Technical Guide

Implementation of SIL3 Safety in Stage Automation Control Systems

Author: Anton Woodward OBE CEng MInstMC FRSA
Document Series: Stage Automation Safety Technical Guides
Revision: 1.0
Date: March 2026

Scope

This technical guide describes the implementation of **Safety Integrity Level 3 (SIL3)** functional safety within stage automation control systems used in theatres, opera houses, and performance venues.

The document outlines typical system architecture, safety principles, and implementation methods used to achieve SIL3 safety performance for **stage flying systems**, particularly automated **fly bars** carrying scenery, lighting equipment, or stage elements.

This guide is intended for:

- stage automation system designers
- theatre consultants
- system integrators
- theatre technical managers
- safety engineers

Normative References

The following standards are commonly referenced in the design of safety-related stage automation systems:

- IEC 61508 – Functional Safety of Electrical / Electronic / Programmable Electronic Safety Systems
- IEC 62061 – Safety of Machinery: Functional Safety of Safety-Related Control Systems
- EN ISO 13849 – Safety of Machinery – Safety Related Parts of Control Systems
- EN 17206 – Entertainment Technology – Machinery for Stages and Other Production Areas

---

Definitions

Safety Integrity Level (SIL)

Safety Integrity Level is a discrete level used to specify the safety integrity requirements of safety functions.

SIL levels range from **SIL1 to SIL4**, where SIL4 represents the highest level of risk reduction.

SIL3

SIL3 represents a high level of functional safety performance providing a **risk reduction factor typically between 1,000 and 10,000**.

Safety Instrumented Function (SIF)

A safety function designed to detect hazardous conditions and place the machinery into a safe state.

Safe State

The condition in which hazardous motion is prevented or safely stopped.

For stage flying systems the safe state typically includes:

- removal of drive torque
- controlled stop of the winch
- engagement of holding brakes

Application of SIL3 in Stage Automation

Stage automation systems involve the controlled movement of heavy scenic elements above performers and technical staff.

Where automated flying systems operate above occupied stage areas, hazards may include:

- falling scenery
- uncontrolled movement of fly bars
- excessive speed of suspended loads
- collision between moving bars

Due to the potential severity of these hazards, **SIL3 safety functions are commonly applied to automated flying systems**.

In contrast, other stage machinery such as **stage lifts and turntables** often achieve the required safety performance through alternative safety architectures and therefore are not typically implemented as full SIL3 systems.

Functional Safety Concept

Functional safety in stage automation systems is implemented through a **Safety Instrumented System (SIS)**.

Each safety function consists of three primary elements:

1. **Sensors** – detect hazardous conditions

2. **Logic Solver** – evaluates safety logic
3. **Final Elements** – place machinery into a safe state

The SIL rating applies to the **complete safety function**, not individual components.

Typical SIL3 System Architecture

SIL3 systems typically use **fault tolerant architectures** designed to ensure that a single fault does not result in loss of the safety function.

Common design measures include:

- dual-channel safety inputs
- redundant safety controllers
- safety-rated communication networks
- monitored safety outputs

Redundant Safety Controllers

Safety logic is typically executed in **dual-processor safety PLC systems** with internal diagnostics and cross-monitoring.

Safety Communication Networks

Safety data is transmitted using certified protocols such as:

- PROFIsafe
- Safety over EtherCAT
- CIP Safety

These protocols include error detection mechanisms including:

- CRC checks
- time monitoring
- sequence monitoring

Redundant Input Devices

Safety inputs may include:

- dual channel emergency stop circuits
- safety-rated position encoders
- redundant limit switches
- load monitoring sensors

Input signals are continuously compared to detect discrepancies.

Safety Output Devices

Final safety elements may include:

- safe torque off (STO) on drive systems
- safety contactors
- monitored braking systems
- mechanical holding brakes

Outputs are monitored using feedback circuits to ensure correct operation.

Diagnostic Coverage

To achieve SIL3 performance, the safety system must detect a high proportion of potential failures.

Typical diagnostic techniques include:

- cross monitoring of redundant channels
- watchdog monitoring of safety processors
- drive feedback verification
- encoder signal validation
- communication integrity monitoring

Where faults are detected, the system transitions to the defined safe state.

Emergency Stop Systems

Emergency stop systems provide an independent safety function.

Emergency stop devices shall:

- be wired using dual channel safety circuits
- directly interrupt motion commands
- be monitored by the safety control system

Activation of an emergency stop shall immediately place the machinery into the safe state.

Safety Lifecycle

SIL3 safety must be maintained throughout the entire lifecycle of the stage automation system.

Lifecycle phases include:

- hazard analysis
- safety requirements specification

- system design
- verification and validation
- commissioning
- operation and maintenance

Regular **proof testing and inspection** are required to confirm continued safety performance.

Documentation Requirements

SIL3 systems require comprehensive documentation including:

- hazard and risk assessment reports
- safety requirement specifications
- hardware architecture documentation
- validation and commissioning records
- maintenance procedures

Independent functional safety assessment may be required for major installations.

Maintenance and Proof Testing

To maintain SIL3 performance, safety systems must be periodically tested.

Typical procedures include:

- testing emergency stop circuits
- verifying limit switches
- checking encoder redundancy
- confirming brake operation
- validating safety PLC diagnostics

Proof test intervals should be defined during system design.

Summary

SIL3 safety systems provide a high level of protection for stage automation systems where hazardous motion could present significant risk to performers or technical staff.

By implementing redundant architectures, continuous diagnostics, and safety-certified components, automated flying systems can achieve the required level of functional safety.

Proper design, verification, and ongoing maintenance are essential to ensure that safety performance is maintained throughout the operational life of the installation.

Author: Anton Woodward
Document Series: Stage Automation Safety Technical Guides