Scenarios

MARITIME INFRASTRUCTURE PROTECTION SCENARIO

Context

Critical undersea infrastructure, including communication cables and energy pipelines, faces increasing threats from both state and non-state actors. This scenario challenges teams to develop an autonomous system for continuous monitoring and protection of these vital assets across vast oceanic areas. The system must operate in harsh underwater environments, process data at the edge, and coordinate responses to potential threats while minimizing false alarms.

Primary Objective

Design and deploy an autonomous underwater surveillance network capable of monitoring a 100km stretch of critical undersea infrastructure, detecting and classifying threats, and coordinating rapid response actions while operating with minimal surface support for extended periods.

Key Requirements

- Continuous 24/7 surveillance of designated area
- Multi-modal threat detection (acoustic, magnetic, optical)
- Autonomous threat classification and prioritization
- Real-time data processing at the edge
- Secure, low-bandwidth communication to surface assets
- Long-duration operation with minimal maintenance
- Adaptation to varying oceanographic conditions

Mission Success Criteria

1. Coverage: Maintain 99.9% surveillance coverage of designated area
2. Detection: Identify 95% of potential threats within 1km of protected assets
3. Classification: Accurately classify threats with 90% accuracy within 2 minutes
4. Endurance: Sustain operations for 90 days without direct human intervention
5. Communication: Maintain secure data links despite attempts at interference
6. Environmental Impact: Minimize acoustic and electromagnetic emissions

Operational Constraints

- Extreme depth and pressure conditions
- Limited communication bandwidth
- Power management for long-term deployment
- Corrosive saltwater environment
- Variable oceanic conditions (currents, temperature, salinity)
- Potential for adversary countermeasures
- Strict regulations on underwater activities

Technical Objectives Table

	Phase	Goal	Constraints	Details and Notes
1	Pre-Deployment	Patrol Route Optimization	- Ocean currents - Seafloor topology - Energy efficiency	- Generate optimal AUV paths - Consider seasonal variations - Plan for varying depths - Optimize coverage patterns
2	Pre-Deployment	Sensor Network Design	- Detection ranges - Power limitations - Environmental impact	- Optimize sensor placement - Balance fixed and mobile sensors - Plan for redundancy - Consider multi-modal sensing
3	Pre-Deployment	Threat Scenario Modeling	- Incomplete intelligence - Environmental variables - Computational resources	- Simulate various attack methods - Model oceanographic impacts - Develop response strategies - Test edge case scenarios
4	Deployment	AUV Launch and Initialization	- Launch platform limitations - Initial positioning accuracy - System calibration needs	- Coordinate multi-vehicle deployment - Establish initial formations - Calibrate sensors to conditions - Verify system integrity
5	Deployment	Communication Network Establishment	- Acoustic propagation limits - Bandwidth constraints - Security requirements	- Set up underwater acoustic networks - Establish surface relay points - Implement encryption protocols - Test network resilience
6	Deployment	Environmental Adaptation	- Real-time data processing - Sensor recalibration - Energy management	- Adjust to local conditions - Optimize sensor settings - Implement adaptive behaviors - Establish baseline readings
7	Operations	Multi-Vehicle Coordination	- Communication latency - Positioning errors - Task allocation complexity	- Maintain optimal coverage - Coordinate sensor overlap - Implement swarming behaviors - Manage energy usage across fleet
8	Operations	Threat Detection and Classification	- False positive mitigation - Processing at the edge - Classification speed	- Fuse multi-modal sensor data - Implement ML for pattern recognition - Develop confidence scoring - Enable autonomous decision-making
9	Operations	Adaptive Patrol Patterns	- Real-time threat assessment - Energy constraints - Coverage requirements	- Dynamically adjust to threats - Optimize search patterns - Balance coverage and endurance - Coordinate with fixed sensors
10	Operations	Data Transmission Management	- Bandwidth limitations - Energy constraints - Prioritization needs	- Implement data compression - Develop transmission schedules - Prioritize critical information - Manage surface communication windows
11	Post-Mission	Coverage Analysis	- Data integration challenges - Long-term trend identification - Performance metric definition	- Evaluate patrol effectiveness - Identify coverage gaps - Analyze detection rates - Assess environmental impacts
12	Post-Mission	Threat Assessment Review	- Data quality variations - False alarm analysis - Pattern recognition	- Evaluate classification accuracy - Identify emerging threat patterns - Assess response effectiveness - Refine threat models
13	Post-Mission	System Performance Evaluation	- Long-term reliability metrics - Energy efficiency analysis - Maintenance need prediction	- Analyze component wear - Evaluate power consumption - Assess communication reliability - Identify areas for improvement
14	Post-Mission	Environmental Impact Assessment	- Regulatory compliance - Long-term ecological effects - Data collection limitations	- Analyze acoustic emissions - Assess impact on marine life - Evaluate chemical/physical disturbances - Develop mitigation strategies

UAV / UGV / CUAS SCENARIO

Context

Forward Operating Bases (FOBs) face increasing threats from both individual drones and coordinated UAS attacks. This scenario challenges teams to develop an autonomous defense system that can detect, track, classify, and neutralize hostile UAS threats while minimizing interference with friendly air operations. The system must operate 24/7, process data at the edge to enable split-second decisions, and adapt to evolving threat tactics.

Primary Objective

Create an autonomous, multi-layered defense system capable of protecting a $1km^2$ FOB from UAS threats, providing early warning, threat assessment, and appropriate countermeasures while maintaining a less than 0.1% false positive rate against friendly aircraft.

Key Requirements

- Multi-modal detection (RF, optical, acoustic, radar)
- Autonomous threat classification and prioritization
- Real-time trajectory prediction
- Automated countermeasure selection and deployment
- Integration with existing air defense systems
- Friendly force identification and deconfliction
- Operation in degraded network conditions

Mission Success Criteria

1. Detection: 99.9% detection rate for UAS threats within 2km
2. Classification: Threat assessment within 3 seconds of detection
3. Response Time: Countermeasure deployment within 5 seconds of classification
4. Accuracy: False positive rate below 0.1%
5. Coverage: 360-degree protection with multi-layer redundancy
6. Resilience: Maintain effectiveness despite electronic attacks

Operational Constraints

- Must operate in all weather conditions
- Limited power availability
- Restricted RF emissions in certain sectors
- Complex urban/rural environment
- High consequence of failure
- Civilian air traffic deconfliction
- Rules of Engagement (ROE) compliance

Technical Objectives Table

	Phase	Goal	Constraints	Details and Notes
1	Pre-Deployment	Defensive Zone Mapping	- Terrain features - Existing infrastructure - Line of sight limitations	- Create 3D coverage model - Identify blind spots - Map RF interference zones - Consider seasonal variations
2	Pre-Deployment	Sensor Network Design	- Power availability - Physical security - Cost constraints	- Optimize sensor placement - Ensure overlapping coverage - Plan redundant systems - Calculate detection ranges
3	Pre-Deployment	ROE Implementation	- Legal requirements - Processing speed - Decision complexity	- Codify engagement rules - Define threat levels - Create decision trees - Set authorization levels
4	Pre-Deployment	Response Modeling	- System latency - Environmental factors - Resource limitations	- Simulate various attacks - Test response sequences - Validate kill chains - Model collateral effects
5	Deployment	System Activation	- Network bandwidth - Security protocols - Integration timing	- Coordinate startup sequence - Verify communications - Test fail-safes - Validate configurations
6	Deployment	Coverage Verification	- Testing windows - Operational security - Weather conditions	- Run diagnostic sweeps - Validate detection zones - Test sensor fusion - Verify tracking handoff
7	Deployment	Integration Testing	- Legacy systems - Protocol compatibility - Security requirements	- Test data flows - Verify interfaces - Validate permissions - Check redundancy
8	Operations	Threat Detection	- Processing power - False positive rate - Real-time requirements	- Multi-sensor fusion - Signal processing - Pattern recognition - Anomaly detection
9	Operations	Classification Engine	- AI model size - Processing speed - Accuracy requirements	- Threat categorization - Behavior analysis - Intent determination - Priority assignment
10	Operations	Response Coordination	- Time constraints - Resource availability - Collateral damage	- Select countermeasures - Coordinate responses - Track effectiveness - Manage resources
11	Operations	System Adaptation	- Learning rate - Memory constraints - Validation needs	- Update threat models - Adjust parameters - Improve accuracy - Enhance efficiency
12	Post-Mission	Engagement Analysis	- Data volume - Analysis time - Storage capacity	- Evaluate effectiveness - Assess accuracy - Measure response time - Calculate kill chain
13	Post-Mission	System Performance	- Metric complexity - Data quality - Analysis scope	- Review detection rates - Analyze false positives - Evaluate latency - Assess coverage
14	Post-Mission	Threat Evolution	- Data integration - Pattern recognition - Prediction accuracy	- Identify new tactics - Update threat models - Enhance responses - Predict adaptations
15	Post-Mission	Resource Optimization	- Cost constraints - Performance targets - Operational needs	- Analyze usage patterns - Optimize deployment - Improve efficiency - Plan upgrades

---

These scenarios are help for history, and will have their content merged into the primary 2 above.

DRONE SWARM RECONNAISSANCE SCENARIO

Context

In denied or contested environments, traditional reconnaissance methods face significant risks and limitations. This scenario challenges teams to develop an autonomous drone swarm system capable of rapidly mapping and assessing unknown territory while maintaining resilience against counter-measures. The swarm must operate with minimal communication back to command centers, process data at the edge, and adapt to emerging threats in real-time.

Primary Objective

Deploy and coordinate a swarm of 15-20 autonomous drones to create an accurate, real-time battlefield picture across a 10km² area within 45 minutes, while operating under emissions control (EMCON) conditions and potential electronic warfare (EW) threats.

Key Requirements

- Autonomous operation in GPS-denied environments
- Resilient mesh networking with minimal emissions
- Edge processing for real-time threat detection
- Dynamic swarm reconfiguration based on threats or failures
- Maintain operational capability with up to 30% unit losses
- Secure data collection and transmission
- Battery life optimization for minimum 2-hour mission duration

Mission Success Criteria

1. Area Coverage: Complete mapping of designated area with >95% coverage
2. Speed: Initial surveillance picture available within 15 minutes
3. Accuracy: Terrain mapping accuracy within 1-meter resolution
4. Resilience: Maintain operational effectiveness despite EW interference
5. Detection: Identify and classify static and mobile threats with >90% accuracy
6. Data Security: Ensure all transmitted data is encrypted and resistant to interception

Operational Constraints

- Limited communication bandwidth
- Intermittent connectivity to command center
- Variable terrain and weather conditions
- Active electronic countermeasures
- Size, Weight, and Power (SWAP) limitations
- Autonomous decision-making required
- Emissions control requirements

Technical Objectives Table

	Phase	Goal	Constraints	Details and Notes
1	Pre-Deployment	Flight Path Optimization	- Terrain limitations - Battery life - Communication range	- Calculate optimal routes considering elevation - Plan for line-of-sight maintenance - Include weather impact modeling
2	Pre-Deployment	Communication Relay Planning	- Signal strength - Network capacity - Physical limitations	- Optimize relay positions - Ensure redundant coverage - Consider dynamic repositioning needs
3	Pre-Deployment	Swarm Behavior Definition	- Processing power - Communication latency - Memory constraints	- Define formation parameters - Set collision avoidance rules - Create adaptive behaviors
4	Pre-Deployment	Contingency Planning	- Processing complexity - Scenario scope - Memory limitations	- Develop fallback behaviors - Plan emergency responses - Create recovery procedures
5	Deployment	Autonomous Launch Sequence	- Launch zone constraints - Weather conditions - Time constraints	- Coordinate multiple launches - Maintain safe separation - Establish initial formation
6	Deployment	Mesh Network Formation	- Bandwidth limitations - Power consumption - Node density	- Self-healing network design - Dynamic routing protocols - Quality of service management
7	Deployment	Environmental Adaptation	- Sensor limitations - Processing speed - Real-time constraints	- Adjust for weather conditions - Modify flight parameters - Optimize sensor settings
8	Operations	Real-time Mapping	- Processing at edge - Data storage - Transmission bandwidth	- Coordinate sensor coverage - Process imagery in real-time - Generate terrain models
9	Operations	Target Recognition	- False positive rate - Processing speed - Model size	- Edge-based ML processing - Multi-sensor fusion - Confidence scoring
10	Operations	Dynamic Reformation	- Real-time coordination - Battery management - Threat avoidance	- Adapt to threats - Maintain coverage - Optimize power usage
11	Operations	Resource Management	- Battery life - Coverage requirements - Mission priorities	- Manage power consumption - Coordinate unit rotation - Optimize sensor usage
12	Post-Mission	3D Model Generation	- Data volume - Processing time - Accuracy requirements	- Merge multiple data sources - Generate detailed terrain models - Identify changes from baseline
13	Post-Mission	Mission Analysis	- Data integration - Processing resources - Storage constraints	- Evaluate coverage effectiveness - Analyze battery performance - Optimize future missions
14	Post-Mission	System Health Analysis	- Data quality - Diagnostic depth - Historical tracking	- Evaluate component wear - Assess system performance - Identify maintenance needs
15	Post-Mission	AI Model Refinement	- Training data quality - Computational resources - Version control	- Update recognition models - Improve detection accuracy - Enhance classification systems

DISASTER RESPONSE COORDINATION SCENARIO

Context

In the wake of a major earthquake, a densely populated urban area has suffered widespread damage, leaving many survivors trapped and in need of immediate assistance. Traditional search and rescue operations are hampered by collapsed infrastructure, ongoing aftershocks, and limited resources. This scenario challenges teams to develop an autonomous system that can coordinate and optimize search and rescue efforts across multiple domains (air, ground, and potentially subterranean) in a dynamic, hazardous environment.

Primary Objective

Design and deploy a multi-modal autonomous system capable of rapidly mapping the disaster area, locating and prioritizing survivors, and coordinating rescue efforts to maximize lives saved within the critical 72-hour window following the disaster.

Key Requirements

- Real-time mapping and updating of affected areas
- Multi-sensor integration for survivor detection
- Autonomous path planning and obstacle avoidance
- Dynamic resource allocation and task prioritization
- Secure, robust communication in degraded environments
- Integration with human rescue teams and command centers
- Adaptation to changing conditions and new information

Mission Success Criteria

1. Coverage: Map 90% of a $5km^2$ urban disaster zone within 12 hours
2. Detection: Identify 95% of survivor locations within 24 hours
3. Prioritization: Accurately assess and rank rescue priorities
4. Coordination: Reduce average response time by 50% compared to traditional methods
5. Adaptability: Maintain operational effectiveness despite aftershocks and evolving hazards
6. Integration: Seamlessly coordinate autonomous systems with human rescue teams

Operational Constraints

- Limited power and recharging capabilities
- Degraded or non-existent communication infrastructure
- Hazardous and unstable environments
- Time-critical decision making
- Variable weather conditions
- Limited computational resources at the edge
- Need for 24/7 operation

Technical Objectives Table

	Phase	Goal	Constraints	Details and Notes
1	Pre-Deployment	Area Prioritization	- Limited initial data - Time pressure - Dynamic situation	- Analyze population density - Assess building types and age - Consider critical infrastructure - Integrate seismic data
2	Pre-Deployment	Resource Allocation	- Limited assets - Varied capabilities - Deployment logistics	- Optimize mix of air/ground units - Plan for battery life/fuel - Consider specialized equipment needs - Prepare for scalability
3	Pre-Deployment	Communication Network Design	- Infrastructure damage - Bandwidth limitations - Power constraints	- Plan mesh network deployment - Design for redundancy - Optimize for low-power operation - Ensure encryption and security
4	Deployment	Rapid System Activation	- Time criticality - Potentially hazardous conditions - Coordination complexity	- Automate deployment sequences - Establish communication links - Initialize mapping systems - Verify system integrity
5	Deployment	Initial Area Assessment	- Limited visibility - Rapidly changing conditions - Data processing bottlenecks	- Deploy aerial mapping units - Initiate ground-based scans - Begin data fusion and analysis - Identify immediate hazards
6	Deployment	Search Pattern Generation	- Incomplete information - Resource limitations - Priority balancing	- Create adaptive search algorithms - Integrate multi-modal sensor data - Design for coverage vs. detail trade-offs - Plan for continuous updates
7	Operations	Multi-Modal Search Execution	- Sensor limitations - Environmental interference - Power management	- Coordinate air and ground units - Implement acoustic/thermal/visual sensing - Adapt to environmental conditions - Optimize for battery life
8	Operations	Real-time Survivor Detection	- False positive mitigation - Processing at the edge - Time sensitivity	- Implement ML for pattern recognition - Fuse data from multiple sensors - Develop confidence scoring - Enable human-in-the-loop verification
9	Operations	Dynamic Resource Reallocation	- Changing priorities - Communication latency - Decision complexity	- Develop priority algorithms - Create resource reallocation models - Implement task handoff protocols - Balance efficiency vs. thoroughness
10	Operations	Automated Status Reporting	- Data volume management - Bandwidth limitations - Information prioritization	- Design efficient data compression - Implement priority-based transmission - Create clear visualization tools - Ensure critical alert propagation
11	Post-Mission	Search Coverage Analysis	- Data integration challenges - Analytical complexity - Incomplete information	- Map actual vs. planned coverage - Identify search pattern effectiveness - Analyze time-to-detection metrics - Assess environmental impact on performance
12	Post-Mission	Response Time Assessment	- Data quality variations - Benchmark establishment - Multifactor analysis	- Calculate end-to-end response times - Identify bottlenecks in processes - Compare autonomous vs. manual operations - Develop improvement recommendations
13	Post-Mission	Resource Efficiency Evaluation	- Complex utilization patterns - Varied asset capabilities - Situational impact factors	- Analyze asset utilization rates - Assess energy efficiency - Evaluate task completion rates - Identify underutilized capabilities
14	Post-Mission	System Improvement Planning	- Balancing short vs. long-term goals - Technology evolution - Budget constraints	- Prioritize system enhancements - Plan for technology integration - Develop training recommendations - Create scalability strategies

SUPPLY CHAIN SECURITY SCENARIO

Context

Maritime supply chains face increasingly sophisticated threats from both state and non-state actors. This scenario challenges teams to develop an autonomous system to protect merchant vessels through high-risk transit zones. The system must coordinate multiple autonomous platforms (surface, subsurface, and aerial), anticipate potential threats, and respond to complex attacks while maintaining commercial shipping efficiency.

Primary Objective

Create an autonomous defense network capable of protecting a convoy of 3-5 commercial vessels through a 500nm high-risk transit zone, providing comprehensive threat detection, assessment, and response while minimizing impact on commercial operations.

Key Requirements

- 360-degree surface/subsurface surveillance
- Multi-domain threat detection and tracking
- Autonomous escort vessel coordination
- Dynamic route optimization
- Real-time risk assessment and response
- Minimal impact on commercial operations
- Operation in denied/degraded environments

Mission Success Criteria

1. Detection: Identify 99% of potential threats beyond engagement range
2. Assessment: Classify threats within 30 seconds with 95% accuracy
3. Protection: Maintain defensive coverage despite adversary deception
4. Efficiency: Less than 10% impact on transit time
5. Resilience: Maintain effectiveness despite loss of up to 25% of defensive assets
6. Integration: Seamless coordination with merchant vessel operations

Operational Constraints

- International maritime law compliance
- Variable weather and sea states
- Limited communication bandwidth
- Mixed-nationality vessel crews
- Varied vessel capabilities
- Fuel/energy efficiency requirements
- Commercial schedule pressures

Technical Objectives Table

	Phase	Goal	Constraints	Details and Notes
1	Pre-Deployment	Route Risk Assessment	- Incomplete intelligence - Dynamic threats - Weather variability	- Analyze historical threat data - Assess environmental factors - Consider geopolitical situations - Map friendly/neutral assets
2	Pre-Deployment	Defensive Formation Design	- Vessel capabilities - Weather impact - Commercial requirements	- Optimize escort positioning - Plan sensor coverage - Consider vessel limitations - Design adaptive formations
3	Pre-Deployment	Resource Distribution	- Asset availability - Coverage requirements - Endurance needs	- Allocate defensive platforms - Position resupply points - Plan maintenance windows - Configure backup systems
4	Pre-Deployment	Response Protocol Development	- ROE constraints - International laws - Commercial priorities	- Define escalation levels - Create response matrices - Plan contingencies - Set authorization levels
5	Deployment	Escort Position Assignment	- Formation constraints - Sea state impact - Communication limits	- Initialize defensive positions - Establish command links - Verify sensor coverage - Test response times
6	Deployment	Sensor Network Activation	- Environmental interference - Power management - Detection ranges	- Deploy mobile sensors - Calibrate detection systems - Initialize fusion engines - Verify coverage overlap
7	Deployment	Communication Grid Establishment	- Bandwidth limitations - Security requirements - Range constraints	- Set up mesh networks - Enable secure channels - Verify redundancy - Test fail-safes
8	Operations	Threat Monitoring	- False alarm rates - Processing power - Data fusion complexity	- Monitor multiple domains - Process sensor data - Track potential threats - Assess behavioral patterns
9	Operations	Formation Management	- Vessel maneuverability - Traffic interaction - Weather impact	- Maintain optimal spacing - Adapt to conditions - Manage vessel interactions - Optimize fuel efficiency
10	Operations	Route Adaptation	- Navigation constraints - Traffic density - Threat avoidance	- Update risk assessments - Calculate optimal paths - Consider weather routing - Maintain schedule efficiency
11	Operations	Defense Coordination	- Asset limitations - Response timing - ROE compliance	- Coordinate responses - Manage asset deployment - Track effectiveness - Maintain coverage
12	Post-Mission	Security Assessment	- Data completeness - Analysis complexity - Pattern identification	- Evaluate threat responses - Assess defensive effectiveness - Analyze formation performance - Review incident data
13	Post-Mission	Efficiency Analysis	- Multiple variables - Commercial impacts - Cost considerations	- Calculate time impacts - Assess fuel efficiency - Evaluate route optimization - Measure schedule adherence
14	Post-Mission	System Performance Review	- Data integration - Performance metrics - Multiple stakeholders	- Review system reliability - Assess coordination effectiveness - Evaluate response times - Analyze coverage gaps
15	Post-Mission	Capability Enhancement	- Resource limitations - Implementation time - Integration requirements	- Identify improvements - Update threat models - Enhance formations - Optimize responses

Team Deliverables and Expectations

CORE DELIVERABLES

1. Technical Solution

- Working prototype or proof-of-concept using AWS services
- Documentation/Presentation of architecture and implementation
- Demonstration of edge/cloud integration
- Evidence of testing and validation approaches

2. Integration Strategy

- Clear definition of solution boundaries
- Identified interfaces with other system components
- Required inputs and expected outputs
- Integration considerations with potential partners
- Security and compliance considerations
- Data flow and API specifications

3. Critical Analysis

- Documented assumptions and constraints
- Known limitations and technical debt
- Scalability considerations
- Security implications
- Cost considerations
- Performance tradeoffs
- Lessons learned and future improvements

PRESENTATION REQUIREMENTS

20-minute presentation covering:

1. Problem Space
    a. Challenge definition
    b. Scope boundaries
    c. Success criteria
2. Technical Solution
    a. Architecture overview
    b. AWS services utilized
    c. Edge/cloud balance
    d. Demo or simulation
3. Integration Approach
    a. System interfaces
    b. Partner integration points
    c. Data flows

4. Critical Analysis
    a. Strengths and weaknesses
    b. Lessons learned
    c. Future work

WORKING GUIDELINES

1. Scope Management

- Focus on solving one or two specific challenges well
- Clearly document assumptions and limitations
- Define realistic minimum viable product (MVP)

2. AWS Implementation

- Utilize at least one edge computing service
- Implement appropriate cloud services
- Consider cost and performance optimization
- Address security requirements

3. Integration Considerations

- Document all external dependencies
- Define clear interfaces
- Consider real-world constraints
- Include security and compliance requirements

4. Documentation

- Maintain clear technical documentation
- Document decision rationale
- Track lessons learned throughout
- Include setup/deployment instructions

RESOURCES PROVIDED

- AWS Environment Access
- Technical Mentors
- Documentation Resources
- Collaboration Spaces

TEAMWORK EXPECTATIONS

- Assign clear roles within team
- Maintain regular communication
- Document key decisions
- Share knowledge and findings

- Engage with mentors proactively
- Be prepared to pivot based on discoveries

KEY REMINDERS

- Perfect is the enemy of good
- Document failures as well as successes
- Focus on practical, implementable solutions
- Consider real-world constraints
- Leverage team diversity
- Ask for help when needed