TOSCA Safety Shutdown Policy

Architecture Diagrams

Document Version: 1.1 **Last Updated:** 2025-10-26 **Status:** Active Policy **Priority:** CRITICAL

Selective Shutdown Principle

Core Policy

When safety interlocks fail or unsafe conditions are detected, **only the treatment laser** is immediately disabled. All other systems remain operational to support safe assessment and recovery.

This policy supersedes any previous documentation indicating full system shutdown.

Shutdown Hierarchy

```
1. **Safety Interlock Failure Detected**
2. **IMMEDIATE** - Treatment Laser Shutdown
3. **• Laser output  OFF**
4. **• Laser power  0 mW**
5. **• Laser driver  DISABLED**
6. **• Response time** - <100ms
7. **MAINTAINED** - Support Systems
8. **[DONE] Camera (visual monitoring)**
```

9. **[DONE] Actuator (position control)**
10. **[DONE] Aiming Laser (low-power alignment)**
11. **[DONE] Laser Spot Smoothing Module (if not fault src)**
12. **[DONE] GPIO monitoring**
13. **[DONE] Event logging**
14. **[DONE] UI responsiveness**

System-by-System Shutdown Rules

Treatment Laser (SHUTDOWN)

Action: Immediate disable **Methods:**

```
laser_controller.set_output(False)  # Disable output
laser_controller.set_current(0.0)    # Zero power
```

Rationale: - Primary hazard source - Therapeutic power levels (up to 2000 mW) - Immediate shutdown prevents tissue damage

Recovery: Requires manual safety clearance and system reset

Camera System (MAINTAIN)

Action: Continue streaming **Rationale:** - **Essential for post-fault assessment:** Operator needs to see treatment area - **Visual verification:** Confirms laser is actually off - **Diagnostic value:** May show what caused the fault - **No safety hazard:** Passive imaging only

Example Use Cases: - Verify laser spot has disappeared - Check for unexpected tissue reactions - Document fault conditions - Guide repositioning if needed

---

Actuator System (MAINTAIN)

Action: Remain controllable **Rationale:** - **Safe repositioning:** May need to move away from treatment site - **Controlled shutdown:** Allows precise parking position - **Diagnostic access:** Can move to verify mechanical issues - **Limited hazard:** Motion at controlled speeds, low force

Restrictions After Fault: - Manual control only (no automatic protocols) - Reduced speed limits (safety mode) - Position bounds enforced - Continuous operator supervision required

Example Use Cases: - Move away from tissue after emergency stop - Return to home position - Clear workspace for fault investigation - Position for camera inspection

---

Aiming Laser (MAINTAIN)

Action: Keep available **Rationale:** - **Low power:** Typically <5 mW (Class 2, inherently safe) - **Alignment verification:** Can check optical path alignment - **Visual reference:** Shows where treatment would occur - **Diagnostic tool:** Helps identify optical misalignment faults

Safety Notes: - Class 2 laser (eye-safe with blink reflex) - Different controller from treatment laser - Independent power supply - Can be manually disabled if desired

Example Use Cases: - Verify optical alignment after fault - Check for obstruction in beam path - Confirm targeting accuracy - Diagnose pointing stability issues

---

Laser Spot Smoothing Module (CONDITIONAL)

Action: Depend on fault source

If Laser Spot Smoothing Module IS the fault source: - Motor → OFF - Safety interlock recognizes motor failure - Treatment laser disabled (per policy)

If Laser Spot Smoothing Module is NOT the fault source: - Motor continues running if already active - Can be manually controlled - Helps maintain component temperature stability - May aid in diagnosis

Rationale: - Device failure triggers selective shutdown (laser only) - Device can continue if not implicated in fault - Thermal stability may aid recovery - No direct safety hazard from motor operation

---

GPIO Monitoring (MAINTAIN)

Action: Continue all monitoring functions **Rationale:** - Heartbeat monitoring must continue (watchdog still active) - photodiode laser pickoff measurement feedback confirms laser is off - Vibration sensor shows motor state - Essential for diagnosing root cause

Monitored Signals: - photodiode laser pickoff measurement voltage → Should drop to <0.1V after laser shutdown - Smoothing device vibration → Continues if motor running - Watchdog heartbeat → Must continue for system health - Safety interlock states → Track for diagnostics

---

Implementation in Code

Safety Manager Emergency Stop

```python
class SafetyManager:
    def emergency_stop(self, reason: str):
        """
        Selective emergency shutdown - TREATMENT LASER ONLY.

        Maintains operational: Camera, Actuator, Aiming Laser, GPIO monitoring
        """
        logger.critical(f"EMERGENCY STOP: {reason}")

        # 1. IMMEDIATE: Disable treatment laser only
        if self.laser_controller:
            self.laser_controller.set_output(False)
            self.laser_controller.set_current(0.0)
            logger.info("Treatment laser disabled (selective shutdown)")

        # 2. MAINTAIN: Other systems remain operational
        # - Camera continues streaming
        # - Actuator remains controllable
        # - Aiming laser stays available
        # - GPIO monitoring continues
        # - Event logging active

        # 3. Update system state
        self.system_state = SystemState.FAULT
        self.laser_enabled = False

        # 4. Log event
        self.event_logger.log_event(
            event_type=EventType.EMERGENCY_STOP,
            description=f"Emergency stop: {reason} (selective shutdown - laser only)",
            severity=EventSeverity.EMERGENCY
        )

        # 5. Notify UI
        self.safety_event.emit("emergency_stop", reason)
```

Watchdog Failure Handler

```python
class SafetyWatchdog:
```

```
    def _handle_critical_failure(self):
        """
        Watchdog failure → Selective shutdown (treatment laser only).

        IMPORTANT: Does not shutdown entire system.
        """
        logger.critical("Watchdog critical failure - disabling TREATMENT LASER only")

        # 1. Disable treatment laser (selective shutdown)
        if self.laser_controller:
            self.laser_controller.set_output(False)
            self.laser_controller.set_current(0.0)

        # 2. Other systems maintained:
        # - Camera: Continues monitoring
        # - Actuator: Remains controllable
        # - Aiming laser: Available
        # - GPIO: Heartbeat stops but monitoring continues

        # 3. Stop watchdog heartbeat (connection lost)
        self.stop()

        # 4. Emit critical signal
        self.watchdog_timeout_detected.emit()

        # 5. Log event
        self.event_logger.log_event(
            event_type=EventType.WATCHDOG_FAILURE,
            description="Watchdog failure - treatment laser disabled (selective shutdown)",
            severity=EventSeverity.EMERGENCY
        )
```

Protocol Engine Safety Check

```
class ProtocolEngine:
    def _on_safety_failure_during_protocol(self):
        """
        Real-time safety failure during protocol execution.

        Selective shutdown: Stops laser, maintains monitoring.
        """
        logger.critical("Safety interlock failure during protocol execution")

        # 1. Stop protocol execution
        self.stop()  # Stops protocol, sets state to STOPPED

        # 2. Disable treatment laser (selective shutdown)
        if self.laser:
            self.laser.set_output(False)
            self.laser.set_current(0.0)

        # 3. Maintain support systems:
        # - Camera continues (operator can see what happened)
        # - Actuator controllable (can reposition if needed)
        # - Event log captures full context

        # 4. Log event
        self.event_logger.log_event(
            event_type=EventType.PROTOCOL_SAFETY_STOP,
            description="Protocol stopped due to safety interlock failure (selective shutdown)",
            severity=EventSeverity.CRITICAL
        )
```

Rationale for Selective Shutdown

Patient Safety Benefits

1. **Visual Confirmation:** Operator can immediately see treatment area after fault
2. **Repositioning:** Can move away from target safely if needed

3. **Assessment:** Camera shows tissue state and reaction
4. **Documentation:** Visual record of fault conditions

Diagnostic Benefits

1. **Root Cause Analysis:** Systems remain available for testing
2. **State Preservation:** Actuator position, camera view maintained
3. **Signal Monitoring:** GPIO continues reading sensor states
4. **Reproducibility:** Can attempt to reproduce fault with laser disabled

Operational Benefits

1. **Reduced Downtime:** Don't need to restart entire system
2. **Faster Recovery:** Selective re-enable after fault clearance
3. **Better UX:** Operator retains control and visibility
4. **Training:** Safer environment for operator training

Safety Validation

Key Principle: Treatment laser is the **only** hazard requiring immediate shutdown.

System Risk Analysis: - **Camera:** No harm possible (passive imaging) - **Actuator:** Low force, controlled motion, operator supervised - **Aiming Laser:** Class 2, eye-safe, inherently low risk - **Laser Spot Smoothing Module:** Mechanical device, no direct patient contact - **Treatment Laser:** High power (2000 mW), tissue-damaging, **must** be disabled

Conclusion: Selective shutdown optimizes both safety and functionality.

Recovery Procedures

After Selective Shutdown

Immediate Actions: 1. [DONE] Verify treatment laser OFF (check photodiode laser pickoff measurement < 0.1V) 2. [DONE] Assess patient/tissue status visually (camera) 3. [DONE] Document fault conditions in event log 4. [DONE] Determine root cause

Before Re-enabling Treatment Laser: 1. Clear the fault condition 2. Verify all safety interlocks pass 3. Confirm support systems operational 4. Reset safety manager state 5. Supervisor authorization required 6. Document recovery in event log

System State Transitions

```
FAULT (Laser Disabled)

           Camera: Operational (monitoring)
           Actuator: Operational (controllable)
           Aiming Laser: Operational (available)
           GPIO: Operational (monitoring)
           Event Log: Operational (recording)

        ▼
    [Fault Investigation & Clearance]

        ▼
    [Supervisor Authorization]

        ▼
    [Safety Checks Pass]

        ▼
READY (All Systems Operational, Laser Can Be Enabled)
```

Testing Requirements

Selective Shutdown Tests

Test 1: Emergency Stop Button - Press E-stop during treatment - **Verify:** Laser OFF, camera ON, actuator controllable - **Verify:** photodiode laser pickoff measurement reads <0.1V - **Verify:** UI shows fault state but remains responsive

Test 2: Watchdog Timeout - Simulate GUI freeze - **Verify:** Treatment laser OFF after 1 second - **Verify:** Camera still streaming - **Verify:** Event log records fault

Test 3: Safety Interlock Failure (Laser Spot Smoothing Module) - Stop laser spot smoothing module during treatment - **Verify:** Laser OFF immediately - **Verify:** Motor stops, but camera/actuator available - **Verify:** Operator can reposition

Test 4: Selective Recovery - After fault, clear root cause - **Verify:** Can re-enable laser with supervisor auth - **Verify:** All interlocks must pass before re-enable - **Verify:** Event log documents full recovery sequence

---

Related Documents

- `docs/CODE_REVIEW_2025-10-26.md` - Code review findings
- `docs/architecture/03_safety_system.md` - Overall safety architecture
- `docs/architecture/06_safety_watchdog.md` - Watchdog implementation
- `presubmit/reviews/plans/IMPLEMENTATION_PLAN_WATCHDOG.md` - Original plan

Revision History

Version	Date	Change	Author
1.0	2025-10-15	Initial safety architecture	TOSCA Team
1.1	2025-10-26	Selective shutdown policy defined	Code Review

Policy Owner: Safety Engineer **Approval Required:** Project Lead, Safety Committee **Review Frequency:** Before each development phase **Next Review:** After Phase 1 implementation