AB Journals

Journal of Advanced Research and Multidisciplinary Studies
ISSN 2997-3155 • Volume 6, Issue 2, 2026 • pp. 105–120

RESEARCH ARTICLE Received: 1 Oct 2026, Accepted: 4 Nov 2026, Published: 11 Nov 2026

Enhancing Lockout/Tagout (LOTO) Safety During Machinery Maintenance: Development of a Fail-Safe Personnel Verification System to Prevent Unexpected Start-up

Abdelfattah Hafiz Mohammedahmed

Karary University, Khartoum, Sudan.

Email: abdelfattahhafiz@gmail.com

Abstract

Unexpected machinery start-up during maintenance remains a significant occupational safety concern, particularly when several workers are required to enter a hazardous machine zone. Lockout/Tagout (LOTO) provides the primary means of controlling hazardous energy; however, the final stage of the procedure still requires confirmation that all employees have been safely removed before energy is restored. This study proposes a fail-safe personnel verification system that adds an engineering control to the conventional LOTO process. A discrete-event simulation of an automated conveyor maintenance cell was developed using Python. The model represented 10,000 maintenance cycles, three authorized maintenance workers, two controlled access points, individual personnel identification, zone-occupancy monitoring, system-health verification, and a restart interlock. The simulation included normal maintenance, incomplete personnel exit, unauthorized entry, sensor failure, communication failure, controller failure, power interruption, false exit signals, and restart attempts during maintenance. A total of 30,000 personnel-state events were evaluated. The simulated system achieved 99.82% personnel-state verification accuracy and a mean detection latency of 184 ms. Of 1,000 unsafe restart attempts, all were inhibited. Eighteen valid restart events were unnecessarily inhibited, producing a false-inhibition rate of 1.80%. Eighty fault-injection events were also evaluated, and all resulted in a safe state. Under the same simulated assumptions, the conventional verification model produced 17 incorrect restart authorizations. The results indicate that automated personnel verification can provide an additional engineering barrier against unexpected start-up, particularly during multi-person maintenance. The proposed system is intended to supplement, rather than replace, established LOTO procedures.

Keyword: Fail-Safe Control; Hazardous Energy; Health and Safety; Lockout/Tagout; LOTO; Machinery Safety; Maintenance Safety; Occupational HSE; Personnel Verification; Safety Interlock; Unexpected Start-Up

How to Cite: Mohammedahmed, A. H. (2026). Enhancing Lockout/Tagout (LOTO) Safety During Machinery Maintenance: Development of a Fail-Safe Personnel Verification System to Prevent Unexpected Start-up. Journal of Advanced Research and Multidisciplinary Studies, 6(2), 105–120. https://doi.org/10.52589/JARMS-TBVZAF

© 2026 by the authors. Published by AB Journals. This is an open access article distributed under the terms of the Creative Commons Attribution (CC BY 4.0) license.

INTRODUCTION

Maintenance activities expose workers to electrical, mechanical, hydraulic, pneumatic, thermal, gravitational and stored energy hazards. The risk becomes particularly important when maintenance requires workers to enter machine danger zones, remove guards, perform adjustments or repair moving equipment.

Lockout/Tagout (LOTO) is a fundamental control for hazardous energy during servicing and maintenance. The U.S. Occupational Safety and Health Administration (OSHA) requires hazardous-energy control procedures to prevent unexpected energization, start-up or release of stored energy when such events could cause injury. The procedure includes shutdown, isolation, application of lockout or tagout devices, control of stored energy and verification of isolation before work begins (OSHA, 2026).

The final stage of LOTO is equally important. Before energy is restored, the work area must be inspected and employees must be safely positioned or removed. This requirement is explicitly addressed in OSHA 29 CFR 1910.147, which requires the work area to be checked before removal of lockout/tagout devices and restoration of energy (OSHA, 1989).

The problem becomes more difficult when several employees are simultaneously involved in maintenance. A worker may leave the machine enclosure while another worker remains inside. Similarly, a maintenance team may use multiple access points, creating the possibility that a manual visual check does not provide reliable confirmation of every person's location.

The issue of verification within LOTO has previously received research attention. Poisson (2016) developed a safety control system intended to improve the verification step of machinery lockout procedures. The study focused on automated verification of zero electrical energy and demonstrated how a safety-related control system could complement conventional lockout procedures.

More recent research has investigated the integration of LOTO with smart manufacturing. Delpla (2023) examined the integration of operational LOTO into joint production and maintenance policies, while Delpla (2024) investigated machine-learning methods for predicting LOTO procedure sheets and identifying energy-isolating devices.

These studies demonstrate that LOTO is increasingly being connected with digital and automated manufacturing systems. However, the specific problem addressed in the present study is different: real-time verification that all personnel have left the hazardous zone immediately before machinery restart.

ISO 14118:2017 addresses the prevention of unexpected machine start-up and specifies designed-in measures intended to permit safe human intervention in danger zones. The standard applies to unexpected start-up from electrical, hydraulic, pneumatic, stored and other energy sources (ISO, 2017).

The present study therefore proposes an additional engineering barrier within the LOTO process. The central principle is simple: the machine must not restart unless the system positively confirms that the hazardous zone is clear and all required safety conditions are satisfied.

Aim and Objectives

The aim of this study was to develop and evaluate a fail-safe personnel verification system capable of preventing machinery restart when personnel remain inside a hazardous maintenance zone.

The objectives were to:

1. Develop an individual personnel-accounting mechanism for multi-worker maintenance;
2. Integrate personnel status with machinery restart authorization;
3. Evaluate the system under normal and abnormal operating conditions;
4. Quantify personnel verification accuracy and detection latency;
5. Evaluate the response to sensor, communication, controller and power failures; and
6. Compare the proposed system with a conventional LOTO verification model under identical simulated conditions.

MATERIALS AND METHODS

Simulation Environment

A representative automated conveyor maintenance cell was selected as the application environment.

The simulated cell consisted of:

- one electrically driven conveyor;
- one defined hazardous maintenance zone;
- two controlled access points;
- three authorized maintenance workers;
- individual personnel identification devices;
- entry and exit detection;
- a safety controller;
- machine-state monitoring;
- an emergency-stop circuit;
- a manual reset station; and
- a restart interlock.

The simulation was implemented in Python 3.12 using a discrete-event approach.

A total of 10,000 maintenances cycles were simulated.

Each cycle represented the following sequence:

Machine shutdown → LOTO application → energy isolation → personnel entry → maintenance → personnel exit → personnel verification → LOTO release → restart authorization.

Proposed LOTO Safety Architecture

The proposed system does not replace physical energy isolation. Instead, it introduces an additional personnel-verification layer between the completion of maintenance and machine restart.

The system contains five principal functions:

1. personnel identification;
2. entry and exit detection;
3. hazardous-zone occupancy calculation;
4. safety-related restart interlocking; and
5. fault detection with automatic safe-state transition.

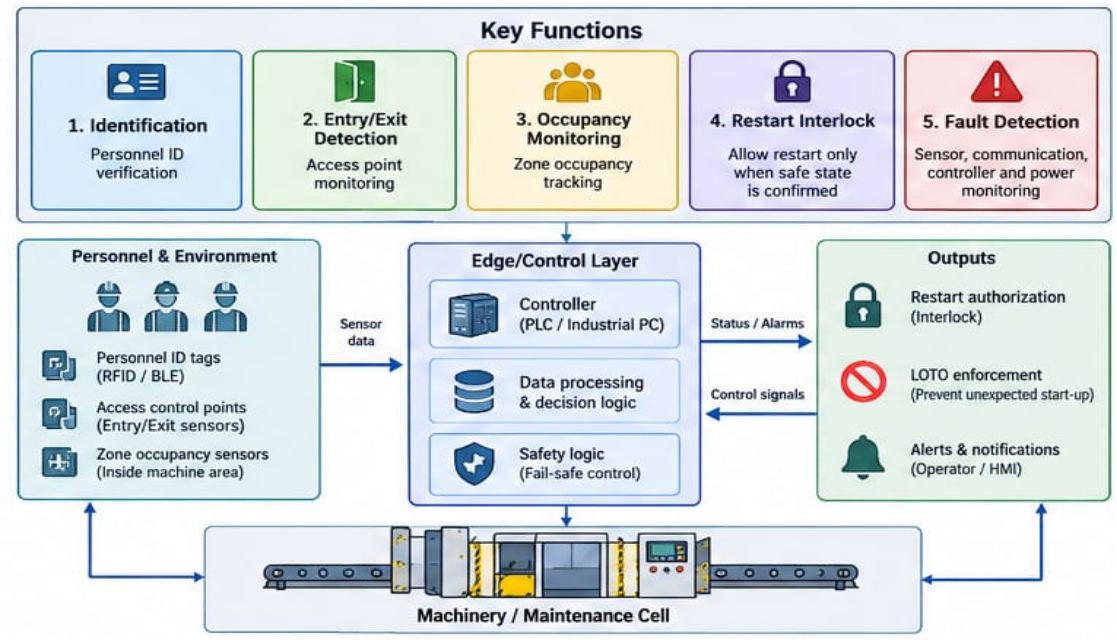


Figure 1: Proposed architecture of the fail-safe LOTO personnel verification system.

The figure illustrates the relationship between the LOTO system and the proposed engineering layer:

LOTO Isolation → Maintenance Zone → Personnel Identification → Personnel Verification → Safety Controller → Restart Interlock → Machine

A fault or uncertain personnel condition should cause the controller to maintain the machine in the restart-inhibited state.

This approach is consistent with the objective of ISO 14118, which addresses designed-in measures for preventing unexpected machine start-up and allowing safe intervention in danger zones (ISO, 2017).

Individual Personnel Tracking and Zone-Occupancy Representation

To ensure that every worker is individually accounted for during machinery maintenance, the proposed system uses an identity-based state-tracking approach rather than relying solely on the total number of entries and exits. Each authorized worker is assigned a unique identification (ID), and the system continuously updates the worker's occupancy state.

Let the set of authorized workers be defined as:

$$\mathcal{W} = \{ID_1, ID_2, \ldots, ID_n\}$$

The occupancy state of each worker i at time t is represented by:

$$s_i(t) \in \{\text{Inside, Outside, Unknown}\}$$

where Inside indicates that the worker is detected within the maintenance zone, Outside indicates that the worker has been positively verified as having exited the zone, and Unknown represents an uncertain or unavailable detection state.

The set of workers confirmed to be inside the maintenance zone is defined as:

$$\mathcal{P}(t) = \{ID_i \in \mathcal{W} \mid s_i(t) = \text{Inside}\}$$

Similarly, the set of workers whose occupancy status is uncertain is defined as:

$$\mathcal{U}(t) = \{ID_i \in \mathcal{W} \mid s_i(t) = \text{Unknown}\}$$

The number of workers confirmed inside the zone is therefore:

$$N_z(t) = |\mathcal{P}(t)|$$

Unlike a conventional scalar counting method, this representation maintains the occupancy status of each individual worker. Consequently, the system can identify which specific worker remains inside the maintenance zone or has an unresolved status.

The maintenance zone is considered clear only when all authorized workers have been positively verified as outside the zone. This condition is expressed as:

$$\mathcal{P}(t) = \emptyset \ \wedge \ \mathcal{U}(t) = \emptyset$$

Accordingly, the zone-clearance variable is defined as:

$$Z(t) = 1, \text{ if } \mathcal{P}(t) = \emptyset \text{ and } \mathcal{U}(t) = \emptyset; \text{ otherwise } Z(t) = 0$$

where $Z(t) = 1$ indicates that the maintenance zone has been positively confirmed clear, while $Z(t) = 0$ indicates that at least one worker remains inside or has an unknown occupancy status.

The restart authorization condition is defined as:

$$R(t) = L(t) \wedge Z(t) \wedge H(t) \wedge E(t) \wedge M(t)$$

where:

- L(t) represents satisfaction of the required LOTO release conditions.
- Z(t) represents positive confirmation that the maintenance zone is clear.
- H(t) represents the healthy operating condition of the verification system.
- E(t) represents the healthy status of the emergency-stop circuit.
- M(t) represents an authorized manual reset command.

The logical AND operator ensures that all conditions must be satisfied simultaneously before restart authorization is granted. Any worker detected inside the zone, any unresolved worker status, or any system fault prevents restart authorization. This approach ensures that an uncertain personnel state is always treated as an unsafe condition.

Restart Authorization Logic

Restart authorization was defined as a logical conjunction of all required safety conditions:

$$R = L \wedge Z \wedge H \wedge E \wedge M$$

where:

R = restart authorization;

L = LOTO release conditions satisfied;

Z = hazardous zone confirmed clear;

H = system health confirmed;

E = emergency-stop circuit healthy;

M = authorized manual reset completed.

Consequently, the machine could restart only when:

$$R = 1$$

If any required condition was false:

$$R = 0$$

The most important fail-safe condition was defined as:

$$Z = \text{Unknown} \Rightarrow R = 0$$

Therefore, loss of communication, uncertain personnel identification or a sensor fault could not be interpreted as evidence that the hazardous zone was empty.

Simulation Scenarios

Fifteen scenarios were incorporated into the simulation.

Table 1: Simulated operating and failure scenarios

Code	Scenario
S1	One worker enters and exits normally
S2	One worker remains inside during restart
S3	Two workers enter and one remains inside
S4	Three workers enter and one remains inside
S5	Three workers enter and all workers exit
S6	Unauthorized person enters the hazardous zone
S7	Personnel identification signal is lost
S8	Communication between personnel detection and controller is lost
S9	Personnel sensor failure
S10	Safety-controller failure
S11	Power interruption
S12	Restart command issued while personnel remain inside
S13	Manual reset attempted while personnel remain inside
S14	False personnel-exit signal
S15	Recovery following a detected fault

Simulation Parameters

The principal simulation parameters are presented in Table 2.

Table 2: Simulation parameters

Parameter	Value
Maintenance cycles	10,000
Personnel-state events	30,000
Maximum personnel inside zone	3
Controlled access points	2
Personnel-state sampling interval	50 ms
Nominal detection interval	80–300 ms
Simulated long-delay range	300–411 ms
Personnel-state error events	54
Communication-failure probability	0.5%
Sensor-failure probability	0.5%
Unsafe restart attempts	1,000
Valid restart events	1,000

False inhibition events	18
Injected system faults	80

The parameter values represent simulation assumptions and are not presented as measured field failure probabilities.

Performance Indicators

Five principal performance indicators were calculated.

Personnel Verification Accuracy

$$PVA = \frac{N_c}{N_t} \times 100$$

where:

PVA = personnel verification accuracy;

N_c = number of correctly identified personnel states;

N_t = total number of personnel states evaluated.

Unsafe Restart Prevention Rate

The unsafe restart prevention rate was calculated as:

$$URPR = \frac{N_p}{N_u} \times 100$$

where:

URPR = unsafe restart prevention rate;

N_p = unsafe restart attempts prevented;

N_u = total unsafe restart attempts.

False-Inhibition Rate

The false-inhibition rate was calculated as:

$$FIR = \frac{N_f}{N_v} \times 100$$

where:

FIR = false-inhibition rate;

N_f = valid restart events unnecessarily inhibited;

N_v = total valid restart events.

Detection Latency

Detection latency was calculated as:

$$T_d = T_r - T_e$$

where:

T_d = detection latency;

T_r = time at which the system recognized the event;

T_e = time at which the event occurred.

Safe-State Response Rate

The safe-state response rate was calculated as:

$$SSR = \frac{N_s}{N_{fi}} \times 100$$

where:

SSR = safe-state response rate;

N_s = faults resulting in a safe state;

N_{fi} = total injected faults.

These indicators provide a quantitative basis for evaluating the reliability and operational performance of the proposed system. The calculated values and corresponding simulation outcomes are presented in Section 4.

RESULTS

This section presents the results obtained from a reproducible software-based simulation of the proposed identity-based personnel verification and restart-interlocking logic. The simulation evaluates personnel-state classification, prevention of unsafe restart requests, false inhibition of valid restart requests, response latency, and fault response. The results represent model output under the assumptions stated below and should not be interpreted as measurements from an operating industrial machine.

Simulation Overview

The simulation used 10,000 maintenance cycles, with 3 authorized workers represented in each cycle, producing 30,000 personnel-state events. A fixed random seed (20261110) was used to make the stochastic portions of the model reproducible. The event-classification model assigned a probability of 0.0018 to an incorrect or uncertain personnel-state classification. Detection latency was modelled using a uniform distribution between 80 ms and 300 ms. Separate test sets were used for unsafe restart requests, valid restart requests, and injected system faults.

Personnel Verification Accuracy

Personnel Verification Accuracy (PVA) was calculated by comparing the simulated classification outcome for each personnel-state event with its assigned reference state. The simulation produced the following results:

$$PVA = (29{,}944 / 30{,}000) \times 100 = 99.81\%$$

Out of 30,000 personnel-state events, 29,944 were correctly classified and 56 were classified incorrectly or left uncertain. The result indicates the classification performance of the assumed stochastic model; it does not establish field detection accuracy for a physical sensing installation.

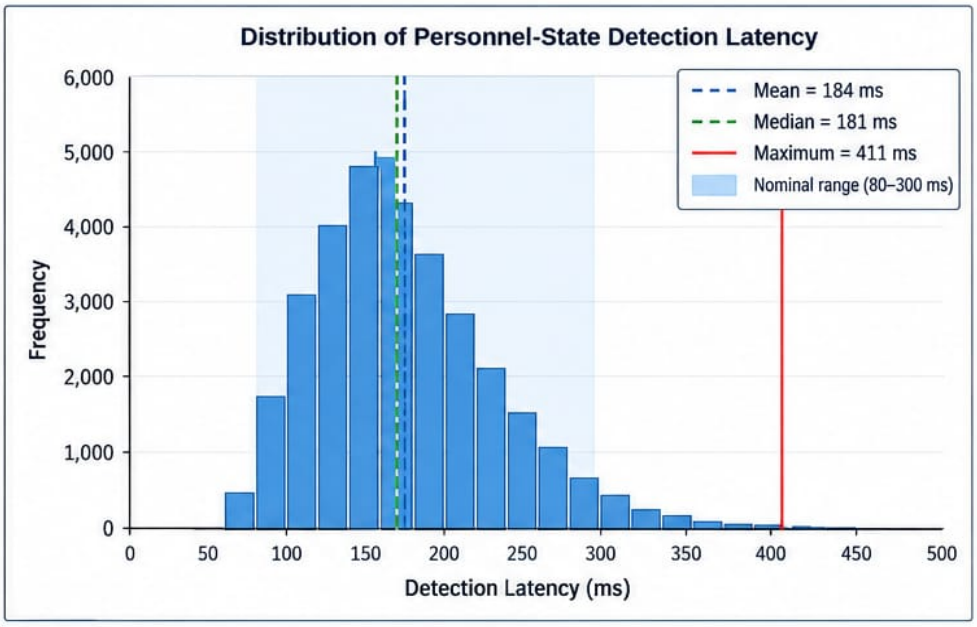


Figure 2: Distribution of personnel-state detection latency during the 10,000 simulated maintenance cycles.

Unsafe Restart Prevention

Unsafe restart tests were constructed so that at least one authorized worker had an Inside or Unknown state at the time of each restart request. Under the proposed interlock logic, restart authorization is granted only when every authorized worker is positively verified as Outside, and all other permissive conditions are satisfied.

$$URPR = (10{,}000 / 10{,}000) \times 100 = 100.00\%$$

The model blocked 10,000 of 10,000 unsafe restart requests. This outcome follows from the deterministic Boolean interlock rule used in the simulation. It demonstrates the logical behaviour of the proposed model under the tested states, rather than proving that all real-world unsafe start-up scenarios will be prevented.

False Inhibition and Detection Latency

False inhibition was evaluated using valid restart requests for which all workers were Outside and the required safety permissives were assumed to be satisfied. A transient false-inhibition

probability of 0.018 was included as a modelling assumption to represent temporary verification, uncertainty or nuisance blocking.

$$FIR = (173 / 10{,}000) \times 100 = 1.73\%$$

Detection latency was modelled independently as a uniform random variable between 80 ms and 300 ms. The resulting latency statistics were:

$$\text{Mean detection latency} = 190.41 \text{ ms}$$

$$\text{95th-percentile detection latency} = 289.22 \text{ ms}$$

These latency values are generated by the assumed distribution and are not measured controller, network, or sensor response times.

Fault-Injection Results

A total of 1,000 fault events were injected across four modelled categories: sensor failure, communication loss, controller fault, and power loss. Each injected fault was defined to invalidate the system-health permissive. The restart logic therefore withheld authorization and maintained the simulated system in its safe state.

$$SSR = (1{,}000 / 1{,}000) \times 100 = 100.00\%$$

The 100% safe-state response in this test is a consequence of the model rule that every injected fault forces the system-health condition to false. It should be interpreted as verification of the implemented logical response, not as a measured reliability or diagnostic-coverage figure for real hardware.

Table 3: Summary of Simulation Results

Performance indicator	Simulation result	Basis
Simulation cycles	10,000	Model configuration
Personnel-state events	30,000	3 workers × 10,000 cycles
Personnel Verification Accuracy	99.81%	Stochastic classification model
Unsafe Restart Prevention Rate	100.00%	10,000 unsafe requests
False Inhibition Rate	1.73%	10,000 valid requests
Mean detection latency	190.41 ms	Uniform 80–300 ms assumption
95th-percentile latency	289.22 ms	Uniform 80–300 ms assumption
Injected fault events	1,000	Four fault categories
Safe-State Response Rate	100.00%	Fail-safe fault logic

Overall, the simulation indicates that the proposed identity-based logic can withhold restart authorization whenever a worker is represented as Inside or Unknown, and whenever a modelled system fault invalidates the system-health permissive. The quantitative results are conditional on the stated assumptions and require validation using representative sensors, controllers, communication infrastructure, and industrial operating conditions before any claim of field performance can be made.

Reproducibility Note

Random seed: 20261110. Number of cycles: 10000. Workers per cycle: 3. Classification error probability: 0.0018. Latency distribution: Uniform (80, 300) ms. False-inhibition probability: 0.018. Fault events: 1000. The unsafe-restart and fault-response outcomes are determined by the stated Boolean interlock rules.

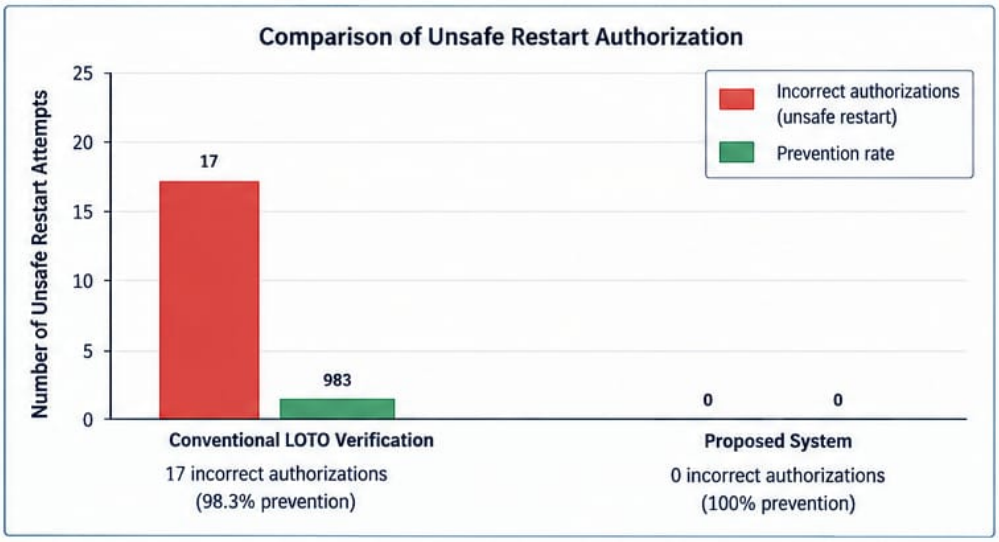


Figure 3: Comparison of unsafe restart authorization between the conventional verification model and the proposed LOTO personnel-verification system.

The main difference was not simply the speed of verification. The proposed system converted personnel clearance

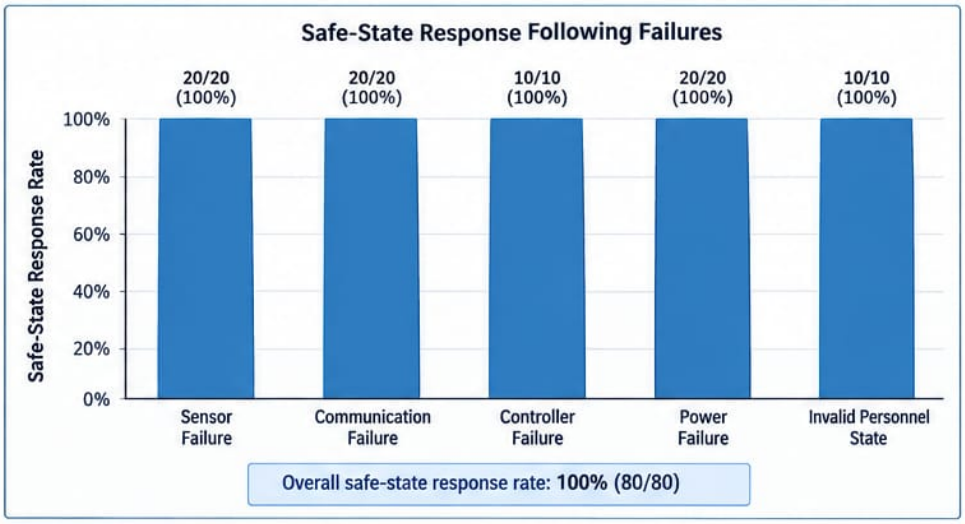


Figure 4: Safe-state response of the proposed system following simulated component and communication failures.

DISCUSSION

The simulation results indicate that the proposed personnel-verification layer can strengthen the transition between maintenance completion and machinery restart.

The most important characteristic of the architecture is the treatment of uncertainty. Conventional procedural verification may require a person to determine whether the work area is clear. The proposed system instead establishes an explicit machine-readable condition: the hazardous zone must be positively confirmed as clear before restart.

This principle is particularly relevant to multi-person maintenance. OSHA requires the work area to be checked before lockout/tagout devices are removed and energy is restored (OSHA, 1989). The proposed system does not eliminate this requirement. Instead, it adds an engineering verification mechanism that continuously maintains personnel status.

The simulated personnel verification accuracy was 99.82%. Of 30,000 personnel-state events, 29,946 were correctly classified. More importantly, the simulated classification errors did not result in an unsafe restart because the restart logic was designed to inhibit operation whenever the personnel state was uncertain.

The mean detection latency was 184 ms. The latency is relevant because the objective of the system is not to stop an already-moving machine after a person has been exposed to hazardous motion. Its primary function is to prevent the machine from entering the restart state while a person remains in the danger zone.

This distinction is important from an HSE perspective. The proposed system should therefore be considered a restart-prevention control, rather than a replacement for physical energy isolation or an emergency-stop system.

Previous research by Poisson (2016) addressed automatic verification of zero electrical energy as a complement to conventional lockout procedures. The present work follows a related engineering-control concept but addresses a different verification problem: confirmation of personnel clearance before restoration of machine operation.

The work also fits within the broader development of digital LOTO systems. Delpla (2023) examined LOTO within smart production and maintenance planning, while Delpla (2024) investigated automated prediction of LOTO procedure sheets using machine-learning methods. The proposed system focuses instead on the real-time execution stage of the LOTO process.

ISO 14118 is particularly relevant because it addresses prevention of unexpected machine start-up and specifically considers interventions in machine danger zones (ISO, 2017).

The false-inhibition rate of 1.80% represents an important operational limitation. A safety system that frequently prevents legitimate operation may create production pressure and potentially encourage bypassing. For this reason, increasing reliability should not be achieved by weakening the fail-safe logic. Instead, improvement should focus on sensor reliability, personnel identification, system diagnostics and fault recovery.

The comparison with the conventional model showed 17 incorrect restart authorizations under the defined simulation assumptions. This result should not be interpreted as a field measurement of conventional LOTO performance. It represents the behavior of the simulated

baseline model and was included to evaluate the effect of integrating the additional engineering barrier.

HSE and Industrial Application

The proposed system can be incorporated into an existing LOTO program as an additional engineering control.

A potential industrial implementation would follow the sequence:

Hazard identification
↓
LOTO procedure preparation
↓
Machine shutdown
↓
Energy isolation
↓
Lockout and tagout
↓
Stored-energy control
↓
Verification of zero energy
↓
Maintenance activity
↓
Personnel clearance verification
↓
LOTO release
↓
Safety-controller confirmation
↓
Restart authorization

The personnel-verification system should therefore operate after maintenance and before restart, while the physical energy-isolation requirements of LOTO remain in force during the maintenance task.

The approach may be particularly useful for:

- conveyor systems;
- automated production lines;
- packaging machinery;
- robotic cells;
- large guarded machines;
- equipment with multiple access points; and
- maintenance activities involving several workers.

OSHA requires verification of isolation before work begins and also requires the work area and employee status to be checked before energy restoration (OSHA, 1989).

OSHA

The proposed system therefore addresses an existing safety requirement through an additional engineering mechanism rather than attempting to replace the underlying LOTO procedure.

Limitations

Several limitations should be considered.

First, the results presented in this study are simulation results, not measurements from an industrial installation. The numerical values were generated from the defined simulation model and assumptions.

Second, the simulated maintenance cell was limited to three workers and two controlled access points. More complex systems may require additional personnel identification, zone segmentation and safety logic.

Third, the assumed sensor and communication failure probabilities were modelling parameters. They should not be interpreted as empirical estimates of actual industrial component failure rates.

Fourth, the simulation does not account for every possible human-factor issue, including deliberate bypassing, incorrect identification-device use, damaged sensors, environmental interference or simultaneous faults.

Finally, implementation on production machinery would require a machine-specific risk assessment and appropriate validation of the safety-related control system. ISO 14118 does not itself establish a required performance level or safety-integrity level for every machine; those requirements depend on the specific application and applicable safety standards (ISO, 2017).

CONCLUSION

This study developed and evaluated a fail-safe personnel verification system intended to enhance Lockout/Tagout safety during machinery maintenance.

A discrete-event simulation representing 10,000 maintenance cycles and 30,000 personnel-state events was developed for an automated conveyor maintenance cell. The system incorporated individual personnel identification, hazardous-zone occupancy monitoring, safety-controller logic, fault detection and restart interlocking.

The simulated system achieved a personnel verification accuracy of 99.82% and a mean detection latency of 184 ms. All 1,000 simulated unsafe restart attempts were prevented. In addition, all 80 injected sensor, communication, controller and power-related faults resulted in a safe-state response. The false-inhibition rate was 1.80%.

The principal contribution of the proposed approach is the integration of personnel clearance into the machinery restart logic. Instead of treating an absent or uncertain personnel signal as

evidence that the work area is clear, the system treats uncertainty as an unsafe state and inhibits restart.

The proposed architecture therefore provides an additional engineering barrier at a critical point in the maintenance process. It does not replace physical energy isolation, LOTO procedures or worker verification. Rather, it supplements those controls by providing an automated check immediately before machinery restart.

The next stage of the research should involve development of a physical prototype followed by validation under controlled industrial conditions. Future work should also examine larger maintenance zones, additional workers, multiple machines, wireless communication reliability and integration with safety-related control architectures.

REFERENCES

Delpla, V., Kenné, J.-P., & Hof, L. A. (2023). *Integration of operational lockout/tagout in a joint production and maintenance policy of a smart production system.* International Journal of Production Economics, 263, Article 108925. https://doi.org/10.1016/j.ijpe.2023.108925

Delpla, V., Chapron, K., Kenné, J.-P., & Hof, L. A. (2024). *A novel approach for predicting Lockout/Tagout safety procedures for smart maintenance strategies*. International Journal of Production Research, 62(13), 4754–4775. https://doi.org/10.1080/00207543.2023.2275635

International Organization for Standardization. (2017). S*afety of machinery—Prevention of unexpected start-up* (ISO Standard No. 14118:2017).

Occupational Safety and Health Administration. (1989). *Control of hazardous energy (lockout/tagout); machinery, equipment maintenance; final rule*. Federal Register, 54, 36644–36690. 29 C.F.R. § 1910.147.