Contents

SOUTHGATE TERMINAL 2

## Port Operations Security Documentation 2

Multi-System Failure Coordination Guide 2

Document Information 2

Purpose 2

When to Use This Guide 2

Multi-System Failure Assessment Framework 2

System Criticality Matrix 2

Failure Combination Assessment 3

Multi-System Response Protocols 3

Phase 1: Rapid Assessment (0-10 minutes) 3

Phase 2: Coordination and Prioritization (10-30 minutes) 4

Phase 3: Coordinated Response Execution (30+ minutes) 5

System-Specific Coordination Procedures 6

AIS + CCTV Failure Coordination 6

Network + Authentication Failure Coordination 7

Container + CCTV + Authentication Triple Failure 7

Communication Protocols During Multi-System Failures 8

Enhanced Communication Schedule 8

Communication Priority Matrix 8

Alternative Communication Methods 9

Decision Points and Escalation Triggers 9

Operations Halt Decision Matrix 9

Executive Escalation Triggers 9

Resource Allocation During Multi-System Failures 10

Personnel Assignment Matrix 10

Equipment and Resource Priority 11

Recovery and Transition Planning 11

Phased System Restoration 11

Transition Back to Automated Operations 11

Success Criteria for Multi-System Coordination 12

Immediate Response Success 12

Sustained Response Success 12

Recovery Success 12

Overall Coordination Success 12

SOUTHGATE TERMINAL

## Port Operations Security Documentation

Multi-System Failure Coordination Guide

Document Information

Document Type: Crisis Response Framework **Intended Users:** All Teams - Coordinated Response **Usage Context:** When multiple critical systems fail simultaneously **Related Scenarios:** AIS + CCTV + Network failures, Container + Authentication + CCTV failures

---

Purpose

This guide provides systematic coordination procedures when multiple critical systems fail simultaneously, ensuring effective cross-team response, resource prioritization, and operational continuity during complex multi-system incidents.

When to Use This Guide

- Two or more critical systems failing within 30 minutes of each other
- Evidence of coordinated or systematic attack affecting multiple systems
- Operational capacity reduced below 50% due to system failures
- Manual operations required across multiple operational areas
- Cross-team resource conflicts due to competing system failures

---

Multi-System Failure Assessment Framework

System Criticality Matrix

TIER 1 CRITICAL SYSTEMS (Immediate Operations Impact)

- **AIS/GPS Navigation:** Ship tracking and collision avoidance
- **CCTV Surveillance:** Visual safety monitoring and security
- **Crane Control Systems:** Container handling operations
- **Container Routing:** Cargo movement and placement
- **Authentication Systems:** Access control and system security

TIER 2 SUPPORTING SYSTEMS (Operational Efficiency Impact)

- **Network Infrastructure:** Communications and data flow
- **Vendor Gateway:** External partner coordination

- **Log Management:** Audit trail and forensic capability
- **Communication Systems:** Internal and external coordination

TIER 3 ADMINISTRATIVE SYSTEMS (Management Impact)

- **HR Systems:** Staff management and scheduling
- **Policy Systems:** Procedure access and compliance
- **Media Systems:** Public relations and communications

Failure Combination Assessment

CATASTROPHIC COMBINATIONS (Immediate Operations Halt Required)

- **AIS + CCTV + Crane Control:** Complete operational blindness with safety risk
- **Authentication + Container + CCTV:** Security compromise with operational impact
- **Network + AIS + Container:** Complete system isolation with navigation loss

CRITICAL COMBINATIONS (Major Operations Reduction Required)

- **AIS + CCTV:** Navigation and visual monitoring lost
- **CCTV + Crane Control:** Visual confirmation and operational control lost
- **Container + Authentication:** Operational disruption with potential security issues
- **Network + Authentication:** Communication and security control lost

SIGNIFICANT COMBINATIONS (Enhanced Procedures Required)

- **AIS + Network:** Navigation data loss with communication issues
- **CCTV + Network:** Visual monitoring lost with communication challenges
- **Vendor + Authentication:** External coordination lost with security concerns

---

Multi-System Response Protocols

Phase 1: Rapid Assessment (0-10 minutes)

RAPID DECISION TREE (Use when under time pressure)

```
Multiple systems failing?
+- YES - Are they safety-critical systems?
| +- YES - Can safety be maintained with manual procedures?
| | +- YES - Continue with enhanced manual operations
| | +- NO - Consider operations halt - Escalate to executive
| +- NO - Implement enhanced procedures - Continue investigation
+- NO - Standard incident response procedures
```

10-MINUTE ASSESSMENT CHECKLIST **IMMEDIATE (0-3 minutes):** - [ ] **Life Safety Check:** Any immediate danger to personnel? - [ ] **System Count:** How many critical systems affected? - [ ] **Timeline:** Did failures happen together or cascading?

RAPID IMPACT (3-7 minutes): - [ ] **Operational Capacity:** Can we maintain safe operations? - [ ] **Manual Capability:** Do we have personnel for manual procedures? - [ ] **External Visibility:** Are failures visible to customers/public?

COORDINATION SETUP (7-10 minutes): - [ ] **Team Assignments:** Which teams focus on what? - [ ] **Communication Schedule:** How often will teams update? - [ ] **Escalation Triggers:** When do we escalate to executive?

Immediate Situation Assessment **Incident Coordinator Actions:** - [ ] **System Status Verification:** Confirm which systems are actually failed vs. degraded - [ ] **Timeline Correlation:** Determine if failures occurred simultaneously or cascading - [ ] **Impact Assessment:** Evaluate immediate operational and safety implications - [ ] **Resource Availability:** Identify available teams and manual capabilities

All Teams Parallel Actions: - [ ] **Technical Team:** Begin systematic investigation of each failed system - [ ] **Operations Team:** Implement immediate safety measures and capacity assessment - [ ] **Legal Team:** Assess regulatory notification requirements for multi-system incident - [ ] **Media Team:** Prepare holding statements for potential external visibility - [ ] **Executive Team:** Prepare for potential escalation to operations halt decision

Safety-First Decision Point (5 minutes) **HALT OPERATIONS IMMEDIATELY IF:** - Cannot ensure safe container movements without multiple systems - Crew expressing serious safety concerns about working without key systems - Risk of collision or injury due to lack of visibility/navigation - Evidence of ongoing attack requiring immediate containment

CONTINUE WITH ENHANCED PROCEDURES IF: - Manual procedures can safely replace failed systems - Adequate crew available for enhanced spotting/communication - No immediate safety threats identified - Systems appear to be failing independently rather than coordinated attack

Phase 2: Coordination and Prioritization (10-30 minutes)

Multi-Team Coordination Meeting **Immediate Virtual/Physical Huddle (10 minutes maximum):**

Incident Coordinator Leads: - [ ] **Situation Brief:** 2-minute status update from each team - [ ] **Priority Matrix:** Establish system restoration priorities - [ ] **Resource Allocation:** Assign teams to primary vs. supporting roles - [ ] **Communication Protocol:** Establish enhanced communication schedule - [ ] **Decision Authority:** Clarify who makes what decisions during crisis

Team Assignment Matrix:

Failed Systems	Primary Response Team	Supporting Teams	Expected Timeline
AIS + CCTV	Technical + Operations	Legal (notifications), Media (communications)	2-4 hours
CCTV + Container	Operations + Technical	Legal (liability), Executive (decisions)	1-3 hours
Network + Authentication	Technical + Legal	Operations (manual procedures), Executive (escalation)	3-6 hours
AIS + Container + CCTV	ALL TEAMS	Incident Coordinator orchestrates	4-8 hours

Resource Prioritization Framework **PRIORITY 1: IMMEDIATE SAFETY** - Manual spotters for crane operations - Alternative navigation procedures - Enhanced communication protocols - Emergency system isolation if needed

PRIORITY 2: OPERATIONAL CONTINUITY - Manual override authorization - Alternative routing procedures - Backup communication systems - Vendor coordination for critical functions

PRIORITY 3: INVESTIGATION AND RECOVERY - Systematic technical investigation - Evidence preservation - System restoration planning - External coordination

PRIORITY 4: COMPLIANCE AND COMMUNICATIONS - Regulatory notifications - Media management - Legal documentation - Stakeholder communications

Phase 3: Coordinated Response Execution (30+ minutes)

Parallel Response Streams **TECHNICAL INVESTIGATION STREAM Lead:** Technical Team **Timeline:** Ongoing throughout incident **Key Actions:** - [ ] **VM Investigation:** Systematic examination of each affected VM - [ ] **Evidence Collection:** Secure logs and artifacts before they can be tampered with - [ ] **Correlation Analysis:** Identify connections between different system failures - [ ] **Recovery Assessment:** Determine what can be restored vs. what requires replacement

OPERATIONAL CONTINUITY STREAM Lead: Operations Team **Timeline:** Immediate and ongoing **Key Actions:** - [ ] **Manual Procedures:** Implement comprehensive manual operations across all affected areas - [ ] **Safety Monitoring:** Enhanced safety protocols with additional personnel - [ ] **Capacity Management:** Calculate and communicate reduced operational capacity - [ ] **Crew Coordination:** Manage personnel assignments and fatigue during extended manual operations

LEGAL AND COMPLIANCE STREAM Lead: Legal Team **Timeline:** Within regulatory deadlines **Key Actions:** - [ ] **Notification Matrix:** Determine all required regulatory notifications for multi-system incident - [ ] **Evidence Preservation:** Implement legal hold across all affected systems - [

] **Liability Assessment:** Evaluate exposure from multi-system operational impacts - [ ] **Insurance Coordination:** Coordinate with multiple insurance policies potentially affected

COMMUNICATIONS STREAM Lead: Media Team **Timeline:** Proactive and responsive **Key Actions:** - [ ] **Stakeholder Communications:** Coordinate messaging across all stakeholder groups - [ ] **Media Management:** Handle external inquiries about visible operational disruptions - [ ] **Internal Communications:** Keep staff informed about status and expectations - [ ] **Crisis Messaging:** Develop consistent narrative across all communication channels

EXECUTIVE DECISION STREAM Lead: Executive Team **Timeline:** Real-time decision support **Key Actions:** - [ ] **Strategic Decisions:** Make high-level decisions about operations continuation vs. halt - [ ] **Resource Authorization:** Approve resource allocation and emergency expenditures - [ ] **Stakeholder Management:** Handle board, government, and major customer communications - [ ] **Recovery Planning:** Plan for post-incident recovery and business continuity

---

System-Specific Coordination Procedures

AIS + CCTV Failure Coordination

Immediate Actions (0-15 minutes) **Technical Team:** - [ ] Investigate correlation between AIS vm-coretech and CCTV vm-opsnode - [ ] Check for evidence of coordinated GPS jamming affecting both systems - [ ] Preserve logs from both systems before potential tampering

Operations Team: - [ ] Deploy enhanced spotter network for visual navigation confirmation - [ ] Implement reduced speed protocols for all vessel movements - [ ] Establish direct radio contact with all vessels in terminal area

Incident Coordinator: - [ ] Assess if this constitutes coordinated attack requiring immediate escalation - [ ] Coordinate manual procedures that address both navigation and visual monitoring loss - [ ] Determine if operations can continue safely with enhanced manual procedures

Coordination Challenges:

- **Competing Resource Demands:** Both systems require technical investigation and operational workarounds
- **Safety Risk Multiplication:** Loss of both navigation data and visual confirmation creates compounded risk
- **Communication Complexity:** Need for enhanced coordination when normal systems compromised

Success Criteria:

- Safe operations maintained despite loss of both automated systems
- Technical investigation proceeding in parallel without compromising operations

- Clear communication maintained between all teams and with vessels

Network + Authentication Failure Coordination

Immediate Actions (0-15 minutes) **Technical Team:** - [ ] Investigate if network failure caused authentication system breakdown - [ ] Check for evidence of credential compromise or unauthorized access - [ ] Implement emergency authentication procedures using alternative methods

Legal Team: - [ ] Assess if authentication failure constitutes reportable security incident - [ ] Implement evidence preservation before systems can be further compromised - [ ] Coordinate with technical team on investigation to preserve legal privilege

Operations Team: - [ ] Switch to manual authorization procedures for all operational decisions - [ ] Implement enhanced verification protocols for personnel access - [ ] Establish alternative communication methods not dependent on network

Coordination Challenges:

- **Security vs. Operations:** Need to maintain security while enabling operational continuity
- **Investigation vs. Recovery:** Balance between preserving evidence and restoring systems
- **Communication Breakdown:** Network failure complicates coordination between teams

Container + CCTV + Authentication Triple Failure

Immediate Actions (0-20 minutes) **ALL TEAMS EMERGENCY COORDINATION:**

Phase 1 (0-5 minutes): **Safety Assessment** - [ ] **IMMEDIATE QUESTION:** Can container operations continue safely without visual confirmation and automated authentication? - [ ] **OPERATIONS:** Deploy maximum spotter coverage for all container areas - [ ] **TECHNICAL:** Begin rapid assessment of all three system failures for correlation - [ ] **INCIDENT COORDINATOR:** Prepare for potential operations halt decision

Phase 2 (5-15 minutes): **Operational Decision** - [ ] **OPERATIONS:** Calculate safe operational capacity with manual procedures for all three systems - [ ] **TECHNICAL:** Report initial findings on whether failures appear coordinated - [ ] **LEGAL:** Assess regulatory requirements for triple system failure - [ ] **EXECUTIVE:** Make operations continuation vs. halt decision

Phase 3 (15-20 minutes): **Implementation** - [ ] **If Continuing:** Implement comprehensive manual procedures with enhanced safety measures - [ ] **If Halting:** Execute safe operations shutdown while maintaining investigation capability - [ ] **ALL TEAMS:** Switch to maximum coordination mode with 15-minute status updates

---

Communication Protocols During Multi-System Failures

Enhanced Communication Schedule

IMMEDIATE PHASE (First 30 minutes)

- **Every 5 minutes:** Safety status updates between Operations and Incident Coordinator
- **Every 10 minutes:** Technical investigation updates to all teams
- **Every 15 minutes:** All-team status briefing led by Incident Coordinator

ACTIVE RESPONSE PHASE (30 minutes - 2 hours)

- **Every 15 minutes:** Technical progress updates
- **Every 30 minutes:** Operational status and capacity assessments
- **Every 30 minutes:** Legal and compliance status updates
- **Every 60 minutes:** Executive briefing with decision points

SUSTAINED RESPONSE PHASE (2+ hours)

- **Every 30 minutes:** All-team coordination calls
- **Every 60 minutes:** Stakeholder communication updates
- **Every 2 hours:** Shift change briefings and handover
- **Every 4 hours:** Executive strategic review and planning

Communication Priority Matrix

PRIORITY 1: IMMEDIATE SAFETY

- Operations Team safety concerns
- Technical Team critical findings requiring immediate action
- Evidence of ongoing attack or system compromise

PRIORITY 2: OPERATIONAL COORDINATION

- Manual procedure implementation status
- System restoration progress updates
- Resource allocation and personnel management

PRIORITY 3: COMPLIANCE AND STAKEHOLDER

- Regulatory notification requirements
- Legal documentation and evidence preservation
- Media and external communications

Alternative Communication Methods

Primary Network Failure Backup:

- **Mobile phones:** Direct calling for urgent communications
- **Radio systems:** Operational coordination and safety communications
- **Physical meetings:** Face-to-face coordination for complex decisions
- **Runner system:** Physical message delivery for non-urgent coordination

---

Decision Points and Escalation Triggers

Operations Halt Decision Matrix

IMMEDIATE HALT REQUIRED:

- **Safety Risk:** Cannot ensure safe operations with available manual procedures
- **Security Threat:** Evidence of ongoing coordinated attack requiring complete isolation
- **Regulatory Requirement:** Legal or regulatory requirement to cease operations
- **Resource Exhaustion:** Insufficient qualified personnel for safe manual operations

OPERATIONS REDUCTION REQUIRED:

- **Partial Safety Risk:** Can ensure safety but at significantly reduced capacity
- **System Uncertainty:** Unable to determine if systems are stable or continuing to degrade
- **Personnel Stress:** Crew expressing significant safety concerns about continued operations
- **Investigation Needs:** Technical investigation requires operational systems to be isolated

ENHANCED PROCEDURES SUFFICIENT:

- **Manageable Risk:** Manual procedures can adequately replace failed systems
- **Stable Failure State:** Systems appear to have failed to a stable state rather than continuing to degrade
- **Adequate Resources:** Sufficient qualified personnel for enhanced manual procedures
- **Clear Recovery Path:** Technical team has clear plan for system restoration

Executive Escalation Triggers

IMMEDIATE EXECUTIVE INVOLVEMENT:

- Three or more Tier 1 systems failed simultaneously
- Evidence of coordinated cyber attack
- Operations halt decision required
- Major customer or regulatory escalation
- Media crisis requiring executive spokesperson

EXECUTIVE MONITORING REQUIRED:

- Two Tier 1 systems failed
- Extended duration incident (>2 hours)
- Significant operational capacity reduction
- Legal notifications required
- Insurance claims likely

EXECUTIVE AWARENESS SUFFICIENT:

- Single system failures with workarounds
- Normal technical investigations
- Routine regulatory notifications
- Standard operational disruptions

Resource Allocation During Multi-System Failures

Personnel Assignment Matrix

CATASTROPHIC MULTI-SYSTEM FAILURE: **Technical Team:** - 50% investigation and evidence preservation - 30% system restoration attempts - 20% supporting manual operations with technical expertise

Operations Team: - 70% manual operations implementation and safety - 20% coordination with technical team - 10% capacity assessment and planning

Legal Team: - 40% regulatory notifications and compliance - 40% evidence preservation and legal hold - 20% supporting decision-making with legal advice

Media Team: - 60% external communications and media management - 30% internal communications and staff updates - 10% supporting executive communications

Executive Team: - 50% strategic decision-making and high-level coordination - 30% stakeholder management (board, government, major customers) - 20% resource authorization and recovery planning

CRITICAL MULTI-SYSTEM FAILURE:

- Technical Team: 60% investigation, 40% restoration
- Operations Team: 80% manual operations, 20% coordination
- Legal Team: 60% compliance, 40% support
- Media Team: 50% external, 50% internal/support
- Executive Team: 40% decisions, 60% monitoring and planning

Equipment and Resource Priority

IMMEDIATE ALLOCATION:

- **Manual equipment:** Radios, spotting equipment, alternative communication devices
- **Investigation tools:** Laptops, mobile devices for technical investigation
- **Safety equipment:** Additional safety gear for enhanced manual operations
- **Communication backup:** Mobile phones, alternative internet connections

SECONDARY ALLOCATION:

- **Recovery equipment:** Replacement components, backup systems
- **Documentation tools:** Cameras, evidence bags, chain-of-custody materials
- **Comfort support:** Food, beverages, additional lighting for extended operations
- **External support:** Vendor emergency contacts, external technical support

---

Recovery and Transition Planning

Phased System Restoration

Phase 1: Safety-Critical Restoration **Priority Order:** 1. **CCTV Systems:** Restore visual monitoring for safety 2. **Communication Systems:** Ensure reliable coordination capabilities 3. **Authentication Systems:** Restore secure access control 4. **Primary Navigation:** Restore AIS/GPS for vessel safety

Phase 2: Operational Restoration **Priority Order:** 1. **Container Control Systems:** Restore automated container handling 2. **Crane Control Systems:** Restore automated crane operations 3. **Network Infrastructure:** Restore full network capabilities 4. **Vendor Systems:** Restore external partner coordination

Phase 3: Full Capability Restoration **Priority Order:** 1. **Administrative Systems:** Restore HR, policy, and management systems 2. **Audit and Compliance Systems:** Restore full logging and monitoring 3. **Media and Communications Systems:** Restore full public relations capabilities 4. **Advanced Features:** Restore all non-essential but beneficial capabilities

Transition Back to Automated Operations

Pre-Transition Checklist

☐ **Technical Verification:** All systems tested and verified stable
☐ **Safety Assessment:** Comprehensive safety review completed
☐ **Personnel Briefing:** All staff briefed on transition plan and timing
☐ **Gradual Implementation:** Phased transition plan developed and communicated

Transition Process

1. **Announcement Phase (30 minutes before):** Notify all personnel of upcoming transition
2. **Gradual Implementation:** Restore one system at a time with verification
3. **Parallel Operation:** Run manual and automated procedures in parallel initially
4. **Full Transition:** Complete transition to automated operations
5. **Enhanced Monitoring:** Increased monitoring for first 2 hours after transition

Post-Transition Monitoring

- Enhanced monitoring of all restored systems for 24 hours
- Regular status checks with all operational teams
- Immediate rollback procedures ready if any system shows instability
- Comprehensive after-action review within 48 hours

Success Criteria for Multi-System Coordination

Immediate Response Success

- Safe operations maintained or safely halted within 15 minutes of failure recognition
- All teams coordinated and assigned roles within 30 minutes
- Enhanced communication protocols established and functioning
- Investigation begun without compromising operational safety

Sustained Response Success

- Manual operations maintaining adequate safety standards
- Technical investigation proceeding systematically across all failed systems
- Regulatory notifications completed within required timeframes
- Stakeholder communications maintaining confidence and providing accurate information

Recovery Success

- Systems restored in logical priority order
- Transition back to automated operations completed safely
- Comprehensive documentation of incident for lessons learned
- All regulatory and legal requirements met throughout incident

Overall Coordination Success

- Effective resource allocation across competing priorities
- Clear decision-making authority maintained throughout incident
- Cross-team communication effective despite system failures

- External stakeholder confidence maintained throughout incident

---

Owner: Incident Coordinator **Reference:** CRISIS-01 **Version:** 1.0 **Approved by:** Executive Crisis Team