ADR-006: Selective Shutdown Policy for Safety Faults

Architecture Diagrams

Status: Accepted **Date:** 2025-10-28 **Deciders:** Safety Engineer, System Architect, Clinical Advisors **Technical Story:** Safety system behavior on interlock failure

Context and Problem Statement

When a safety interlock fails (footpedal release, smoothing module failure, photodiode mismatch, watchdog timeout), the system must respond to protect the patient. Two competing design philosophies:

1. **Total Shutdown:** Disable ALL systems (laser, camera, actuator, monitoring) on safety fault
2. **Selective Shutdown:** Disable ONLY the treatment laser, preserve other systems for diagnosis

Which approach should TOSCA use?

Decision Drivers

- **Patient Safety:** Highest priority - ensure laser cannot fire during fault
- **Diagnostic Capability:** Enable troubleshooting without requiring system restart
- **Controlled Recovery:** Allow safe actuator retraction after fault
- **Visual Feedback:** Maintain camera feed for operator situational awareness
- **Interlock Monitoring:** Continue monitoring safety signals for diagnostics
- **Event Logging:** Maintain ability to log fault details for audit trail
- **Clinical Workflow:** Minimize disruption from transient faults (e.g., footpedal slip)

Considered Options

- **Option A: Total Shutdown** - Disable all systems on safety fault (laser, camera, actuator, GPIO monitoring)
- **Option B: Selective Shutdown** - Disable only treatment laser, preserve camera, actuator, monitoring, aiming beam
- **Option C: Laser Only** - Disable laser but also disable camera (middle ground)

Decision Outcome

Chosen option: “Selective Shutdown (Option B)”, because it maximizes patient safety while preserving diagnostic capability and allowing controlled recovery. Treatment laser is the ONLY hazard requiring immediate shutdown. All other systems support safe diagnosis and recovery.

Positive Consequences

- **Safety Maintained:** Treatment laser (5W, Class 4) immediately disabled on fault
- **Visual Feedback:** Camera feed continues, operator sees treatment site during fault
- **Controlled Retraction:** Actuator remains operational, can retract laser ring safely
- **Aiming Beam Preserved:** SEMINEX aiming beam (<1mW, Class 2) aids realignment after fault recovery
- **Diagnostic Capability:** GPIO monitoring continues, operator can see which interlock failed
- **Event Logging:** Fault details logged with timestamp, interlock states, operator actions
- **Faster Recovery:** Operator can diagnose and fix fault (e.g., reposition footpedal) without restarting system
- **Reduced Downtime:** Transient faults (footpedal slip) don’t require full system reboot

Negative Consequences

- **Complexity:** More complex than total shutdown (requires selective disable logic)
- **Testing Burden:** Must verify treatment laser shutdown while other systems continue
- **Documentation Required:** Clear explanation of which systems remain active during fault
- **Operator Training:** Technicians must understand partial system state (laser off, camera on)

Pros and Cons of the Options

Option A: Total Shutdown

- Good, because simplest implementation (shut down everything)
- Good, because most conservative safety approach (no ambiguity)
- Good, because reduces complexity in safety state machine
- Bad, because loses visual feedback (camera off, operator blind)
- Bad, because prevents controlled actuator retraction (laser ring stuck in position)
- Bad, because prevents diagnosis (can’t see which interlock failed)
- Bad, because requires full system restart for transient faults
- Bad, because longer recovery time (patient repositioning, camera realignment)

Option B: Selective Shutdown (CHOSEN)

- Good, because treatment laser (hazard) immediately disabled
- Good, because camera feed preserved (visual situational awareness)
- Good, because actuator operational (controlled retraction possible)
- Good, because aiming beam preserved (<1mW Class 2, aids realignment)
- Good, because GPIO monitoring continues (diagnostic capability)
- Good, because event logging continues (immutable audit trail)
- Good, because faster recovery from transient faults
- Good, because reduces clinical workflow disruption
- Bad, because more complex than total shutdown
- Bad, because requires additional testing (verify partial shutdown)
- Bad, because requires operator training (understand partial state)

Option C: Laser + Camera Shutdown

- Good, because disables both laser and visual feedback (middle ground)
- Good, because simpler than selective shutdown
- Bad, because loses visual feedback (operator blind)
- Bad, because doesn't prevent camera operation (inconsistent with safety philosophy)
- Bad, because provides no diagnostic advantage over total shutdown

Links

- SAFETY_SHUTDOWN_POLICY.md (Detailed policy documentation)
- 03_safety_system.md (Safety system architecture)
- Related: [ADR-007-safety-state-machine.md]

Implementation Notes

Selective Shutdown Implementation (`safety.py`):

```
class SafetyManager:
    def _handle_safety_fault(self, fault_reason: str):
        """Selective shutdown on safety fault"""
        # DISABLE: Treatment laser only
        self.laser_controller.set_power(0.0)
        self.laser_controller.disable_output()

        # PRESERVE: All other systems
        # - Camera: Continue streaming (visual feedback)
        # - Actuator: Keep operational (controlled retraction)
        # - GPIO: Continue monitoring (diagnostics)
        # - Aiming beam: Keep on (Class 2, aids realignment)
        # - Event logging: Continue logging

        # Transition to UNSAFE state
        self.state = SafetyState.UNSAFE

        # Log fault with full context
        self.event_logger.log_safety_fault(
            reason=fault_reason,
            interlock_states=self.gpio_controller.get_all_interlocks(),
            timestamp=time.time()
        )

        # Emit signal to UI
        self.safety_fault_occurred.emit(fault_reason)
```

Systems Disabled on Safety Fault: 1. **Treatment Laser (Arroyo 6300):** - Immediate power → 0W - Output disabled (hardware disable signal) - Cannot be re-enabled until fault cleared + operator manually re-arms

Systems Preserved on Safety Fault: 1. **Allied Vision Camera:** - Continues streaming at 30 FPS - Operator maintains visual contact with treatment site - Aids in fault diagnosis (e.g., footpedal slipped off table)

2. **Xeryon Linear Actuator:**
    - Remains operational
    - Allows controlled retraction of laser ring if needed
    - Prevents mechanical "stuck" state
3. **Arduino GPIO Controller:**
    - Continues monitoring all interlocks
    - Provides diagnostic data (which interlock failed)
    - Watchdog heartbeat continues (safety layer remains active)
4. **SEMINEX Integrated Aiming Beam:**
    - Remains on (<1mW, Class 2 laser, inherently safe)
    - Aids in realignment after fault recovery
    - Controlled via MCP4725 DAC (independent of treatment laser)
5. **Event Logger:**

- Continues logging all events
- Fault details, recovery actions, operator input logged
- Immutable audit trail preserved

Safety Fault Recovery Workflow: 1. Safety fault detected (e.g., footpedal released) 2. System transitions: TREATING → UNSAFE 3. Treatment laser disabled immediately (<10ms) 4. Camera feed continues (operator sees treatment site) 5. UI displays fault reason and affected interlock 6. Operator diagnoses fault (e.g., “Footpedal signal lost - check connection”) 7. Operator fixes fault (e.g., reconnect footpedal) 8. System verifies all interlocks pass 9. Operator manually clicks “CLEAR FAULT” button 10. System transitions: UNSAFE → SAFE 11. Operator can re-arm and resume treatment

Clinical Example - Transient Footpedal Slip: - **Without Selective Shutdown:** Footpedal slips → Total shutdown → 5 minutes to restart system, realign camera, reposition patient - **With Selective Shutdown:** Footpedal slips → Laser off, camera on → 30 seconds to reconnect pedal, verify alignment, re-arm

Testing Requirements: 1. Verify treatment laser disables within 10ms of fault detection 2. Verify camera continues streaming during fault state 3. Verify actuator remains operational during fault state 4. Verify GPIO monitoring continues during fault state 5. Verify aiming beam remains on during fault state 6. Verify event logging continues during fault state 7. Verify treatment laser CANNOT be re-enabled until: - All interlocks pass - Operator manually clears fault - Operator manually re-arms system

Regulatory Compliance: - IEC 60601-1 (Medical Electrical Equipment Safety): Selective shutdown meets requirement for “predictable hazard reduction” - IEC 60601-2-22 (Surgical, Cosmetic, Therapeutic Lasers): Treatment laser shutdown sufficient (aiming beam <1mW exempt) - FDA 21 CFR 1040.10 (Laser Products): Class 4 laser (treatment) disabled, Class 2 laser (aiming) allowed

Review History

Date	Reviewer	Notes
2025-10-28	Safety Engineer	Selective shutdown policy proposed
2025-10-29	Clinical Advisors	Reviewed clinical workflow benefits
2025-10-30	System Architect	Approved selective shutdown implementation
2025-11-04	Documentation Review	Formalized as ADR-006

Template Version: 1.0 **Last Updated:** 2025-11-04