

SOUTHGATE TERMINAL

Port Operations Security Documentation

Multi-System Failure Coordination Guide

Document Information

Document Type: Technical Coordination Framework

Intended Users: Technical Team, Operations Team, Incident Coordinators

Usage Context: When multiple operational systems fail simultaneously

Related Scenarios: Network + AIS + CCTV failures, coordinated system impacts

Purpose

This guide provides coordination framework for incidents affecting multiple operational systems simultaneously, ensuring systematic response prioritization and effective cross-team coordination when normal escalation paths are overwhelmed.

When to Use This Guide

- Three or more operational systems affected simultaneously
 - System failures that appear coordinated or related
 - Cascading failures affecting dependent systems
 - Resource conflicts between multiple system restoration efforts
 - Cross-system impacts requiring integrated response
-

Multi-System Failure Classification

Type A: Cascading Failures

Characteristics: - One system failure causes others to fail - Clear dependency relationships - Predictable failure sequence - Single root cause

Examples: - Network failure → AIS data loss → Manual operations → CCTV reliance - Power failure → Multiple system shutdowns - Database corruption → Multiple application failures

Type B: Coordinated Attacks

Characteristics: - Multiple systems targeted simultaneously - No clear dependency relationship - Sophisticated attack patterns - Evidence of deliberate action

Examples: - Network interference + AIS spoofing + CCTV blackout - Unauthorized access to multiple unrelated systems - Systematic log deletion across multiple platforms

Type C: Environmental/External

Characteristics: - External factor affecting multiple systems - Natural or infrastructure-related cause - Affects systems sharing common dependencies - Typically affects physical layer

Examples: - Weather affecting antenna systems - Utility failures affecting multiple systems - Vendor outage affecting multiple services

Coordination Framework

Phase 1: Initial Response (0-15 minutes)

Multi-System Triage Process

1. **System Impact Assessment**
 - ☐ **Primary Systems:** AIS, CCTV, Network, Container Management
 - ☐ **Secondary Systems:** Communications, Email, HVAC, Access Control
 - ☐ **Safety Systems:** Emergency communications, Safety monitoring
 - ☐ **Support Systems:** Backup power, Environmental controls
2. **Failure Pattern Analysis**
 - ☐ **Timing:** All at once vs. sequential failures
 - ☐ **Geography:** Localized vs. distributed
 - ☐ **Dependencies:** Related vs. independent systems
 - ☐ **Severity:** Complete failure vs. degraded performance
3. **Safety Impact Evaluation**
 - ☐ **Immediate Dangers:** Active operations requiring immediate attention
 - ☐ **Safety Monitoring:** Systems critical for personnel safety
 - ☐ **Emergency Response:** Capability to respond to emergencies
 - ☐ **Evacuation Capability:** Ability to safely evacuate if needed

Priority Matrix for Multi-System Response

System	Safety Impact	Operational Impact	Restoration Complexity	Priority
Emergency Communications	Critical	High	Low	1

System	Safety Impact	Operational Impact	Restoration Complexity	Priority
CCTV (Safety Areas)	Critical	Medium	Medium	2
AIS (Active Vessels)	High	Critical	Medium	3
Network (Core)	Medium	Critical	High	4
Container Management	Low	High	Low	5
Email/Ad-hoc Systems	Low	Low	Low	6

Phase 2: Coordination Structure (15-30 minutes)

Multi-System Response Team Structure Incident Commander: Senior Operations Manager or designated authority - Overall coordination and resource allocation - Safety decision authority - Executive communication

Technical Coordinator: Senior Technical Lead - Technical restoration prioritization - Resource allocation for technical teams - Cross-system dependency management

Operations Coordinator: Operations Team Lead - Operational continuity planning - Manual procedure implementation - Personnel safety coordination

Communications Coordinator: Incident Communications Lead - Internal team coordination - External stakeholder communication - Information flow management

Team Coordination Protocols

1. Situation Briefings

- ☐ Every 15 minutes for first hour
- ☐ Every 30 minutes thereafter
- ☐ Emergency briefings as required

2. Decision Authority

- ☐ Safety decisions: Operations Coordinator (immediate implementation)
- ☐ Resource allocation: Technical Coordinator (technical resources)
- ☐ Strategic decisions: Incident Commander (overall direction)
- ☐ External communication: Communications Coordinator

3. Information Flow

- ☐ All teams report to coordinators every 15 minutes
- ☐ Coordinators brief Incident Commander every 30 minutes
- ☐ Critical updates communicated immediately

Phase 3: Integrated Response Strategy (30-60 minutes)

System Restoration Prioritization

1. Critical Path Analysis

- ☐ Identify systems that enable restoration of other systems
- ☐ Map dependencies and restoration sequences
- ☐ Identify parallel vs. sequential restoration opportunities

2. Resource Allocation Strategy

- ☐ **Concentrated Approach:** All resources on highest priority
- ☐ **Parallel Approach:** Resources split across critical systems
- ☐ **Hybrid Approach:** Staged resource reallocation

3. Risk vs. Benefit Assessment

- ☐ **Quick Wins:** Low-effort, high-impact restorations
- ☐ **Foundation Systems:** Systems that enable other restorations
- ☐ **Safety Critical:** Systems essential for safe operations

Integration Challenges and Solutions **Challenge:** Competing Resource Demands - **Solution:** Establish clear priority hierarchy - **Process:** Technical Coordinator allocates based on priority matrix - **Escalation:** Incident Commander resolves conflicts

Challenge: Cross-System Dependencies - **Solution:** Map dependencies and coordinate restoration sequence - **Process:** Technical teams provide dependency information - **Coordination:** Shared timeline with checkpoints

Challenge: Information Overload - **Solution:** Structured reporting with standardized updates - **Process:** 15-minute status reports using standard format - **Filtering:** Coordinators filter information for decision makers

System-Specific Coordination Procedures

Network + AIS Failure Coordination

Immediate Actions: - [] Determine if network failure is causing AIS issues - [] Implement manual vessel tracking if AIS dependent on network - [] Prioritize network restoration if it enables AIS recovery

Resource Coordination: - [] Assign network team to core infrastructure - [] Deploy operations team for manual AIS tracking - [] Coordinate vessel communications through harbor master

CCTV + Operations System Failures

Immediate Actions: - [] Deploy manual spotters for safety-critical areas - [] Implement enhanced radio communication - [] Slow operations in areas without visual coverage

Resource Coordination: - [] Operations personnel for manual monitoring - [] Technical personnel for system restoration - [] Safety personnel for enhanced oversight

Multi-System + Network Failures

Immediate Actions: - [] Establish alternative communication methods - [] Implement manual coordination procedures - [] Consider external technical assistance

Resource Coordination: - [] Contact external technical support - [] Implement manual inter-team coordination - [] Establish physical coordination center if needed

Communication Protocols

Internal Coordination Messages

Multi-System Status Update Template **TO:** All Coordinators

FROM: [System Team Lead]

SUBJECT: Multi-System Status - [Timestamp]

SYSTEM STATUS: - Primary System: [Status/ETA] - Secondary Impact: [Description] - Resource Needs: [Specific requirements] - Coordination Requirements: [Dependencies on other teams]

Coordinator Briefing Template **TO:** Incident Commander

FROM: [Coordinator]

SUBJECT: Coordination Status - [Timestamp]

OVERALL STATUS: [Green/Yellow/Red] **KEY DEVELOPMENTS:** [Major changes since last update] **RESOURCE ALLOCATION:** [Current assignments] **CRITICAL DECISIONS NEEDED:** [Items requiring IC input] **ESTIMATED RESOLUTION:** [Timeline assessment]

External Communication

Stakeholder Notification Template **TO:** [External Stakeholders]

SUBJECT: Operational Status Update - Multi-System Incident

SITUATION: We are managing a multi-system technical incident affecting [general description].

CURRENT STATUS: Operations continuing with [enhanced safety procedures/reduced capacity/manual procedures].

SAFETY: All safety measures remain in place and are being enhanced during response.

TIMELINE: We expect [gradual restoration over X hours/significant progress by X time].

NEXT UPDATE: [Specific time for next communication]

Escalation Triggers

Technical Escalation

Escalate to External Technical Support When: - ☐ Multiple systems failing faster than restoration capability - ☐ Evidence of coordinated cyber attack - ☐ Technical teams overwhelmed or lacking expertise - ☐ Restoration timeline exceeds acceptable operational impact

Executive Escalation

Escalate to Executive Team When: - ☐ Safety concerns requiring operations shutdown - ☐ Estimated restoration time exceeds 4 hours - ☐ Evidence suggesting deliberate attack requiring legal response - ☐ External assistance or emergency declaration needed

Emergency Services Escalation

Escalate to Emergency Services When: - ☐ Personnel safety cannot be assured - ☐ Emergency response capability compromised - ☐ Environmental or public safety risks identified - ☐ Criminal activity suspected

Recovery Coordination

Restoration Verification Process

1. **Individual System Testing**
 - ☐ Verify each system functions independently
 - ☐ Test core functionality before integration
 - ☐ Document any ongoing issues or limitations
2. **Integration Testing**
 - ☐ Verify cross-system communications
 - ☐ Test dependent system functionality
 - ☐ Confirm data synchronization and integrity
3. **Operational Verification**

- ☐ Test operational procedures with restored systems
- ☐ Verify safety systems and monitoring
- ☐ Confirm normal operational capacity

Lessons Learned Process

1. **Immediate Debrief (Within 24 hours)**
 - ☐ What worked well in coordination?
 - ☐ What communication challenges occurred?
 - ☐ Which resource allocation decisions were effective?
 2. **Technical Analysis (Within 72 hours)**
 - ☐ Root cause analysis for each system failure
 - ☐ Dependency mapping accuracy assessment
 - ☐ Technical response time evaluation
 3. **Process Improvement (Within 1 week)**
 - ☐ Update coordination procedures based on experience
 - ☐ Revise priority matrices if needed
 - ☐ Enhance training for multi-system scenarios
-

Success Criteria

- Safe coordination of response to multiple simultaneous system failures
 - Effective resource allocation and priority management
 - Clear communication and decision-making structure
 - Minimized operational impact through coordinated response
 - Successful restoration of all systems with lessons learned integration
-

Related Documents

- Safety Risk Assessment Template
- Crisis Decision Authority Matrix
- Network Diagnostics SOP
- CCTV Blackout Response SOP
- AIS Signal Validation Procedures