SOUTHGATE TERMINAL

Port Operations Security Documentation

Technical / Ops Procedures – Signal Anomaly Response

Purpose:
To guide technical teams through the identification, investigation, and response process when signal-based anomalies (e.g. GPS spoofing, AIS manipulation, phantom traffic) are detected within maritime operational environments.

When to Use

- Unexpected or conflicting signal data is detected (location, vessel ID, or timing mismatch)
- Reports from on-site Ops or dashboards show movement discrepancies
- Logs or monitoring tools show anomalies in feed sources (e.g. spoofed coordinates, missing timestamps)

Signal Architecture Context

- AIS and GPS data are ingested via:
- Serial or USB interfaces (e.g. /dev/ttyUSB0)
- Network streams (UDP port 10110 or 2947)
- Signal processing is performed in:
- AIS Collector container or service
- GPSD daemon running on the Comms VM
- Reference data and known vessel IDs stored in /opt/reference/gps-clean.nmea and /opt/reference/ais-index.json

Immediate Detection Actions

- Validate real-time signal input:
- cat /dev/ttyUSB0 | tee /tmp/raw-nmea.log
- netstat -anu | grep 10110
- Cross-reference feeds:
- AIS: /opt/ais/logs/ais-feed.log
- GPS: /var/gps/raw-feed.nmea
- grep -i lat /opt/ais/logs/ais-feed.log | tail -n 20
- tail -n 50 /var/gps/raw-feed.nmea
- diff /var/gps/raw-feed.nmea /opt/reference/gps-clean.nmea

- Check for ghost or duplicate MMSI entries:
- grep ”MMSI” /opt/ais/logs/ais-feed.log | sort | uniq -c | sort -nr

Feed Validation Techniques

- Use gpsdecode or gpspipe (if installed):
- gpspipe -r | tee /tmp/gpspipe.log
- gpsdecode < /tmp/gpspipe.log
- Inspect NTP time sync drift:
- timedatectl status
- Confirm AIS format consistency:
- grep -v '^!' /opt/ais/logs/ais-feed.log

Network Traffic Inspection

- Monitor incoming signal traffic:
- tcpdump -i any port 10110 -n -c 100
- netstat -tunap | grep 10110
- Use nc (netcat) to test signal port:
- nc -vu localhost 10110
- Capture entire session for later review:
- tcpdump -i any port 10110 -w /var/log/evidence/ais-signal.pcap

Anomaly Classification & Evidence Collection

- Classify:
- Position drift beyond expected margins
- Ghost signals (phantom vessels)
- Duplicate or malformed NMEA sentences
- Out-of-order signal bursts
- Preserve evidence:
- cp /var/gps/raw-feed.nmea /var/log/evidence/gps-anomaly-$(date +%F-%H%M).nmea
- sha256sum /var/log/evidence/*.nmea
- docker export ais_collector > /var/log/evidence/ais_collector_snapshot.tar

Red Flags & Escalation

Immediately escalate to Incident Lead and Legal if:

- Feeds originate from unknown internal IPs
- AIS data contains duplicate MMSI with divergent paths
- Timestamped feeds do not match system or NTP time
- Container or script found manipulating NMEA before logging

AIS Signal Validation and Correlation Procedures

Purpose

This procedure provides real-time validation steps for AIS signal integrity and correlation with other system anomalies. Use when vessels disappear from displays, position data appears incorrect, or timing correlates with other system issues.

When to Use

- Individual vessels missing from AIS display
- Multiple vessels simultaneously disappearing
- Position jumps or erratic vessel tracking
- AIS anomalies coinciding with network or CCTV issues
- Reports of vessels being visible but not on AIS

AIS Signal Validation Steps

Phase 1: Immediate Verification (First 3 minutes)

1. Visual Confirmation

☐ Check physical vessel presence through CCTV (if available)
☐ Coordinate with dock personnel for visual verification
☐ Confirm vessel should be in reported location

2. System Status Check

☐ Verify AIS receiver operational status
☐ Check antenna connections and power
☐ Review recent AIS system configuration changes

3. Signal Strength Analysis

☐ Check signal strength indicators for affected area
☐ Compare with baseline signal levels
☐ Note any interference patterns

Phase 2: Cross-System Correlation (Next 5 minutes)

1. Network Correlation

☐ Compare AIS anomaly timing with network issues
☐ Check if packet routing delays affect AIS data processing
☐ Review network traffic for AIS data streams

2. CCTV Correlation

☐ Compare AIS vessel positions with CCTV visual confirmation
☐ Check if CCTV blackouts coincide with AIS losses
☐ Verify independent visual tracking capability

3. Operational Correlation

☐ Check if missing vessels are actively loading/unloading
☐ Verify vessel scheduling matches AIS displays
☐ Confirm harbor pilot communications with “missing” vessels

Phase 3: Pattern Analysis (Next 7 minutes)

1. Single vs. Multiple Vessel Analysis

- Single vessel missing: Likely equipment issue on vessel
- Multiple vessels missing: Likely shore-side AIS system issue
- All vessels missing: Likely AIS receiver or network failure

2. Geographic Pattern Analysis

☐ Map affected area boundaries
☐ Check if pattern suggests directional antenna issues
☐ Verify if specific berths or anchorage areas affected

3. Temporal Pattern Analysis

☐ Note exact timing of signal loss
☐ Check for periodic or intermittent patterns
☐ Correlate with other system event timestamps

Cross-System Correlation Matrix

Network + AIS Anomalies = HIGH PRIORITY

- Indicators: Packet delays AND vessel tracking issues
- Action: Immediate technical team coordination
- Escalation: Consider external interference possibility

CCTV + AIS Anomalies = OPERATIONAL RISK

- Indicators: Camera blackout AND vessel position loss
- Action: Manual operations protocols

- Escalation: Safety assessment required

Network + CCTV + AIS = POTENTIAL CYBER EVENT

- Indicators: Multiple systems affected simultaneously
- Action: Cyber team escalation
- Escalation: Executive notification required

Real-Time Validation Procedures

For Missing Individual Vessels

1. Radio Contact: Attempt direct VHF contact with vessel
2. Harbor Pilot: Confirm vessel position through pilot services
3. Visual Verification: Send personnel to physically locate vessel
4. AIS Transponder: Request vessel to reset AIS equipment

For Multiple Missing Vessels

1. System Restart: Consider AIS receiver restart if safe to do so
2. Backup Systems: Switch to backup AIS receiver if available
3. Alternative Tracking: Use radar or CCTV for vessel positions
4. Harbor Coordination: Alert harbor master to tracking limitations

For All Vessels Missing

1. Emergency Mode: Declare AIS system failure
2. Manual Tracking: Implement full manual vessel tracking
3. Safety Protocol: Increase visual watch and radio monitoring
4. System Investigation: Full technical investigation required

Communication Protocols

To Operations Team

- “AIS anomaly confirmed: [number] vessels affected in [area]. Manual tracking [required/not required]. Operations impact: [description]”

To Technical Team

- “AIS signal loss correlates with [network/CCTV] issues at [time]. Cross-system investigation recommended. Technical coordination needed.”

To Harbor Master

- “AIS tracking compromised for [vessels/area]. Implementing [backup procedures]. Request increased radio coordination.”

To Incident Coordinator

- "AIS Status: [X] vessels tracking normally, [Y] vessels missing. Backup procedures [implemented/not needed]. Safety [maintained/at risk]."

Decision Matrix: Manual vs. Automated Operations

CONTINUE AUTOMATED OPERATIONS IF:

- Less than 20% of vessels affected
- Clear equipment malfunction identified
- Backup tracking methods functional
- No correlation with other system issues

SWITCH TO MANUAL TRACKING IF:

- More than 50% of vessels affected
- Multiple system correlation identified
- Safety concerns about vessel positions
- Extended restoration time expected

EMERGENCY PROTOCOLS IF:

- All vessels missing from AIS
- Active vessel movements with no tracking
- Safety concerns about vessel collisions
- Unknown vessel positions in active channels

Escalation Triggers

Technical Escalation (Network Team)

- AIS anomalies correlate with network timing
- Signal patterns suggest technical interference
- Cross-system timing indicates common cause

Cyber Escalation (Security Team)

- Multiple systems affected simultaneously
- Patterns suggest deliberate interference
- Evidence of external signal manipulation

Executive Escalation

- Safety concerns about continued operations
- Extended AIS outage affecting multiple vessels
- Media attention to vessel tracking issues

Success Criteria

- Accurate determination of AIS system status
- Cross-system correlations identified and documented
- Appropriate backup procedures implemented
- Safety maintained through alternative tracking methods
- Clear communication to all affected teams

Related Procedures

- Use with: Network Diagnostics SOP (for correlation analysis)
- Coordinate with: Manual Override Authorization (if manual tracking needed)
- Reference: Technical Containment Guide (if cyber threat suspected)
- Escalate to: Crisis Communications SOP (if public safety implications)

Owner: Technical Lead
Reference: TECH-02
Version: 1.1
Approved by: Cyber-Ops Coordination Cell