Frontera Space Emergency Procedure: Power Loss or Critical System Failure

Revision: 01

Frontera Space Document: 000018

12/10/2025

1 PURPOSE

The purpose of this procedure is to define required response actions for loss of electrical power or critical system failures affecting the PTSD (Portable Test Stand by Dan) or associated support systems. This document establishes:

• Classification of power-loss and system-failure severity levels
• Required personnel response and PPE posture by failure state
• Stand safing and hazard isolation requirements
• Use of backup power and fail-safe systems
• Fallback, evacuation, and stabilization procedures
• Documentation, reporting, and return-to-operations criteria

These actions ensure personnel safety, prevent uncontrolled hazardous conditions, and maintain system integrity during abnormal or degraded operating condition

2 SCOPE

This procedure applies to:

- All personnel working in or around the PTSD stand
- All operations involving hypergolic propellants, oxidizers, pressurants, purges, and ignition systems
- All electrical power systems, control systems, PLCs, sensors, actuators, and communications
- All testing, conditioning, troubleshooting, and recovery activities

Compliance with this procedure and associated training is mandatory for all personnel.

Level 1 – Minor / Non-Critical Power Interruption

- **Conditions:**
- Momentary power fluctuation or brief outage
- No loss of control authority
- All critical valves fail closed as designed
- No alarms indicating hazardous release
- **Required Actions:**
  Pause operations
- Maintain current PPE posture
- Verify system status via instrumentation and camera feeds
- Confirm fail-safe states are achieve
- Resume operations only after system checks are complete

Level 2 – Loss of Primary Power with Backup Available

Conditions:

- Loss of primary electrical power
- Automatic transfer to UPS, battery backup, or generator
- Control and monitoring remain functional
- No active hazardous release detected

Required Actions:

- Stop all active testing or pressurization
- Maintain PPE Posture B inside the fenced area
- Verify backup power status and remaining capacity
- Confirm valve states, pressures, and purge conditions
- Prepare for escalation if backup power degrades

Level 3 – Loss of Control Authority or Partial System Failure

Conditions:

- Loss of PLC, control network, or sensor feedback
- Inability to command valves or actuators reliably
- Incomplete or uncertain system state
- No confirmed hazardous release, but elevated risk exists

Required Actions:

- Immediately safe the stand using pre-defined fail-safe logic
- Personnel fall back to the fence line
- PPE Posture B permitted only at the fence line
- No manual intervention unless explicitly authorized
- Troubleshooting conducted remotely using available telemetry

If system state cannot be positively confirmed, escalate to Level 4.

Level 4 – Complete Power Loss or Critical Safety System Failure

Conditions:

- Total loss of electrical power
- Loss of control, monitoring, or communications
- Failure of purge, vent, or isolation systems
- Any concurrent toxic-gas alarm or pressure anomaly

Required Actions:

- Immediate evacuation of all personnel from the fenced area
- Treat the stand as potentially hazardous until proven otherwise
- No re-entry permitted without Safety Officer authorization

- PPE Posture C required for any emergency intervention
- Stand remains secured until power and control are restored and verified

3 Stand Safing & Hazard Isolation

Upon any Level 2–4 event:

- Verify all valves fail to their safe state (normally closed or vented)
- Confirm pressure decay or stabilization via available instrumentation
- Ensure ignition sources are de-energized
- Disable restart or automatic sequencing until authorized

No attempt to resume operations may occur until safing is confirmed.

4 Exclusion Zones & Personnel Control

- The PTSD fence line defines the exclusion zone
- Only essential personnel are permitted inside the exclusion zone
- No personnel may enter during Level 4 events without PPE Posture C
- The exclusion zone remains in effect until clearance is granted by the Safety Officer

5 Stabilization & Recovery

Once power or control is restored:

- Verify system integrity remotely
- Confirm sensor health and communication links
- Inspect valves, regulators, and actuators for abnormal conditions
- Re-establish purge and vent path
- Lock out failed subsystems pending inspection

Hardware suspected of contributing to the failure shall be tagged and removed from service.

6 Coordination With External Resources

EMS Activation

EMS shall be activated for:

Personnel injury during loss-of-power events

Heat stress, inhalation symptoms, or trauma

Any condition beyond on-site treatment capability

7 DOCUMENTATION & INCIDENT REPORTING

Immediate Documentation

Following stabilization of any Level 2–4 event:

- Record time, duration, and scope of power loss
- Identify affected systems and subsystems
- Capture alarm logs, telemetry, and camera footage
- Document personnel locations and PPE posture

Record weather conditions if relevant

Formal Incident Report

A written incident report shall be completed within **24 hours**, including:

- Timeline of the event
- Root cause (if known) or suspected failure mode
- System and safety impacts
- Actions taken to safe and stabilize
- Personnel exposure or injury assessment
- Corrective actions and recommendations

Root-Cause Analysis & Corrective Actions

- Perform engineering review of electrical and control systems
- Identify hardware, software, or procedural contributors
- Implement corrective actions
- Update SOPs, training, or system design as required
- Track actions to closure via QA processes

Return-to-Operations Authorization

- Operations may resume only when:
- Power and control systems are fully restored
- Stand safing has been verified
- All failed components are replaced or cleared
- Safety Officer grants clearance
- Test Director issues formal return-to-operations authorization

8 PROGRAM MAINTENANCE

This document shall be:

- Reviewed annually

- Updated following any power-loss or critical-system incident
- Revised when electrical, control, or safety systems change