

# Standard Operating Procedure

---

**Document Number:** [GUIDANCE-SYS-001]

**Standard Operating Procedure (SOP):** Shuttle Digital  
Autopilot Guidance System

**Revision:** 1.0

**Last Updated:** [DATE]

---

## Contents

---

1. Introduction
  - 1.1 Purpose
  - 1.2 System Overview
  - 1.3 Regulatory Compliance
2. System Specifications
  - 2.1 Technical Parameters
  - 2.2 Equipment Configuration
3. Operational Protocols
  - 3.1 Standard Operating Procedures
    - 3.1.1 Startup Procedure
    - 3.1.2 Normal Operation
  - 3.2 Performance Optimization
    - 3.2.1 Monitoring Parameters
    - 3.2.2 Adjustment Procedures
4. Emergency Operations
  - 4.1 Emergency Response Protocols
  - 4.2 System Recovery
5. Maintenance Requirements
  - 5.1 Preventive Maintenance Schedule
  - 5.2 Predictive Maintenance Implementation

- 6. Quality Assurance
    - 6.1 Performance Metrics
    - 6.2 Documentation Requirements
  - 7. Security Protocols
    - 7.1 Physical Access Control
    - 7.2 Data and System Security
  - 8. Environmental Considerations
    - 8.1 Environmental Impact
    - 8.2 Sustainability Measures
  - 9. Training Requirements
    - 9.1 Personnel Qualifications
    - 9.2 Training Programs
  - 10. Document Control
    - 10.1 Revision History
    - 10.2 Authorization
  - 11. Process Flows and State Transitions
    - 11.1 System States
    - 11.2 Operational Workflows
    - 11.3 Resource Management
- 

# 1. Introduction

---

## 1.1 Purpose

---

Defines when the Shuttle's digital autopilot should engage emergency (3E/0) guidance based on flight conditions.

## 1.2 System Overview

---

- Continuously checks key flight parameters: velocity, altitude, pitch, and pressure.
- Reacts autonomously to deviations from nominal flight conditions.

- Triggers different operational branches based on current flight mode and state.

Monitors altitude, velocity, dynamic pressure, and other sensor inputs to determine the correct abort procedure or emergency region.

### 1.3 Regulatory Compliance

---

Complies with NASA abort guidance protocol and on-orbit emergency safety regulations.

---

## 2. System Specifications

---

### 2.1 Technical Parameters

---

- Monitors: Velocity, vertical speed, angle of attack, dynamic pressure
- Flags: `cont_3EO_start`, `RTLS_abort_declared`, `region_selected`
- Modes: `mm102` (ascent), `mm103` (coast), `mm601` (abort/RTLS)

### 2.2 Equipment Configuration

---

All logic runs through onboard flight control computers. Inputs sourced from IMU, barometric sensors, and mission timers.

---

## 3. Operational Protocols

---

### 3.1 Standard Operating Procedures

---

#### 3.1.1 Startup Procedure

- Set all internal control flags to default or false.
- Assign `step = undef` to reset the logic flow.

- Initialize region register to `reg-1` (unset).
- Await activation via `start_cont_3eo_mode_select`.
- Initialize step to undefined
- Clear emergency flags and assign initial region (`reg-1`)
- Wait for `start_cont_3eo_mode_select` to trigger

### 3.1.2 Normal Operation

- Read flight parameters from sensors (e.g., IMU, velocity meters).
- Evaluate abort conditions based on velocity and MECO.
- Assign region: `reg1-reg4` for various emergency levels, or `reg102` for early ascent.
- Set `region_selected = TRUE` upon successful region assignment.
- If no abort required, exit without engaging emergency logic.
- Step through logic using flight parameters
- If MECO occurs or abnormal flight detected, transition to emergency mode
- Set region and guidance flags based on matching conditions

## 3.2 Performance Optimization

---

### 3.2.1 Monitoring Parameters

- Track velocity thresholds for abort triggers
- Monitor apogee vs reference altitude
- Check dynamic pressure for region assignment

### 3.2.2 Adjustment Procedures

- Region logic allows dynamic transition between `reg1-4` or `reg102`

- Abort flag resets if region not selected or emergency condition no longer exists
- 

## 4. Emergency Operations

---

### 4.1 Emergency Response Protocols

---

- Detect abnormal flight status post-MECO.
- Evaluate downrange distance and velocity profile.
- Assign region based on emergency type and severity.
- Activate guidance system for tank separation and pitch adjustment.
- If velocity low and MECO confirmed, set `cont_3EO_start = TRUE`
- Determine region (RTLS, region 1-4, or fast separation)

### 4.2 System Recovery

---

- Execute pitch and dump maneuvers per region logic
  - Transition to MM601 after RTLS declared
- 

## 5. Maintenance Requirements

---

### 5.1 Preventive Maintenance Schedule

---

- Confirm thresholds and transition logic before launch
- Validate region outputs in simulation

### 5.2 Predictive Maintenance Implementation

---

- Use telemetry data from past missions to refine parameter thresholds
  - Apply redundancy checks for key region signals
-

## 6. Quality Assurance

---

### 6.1 Performance Metrics

---

- Region assignment accuracy under stress conditions.
- Mean time from trigger to emergency guidance activation.
- Integrity of abort sequences during regression testing.
- Accuracy of region selection
- Time-to-decision under MECO/abort conditions

### 6.2 Documentation Requirements

---

- Log each invocation of `cont_3E0_start`
  - Record final region, guidance actions, and result
- 

## 7. Security Protocols

---

### 7.1 Physical Access Control

---

- Guidance logic secured in onboard computers with tamper detection

### 7.2 Data and System Security

---

- Abort logic verified pre-flight
  - Region transitions not externally modifiable during mission
- 

## 8. Environmental Considerations

---

### 8.1 Environmental Impact

---

- System ensures controlled reentry and tank jettison

## 8.2 Sustainability Measures

---

- Reduces risk of uncontrolled failure or debris

---

## 9. Training Requirements

---

### 9.1 Personnel Qualifications

---

- Engineers must understand model-checking logic.
- Controllers must interpret flight mode transitions.
- All personnel must pass abort guidance simulation tests.
- Mission controllers must understand abort logic flow
- Flight software engineers must validate logic against models

### 9.2 Training Programs

---

- Simulation training for all emergency conditions
- Pre-flight briefings on region-based guidance logic

---

## 10. Document Control

---

### 10.1 Revision History

---

- Rev 1.0 – Initial SOP based on guidance.txt formal specification

### 10.2 Authorization

---

- Authorized by Flight Software Group Lead
  - Reviewed by Mission Operations Directorate
-

# 11. Process Flows and State Transitions

---

## 11.1 System States

---

- `step` variable transitions: `1 → a1 → 2... → exit`
- Conditional transitions based on altitude, speed, and pitch

## 11.2 Operational Workflows

---

### 11.2.1 Workflow 1

1. Evaluate mode and velocity
  - If `mm102` : set `reg102`
  - If velocity above limit: exit
2. Assign region based on:
  - Apogee, *qbar*, *h*<sub>dot</sub>, and angle
3. Set `region_selected = TRUE` and exit

### 11.2.2 Workflow 2

1. Engage guidance
2. Trigger tank separation
3. Command OMS dump
4. Adjust pitch and attitude
5. Finalize entry and abort state

## 11.3 Resource Management

---

### 11.3.1 Resource Allocation

- Region assigned based on live telemetry
- State transitions gated by sensor thresholds



### **11.3.2 Synchronization Procedures**

- Abort flags, separation commands, and entry orientation are interlocked
- Once triggered, system cannot re-enter mode select unless reset