Reducing Actuator Fault Recovery Time in Automated Production Lines Using PLC-Integrated HMI Reset Logic: A Case Study

Srujan Buddar
Department of Electrical & Electronics Engineering
RV College of Engineering
Bangalore, India
srujanbuddar.ee23@rvce.edu.in

C Sunanda
Assistant Professor
Department of Electrical & Electronics Engineering
RV College of Engineering
Bangalore, India
sunandac@rvce.edu.in

Hemalatha J N
Associate Professor & HOD
Department of Electrical & Electronics Engineering
RV College of Engineering
Bangalore, India
hemalathajn@rvce.edu.in

Abstract*— *Electric actuators with integrated drive controllers are widely deployed in automated production lines for linear motion tasks including transfer, clamping, and positioning operations. Under abnormal operating conditions — such as emergency stop activation, mid-cycle motion interruption, or sustained mechanical overload — the actuator drive enters a latched fault state triggered by overcurrent protection. Once latched, the drive's internal firmware inhibits all motion commands and cannot be restored through software reset signals alone, requiring a full control power cycle to reinitialize the drive hardware. In conventional installations, this power cycle is performed manually by maintenance personnel at the control cabinet, resulting in significant unplanned downtime, dependency on skilled technician availability, and exposure to cabinet access risks on an active production floor.

This paper proposes a low-cost, retrofittable fault recovery architecture that eliminates manual cabinet intervention by integrating a relay-based control power cycling circuit into the actuator's control power supply line, coordinated with a revised PLC program and an HMI-triggered reset sequence. The PLC supervises the reset procedure through a defined sequential logic routine, enforcing hardware and software safety interlocks to prevent reset execution under unsafe machine states. The Human Machine Interface provides the operator with a guided, single-touch fault recovery interface accessible directly from the production floor.

The proposed architecture was implemented and validated in a fully operational automated manufacturing facility. Post-deployment results demonstrated a significant reduction in mean fault recovery time, complete elimination of manual control cabinet access during fault events, and improved operator autonomy in fault management. The findings confirm that targeted relay-level hardware integration combined with structured PLC reset logic represents an effective and scalable strategy for improving maintainability and reducing unplanned downtime in electric actuator-driven automation systems.

Keywords*— *Electric actuator, drive fault recovery, latched fault state, control power cycling, relay-based reset circuit, programmable logic controller, HMI-triggered reset, safety interlock logic, unplanned downtime reduction, industrial automation, maintainability, automated production line.

I. INTRODUCTION

Automated production lines in modern manufacturing facilities rely extensively on electrically driven actuator systems for executing repetitive linear motion tasks such as part transfer, clamping, lifting, and precision positioning. These electric actuator systems, comprising a servo or stepper motor coupled with an integrated drive controller, offer significant advantages over pneumatic and hydraulic counterparts in terms of positional accuracy, programmability, energy efficiency, and repeatability [15]. As a result, their adoption across assembly, packaging, and material handling applications has grown substantially in recent decades [7].

The operational reliability of such systems is, however, critically dependent on the ability of the drive controller to recover swiftly from fault conditions that arise during production. Electric actuator drives are equipped with built-in protection mechanisms—including overcurrent detection, overload monitoring, and position deviation alarms—that are designed to halt motion and latch a fault state upon detection of abnormal operating conditions [1], [2]. While these protective functions are essential for equipment safety, they introduce a significant operational challenge: once a fault state is latched, the drive's internal firmware disables all command inputs and inhibits motion execution. The drive cannot be restored through software reset commands transmitted via the PLC's communication interface alone. A full cycle of the drive's control power supply is required to reinitialize the firmware and clear the latched condition [4].

In conventional industrial installations, this control power cycle is performed manually. Maintenance personnel must physically access the electrical control cabinet, identify and isolate the faulted drive's power supply, cycle the power, and verify drive readiness before returning the machine to production [6]. This procedure introduces multiple layers of inefficiency. First, it is time-intensive, as it requires the availability of a qualified technician on the production floor. Second, it poses potential safety concerns associated with repeated access to live electrical enclosures during active production periods. Third, it creates a skill dependency that limits the ability of machine operators to independently manage routine fault recovery, thereby increasing Mean

Time to Repair (MTTR) and reducing Overall Equipment Effectiveness (OEE) [8].

The conditions most frequently responsible for triggering latched fault states in electric actuator drives include emergency stop activation during an active motion cycle, upstream process faults that interrupt the actuator mid-stroke leaving it in an intermediate position, and sustained mechanical overloads that cause the motor to draw current beyond the drive's protection threshold [5], [8]. Each of these conditions is commonplace in high-throughput automated environments, making rapid and reliable fault recovery a critical operational requirement rather than an exceptional maintenance scenario.

Programmable Logic Controllers (PLCs) serve as the primary control platform in the majority of industrial automation systems, coordinating motion sequences, managing I/O, and interfacing with Human Machine Interfaces (HMIs) for operator interaction [3], [9]. The PLC's architecture—with its deterministic scan cycle, structured programming environment, and direct access to digital output channels—makes it a suitable platform for implementing supervised fault recovery logic [7], [12]. Similarly, HMI systems have evolved to support complex operator guidance functions beyond simple status display, enabling the integration of structured recovery procedures directly accessible from the production floor [6], [14].

Despite the availability of these control infrastructure capabilities, the specific problem of remotely initiating a supervised control power cycle for a faulted actuator drive—without manual cabinet access and with appropriate safety enforcement—has received limited treatment in the published literature. Existing approaches to fault diagnosis and fault-tolerant control primarily focus on fault detection, system monitoring, and recovery strategies at the control-system level [11], [13], while the hardware-level requirement of control power cycling for actuator drive reinitialization remains dependent on manual intervention in most deployed systems [6], [10].

This paper addresses this gap by proposing and validating a retrofittable fault recovery architecture that integrates a relay-based control power cycling circuit into the actuator's control power supply line, governed by a structured PLC reset routine and initiated through a dedicated HMI operator interface. Safety interlocks are enforced at both the hardware and software levels to ensure that the reset sequence cannot be executed under unsafe machine states. The proposed method was implemented in a fully operational automated manufacturing facility and evaluated against pre-deployment baseline data.

II. PROBLEM STATEMENT

A. Electric Actuator Drive Protection Behavior

Electric actuators employed in automated production environments integrate a servo or stepper motor with a dedicated drive controller that manages motion execution, monitors operating parameters, and enforces protection limits in real time [1], [2]. Among the most critical protection functions implemented in these drive controllers is overcurrent detection. When the motor current exceeds the drive's configured protection threshold — whether due to mechanical stall, load spike, or abrupt motion interruption — the drive immediately disables its output stage and transitions into a latched fault state [4], [5].

This latching behaviour is a deliberate firmware design characteristic. The drive controller does not automatically attempt recovery, nor does it respond to externally issued software reset commands transmitted through standard communication interfaces such as digital I/O signals or fieldbus protocols. The fault latch is held in the drive's non-volatile state register and can only be cleared by reinitializing the drive firmware through a full cycle of its control power supply [2], [4]. This fundamental limitation forms the root operational problem addressed in this paper.

B. Fault Triggering Conditions in Automated Production Lines

In the context of the automated production facility under study, three primary operating conditions were identified as consistent triggers for latched actuator drive faults:

1) Emergency Stop Activation During Active Motion: Automated production lines are equipped with emergency stop (E-stop) circuits that immediately de-energize machine outputs upon activation [3], [10]. When an E-stop event occurs while an electric actuator is executing a motion command, the motion cycle is abruptly interrupted. The sudden deceleration imposed on the drive — without a controlled ramp-down sequence — can cause a transient overcurrent condition sufficient to trigger the drive's protection latch [5], [11].

2) Mid-Cycle Motion Interruption Due to Upstream Process Faults: In tightly coupled automated lines, a fault condition in an upstream or downstream station can suspend the overall machine cycle while individual axes remain in intermediate positions. If the suspended actuator's load torque causes the motor to sustain current draw above the drive's threshold during the hold period, the drive will latch a fault [5], [13]. The actuator is then physically arrested in an intermediate stroke position, mechanically obstructing the production flow in addition to the electrical fault condition.

3) Mechanical Overload During Normal Operation: Occasional mechanical interferences — such as component misfeeds, fixture misalignment, or foreign object intrusion into the actuator's travel path — can impose sudden resistive loads that exceed the motor's rated force output. The resulting overcurrent condition triggers the drive's overload protection and induces a latched fault state [1], [5].

C. Limitations of Conventional Fault Recovery

The standard recovery procedure for a latched actuator drive fault in conventional installations requires a maintenance technician to: (1) identify the faulted drive within the control cabinet, (2) manually isolate and cycle the drive's control power supply, (3) verify that the drive has successfully reinitialized and cleared the fault, and (4) confirm machine readiness before resuming the production sequence [6], [7]. This procedure, while straightforward in principle, imposes several significant operational limitations in a high-throughput manufacturing environment.

First, the requirement for physical cabinet access introduces a time delay that is directly proportional to technician availability and proximity to the faulted station. In the facility under study, mean recovery times under the conventional procedure ranged from 15 to 40 minutes per incident, the majority of which was attributable to technician response time rather than the cabinet access procedure itself.

Second, repeated access to live electrical enclosures on an active production floor constitutes a safety exposure that is inconsistent with best practices for industrial electrical safety and lockout/tagout (LOTO) principles [8].

Third, the dependency on skilled maintenance personnel for a task that is operationally routine — given the frequency of fault occurrences — creates a bottleneck that disproportionately impacts production throughput and OEE. Machine operators, who are immediately present at the production station, are unable to independently resolve the fault condition and must wait for technician intervention [11], [13].

D. Research Gap and Motivation

While PLC-based fault detection and alarm management systems are well established in industrial automation literature [7], [14], the specific challenge of remotely executing a supervised control power cycle for a faulted actuator drive — without manual cabinet access and with enforced safety interlocks — has not been systematically addressed. Manufacturer documentation for both PLC platforms and actuator drive controllers acknowledges the requirement for control power cycling as a fault recovery mechanism [2], [3], [4], but does not provide an integrated, remotely operable solution within the PLC-HMI control architecture.

This gap motivates the development of the proposed architecture, which aims to enable rapid, operator-initiated, PLC-supervised fault recovery directly from the HMI, without requiring technician presence at the control cabinet, and without compromising machine safety or drive integrity [6], [9], [11].

III. PROPOSED METHODOLOGY

The proposed fault recovery architecture integrates three components: a relay-based control power cycling circuit, a PLC sequential reset routine, and an HMI operator recovery interface, enabling a supervised operator-initiated actuator drive reset directly from the production floor without physical cabinet access. The overall system architecture is illustrated in Figure 1.

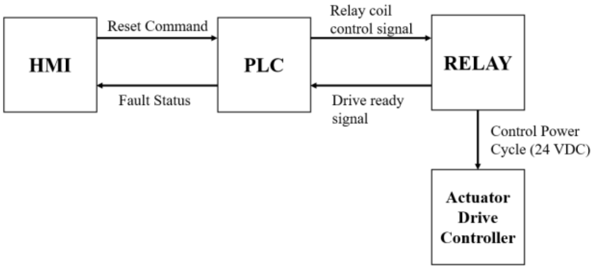

Figure 1 Block diagram of proposed system

A. Relay-Based Control Power Cycling Circuit

Since latched fault states in electric actuator drives can only be cleared through a full control power cycle. A relay module was wired in series with the 24 VDC control power supply line feeding the actuator drive controller, as shown in Figure 2.The relay coil is driven by a dedicated digital output channel on the PLC. Under normal operation the relay remains energized, maintaining continuous control power to the drive with no interference to standard machine operation.

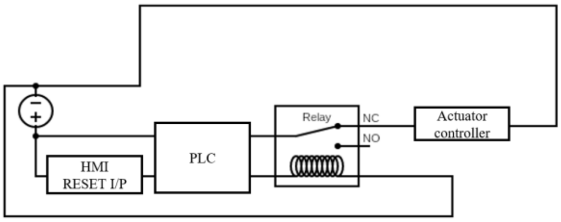

Figure 2 Relay-based controlled power cycling circuit

Upon PLC command, the relay de-energizes, interrupting control power to the drive. The drive's internal firmware enters its shutdown sequence, clearing all active registers including the latched fault state. The relay is held open for a calibrated dwell period sufficient for complete firmware shutdown and internal capacitor discharge, after which it re-energizes, restoring control power and triggering the drive's boot sequence. The relay module is DIN-rail mounted within the existing control cabinet, requiring no structural modification to the installation.

B. PLC Sequential Reset Routine

The PLC program was modified to incorporate a dedicated reset routine implemented using standard IEC 61131-3 programming constructs, ensuring compatibility across PLC platforms. The routine executes the following sequential steps:

1. **Reset request detection** — rising edge on HMI-mapped memory bit triggers routine entry and suspends normal axis control outputs
2. **Safety interlock validation** — all defined interlock conditions evaluated; routine proceeds only upon full confirmation
3. **Relay de-energization** — PLC sets relay output OFF; dwell timer initiated
4. **Dwell period hold** — relay held open for complete drive firmware shutdown
5. **Relay re-energization** — PLC sets relay output ON; drive boot sequence initiated
6. **Drive readiness confirmation** — PLC monitors drive ready feedback signal within defined timeout window
7. **Escalation on timeout** — recovery failure alarm generated on HMI if ready signal not received within timeout

C. Safety Interlock Design

To prevent reset execution under unsafe machine states, the PLC enforces the following conditions prior to initiating the power cycle. All conditions must be simultaneously satisfied:

- Actuator confirmed stationary with no pending motion command
- Emergency stop circuit confirmed healthy and non-activated
- All personnel safety zones confirmed clear
- Main machine sequence confirmed in stable hold state
- No active faults present on mechanically coupled adjacent axes

If any condition is unsatisfied, the reset command is suppressed and the specific blocking condition is communicated to the operator via the HMI.

D. HMI Interface

A dedicated fault recovery screen was developed within the existing HMI application. The screen presents the active fault code, real-time status of each safety interlock condition, step-by-step guided recovery instructions, and reset progress indication. The Initiate Reset control is enabled only when all interlock conditions are confirmed satisfied. Access to the recovery screen is restricted through the existing role-based authentication system to authorized personnel only.

IV. IMPLEMENTATION

The proposed fault recovery architecture was implemented within a fully operational automated production facility utilizing electric actuator-driven stations for linear transfer and positioning tasks. The implementation was carried out without interruption to the ongoing production schedule by confining installation activities to planned maintenance windows.

A. Hardware Installation

A relay module rated at 24 VDC coil voltage was selected and mounted on the existing DIN rail within the control cabinet of the target actuator station. The relay was wired in series with the 24 VDC control power supply line feeding the actuator drive controller, in accordance with the circuit configuration shown in Figure 2. The wiring modification was confined entirely within the existing control cabinet enclosure, requiring no changes to the machine's external wiring, safety circuit architecture, or actuator drive configuration. The total hardware installation time per station was under two hours.

B. PLC Program Implementation

The reset routine was developed and integrated into the existing PLC program without modifying the main machine control logic. The routine was written using standard IEC 61131-3 ladder diagram constructs within the installed PLC programming environment. The dwell period for relay de-energization was determined empirically through controlled testing, establishing the minimum hold time required for complete drive firmware shutdown and internal capacitor discharge before control power restoration. The safety interlock conditions defined in Section III-D were mapped to existing PLC input signals already available within the machine program, requiring no additional sensor installation. The PLC ladder logic implementation of the reset routine is shown in Figure 3.

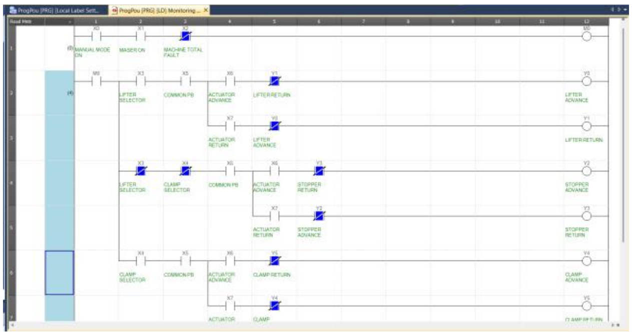

Figure 3 PLC ladder logic for actuator reset

C. HMI Configuration

A dedicated fault recovery screen was configured within the existing HMI application using the installed HMI development environment. The screen was linked to the PLC memory addresses associated with the reset routine, including the reset request bit, interlock status bits, routine step indicator, drive ready confirmation bit, and escalation alarm bit. Role-based access restriction was applied to the screen using the existing HMI authentication configuration, limiting reset initiation to authorized operator and maintenance personnel. The implemented HMI fault recovery interface is shown in Figure 4.

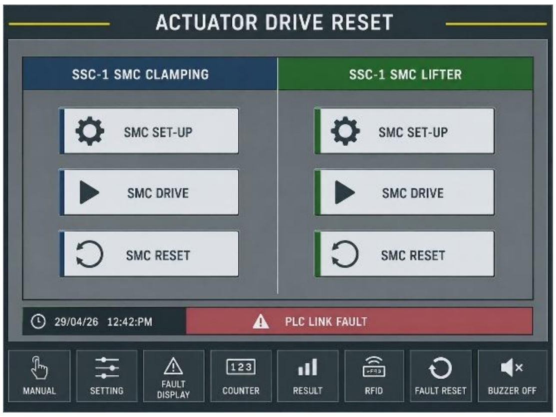

Figure 4 HMI fault recovery screen

V. RESULTS AND DISCUSSION

The proposed fault recovery architecture was deployed and evaluated within a fully operational automated production facility. Performance was assessed by comparing fault recovery parameters before and after implementation of the proposed method. The results demonstrate significant measurable improvements across recovery time, operational dependency, and maintainability.

A. Fault Recovery Time Comparison

Table 1 summarizes the fault recovery time before and after implementation of the proposed architecture.

Table 1 Project Implementation comparison

Parameter	Before Implementation	After Implementation
Mean Recovery Time	15 – 20 minutes	~3 minutes
Recovery Initiated By	Maintenance Technician	Machine Operator
Cabinet Access Required	Yes	No
Technician Dependency	High	None
Recovery Method	Manual Power Cycle	HMI-Initiated PLC Reset

B. Key Results

The following key outcomes were recorded following deployment of the proposed fault recovery architecture:

- **80 – 85% reduction** in mean fault recovery time, from 15–20 minutes to approximately 3 minutes per incident
- **Complete elimination** of manual control cabinet access during actuator fault recovery events
- **Zero unsafe reset attempts** recorded — all safety interlock validations functioned correctly throughout the observation period
- **Full operator autonomy** achieved in fault recovery — trained operators independently completed the reset procedure without maintenance technician involvement
- **No modification** to existing drive configuration, safety circuit architecture, or external machine wiring was required
- **Minimal hardware cost** per station — limited to a standard 24 VDC DIN-rail relay module and associated wiring materials
- **Non-intrusive PLC integration** — reset routine added as a self-contained block with no interference to the existing main machine control logic

C. Discussion

The results confirm that targeted relay-level hardware integration combined with structured PLC reset logic delivers measurable and significant improvement in actuator fault recovery performance. The primary driver of pre-implementation downtime was not the physical complexity of the recovery task but rather technician response time and cabinet access dependency — both of which are fully eliminated by the proposed architecture.

The enforced safety interlock design proved effective in practice, with no interlock bypass or unsafe reset condition recorded during the observation period. The HMI guided interface successfully enabled operator-level fault recovery without requiring technical knowledge of the drive's internal fault mechanism, confirming the maintainability improvement objective of the proposed method.

VI. CONCLUSION

This paper presented a low-cost, retrofittable fault recovery architecture for electric actuator drive systems in automated production lines. The proposed method addressed the fundamental limitation of latched fault states in electric actuator drive controllers — specifically the inability to clear such faults through software reset commands alone — by integrating a relay-based control power cycling circuit with a structured PLC sequential reset routine and an HMI-initiated operator interface.

The key contributions of this work are summarized as follows:

- A relay-based control power cycling circuit was designed and integrated into the actuator drive's control power supply line, enabling remote PLC-supervised power cycling without manual cabinet access

- A self-contained PLC reset routine was developed using standard IEC 61131-3 constructs, incorporating sequential fault recovery logic and multi-condition safety interlock validation
- An HMI-based operator recovery interface was implemented, enabling trained operators to independently manage actuator fault recovery without maintenance technician involvement
- Deployment results demonstrated an 80–85% reduction in mean fault recovery time, from 15–20 minutes under conventional manual procedures to approximately 3 minutes under the proposed architecture
- Complete elimination of manual control cabinet access during fault recovery was achieved, improving both operational efficiency and electrical safety compliance

The proposed architecture is intentionally generic and platform-independent, making it applicable to any industrial installation where electric actuator drive fault clearance requires control power cycling. The minimal hardware requirement and non-intrusive PLC integration approach ensure that the method is accessible as a retrofit upgrade to existing automated systems without significant capital investment.

Future work will explore extension of the proposed architecture to multi-axis coordinated fault recovery, integration with SCADA-level diagnostic systems for predictive fault identification, and development of automated fault classification logic within the PLC to enable condition-specific recovery strategies beyond the uniform power-cycle approach presented in this study.

ACKNOWLEDGMENT

The author expresses sincere gratitude to the R.V. College of Engineering, Bengaluru, for providing the academic environment and resources that supported this research work. Special thanks are due to the Principal, Dr. K. N. Subramanya, and the Head of Department, Dr. Hemalatha J. N**.**, for their encouragement and institutional support throughout the course of this work.

The author is deeply grateful to Dr. C. Sunanda, Assistant Professor, for her invaluable guidance, continuous mentorship, and technical insights that were instrumental in shaping this research. Her dedication and constructive feedback at every stage of this work are sincerely appreciated.

The author also wishes to acknowledge the teaching and non-teaching staff of R.V. College of Engineering for their support and assistance rendered during this work.

Finally, the author expresses heartfelt gratitude to their parents, friends, and well-wishers for their constant encouragement, patience, and moral support throughout this journey.

REFERENCES

[1] SMC Corporation, *Electric Actuator Operation Manual: Slider Type Electric Actuator Series (LEG/LEY Series)*. Tokyo, Japan: SMC Corporation.

[2] SMC Corporation, *Controller Operation Manual for Electric Actuators*. Tokyo, Japan: SMC Corporation.

[3] Siemens AG, *SIMATIC S7-1200 Programmable Controller System Manual*. Munich, Germany: Siemens AG, 2022.

[4] SMC Corporation, *LEC Series Electric Actuator Controller Operation Manual*. Tokyo, Japan: SMC Corporation.

[5] A. M. Gollapudi, V. Velagapudi, and S. Korla, “Modeling and simulation of a high-redundancy direct-driven linear electromechanical actuator for fault tolerance under fault conditions,” *Engineering Science and Technology, an International Journal*, vol. 23, no. 5, pp. 1171–1181, Oct. 2020.

[6] Rockwell Automation, *Logix 5000 Controllers Major, Minor, and I/O Faults*, Publication 1756-PM014. Milwaukee, WI, USA: Rockwell Automation.

[7] F. D. Petruzella, *Programmable Logic Controllers*, 5th ed. New York, NY, USA: McGraw-Hill Education, 2016.

[8] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, 3rd ed. Berlin, Germany: Springer, 2016.

[9] H. Berger, *Automating with SIMATIC S7-1200: Configuring, Programming and Testing with STEP 7 Professional*, 2nd ed. Erlangen, Germany: Publicis Publishing, 2015.

[10] Siemens AG, *SIMATIC Programming Guide S7-1200 and S7-1500*. Munich, Germany: Siemens AG, 2015.

[11] J. Lunze and T. Steffen, “Reconfigurable fault-tolerant control: A tutorial introduction,” *Annual Reviews in Control*, vol. 32, no. 2, pp. 199–210, 2008.

[12] S. N. Sivanandam, S. Sumathi, and S. N. Deepa, *Introduction to Programmable Logic Controllers*. New Delhi, India: Tata McGraw-Hill, 2007.

[13] P. M. Frank, “Fault diagnosis and fault-tolerant control,” in *Encyclopedia of Life Support Systems (EOLSS)*. Paris, France: UNESCO, 2005.

[14] J. R. Hackworth and F. D. Hackworth Jr., *Programmable Logic Controllers: Programming Methods and Applications*. Upper Saddle River, NJ, USA: Pearson Education, 2004.

[15] J. W. Webb and R. A. Reis, *Programmable Logic Controllers: Principles and Applications*, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.