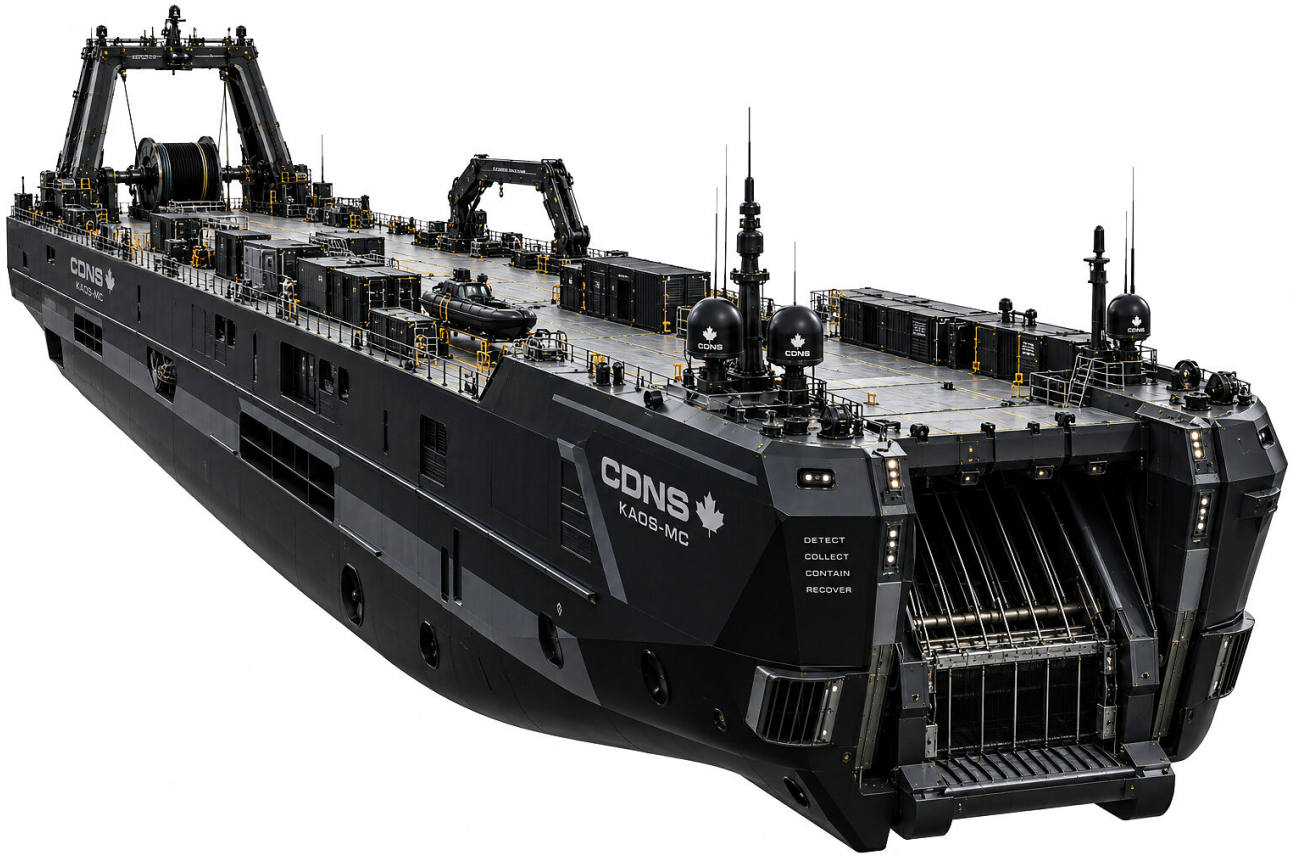
THE WATER FAMILY

KMM-01

THE UNCREWED CLEARANCE WORKBOAT

An uncrewed catamaran that surveys a controlled water area and lifts inert objects through a flooded corridor, each lift approved by a remote supervisor.



13.0–14.5 m
LENGTH OVERALL, DESIGN STUDY RANGE

4,000 kg
BENIGN MISSION PAYLOAD, THE WEIGHT BUDGET

6
CASSETTES, ONE OBJECT IN EACH

7
FLOODED TRANSFER ZONES, MOUTH TO CELL

35,000 W
CONTINUOUS, EACH OF TWO PROPULSORS

AT A GLANCE

NOBODY ABOARD, NO WHEELHOUSE. A PERSON APPROVES EVERY LIFT.

The figures that size the vessel, and the four reasons a customer with a controlled water area and objects in it chooses this design.

NOBODY ABOARD

DRAWN UNCREWED FROM THE FIRST LINE

No wheelhouse, no accommodation and no mission step that waits for a hand. The deck a crew would need is working deck, and every essential state is sensed and telemetered to a supervisor ashore or aboard a support vessel.

THE CORRIDOR

THE OBJECT TRAVELS DOWN THE HULL, NOT OVER THE RAIL

Twin displacement hulls own a sheltered submerged corridor on the centreline. The vessel performs most of the gross positioning, and a seven-zone flooded path carries each object from the forward intake to its own cassette in the central bay.

ONE OBJECT PER CELL

SIX CASSETTES, EACH WITH ITS OWN IDENTITY AND STATE

Every object goes into its own flooded, individually removable cassette with a visible serial, an electronic identity and independent occupancy sensing. The selector does not route to a cell that is occupied or cannot prove its state, and the mission computer holds an inventory record for every cell.

A PERSON APPROVES

THE VESSEL ASKS; THE SUPERVISOR ANSWERS

The remote supervisor approves the mission plan, and each candidate-object interaction is explicitly approved before it proceeds. Shore also holds a stop path that does not run through the mission screen, into a safety subsystem that owns the emergency stop and both motion permissions.

IN THIS SHEET

01 · SPECIFICATION

GROUPED THE WAY AN ENGINEER READS IT. EACH FIGURE BESIDE THE BASIS IT RESTS ON.

Principal dimensions are design study ranges and are given as ranges. Masses are the weight budget's allowances with their growth included, and powers are the power budget's continuous and peak lines.

01 PRINCIPAL DIMENSIONS AND HULL FORM

PARAMETER	VALUE	BASIS
Length overall	13.0–14.5 m	design study range
Length class	13–14 m	the reference configuration
Beam	5.0–6.0 m	design study range
Beam class	5–6 m	the reference configuration
Transit draft	1.0–1.4 m	design study range
Hull form	Catamaran: twin displacement hulls joined by a deep cross-deck around a central wet mission corridor	the naval architecture design basis
Cassette stations	6, nominal	the naval architecture design basis; a mandatory requirement
Crew spaces	None: no permanent wheelhouse and no crew accommodation	design rule, the master design description
Service handling	Aft service gantry/crane	the reference configuration
Mast	Navigation and communications sensors on the roof and mast	the reference configuration
Operator station	Remote, ashore or aboard a support vessel	the reference configuration
Subdivision	Watertight subdivision; one-compartment flooding is a design loading condition	the system breakdown and the stability plan
Design priorities, in order	Low-speed manoeuvrability; work-zone stability; the central mission corridor; simple machinery access; damage tolerance and subdivision; reasonable transit efficiency; transportability only where required	the naval architecture design basis, ranked one to seven

02 MASS BUDGET

PARAMETER	VALUE	BASIS
Hull primary structure	4,620 kg	design value, the weight budget, with its 10 % growth allowance
Cross-deck and mission corridor	1,456 kg	design value, the weight budget, with its 12 % growth allowance
Outfit, rails and hatches	770 kg	design value, the weight budget, with its 10 % growth allowance
Propulsors and drives	1,815 kg	design value, the weight budget, with its 10 % growth allowance
Battery, genset and fuel	3,680 kg	design value, the weight budget, with its 15 % growth allowance
HV and LV distribution	728 kg	design value, the weight budget, with its 12 % growth allowance
Cooling, bilge and utilities	728 kg	design value, the weight budget, with its 12 % growth allowance
Sensors, mast and communications	483 kg	design value, the weight budget, with its 15 % growth allowance
Mission head	1,092.5 kg	design value, the weight budget, with its 15 % growth allowance
Transfer trunk and selector	1,437.5 kg	design value, the weight budget, with its 15 % growth allowance
Six empty cassettes	990 kg	design value, the weight budget, with its 10 % growth allowance
Controls and computers	299 kg	design value, the weight budget, with its 15 % growth allowance
Gantry and service handling	560 kg	design value, the weight budget, with its 12 % growth allowance
Benign mission payload	4,000 kg	design value, the weight budget, carried with no growth allowance
Sum of the thirteen vessel lines	18,659 kg	arithmetic: the sum of the thirteen vessel lines above, payload excluded
Sum of all fourteen lines	22,659 kg	arithmetic: the sum of the thirteen vessel lines above and the 4,000 kg payload

03 PROPULSION AND ELECTRICAL ARCHITECTURE

PARAMETER	VALUE	BASIS
Propulsors	Two independent electric propulsors on independent motor drives	the hybrid-electric reference architecture
Steering	Steering/azimuth control	the system breakdown

PARAMETER	VALUE	BASIS
Propulsion sizing	For acceptable transit performance and for low-speed thrust authority in current and wind during mission mode, never from top speed alone	the resistance and propulsion method
Main bus	High-voltage DC	the hybrid-electric reference architecture
Energy	Battery buffer and genset generation	the hybrid-electric reference architecture
Auxiliary rails	48 V and 24 V, isolated	the hybrid-electric reference architecture
Essential supply	24 V uninterruptible supply	the hybrid-electric reference architecture
Essential supply carries	The safety controller, essential navigation state, command telemetry, bilge and fire monitoring, the event recorder and controlled shutdown	the electrical architecture
Shore connection	Shore charging and service, with shore-power isolation	the reference architecture; a mandatory requirement
Electrical domains	HV propulsion and high-power mission; 48 V sensor and compute; 24 V control and navigation; 24 V essential UPS; safety I/O; shore service	the electrical architecture
Electrical protection	Branch protection, main isolation, emergency propulsion inhibit, insulation monitoring where required, sealed connectors and redundant control-network power	mandatory requirements
EMC segregation	High-current motor and inverter wiring physically separated from sonar, GNSS, analog sensors, Ethernet and safety I/O	the electrical architecture
Low-noise operation	Silent or low-noise mission phases of short duration	an advantage of the hybrid-electric architecture

04 POWER BUDGET

PARAMETER	VALUE	BASIS
Port propulsion	35,000 W continuous; 75,000 W peak	power budget: duty 0.55, main HV domain
Starboard propulsion	35,000 W continuous; 75,000 W peak	power budget: duty 0.55, main HV domain
Mission hydraulic power unit	12,000 W continuous; 30,000 W peak	power budget: duty 0.25, mission HV/AC domain
Mission and perception compute	1,800 W continuous; 2,800 W peak	power budget: duty 1.0, 48 V domain

PARAMETER	VALUE	BASIS
Sonar suite	850 W continuous; 1,500 W peak	power budget: duty 0.9, 48 V domain
Camera suite	650 W continuous; 900 W peak	power budget: duty 1.0, 24/48 V domain
GNSS/INS, DVL, radar and AIS	500 W continuous; 900 W peak	power budget: duty 1.0, 24 V essential domain
Communications	450 W continuous; 900 W peak	power budget: duty 1.0, 24 V essential domain
Network and storage	400 W continuous; 650 W peak	power budget: duty 1.0, 24/48 V essential domain
Bilge and utilities	700 W continuous; 3,500 W peak	power budget: duty 0.2, 24/48 V domain
Lighting	450 W continuous; 1,200 W peak	power budget: duty 0.5, 24 V domain
Growth reserve	9,000 W continuous; 15,000 W peak	power budget: duty 1.0, allocated

05 MISSION MODULE AND FLOODED TRANSFER

PARAMETER	VALUE	BASIS
Objects handled	Inert surrogate objects only	the mission module functional specification
Intake	Forward submerged intake between the hulls, with compliant guide geometry	the reference configuration and the mission module specification
Transfer path	Enclosed flooded transfer trunk in seven zones: guide mouth, intake, primary transfer, inspection, selector, vestibule, cassette	the flooded transfer zone specification
Zone transitions	Six permissions together: upstream occupancy valid, downstream state valid, gate state known, safety permission, drive health, vessel motion inside the envelope	the flooded transfer zone specification
Transfer	Controlled, low-speed and reversible, with occupancy tracked zone by zone	the mission module specification; a mandatory requirement
Occupancy sensing	Arrays in the intake, primary transfer and inspection zones	the sensor register
Mission head	Compliant head motion, mechanical travel stops, replaceable wear surfaces and a service lock	mandatory requirements
Positioning	The vessel performs most gross positioning; the module is not designed to pull large lateral or vertical alignment errors into itself	the mission module specification

PARAMETER	VALUE	BASIS
Forbidden automatic behaviours	Repeated force escalation; uncontrolled high-speed transfer; routing into an unknown cassette; gate closure with uncertain occupancy; transfer under excessive vessel motion; interaction with objects outside the validated inert surrogate family	the mission module specification
Jam detection	Drive load (motor current or hydraulic pressure) against commanded motion, occupancy progression timeout, gate state, and camera and sonar observation	the jam and recovery philosophy
Jam response	The module stops, freezes the gate sequence and alerts the supervisor; it permits only bounded, predefined benign-object clearing motions, and retreats and recovers rather than forcing a jam those motions do not clear	the jam and recovery philosophy
Hydraulic consumers	Head lift, head trim, two transfer drives, selector, isolation gate, flush valve bank and service gantry	the hydraulic consumer register
Hydraulic health and safety	Reservoir level, fluid temperature, filter differential pressure and branch pressure sensed; pressure limiting; maintenance isolation; protected wet-zone routing	mandatory requirements

06 CASSETTES

PARAMETER	VALUE	BASIS
Stations	6 nominal; the architecture scales from four to eight	mandatory requirements; the cassette design specification
Contents	One surrogate per cassette	the cassette design specification; a mandatory requirement
Cell	Individually removable flooded containment cell	the cassette design specification
Identity	Keyed installation, a visible serial and an electronic ID	the cassette design specification
State sensing	Present switch, latch-closed sensing, flooded or level sensor, occupancy sensor and a local visual status marker	the cassette instrumentation list

PARAMETER	VALUE	BASIS
State chain	Absent, installed, latched, empty and flooded, receiving, occupied, isolated, service lock, removal authorized; an unexpected transition blocks motion and raises a fault	the cassette design specification
Interlocks	No routing to an occupied cassette or to one whose state is not verified; no removal outside the service state	the requirements matrix
Inventory record	Cassette ID, install time, mission ID, occupancy state, object track ID, location of acquisition, isolation time, alarms and service history	the cassette instrumentation list
Shore handling	Removable shore cradle, lift interface, and service drain and fill	the cassette design specification

07 NAVIGATION, PERCEPTION AND COMMUNICATIONS

PARAMETER	VALUE	BASIS
GNSS and inertial navigation	Dual-antenna GNSS/INS on the mast; 360°; navigation and heading	the sensor register, essential
Marine radar	On the mast; 360°; surface traffic and obstacles	the sensor register, essential
AIS	On the mast; 360°; surface awareness	the sensor register, supporting
Surface cameras	Four electro-optical: forward, port, starboard and aft; 120° class each	the sensor register; forward essential, the other three supporting
Imaging sonar	Forward centreline, covering the mission corridor; work-zone object sensing	the sensor register, essential
Obstacle sonar	Forward hull, wide sector; underwater collision sensing	the sensor register, essential
Doppler velocity log	Keel and centre, looking down; low-speed velocity aiding	the sensor register
Altimeter	On the mission head, looking down; bottom clearance	the sensor register, essential
Intake cameras	Two, port and starboard of the intake; close-range alignment	the sensor register, essential

PARAMETER	VALUE	BASIS
Localization	Confidence monitored; GNSS degradation detected; inertial aiding fused; a degraded dead-reckoning interval supported	mandatory requirements
Command links	Two RF command links, encrypted, carrying authenticated command messages	the degraded mode matrix, the cyber security plan and a mandatory requirement
Shore link carries	Mission, telemetry, approvals and logs	the master interface register
Remote stop	An independent command path from shore to the safety subsystem, independent of the mission GUI	the interface register and a mandatory requirement

08 SUPERVISION AND SAFETY FUNCTIONS

PARAMETER	VALUE	BASIS
Mission phases	Eighteen, from mission preparation to maintenance and replenishment	the master design description
Supervisor approvals	The mission plan, and each candidate-object interaction before it proceeds	the operations document: explicit approval by the remote supervisor
Approach and acquisition gates	All nine together: approved track ID, valid geofence, localization confidence, acceptable vessel motion, no collision alert, healthy mission module, verified empty cassette, healthy communications state, no safety inhibit	the autonomy state machine
Abort conditions	Eleven, from object classification ambiguity to an obstacle or collision alert; any one cancels or pauses an interaction	the operations document
State transitions	Permission-based: mission software requests; safety and subsystem state must permit	the autonomy state machine

PARAMETER	VALUE	BASIS
Functional segregation	Navigation safety independent of perception AI; propulsion enable independent of the mission computer; acquisition actuation independent of classification; cassette routing interlocked with identity and state; remote E-stop independent of the mission GUI; maintenance mode inhibits through the safety controller	the master design description
Safety subsystem	Independent; owns the hardware emergency stop, propulsion permission and mission-motion permission; read-only status to mission software; defaults to inhibit when safety integrity is uncertain	the safety requirements specification
After an emergency stop	Explicit manual recovery; every safety trip logged with synchronized time	the safety requirements specification; a mandatory requirement
Lost communications	New acquisition blocked	a mandatory safety requirement
Gate-state disagreement	Motion blocked	a mandatory safety requirement
Maintenance mode	Propulsion blocked; a defined safe state for every actuator	mandatory safety requirements
Hazard register	Fifteen hazards: seven critical, seven major and one moderate, each with its design controls	the hazard register
Cyber security	Signed update bundles, secure boot when supported, device identity, unique credentials, least privilege, segmented networks, authenticated command messages, encrypted remote link, locked maintenance mode, audit logs, configuration backup, recovery image, software bill of materials, vulnerability tracking	the cyber security plan
Records	Safety-relevant events logged; operator approvals logged; pose and covariance logged; mission data retained after normal shutdown	the requirements matrix

09 STABILITY AND OPERABILITY

PARAMETER	VALUE	BASIS
Loading conditions	Twelve: lightship; departure; 50 % energy/fuel; full benign cassette payload; maximum forward and maximum aft cassette loading; maximum port and maximum starboard asymmetry; mission head deployed; service gantry benign lift; one-compartment flooding; tow/recovery	the hydrostatics and stability plan
Asymmetric loading	Mission software receives load and cassette state and prohibits further asymmetric loading as the validated stability envelope is approached	the hydrostatics and stability plan
Mission motion envelope	Heave, pitch, roll, sway velocity, yaw rate, current and under-keel clearance, with tighter limits for acquisition than for transit	the seakeeping and operability basis
Outside the envelope	Acquisition inhibited and transfer kept secured; the vessel holds, retreats or returns	the seakeeping and operability basis
Degraded operation	A defined response for each of eight failures, from loss of primary GNSS to a safety controller fault	the degraded mode matrix

10 HANDLING, SUPPORT AND SUSTAINMENT

PARAMETER	VALUE	BASIS
Launch and recovery	Travel lift, launch cradle or heavy trailer; crane lift only with a dedicated certified lifting design	the recovery, tow and launch plan
Disabled-vessel tow	Towed on an approved tow bridle within a validated speed and sea-state envelope; essential bilge and telemetry power stays alive under tow, and tow and recovery is one of the twelve stability loading conditions	the recovery, tow and launch plan and the stability plan
Shore footprint	Berth or stand, shore power, remote station, spares, washdown, mission-module stand, cassette cradles and diagnostic tools	the recovery, tow and launch plan

PARAMETER	VALUE	BASIS
Maintenance levels	Three: operator and mission support; field service; depot	the maintenance plan
Depot work	Propulsor overhaul, structural repair, and battery and genset major service	the maintenance plan
Maintainability	Line-replaceable electronics, a head service position, lockout-tagout points and a diagnostic interface	mandatory requirements
Corrosion protection	Anodes and a coating system; corrosion-compatible materials	the system breakdown, the maintenance task analysis and the requirements matrix

02 · THE PREMISE

SEVEN RULES CAME FIRST. THE HULL WAS DRAWN TO KEEP THEM.

KMM-01 is drawn as an uncrewed machine from first principles, not as a crewed boat with autonomy added later. The design description sets out seven rules before it sets out a single dimension.

KMM-01 is a fully uncrewed, remotely supervised workboat for submerged foreign-object survey and benign recovery: a twin-hull carrier with a submerged centreline acquisition corridor, a flooded transfer trunk, one-object-per-cassette storage, station keeping, marine perception, layered safety control and mission supervision from shore. The seven rules below are what uncrewed means in that design.

- ✓ No permanent wheelhouse.
- ✓ No crew accommodation.
- ✓ No manually dependent mission function.
- ✓ No hazardous maintenance access required during a mission.
- ✓ All essential state is sensed and telemetered.
- ✓ All safety-relevant actuation has a defined de-energized or inhibited behaviour.
- ✓ Mission functions remain subordinate to the safety kernel.

ELEMENT	REFERENCE CONFIGURATION
Hull	Catamaran; length class 13–14 m, beam class 5–6 m
Propulsion	Twin independent propulsors optimized for low speed
Power	Hybrid-electric architecture
Mission path	Forward submerged intake between the hulls, and an enclosed flooded transfer trunk
Storage	Six-cassette central bay
Service handling	Aft service gantry/crane
Sensing	Navigation and communications sensors on the roof and mast; underwater work-zone sensing integrated into the mission head
Supervision	Remote operator station ashore or aboard a support vessel

SCOPE

SURVEY AND BENIGN RECOVERY. INERT SURROGATE OBJECTS, BY DESIGN.

Every acquisition, transfer, cassette and material-handling interface is defined around inert surrogate objects. Specialist work on live ordnance sits outside this configuration: a separate interface document is retained for any independently authorized work, and none of that work's engineering is defined here.

03 · NAVAL ARCHITECTURE

TWO HULLS AROUND A WET CORRIDOR. SIZED FOR WORKING NEARLY STOPPED.

Twin displacement hulls joined by a deep cross-deck surround a central wet mission corridor. The design basis ranks low-speed manoeuvrability first and reasonable transit efficiency sixth.

The corridor decides the hull form. The water between two hulls is sheltered on both sides, so the acquisition corridor runs submerged on the centreline from a forward intake between the hulls, through an enclosed flooded trunk, to a six-cassette central bay. The mechanical philosophy follows from it: the vessel performs most gross positioning, and the mission module is not designed to pull large lateral or vertical alignment errors into itself.

PRINCIPAL DIMENSION	VALUE	BASIS
Length overall	13.0–14.5 m	design study range
Length class	13–14 m	reference configuration
Beam	5.0–6.0 m	design study range
Beam class	5–6 m	reference configuration
Transit draft	1.0–1.4 m	design study range
Cassette stations	6, nominal	mandatory requirement

1. **Low-speed manoeuvrability** Twin independent propulsors optimized for low speed, with station keeping to align the mission head.
2. **Work-zone stability** The mission motion envelope is tighter for acquisition than for transit.
3. **The central mission corridor** The submerged centreline path from the intake to the cassettes.
4. **Simple machinery access** Line-replaceable electronics, a head service position and lockout-tagout points are mandatory requirements.
5. **Damage tolerance and subdivision** Watertight subdivision, with one-compartment flooding carried as a loading condition.
6. **Reasonable transit efficiency** Propulsion is sized for acceptable transit performance and for sufficient low-speed thrust authority in current and wind during mission mode, never from a top-speed requirement alone.
7. **Transportability** Only where required.

04 · MASS AND STABILITY

FOURTEEN LINES IN THE MASS BUDGET. ONLY THE PAYLOAD CARRIES NO GROWTH.

The weight and CG budget carries thirteen vessel groups, each with its own growth allowance, and the benign mission payload at 4,000 kg with none. The stability plan carries twelve loading conditions.

GROUP	GROWTH ALLOWANCE	ALLOWANCE, GROWTH INCLUDED
Hull primary structure	10 %	4,620 kg

GROUP	GROWTH ALLOWANCE	ALLOWANCE, GROWTH INCLUDED
Cross-deck and mission corridor	12 %	1,456 kg
Outfit, rails and hatches	10 %	770 kg
Propulsors and drives	10 %	1,815 kg
Battery, genset and fuel	15 %	3,680 kg
HV and LV distribution	12 %	728 kg
Cooling, bilge and utilities	12 %	728 kg
Sensors, mast and communications	15 %	483 kg
Mission head	15 %	1,092.5 kg
Transfer trunk and selector	15 %	1,437.5 kg
Six empty cassettes	10 %	990 kg
Controls and computers	15 %	299 kg
Gantry and service handling	12 %	560 kg
Benign mission payload	0 %	4,000 kg
Sum of the thirteen vessel lines (arithmetic)	–	18,659 kg
Sum of all fourteen lines (arithmetic)	–	22,659 kg

- ✓ Lightship, and departure.
- ✓ 50 % energy/fuel, and full benign cassette payload.
- ✓ Maximum forward cassette loading, and maximum aft cassette loading.
- ✓ Maximum port asymmetry, and maximum starboard asymmetry.
- ✓ Mission head deployed, and service gantry benign lift.
- ✓ One-compartment flooding, and tow/recovery.

An error in the mission inventory can load the bay unevenly, and the hazard register carries asymmetric loading as a major hazard with a load map and a stability software limit against it. Mission software receives load and cassette state and prohibits further asymmetric loading when the validated stability envelope is approached.

Motion is gated the same way. Acquisition requires tighter limits than transit across heave, pitch, roll, sway velocity, yaw rate, current and under-keel clearance. If measured vessel motion exceeds the validated mission envelope, the vessel inhibits acquisition, keeps the transfer secured, and holds, retreats or returns.

05 · THE FLOODED TRANSFER

SEVEN ZONES FROM MOUTH TO CELL. SIX PERMISSIONS AT EVERY BOUNDARY.

The transfer path is specified zone by zone, from the guide mouth to the cassette cell. Moving an object from one zone to the next needs six conditions to hold together.

ZONE	NAME	PURPOSE
Z1	Guide mouth	Gross alignment and benign capture envelope
Z2	Intake	Establish controlled contact and move the surrogate into the trunk
Z3	Primary transfer	Low-speed progression with occupancy tracking
Z4	Inspection	Verify track continuity and orientation
Z5	Selector	Route to the selected cassette
Z6	Vestibule	Isolate the common trunk from the cassette cell
Z7	Cassette	Individual flooded containment of one surrogate

Every transition needs all six

- Upstream occupancy valid
- Downstream state valid
- Gate state known
- Safety permission
- Drive health
- Vessel motion inside the envelope

Forbidden automatic behaviour

- Repeated force escalation
- Uncontrolled high-speed transfer
- Routing into an unknown cassette
- Gate closure with uncertain occupancy
- Transfer under excessive vessel motion
- Interaction with objects outside the validated inert surrogate family

Occupancy is sensed, not assumed: arrays in the intake, primary transfer and inspection zones track the object's progression, and the inspection zone verifies track continuity and orientation before the selector routes it. Transfer is controlled, low-speed and reversible, and the mission head it starts from has compliant motion, mechanical travel stops, replaceable wear surfaces and a service lock.

A jam is read from drive load, as motor current or hydraulic pressure, against commanded motion, together with an occupancy progression timeout, gate state and what the cameras and sonar observe. When the module detects one it stops, freezes the gate sequence, identifies the occupied zones and alerts the supervisor. It then permits only bounded, predefined benign-object clearing motions, and a jam those motions do not clear is answered by retreat and recovery, never by repeated force.

For physical access the vessel has a controlled service state, in which propulsion and mission motion are both inhibited.

06 · THE CASSETTES

ONE OBJECT IN EACH CASSETTE. IDENTITY AND STATE PROVED APART.

A cassette is an individually removable flooded containment cell with its own identity and state tracking. One surrogate goes in each, and cassette routing is interlocked with the cell's identity and state.

6	4–8	1	9
NOMINAL CASSETTE STATIONS	STATIONS THE ARCHITECTURE SCALES ACROSS	SURROGATE PER CASSETTE	STATES IN THE DECLARED CHAIN

IDENTITY

ONE A PERSON READS, ONE THE MACHINE READS

Keyed installation, a visible serial and an electronic ID. Wrong cassette is a named hazard in the register, with visible and electronic identity and interlocks as its controls.

STATE

PRESENT, LATCHED, FLOODED, OCCUPIED

A present switch, latch-closed sensing, a flooded or level sensor, an independent occupancy sensor, and a local visual status marker at the cell.

RECORD

WHAT THE INVENTORY HOLDS

Cassette ID, install time, mission ID, occupancy state, the associated object track ID, the location of acquisition, isolation time, alarms and service history.

The cell moves through a declared chain: absent, installed, latched, empty and flooded, receiving, occupied, isolated, service lock, and removal authorized. Any unexpected transition blocks motion and raises a fault. Routing to an occupied cassette is prevented, routing to a cassette whose state is not verified is blocked, and removal outside the service state is prevented.

Ashore, the cell comes off on a removable shore cradle through a lift interface, with a service drain and fill. Cassette state also feeds stability: the cassette system supports asymmetry monitoring, and mission software limits further asymmetric loading as the validated envelope is approached.

07 · THE MISSION

EIGHTEEN PHASES, NINE GATES. A PERSON APPROVES EACH INTERACTION.

KMM-01 works a controlled water area with a defined mission polygon, recovery point, weather limit, communications plan, emergency response plan and remote supervisor. The supervisor approves the plan and explicitly approves each candidate-object interaction; in between, the machine maintains the geofence and collision avoidance and stops unsafe state transitions.

1. **Prepare and self-test** The supervisor approves the mission plan, and the vessel runs its systems self-test before departure.
2. **Transit and validate navigation** The vessel enters the area and validates navigation confidence.
3. **Survey and track** It surveys the assigned lanes and develops object tracks from underwater perception.

4. **Review and approval** A candidate-object interaction cannot proceed until it satisfies the validated inert-surrogate classification envelope and is explicitly approved by the remote supervisor.
5. **Restricted-speed approach** Vessel speed and acceleration are reduced, and station keeping aligns the mission head.
6. **Acquisition and flooded transfer** The acquisition system moves the benign surrogate into the flooded corridor, occupancy is tracked zone by zone, and a verified empty cassette is selected.
7. **Receipt, isolation and inventory** Receipt is confirmed, the cassette is isolated and recorded in the mission inventory, and the vessel continues or returns.

The full sequence runs to eighteen phases, closing with recovery and docking, post-mission data export, and maintenance and replenishment. Approach, alignment and acquisition open only when all nine of these hold at once:

- ✓ An approved track ID.
- ✓ A valid geofence.
- ✓ Localization confidence.
- ✓ Acceptable vessel motion.
- ✓ No collision alert.
- ✓ A healthy mission module.
- ✓ A verified empty cassette.
- ✓ A healthy communications state.
- ✓ No safety inhibit.

The remote supervisor

- Approves the mission plan
- Explicitly approves each candidate-object interaction
- Monitors safety state
- Initiates abort or return when needed
- Coordinates recovery
- Authorizes maintenance-mode transitions

The machine

- Maintains the geofence
- Maintains collision avoidance
- Maintains stable vehicle control
- Tracks system health
- Stops unsafe state transitions
- Provides complete logs
- Returns or holds on defined degradations

Any one of eleven conditions cancels or pauses an interaction:

- ✓ Object classification ambiguity.
- ✓ Low localization confidence.
- ✓ Sonar and camera inconsistency.
- ✓ Excessive vessel motion.
- ✓ Cassette state not verified.

- ✓ Gate-state disagreement.
- ✓ Abnormal drive load.
- ✓ A hydraulic or electrical health fault.
- ✓ Loss of command authorization.
- ✓ Intrusion into the geofence buffer.
- ✓ An obstacle or collision alert.

AUTHORITY

MISSION SOFTWARE REQUESTS. SAFETY AND SUBSYSTEM STATE PERMIT.

Every state transition is permission-based, and the interface register writes the link between autonomy and safety as request motion, read inhibits, no bypass.

08 · FUNCTIONAL SEGREGATION

SIX SEPARATIONS BUILT IN. ONE SUBSYSTEM OWNS THE STOP.

The safety argument is written as independence: six statements about what does not run through what, and an independent safety subsystem that owns the emergency stop, propulsion permission and mission-motion permission.

NAVIGATION

INDEPENDENT OF PERCEPTION AI

Navigation safety functions are independent of the perception AI that classifies objects.

PROPULSION

ENABLE INDEPENDENT OF THE MISSION COMPUTER

Propulsion enable is independent of the mission computer. Uncommanded thrust is a critical hazard, with an independent propulsion enable and a drive safety function as its controls.

ACQUISITION

INDEPENDENT OF CLASSIFICATION

Acquisition actuation is independent of object classification.

CASSETTES

ROUTING INTERLOCKED WITH IDENTITY AND STATE

Cassette routing is independently interlocked with cassette identity and state.

REMOTE STOP

INDEPENDENT OF THE MISSION GUI

Shore holds an independent command path to the safety subsystem for the remote emergency stop and health, and recovery from an emergency stop is manual.

MAINTENANCE

INHIBITS THROUGH THE SAFETY CONTROLLER

Maintenance mode inhibits propulsion and mission actuation through the safety controller.

Underneath the six separations sits the subsystem that owns them. The independent safety subsystem:

- ✓ Owns the hardware emergency stop.
- ✓ Owns propulsion permission.
- ✓ Owns mission-motion permission.
- ✓ Monitors the safety watchdogs.
- ✓ Monitors the gate and cassette interlocks identified by hazard analysis.
- ✓ Exposes read-only status to mission software.
- ✓ Defaults to inhibit when safety integrity is uncertain.
- ✓ Requires explicit recovery after an emergency stop.
- ✓ Logs safety trips with synchronized time.

HAZARD	SEVERITY	DESIGN CONTROLS
Collision	Critical	Independent geofence; collision sensing; restricted speeds; emergency stop
Grounding	Major	Depth sensing; operating limits; route validation
Uncommanded thrust	Critical	Independent propulsion enable; drive safety function
Mission-head impact	Major	Compliance; range sensing; travel stops
Transfer jam	Major	Load monitoring; occupancy timeout; stop and reverse
Gate conflict	Major	Dual state sensing; motion inhibit
Wrong cassette	Major	Visible and electronic ID; interlocks
Asymmetric loading	Major	Load map; stability software limit
Flooding	Critical	Subdivision; bilge detection; pumps; return
Electrical fire	Critical	Protection; thermal monitoring; detection; isolation
Hydraulic leak	Moderate	Routing protection; isolation; bilge monitoring
Maintenance entrapment	Critical	Lockout-tagout; mechanical pins; inhibited service state
Sensor ambiguity	Major	Confidence gating; multiple sensors; halt interaction
Cyber command injection	Critical	Authentication; segmentation; independent safety
Prohibited energetic use	Critical	Inert-only boundary; separate specialist interface

Command authority is protected the same way. The remote command links are encrypted and command messages are authenticated; networks are segmented; software updates are signed, with secure boot when supported; maintenance mode is locked; privileged access is logged; and a recovery image, a configuration backup, a software bill of materials and vulnerability tracking are kept. Offline safe operation is retained as a requirement of its own.

09 · SENSING AND DEGRADED MODES

SEEN ON THE SURFACE, HEARD BELOW. A LOST LINK HOLDS OR RETURNS IT.

Sixteen registered sensors cover the surface, the water below the hull and the corridor itself. Every failure the degraded mode matrix names has a written response.

SENSOR	LOCATION	COVERAGE	ROLE
Dual-antenna GNSS/INS	Mast	360°	Navigation and heading
Marine radar	Mast	360°	Surface traffic and obstacles
AIS	Mast	360°	Surface awareness
Forward electro-optical camera	Bow/mast	120° class	Navigation
Port electro-optical camera	Port	120° class	Side view and recovery
Starboard electro-optical camera	Starboard	120° class	Side view and recovery
Aft electro-optical camera	Aft	120° class	Docking and recovery
Imaging sonar	Forward centreline	Mission corridor	Work-zone object sensing
Obstacle sonar	Forward hull	Wide sector	Underwater collision
Doppler velocity log	Keel/centre	Downward	Low-speed velocity aiding
Altimeter	Mission head	Downward	Bottom clearance
Intake camera A	Intake, port	Local	Close-range alignment
Intake camera B	Intake, starboard	Local	Close-range alignment

SENSOR	LOCATION	COVERAGE	ROLE
Occupancy array	Trunk, intake zone	Local	Transfer tracking
Occupancy array	Trunk, primary transfer zone	Local	Transfer tracking
Occupancy array	Inspection zone	Local	Transfer tracking

KMM-01 carries GNSS and a command link. With KAOS-MC Land it is one of the two mine clearance configurations that make the one ruled exception to no radio and no GPS aboard the fleet. Mine clearance is done on water whose perimeter the customer controls and has surveyed, under a supervisor who is watching, and a surface vessel is required by the rules of the road to be seen and to answer.

A lost link is a defined degraded state. With both command links lost, transit is limited, the vessel takes no new survey task, approach and acquisition are not permitted, and it holds or returns. Blocking new acquisition on lost communications is a mandatory safety requirement.

FAILURE	TRANSIT	SURVEY	APPROACH	ACQUISITION	REQUIRED RESPONSE
Primary GNSS lost	Limited	Limited	No	No	Hold or return using validated aiding
Imaging sonar lost	Yes	Limited	No	No	Return or wait
One side camera lost	Yes	Yes	Limited	Limited	Supervisor decision
Both command links lost	Limited	No new task	No	No	Hold or return
One propulsor lost	Limited	No	No	No	Controlled return
Cassette state mismatch	Yes	Yes	No	No	Isolate fault
Hydraulic overtemperature	Yes	Yes	No	No	Cool or return
Safety controller fault	No	No	No	No	Inhibit motion

Seven of the eight failures leave no acquisition at all. The eighth, one side camera lost, limits approach and acquisition and puts the decision to the supervisor.

10 · POWER AND PROPULSION

TWO PROPULSORS ON A DC BUS. AN ESSENTIAL RAIL OUTLASTS THE REST.

Hybrid-electric: two independent electric propulsors on independent motor drives, a high-voltage DC main bus, a battery buffer, genset generation, isolated 48 V and 24 V auxiliary rails, an essential 24 V uninterruptible supply, and shore charging and service.

The hybrid-electric architecture brings five advantages: fine low-speed torque control, a generator decoupled from the propulsor, simpler autonomous command, silent or low-noise mission phases of short duration, and better redundancy options. Low noise matters to the sonar, so cooling pumps, fans and hydraulic components are evaluated for vibration and acoustic interference with underwater perception.

35,000 W
CONTINUOUS, EACH PROPULSOR, DUTY 0.55

75,000 W
PEAK, EACH PROPULSOR

12,000 W
MISSION HYDRAULIC POWER UNIT, DUTY 0.25

9,000 W
GROWTH RESERVE, CONTINUOUS

Each line of the power budget carries a duty beside its continuous and peak figures: 0.25 for the mission hydraulic power unit and 0.2 for bilge and utilities, against 1.0 for the navigation fit, communications, and network and storage on the essential domains. The growth reserve is held as a line of its own.

The electrical architecture runs six domains: HV propulsion and high-power mission, 48 V sensor and compute, 24 V control and navigation, the 24 V essential UPS, safety I/O, and shore service. High-current motor and inverter wiring is physically separated from sonar, GNSS, analog sensors, Ethernet and safety I/O. The essential UPS retains the safety controller, essential navigation state, command telemetry, bilge and fire monitoring, the event recorder, and controlled shutdown.

11 · HANDLING AND SUSTAINMENT

A SHORE FOOTPRINT BEFORE THE LAUNCH. THREE LEVELS OF SERVICE AFTER IT.

The vessel is the near end of a shore arrangement: a berth or stand, shore power, the remote station, spares, washdown, a mission-module stand, cassette cradles and diagnostic tools.

Launch and recovery run on a travel lift, a launch cradle or a heavy trailer; a crane lift is used only if a dedicated certified lifting design is provided. A disabled vessel is towed on an approved tow bridle within a validated speed and sea-state envelope, and its essential supply keeps bilge and telemetry power alive for the tow; tow and recovery is one of the twelve loading conditions the stability plan carries.

LEVEL	WHO	WORK
L1	Operator and mission support	Inspection, cleaning, log export, simple line-replaceable unit swap
L2	Field service	Sensors, hoses, drives, cassettes, mission wear parts
L3	Depot	Propulsor overhaul, structural repair, battery and genset major service

Designed for maintenance

- Line-replaceable electronics
- A head service position
- Lockout-tagout points
- A diagnostic interface

Provided for maintenance

- A spares list
- A preventive maintenance schedule
- A corrosion inspection plan
- A sensor calibration plan

Corrosion protection is by anodes and a coating system, with corrosion-compatible materials. Every mission leaves a record: safety-relevant events, operator approvals, pose and covariance, and the cassette inventory, with mission data retained after a normal shutdown and the logs exported after the mission.

FIT

FOR WATER SOMEONE CONTROLS. NOT A MACHINE THAT DECIDES.

KMM-01 suits a customer with a defined water area, a survey problem and inert objects that have to come out of it, under a remote supervisor who explicitly approves each candidate-object interaction. It is not a live-ordnance system, and it is not armed.

12 · DOCTRINE AND SAFETY

A CLEARANCE WORKBOAT, NOT A WEAPON. HUMAN SAFETY COMES FIRST.

The lines that hold on this configuration for every customer, including the one exception the fleet makes for mine clearance.

- ✓ Carriers, not munitions: KMM-01 is a clearance workboat, not a weapon. There is no warhead, no fuze and no energetic material aboard, in any configuration.
- ✓ Inert objects by design: every acquisition, transfer, cassette and material-handling interface is defined around inert surrogate objects, and interaction with anything outside the validated inert surrogate family is a forbidden automatic behaviour of the mission module.
- ✓ No radio and no GPS aboard the fleet, with the one ruled exception: the two mine clearance configurations, KAOS-MC Land and KMM-01, carry GNSS and a command link.
- ✓ A lost link is a defined degraded state: with both command links lost the vessel takes no new task and holds or returns, and new acquisition is blocked by a mandatory safety requirement.
- ✓ Human safety comes first, on every line: nobody is aboard, the remote supervisor explicitly approves each candidate-object interaction, and an independent safety subsystem owns the emergency stop and propulsion permission.

THE CONVERSATION

BRING THE WATER AREA AND WHO CONTROLS IT. WE BRING THE HULL, THE CORRIDOR AND THE CELLS.

A first conversation needs the water area and its perimeter, the depth band and the bottom, the current and the traffic, what the objects are, and where the supervisor will sit: ashore or aboard a support vessel.

Start a screened enquiry at cdnshield.ca/enquiries.

DOCUMENT	CDN-PROD-SPC-009 · KMM-01 · Specification sheet
REVISION	R1.0 · issued 2026-09-10
WEB VERSION	cdnshield.ca/systems/water/spec-sheets/kmm-01 · carries the current revision
RELATED SHEETS	CS-310 · CS-320
ISSUED BY	Canadian Shield · cdnshield.ca