloads. Payload transport to the control node is carried in its own enclave on the secure network core so that off-board data and payload C2 can be prioritized or throttled independently of vessel control traffic.

5.4 Unmanned Operations, Health and Status, and Resilience

SA-1 executes long-endurance missions in high-traffic environments without continuous C2 connectivity and supports single- and multi-vessel behaviors including transit, rally/formation muster, blockade/intercept, infiltrate/exfiltrate, and coordinated penetration. Health monitoring covers HM&E status, engine performance (temperature, pressure, electrical), alarms, link state, and compute state, with sub-second UDP/RTPS telemetry to the operator and a consolidated alarm panel at the GCS. Built-in watchdogs, automated fault detection, and closed-loop assurance support recovery from onboard faults; the program-level extension is a documented zero-touch provisioning and self-healing sequence that returns the ICT enclave to a mission-ready state after a power interruption without on-site intervention. RF emissions control exists today as EMCON for stealth, extended per program to receive-only radio operation with remote activation by the C2 node. Resilience in contested or degraded environments comes from the multi-link transport with adaptive QoS and from the autonomy's ability to continue the mission, hold station, or return to base when links degrade.

5.5 SATCOM Integration

The current baseline uses commercial LEO SATCOM (Starlink) and Iridium alongside RF and LTE/5G. Integration with a customer's military SATCOM architecture, including national or allied MILSATCOM terminals and government gateways, is delivered per program: the transport tier accepts additional link modules through a defined module ICD, and the first government-furnished or partner-supplied terminal is integrated during the vessel integration phase.

5.6 Application Hosting, PNT, and SWaP

The onboard computer (ruggedized industrial PC with GPU, 64 GB memory, 1 TB NVMe, PCIe and ModBag expansion) hosts autonomy, sensor fusion, computer vision, and the health agent. For customer applications, we offer a containerized Platform-as-a-Service model: the ICT enclave provides orchestration, resource limits, and security policy, and the customer or third parties supply containers built to a published interface. Assured PNT is provided by dual GNSS receivers and a VectorNav VN-300 GNSS/INS with RTK/PPK precision, distributed to onboard systems over NMEA 0183 and the DDS bus, with integrity monitoring and an interface for government assured-PNT sources available per program. The S-class electrical budget (16.2 -24 kWh, 816.9 W total integrated load including a 56 W mock modular payload) demonstrates a compact ICT footprint suitable for small hulls, and the same modular components scale to larger spaces.

6. Capability Maturity Matrix

Table 4 states the maturity of the SA-1 Solution against every attribute in *Table 1*. Of 24 attributes, 12 are Fielded, 7 are Tailored, and 5 are Roadmap. Every Roadmap item is in the cryptographic, cross-domain, or classified-network-services space, where the deliverable depends on the customer's national approval authority and is worked through each program's design and authorization phases.

Attribute	Status	Evidence & Approach
System readiness and rapid deployment	Fielded	Swiftships operates a U.S. shipyard, an integration and training capability, a MENA regional office, and co-production sites globally. S-class USVs offer SA-1 integration.
System integration (onboard autonomy, payloads)	Fielded	SA-1 provides onboard autonomy; local exchange over CAN, Ethernet, RS-232, I2C, SPI, NMEA 0183, DDS, and REST operates on S-class. Third-party autonomy integration via traffic generator, then live interface.
Payload integration and support (transport to control nodes)	Fielded	Modular payload bays with plug-and-play interfaces, isolated power/data, auto-recognition, and API control on S-class. Dedicated payload enclave on the secure network core for transport to control nodes.
Communications framework (common, scalable, standardized ICDs)	Fielded	Three-tier framework defined (Section 4.3) with UMAA/DDS recommendation; ICD set exists for S-class (STANAG 4586, JAUS, NMEA 0183, STANAG 4607). Class-specific ICDs and the Link Quality Advisory message are baselined at program start.
Unmanned operations (remote control, zero-touch provisioning, self-healing)	Fielded	Remote control, watchdogs, automated fault detection, and closed-loop assurance are in place. Documented zero-touch provisioning and automated return to mission-ready after power interruption are implemented and verified in the integration lab.
RF emissions control (receive without emitting; remote activation)	Fielded	EMCON mode exists in SA-1. Receive-only radio state with remote activation from the C2 node is added per link module.
Resilient communications (contested/degraded)	Fielded	Multi-link transport (SATCOM, RF, LTE/5G, mesh) with adaptive QoS is operating. Formal DDIL profiles and measured performance under each profile are established in the integration lab.
SWaP reduction and modularity	Fielded	S-Class integrated electrical load of 816.9 W within a 16.2 kWh budget demonstrates a compact footprint; modular components and payload bays support multiple space sizes.
Configuration management, ICDs, open architecture	Fielded	SA-1 is under configuration control as a versioned software baseline (SS-451-11 on S-class); ICDs exist for S-class interfaces; open architecture per UCI/JAUS/UMAA. A CM plan is delivered at program kick-off.
Lifecycle sustainment (hardware, software, supply chain, training, obsolescence)	Fielded	ILS spares and tools list, global warranty support, and a five-module operator and maintainer training program. Secure supply chain and obsolescence plans are formalized per program.
Tactical control interfaces (government and third-party systems)	Fielded	GCS/UCC provide multi-vessel control and external interfaces via DDS and REST. Specific national system interfaces (tactical data links, C2 systems) are defined with the customer during design.
Health and status to autonomy and C2 node	Fielded	HM&E, engine, alarm, link, and compute status published sub-second over UDP/RTPS to SA-1 and the GCS; alarm panel with active and historical alerts. Level-of-service classification added per program.
Defensive cyber operations	Tailored	IDS, logging, and automated alerting to GCS exist. Onboard response playbooks and reporting to the C2 node are added per program.
Zero-trust architecture (NIST SP 800-207)	Tailored	Zero-trust-based inference, continuous authentication, and access control are built into SA-1. Formal NIST SP 800-207 mapping and documentation are produced per program.
Reliability and maintainability; predictive maintenance	Tailored	Remote system logging and alerting, modular hardware, and easy maintenance are design features of S-class. Predictive maintenance analytics on engine and electrical telemetry are added per program.
Remote patching with automatic rollback	Tailored	SA-1 is delivered as a managed software baseline with remote logging. Dual-image (A/B) update with automatic rollback on failed health check is implemented during Phase 1.
Application hosting; IT service model	Tailored	Onboard GPU compute hosts autonomy and vision today. Containerized PaaS model with published container interface (Section 5.6).
Assured PNT distribution and INS integration	Tailored	Dual GNSS and VN-300 GNSS/INS with RTK/PPK distributed over NMEA and DDS. Assured PNT source interface and integrity monitoring added per program.
Demonstration; digital twin; security authorization	Tailored	SA-1 Simulator is the digital twin; end-to-end unclassified demonstration is available today. Classified end-to-end demonstration follows enclave establishment. Security authorization is pursued with each customer's authority.
Classified information exchange up to Secret	Roadmap	Two-layer approved-cryptography architecture using products from the customer's national approved-components list; capability package selection and registration during design; enclave established for the lab demonstration.
Security designed for national approval; encryption at rest and in transit	Roadmap	Existing AES-256/GCM, TLS, and LUKS controls provide the base. Approved or approval-pathway cryptography delivered through the customer's national program; documentation to the customer's policy set during design.

Attribute	Status	Evidence & Approach
Remote rekey and remote/automated zeroization	Roadmap	Key management concept using eligible devices with remote rekey and remote or automated zeroization triggered by the C2 node or by tamper/geofence events. Designed during Phase 1; verified in the lab prototype.
Onboard classified network web services	Roadmap	Delivered as a service inside the classified enclave once the enclave and the customer's gateway connection are established.
Security domain transfer	Roadmap	Cross-domain solution provided through a partner product accredited by the customer's national authority; the ICT provides enclave separation and transport.

Table 4: Capability maturity matrix

Note: Fielded means the capability exists in the current SA-1 baseline and has been exercised in the stated environment. Tailored means the capability exists and is adapted, formalized, or further verified for each program's platform, policy set, and operating profile. Roadmap means the capability is delivered through the program roadmap, including through partners where noted

7. Verification Status and Performance

Table 5 states the verification status, environment, and performance of the current baseline. Values marked Measured come from the S-class as-built configuration and SA-1 Simulator operation; values marked Target are the key performance parameters we propose to verify in the integration lab and at sea for each program.

Attribute/Parameter	Status	Environment	Performance
Autonomous navigation and collision avoidance (UMAA, COLREGS)	Measured	In-water on USV; SA-1 Simulator with ENC charts	Safe-route planning against ENC data; route corridor enforcement with cross-track error reported; station keeping with inner/outer radius and hold timer.
Platform performance (S-class)	Measured	In-water trials, Morgan City	Sprint 30+ kn at mission load (half fuel, full payload) in 2 ft significant wave height at all headings; economical 20 kn at full load; 1,500+ NM at 30 kn; 1250 NM and 125+ hours at 20 kn; operate/survive Sea State 3 to 4.
Telemetry and health reporting	Measured	In-water on USV; simulator	Sub-second UDP/RTPS navigation and health feedback; engine, alarm, voltage, and fuel status in the operator status bar.
Multi-link transport and adaptive QoS	Measured (unclassified)	In-water on USV (Starlink, RF); simulator	Man-in-the-loop remote operation to 1.5 km LOS; BLOS operation over SATCOM. Throughput/latency per DDIL profile: Target.
Encryption in transit and at rest	Measured (commercial)	USV and GCS	AES-256/GCM with TLS; LUKS full-disk encryption; SSH-key-only access. Two-layer approved-cryptography construct: Target.
Digital twin/simulator	Measured	SA-1 Simulator, VPN-gated web interface	Route planning, autonomous mission execution, station keeping, region geofencing, and in-mission route edits exercised in the simulator before deployment to hardware; used for operator training.
Payload plug-and-play and auto-recognition	Measured	USV with mock modular payload	Mock modular payload (56 W, 4.7 A, 26-pin) recognized and monitored through the payload API.
Multi-vessel supervisory control	Measured	GCS/UCC with simulator; in-water single vessel	Single- and multi-vessel behaviors (transit, muster, blockade/intercept) demonstrated in simulator; multi-vessel in-water demonstration: Target.
DDIL performance profiles (benign/degraded / denied)	Target	Integration lab with link emulation	Benign: full-rate video and payload data. Degraded: prioritized C2 and health at reduced rate with Link Quality Advisory to autonomy. Denied: autonomous continuation, station keep, or return to base with store-and-forward of logs on link recovery.
Recovery to mission-ready after power interruption	Target	Integration lab	Unattended return to mission-ready state, including re-establishment of secure links, within a bounded time agreed with the customer.
Remote rekey and zeroize	Target	Integration lab, approved devices	Rekey and zeroize commanded from the C2 node and by automated trigger, with confirmation reported in health and status.
Remote patch with automatic rollback	Target	Integration lab; simulator	A/B image update; automatic rollback on failed post-update health check.

Table 5: Verification Status, Environment, and Performance

Note: Swiftships designs, builds, and integrates USVs because the ICT enclave is integrated at the same yard that builds the hull; ICT installation, checkout, and in-water verification occur in one location. Co-production and in-country integration arrangements are available for customers with local industrial participation requirements.

9. Systems Engineering, Integration, and Test

9.1 Configuration Management and Interface Control

SA-1 is maintained as a versioned, configuration-controlled software baseline (the S-class configuration carries SA-1 baseline SS-451-11), and the hardware is documented as-built by the ship work breakdown group (hull, machinery, electrical, navigation, and control). For each program, we deliver a Configuration Management Plan at kick-off covering hardware, software, firmware, and cryptographic configuration items; a Configuration Control Board with customer participation; and baseline audits before each demonstration. Every external interface is governed by an ICD: the autonomy bus (UMAA over DDS), legacy control (STANAG 4586, JAUS), navigation sensors (NMEA 0183), radar tracks (STANAG 4607), the payload interface (physical, electrical, and API), the link-manager and Link Quality Advisory interface, and the health and status interface to the C2 node. ICDs are released under the CM plan and made available to vessel and payload vendors through the customer.

9.2 Integration and Test Approach

We use a hybrid integration environment. A physical hardware-in-the-loop (HWIL) laboratory at Morgan City hosts the prototype ICT enclave, representative link modules with link emulation for DDIL profiles, the SA-1 autonomy computer, and payload interface hardware, with the GCS or RCS as the controlling node. A cloud-hosted or customer-hosted software-in-the-loop (SWIL) environment hosts SA-1 Simulator instances and traffic generators so platform and payload vendors can integrate remotely, and regression testing runs continuously against the digital twin before deploying any software to hardware. Test events progress from interface conformance (ICD-level), to enclave-level security verification, to end-to-end controlling-node-to-vessel demonstrations under each DDIL profile, culminating in the laboratory demonstration, vessel installation, and sea trials.

10. Sustainment

Swiftships sustains the ICT system across multiple vessel classes through the same integrated logistics support model used for its vessels. Hardware maintenance is based on modular, plug-and-play components with insulated electrical systems designed for harsh marine environments (vibration, shock, and ingress protection) and replaceable without specialized tooling; each configuration has an onboard and consumable spares list and a specialized tools list, and global warranty support is provided. Software maintenance is delivered as a managed baseline with remote logging and alerting, remote patching with rollback, and simulator-based regression before release. Preventive and predictive maintenance use the engine, electrical, and link telemetry already collected by the health agent. Supply chain security follows a documented plan covering approved sources, component traceability, and counterfeit avoidance for ICT and cryptographic items. Training is delivered through the Swift USV and Autonomy Training Guide, currently five modules (product classification, SA-1, SA-1 Simulator, GCS, and master equipment and systems), with ICT operator, maintainer, and cyber-administrator modules added. Obsolescence is managed through the modular link and compute architecture, which allows individual modules to be refreshed without changing the ICD layer.

11. Export, Disclosure, and Co-Production

SA-1 software is ITAR-controlled technical data under USML Category XI. It is delivered to end users only on AI/ML hardware with an anti-tamper-protected architecture, in accordance with U.S. export regulations (including EAR ECCN 9D515 for associated items), DoDI 5200.39 program protection practices, and applicable foreign disclosure requirements. No source code or algorithmic technical data is released. Swiftships manages export authorization as part of each program schedule and has established co-production and in-country integration arrangements, including its Alexandria, Egypt co-production site, for customers with industrial participation requirements. The customer sources cryptographic components, cross-domain solutions, and military SATCOM terminals through its national channels or through partners accredited by the customer's authority.

Appendix A: Systems Architecture



Appendix B: List of Acronyms

Acronym	Definition
ABL	Autonomy Baseline Layer
ABS	American Bureau of Shipping
ACS	Autonomy Control System
AIS	Automatic Identification System
BLOS	Beyond Line of Sight
C2	Command and Control
CM	Configuration Management
COLREGS	International Regulations for Preventing Collisions at Sea
DDIL	Denied, Degraded, Intermittent, Limited
DDS	Data Distribution Service
EMCON	Emissions Control
ENC	Electronic Navigational Chart
EO/IR	Electro-Optical / Infrared
GCS	Ground Control System
GNSS	Global Navigation Satellite System
HM&E	Hull, Mechanical, and Electrical
HWIL / SWIL	Hardware-in-the-Loop / Software-in-the-Loop
ICD	Interface Control Document
ICT	Information and Communications Technology
IDS	Intrusion Detection System
ILS	Integrated Logistics Support
INS	Inertial Navigation System
ITAR	International Traffic in Arms Regulations
JAUS	Joint Architecture for Unmanned Systems
KPP	Key Performance Parameter
LOS	Line of Sight
LRIP	Low-Rate Initial Production
LUKS	Linux Unified Key Setup
MILSATCOM	Military Satellite Communications
PaaS	Platform as a Service
PNT	Positioning, Navigation, and Timing
QoS	Quality of Service
RCS	Remote Control Station
RTK / PPK	Real-Time Kinematic / Post-Processed Kinematic
RTPS	Real-Time Publish-Subscribe
SA-1	Swift Autonomy
SATCOM	Satellite Communications
STANAG	NATO Standardization Agreement
SWaP	Size, Weight, and Power
UCC	Universal Command Console
UCI	Universal Command and Control Interface
UMAA	Unmanned Maritime Autonomy Architecture
UMS	Unmanned Maritime System
USML	United States Munitions List
USV	Unmanned Surface Vessel
XTE	Cross-Track Error

Acronym	Definition
ZTA	Zero Trust Architecture

Table 6: List of Acronyms