OT-2026-000000058

Zoned Emergency Stop Architecture for Segmented Industrial Lines

Published	September 15, 2026 at 11:56:47 UTC
Permanent URL	https://opentechnical.org/p/OT-2026-000000058
Classification	Industrial Components, Safety & Infrastructure > Machine Safety > Emergency Stop Architecture
Document SHA-256	2f2ae96165922f1edfb14cc8a737ecfe26966a9e7d6f51e5df14ceaa0763c756
Extent	3,802 words, 23 numbered paragraphs, 2 figures

Abstract

This disclosure describes an emergency stop (E-stop) architecture designed for industrial production lines segmented into independently supplied operational zones. The system addresses the challenge of providing localized safety shutdowns without requiring a full line stoppage for every minor incident, while also ensuring comprehensive safety when necessary. It details the interaction between zone-specific E-stop circuits and a global safety network, including propagation rules for safety signals, procedures for system reset, and behavior when a zone's local power supply is interrupted, thereby enhancing operational continuity and safety compliance.

1. Technical Field

[0001] The technical field is industrial machine safety, specifically concerning emergency stop (E-stop) systems for automated production lines and processing equipment. It involves the design and implementation of control architectures that ensure the safe shutdown of machinery or portions thereof in response to detected hazards or operator intervention, while aiming to minimize unnecessary operational disruption.

2. Technical Context

[0002] Industrial production lines often comprise multiple sequential processing stations or segments, each potentially operating with different functional requirements, power demands, and local operators. A common challenge arises in applying emergency stop functionality to such systems. A single, monolithic E-stop circuit spanning an entire long line, while providing ultimate safety, can lead to significant downtime. The activation of any E-stop device, regardless of its proximity to a localized fault, would halt the entire line. This global stoppage can be disproportionate to the actual hazard, affecting upstream and downstream processes unnecessarily. Conversely, purely independent E-stop circuits for each segment might leave adjacent or interconnected hazards unaddressed. For instance, if a machine in one segment stops but a conveyor in an adjacent segment continues to feed material into the stopped machine, a new hazard could be created. Furthermore, the supply of power to individual segments can vary; some zones might draw power from a local main, while others are sub-supplied. An effective E-stop architecture must account for these variations, ensuring safety integrity even when a zone loses its primary power source. The problem, therefore, is to implement a safety system that allows for localized E-stop events to affect only relevant sections, propagates critical safety signals appropriately, and maintains safety in various power supply scenarios, without compromising overall system safety.

3. System Overview

[0003] The arrangement describes a zoned emergency stop system designed for an industrial line composed of multiple, electrically and logically distinct operational zones. Each zone (12, 14, 16) is equipped with its own local E-stop circuit, including E-stop buttons (32) and a dedicated safety relay module (34) or safety controller. These local circuits are responsible for immediately de-energizing the equipment (38) within their respective zones upon activation. A central global safety programmable logic controller (PLC) (10) supervises the entire line. This global PLC (10) is connected to each zone's safety relay module (34) via a safety communication bus (18) or hardwired interlocks. This allows for both localized E-stops to only affect their zone and for certain E-stop events or critical system faults to propagate safety signals across multiple zones or the entire line. The system incorporates logic for safe system reset and specific protocols for handling the loss of power to an individual zone. Zone boundaries are defined by physical separations, safety-rated interlocks (42) between adjacent zones, and distinct power distribution points. FIG. 1 provides an overview of this architecture, showing the interaction between the global safety PLC (10), zone controllers (12, 14, 16), and the global E-stop bus (18). FIG. 2 details the components within a single zone's safety circuit.

4. Components

[0004] The system comprises several key components:

[0005]

- **Global Safety PLC (10)**: This is a safety-rated programmable logic controller responsible for overall system supervision. It monitors the status of all zone safety circuits, manages inter-zone safety logic, and handles system-wide E-stop conditions. It communicates with individual zone controllers (30) and safety relay modules (34).
- **Zone Controller (30)**: Each operational zone has a local control system, often a standard industrial PLC, which manages the non-safety-related functions of the equipment (38) within that zone. It communicates with the global safety PLC (10) for operational coordination and receives safety status from its local safety relay module (34).
- **Zone E-Stop Buttons (32)**: These are manually actuated, safety-rated devices distributed within each zone, designed to initiate an emergency stop. They are typically latching pushbuttons with direct-opening contacts, wired into the local safety relay module (34).
- **Safety Relay Module (34)**: This is a safety-rated device, typically compliant with relevant safety standards (e.g., ISO 13849, IEC 62061), that receives inputs from the zone E-stop buttons (32) and other safety devices within the zone, such as safety light curtains or interlocked guard switches. Upon activation of an E-stop or detection of a safety fault, it immediately removes power to the zone's main power contactor (36), ensuring a safe state for the zone equipment (38). It also provides status outputs to the zone controller (30) and global safety PLC (10).
- **Main Power Contactor (36)**: A contactor located within each zone's power distribution panel. Its control circuit is directly interrupted by the safety relay module (34) to remove power from the zone equipment (38). It is typically a positively guided contactor or a similar safety-rated switching device.
- **Zone Equipment (38)**: This encompasses all machinery, actuators, motors, and other operational components within a specific zone that require immediate de-energization upon an E-stop event.

- **Global E-Stop Bus (18)**: A safety-rated communication network (e.g., PROFIsafe, CIP Safety) or a hardwired series of safety contacts that connects the global safety PLC (10) to the safety relay modules (34) of each zone. This bus facilitates the propagation of E-stop signals across zones and enables the global safety PLC (10) to monitor the safety status of the entire line.
- **Supply Monitor (40)**: A device within each zone that monitors the presence and quality of the zone's primary electrical power supply. It provides a signal to the zone controller (30) and potentially to the safety relay module (34) if power is lost or falls outside acceptable parameters.
- **Adjacent Zone Interlock (42)**: Safety-rated devices, such as interlocked guard switches, light curtains, or safety matting, positioned at the physical boundaries between adjacent zones.## Technical Field

[0006] The technical field is industrial machine safety, specifically concerning emergency stop (E-stop) systems for automated production lines and processing equipment. It involves the design and implementation of control architectures that ensure the safe shutdown of machinery or portions thereof in response to detected hazards or operator intervention, while aiming to minimize unnecessary operational disruption.

5. Technical Context

[0007] Industrial production lines often comprise multiple sequential processing stations or segments, each potentially operating with different functional requirements, power demands, and local operators. A common challenge arises in applying emergency stop functionality to such systems. A single, monolithic E-stop circuit spanning an entire long line, while providing ultimate safety, can lead to significant downtime. The activation of any E-stop device, regardless of its proximity to a localized fault, would halt the entire line. This global stoppage can be disproportionate to the actual hazard, affecting upstream and downstream processes unnecessarily. Conversely, purely independent E-stop circuits for each segment might leave adjacent or interconnected hazards unaddressed. For instance, if a machine in one segment stops but a conveyor in an adjacent segment continues to feed material into the stopped machine, a new hazard could be created. Furthermore, the supply of power to individual segments can vary; some zones might draw power from a local main, while others are sub-supplied. An effective E-stop architecture must account for these variations, ensuring safety integrity even when a zone loses its primary power source. The problem, therefore, is to implement a safety system that allows for localized E-stop events to affect only relevant sections, propagates critical safety signals appropriately, and maintains safety in various power supply scenarios, without compromising overall system safety.

6. System Overview

[0008] The arrangement describes a zoned emergency stop system designed for an industrial line composed of multiple, electrically and logically distinct operational zones. Each zone (12, 14, 16) is equipped with its own local E-stop circuit, including E-stop buttons (32) and a dedicated safety relay module (34) or safety controller. These local circuits are responsible for immediately de-energizing the equipment (38) within their respective zones upon activation. A central global safety programmable logic controller (PLC) (10) supervises the entire line. This global PLC (10) is connected to each zone's safety relay module (34) via a safety communication bus (18) or hardwired interlocks. This allows for both localized E-stops to only affect their zone and for certain E-stop events or critical system faults to propagate safety signals across multiple zones or the entire line. The system incorporates logic for safe system reset and specific protocols for handling the loss of power to an individual zone. Zone boundaries are defined by physical separations, safety-rated interlocks (42) between adjacent zones, and distinct power distribution points. FIG. 1 provides an overview of this architecture, showing the interaction between the global safety PLC (10), zone controllers (12, 14, 16), and the global E-stop bus (18). FIG. 2 details the components within a single zone's safety circuit.

7. Components

[0009] The system comprises several key components:

[0010]

- **Global Safety PLC (10)**: This is a safety-rated programmable logic controller responsible for overall system supervision. It monitors the status of all zone safety circuits, manages inter-zone safety logic, and handles system-wide E-stop conditions. It communicates with individual zone controllers (30) and safety relay modules (34).
- **Zone Controller (30)**: Each operational zone has a local control system, often a standard industrial PLC, which manages the non-safety-related functions of the equipment (38) within that zone. It communicates with the global safety PLC (10) for operational coordination and receives safety status from its local safety relay module (34).
- **Zone E-Stop Buttons (32)**: These are manually actuated, safety-rated devices distributed within each zone, designed to initiate an emergency stop. They are typically latching pushbuttons with direct-opening contacts, wired into the local safety relay module (34).
- **Safety Relay Module (34)**: This is a safety-rated device, typically compliant with relevant safety standards (e.g., ISO 13849, IEC 62061), that receives inputs from the zone E-stop buttons (32) and other safety devices within the zone, such as safety light curtains or interlocked guard switches. Upon activation of an E-stop or detection of a safety fault, it immediately removes power to the zone's main power contactor (36), ensuring a safe state for the zone equipment (38). It also provides status outputs to the zone controller (30) and global safety PLC (10).
- **Main Power Contactor (36)**: A contactor located within each zone's power distribution panel. Its control circuit is directly interrupted by the safety relay module (34) to remove power from the zone equipment (38). It is typically a positively guided contactor or a similar safety-rated switching device.
- **Zone Equipment (38)**: This encompasses all machinery, actuators, motors, and other operational components within a specific zone that require immediate de-energization upon an E-stop event.
- **Global E-Stop Bus (18)**: A safety-rated communication network (e.g., PROFIsafe, CIP Safety) or a hardwired series of safety contacts that connects the global safety PLC (10) to the safety relay modules (34) of each zone. This bus facilitates the propagation of E-stop signals across zones and enables the global safety PLC (10) to monitor the safety status of the entire line.
- **Supply Monitor (40)**: A device within each zone that monitors the presence and quality of the zone's primary electrical power supply. It provides a signal to the zone controller (30) and potentially to the safety relay module (34) if power is lost or falls outside acceptable parameters.
- **Adjacent Zone Interlock (42)**: Safety-rated devices, such as interlocked guard switches, light curtains, or safety matting, positioned at the physical boundaries between adjacent

zones. These interlocks provide inputs to the safety relay modules (34) of connected zones and ensure that a hazard in one zone (e.g., an open guard) can trigger a safety stop in an adjacent zone if necessary.

8. Operation

[0011] The system's operation is characterized by distinct states and transitions.

[0012] **Start-up and Normal Running:** Upon initial power-up, each safety relay module (34) performs self-diagnostics. Once all local E-stop buttons (32) are released and all local safety interlocks (42) are closed, the safety relay module (34) enters a ready state. The global safety PLC (10) monitors the ready status of all zones via the global E-stop bus (18). Once all zones are ready and a global reset command is issued from a master control station (not shown), the global safety PLC (10) enables the zone controllers (30). Each zone controller (30) can then command its main power contactor (36) to close, energizing the zone equipment (38) for normal operation. During normal running, the safety relay module (34) continuously monitors the E-stop buttons (32) and local safety devices.

[0013] **Local E-Stop Event:** If an E-stop button (32) is activated within a specific zone, or a local safety device (e.g., a light curtain) is triggered, the corresponding safety relay module (34) immediately opens its safety outputs, causing the main power contactor (36) for that zone to open. This removes power to the zone equipment (38), bringing it to a safe stop (Category 0 or Category 1, depending on system design). Simultaneously, the safety relay module (34) transmits the E-stop status to its zone controller (30) and to the global safety PLC (10) via the global E-stop bus (18). The global safety PLC (10) then evaluates this local E-stop signal based on pre-defined propagation rules.

[0014] **Propagation Rules:** The global safety PLC (10) applies specific logic for E-stop signal propagation:

[0015]

- **Local Stop**: For most E-stop activations, the signal affects only the zone in which it originated. This prevents unnecessary line-wide shutdowns.
- **Adjacent Zone Stop**: If an E-stop occurs in a zone that directly impacts the safety of an adjacent zone (e.g., a conveyor feeding into a stopped machine), the global safety PLC (10) signals the adjacent zone's safety relay module (34) to initiate an E-stop. This typically involves stopping upstream feeding mechanisms to prevent material accumulation or stopping downstream processes that might be affected by the sudden halt of the current zone. Interlocks (42) at zone boundaries facilitate this.
- **Global Stop**: Certain critical E-stop conditions (e.g., E-stop activation at the primary control panel, detection of a system-wide safety fault by the global safety PLC (10), or E-stop activation in a designated "critical" zone) will cause the global safety PLC (10) to command all zone safety relay modules (34) to open their contactors, resulting in a full line shutdown.

[0016] **Reset Procedure:** After an E-stop event, the affected E-stop button (32) must be released or the safety device reset. The local safety relay module (34) then signals its readiness. For a single-zone E-stop, an operator can issue a local reset command via the zone controller (30) or a dedicated reset button (not shown). This command is forwarded to the safety relay module (34), which then re-energizes its output to the main power contactor (36), allowing the zone equipment (38) to restart under the control of the zone controller (30). For

E-stops that propagated to multiple zones or the entire line, all activated E-stop devices must be cleared, and a global reset command must be issued from the master control station after confirmation by the global safety PLC (10) that all zones are safe and ready. The global safety PLC (10) then enables zones sequentially or concurrently as per programmed logic.

[0017] **Loss of Zone Supply:** Each zone's power supply is monitored by a supply monitor (40). If a zone loses its main electrical supply, the supply monitor (40) detects this and signals the zone controller (30). Crucially, the safety relay module (34) is designed to operate or fail-safe under such conditions. In a power loss scenario, the main power contactor (36) will naturally de-energize and open, bringing the zone equipment (38) to a safe stop. The safety relay module (34) itself often has a sufficient power reserve or is designed to maintain its safety state (outputs open) during transient power interruptions, or if it loses its own control power, it will default to a safe state. The global safety PLC (10) will receive a "zone offline" or "safety fault" signal via the global E-stop bus (18) due to the absence of communication or the specific status from the zone's safety relay module (34). This will trigger appropriate propagation rules, such as stopping upstream zones that feed into the affected zone, to prevent hazards arising from material accumulation. Upon restoration of power, the zone will undergo its normal start-up and reset procedure.

9. Example Embodiments

[0018] **Embodiment 1: Conveyor Line with Feed Control** A long conveyor line is divided into five zones (Z1-Z5). Each zone has local E-stop buttons (32) and a safety relay module (34). Z1 is a feeding station, Z2-Z4 are processing stations, and Z5 is an offloading station. An E-stop activated in Z3 (processing) immediately stops all equipment (38) in Z3. The global safety PLC (10) receives this signal and, based on its logic, also initiates a safe stop of Z2 (upstream processing) and Z1 (feeding station) to prevent further material from entering the now-stopped Z3. Z4 and Z5 (downstream) are allowed to continue operating to clear any material, then enter a safe stop state if no further material is being fed. Reset requires clearing the Z3 E-stop, then a local reset for Z3, and finally, a coordinated restart of Z1, Z2, and Z3 by the global safety PLC (10).

[0019] **Embodiment 2: Robotic Workcell with Adjacent Manual Stations** A robotic workcell forms Zone 2, flanked by a manual loading station (Zone 1) and a manual unloading station (Zone 3). All zones are separated by safety light curtains or interlocked gates (42). An E-stop in Zone 2 (robot cell) immediately stops the robot (38) and all equipment within Zone 2. The global safety PLC (10) prevents the interlocked gates (42) between Zone 1 and Zone 2, and Zone 2 and Zone 3 from opening until the robot is verified to be in a safe, de-energized state. No automatic stop is propagated to Zone 1 or Zone 3 unless an operator attempts to enter Zone 2 through an interlocked gate (42), which would be prevented by the safety system. If an E-stop is activated in Zone 1 (manual loading), only Zone 1 equipment stops; the robot in Zone 2 continues its operation until material supply from Zone 1 ceases.

[0020] **Embodiment 3: Chemical Processing Line with Integrated Utility Zones** A chemical processing line involves three processing zones (P1, P2, P3) and a separate utility zone (U1) providing critical services (e.g., pumps, chillers) to P1 and P2. Each processing zone has its own power supply and E-stop circuit. The utility zone (U1) also has an independent power supply and E-stop. An E-stop in P1 (processing) stops only P1's equipment (38). However, the global safety PLC (10) detects that P1 requires utilities from U1, so it commands specific pumps or chillers within U1 that service P1 to enter a safe state (e.g., slow down or stop, depending on hazard analysis). An E-stop in U1, due to its critical nature, triggers a global stop across P1, P2, and P3, as the loss of utilities impacts their safe operation. This ensures that the entire process is brought to a controlled shutdown in the event of a utility failure or E-stop.

10. Alternative Configurations

[0021] The global E-stop bus (18) can be implemented as a hardwired series circuit of safety contacts from each safety relay module (34), rather than a safety communication network. While a hardwired solution may offer a simpler implementation for a smaller number of zones, it lacks the diagnostic capabilities and flexibility of a safety bus. Another alternative involves integrating the safety relay module (34) functionality directly into the zone controller (30) if it is a safety-rated PLC. This can reduce component count but might increase the complexity of programming and certification for each zone. For zones with minimal hazards, a basic E-stop circuit directly interrupting the main power contactor (36) without a dedicated safety relay module (34) or communication to the global safety PLC (10) could be used, provided that the risk assessment justifies such a simplification and no inter-zone propagation is required.

11. Parameter Variations

Parameter	Realistic Range	Effect of Variation
Number of Zones	2 to 50	More zones increase complexity of global safety PLC (10) logic and bus (18) bandwidth requirements.
E-Stop Category (per zone)	Category 0, 1, or 2	Category 0 (immediate power removal) is simplest; Category 1 (controlled stop, then power removal) requires more complex zone controller (30) integration.
Reset Type	Local, Zoned, Global	Local reset allows faster recovery for isolated faults; global reset ensures all areas are confirmed safe.
Propagation Delay	10 ms to 200 ms	Shorter delays enhance safety response time but may require faster safety PLCs (10) and communication (18).
Zone Power Disconnect Time	50 ms to 500 ms	Faster disconnect times reduce exposure to hazards but may require specialized contactors (36) or solid-state devices.
Communication Bus Type	Hardwired, Safety Network	Hardwired is simple but less flexible; safety network (18) allows advanced diagnostics and dynamic propagation logic.
Interlock Redundancy	Single, Dual Channel	Dual channel redundancy (e.g., two switches for one guard) increases fault tolerance and safety integrity level.
Zone Power Supply Voltage	24 VDC to 690 VAC	Affects selection of power contactors (36) and associated wiring and electrical protection within the zone.

12. Additional Implementations

[0023] This zoned E-stop architecture can be extended to include other safety functions beyond simple E-stops. For instance, safety light curtains or laser scanners could define flexible zone boundaries, automatically initiating a safe stop in a zone when an intrusion is detected, and dynamically adjusting propagation rules based on the intrusion location. The system can also be integrated with predictive maintenance systems, where detected anomalies in zone equipment (38) could trigger a controlled zone shutdown before a catastrophic failure occurs, acting as a preventative safety measure. Furthermore, the architecture supports the implementation of "safe speed" or "safe limited position" functions within zones, where the safety relay module (34) or safety drive allows equipment (38) to operate at reduced speeds or within defined safe envelopes under specific conditions (e.g., during maintenance or setup), rather than a full power removal. This requires a safety-rated drive with integrated safety functions. The principle of zoned control and safety propagation can also be applied to non-electrical hazards, such as pneumatic or hydraulic systems, by using safety-rated valves to vent pressure or block fluid flow within a zone upon an E-stop event. This system allows for modular expansion of a line by simply adding new zones, each with its own safety circuit, and integrating it into the global safety PLC (10) via the safety bus (18), minimizing redesign of existing safety infrastructure.

13. Figures

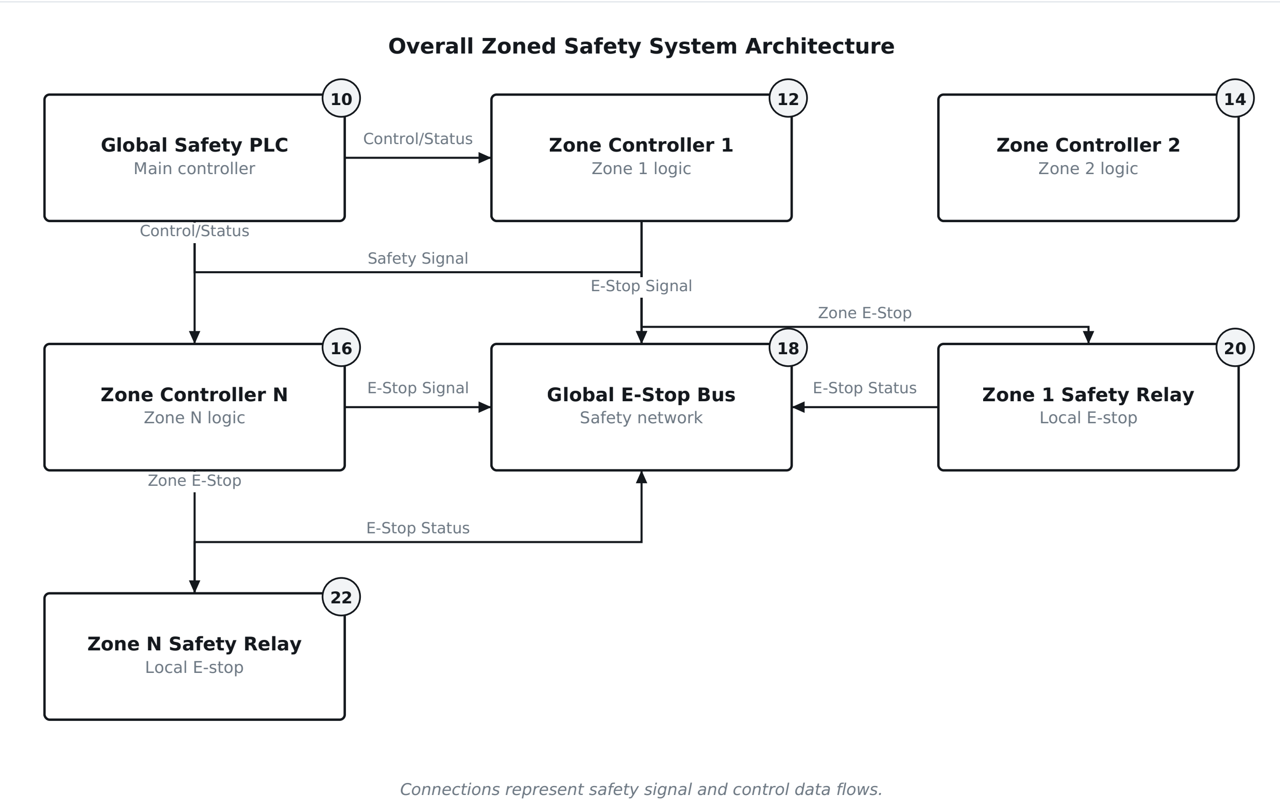

FIG. 1 A block diagram illustrating the interaction between multiple operational zones and a global safety control system. PNG

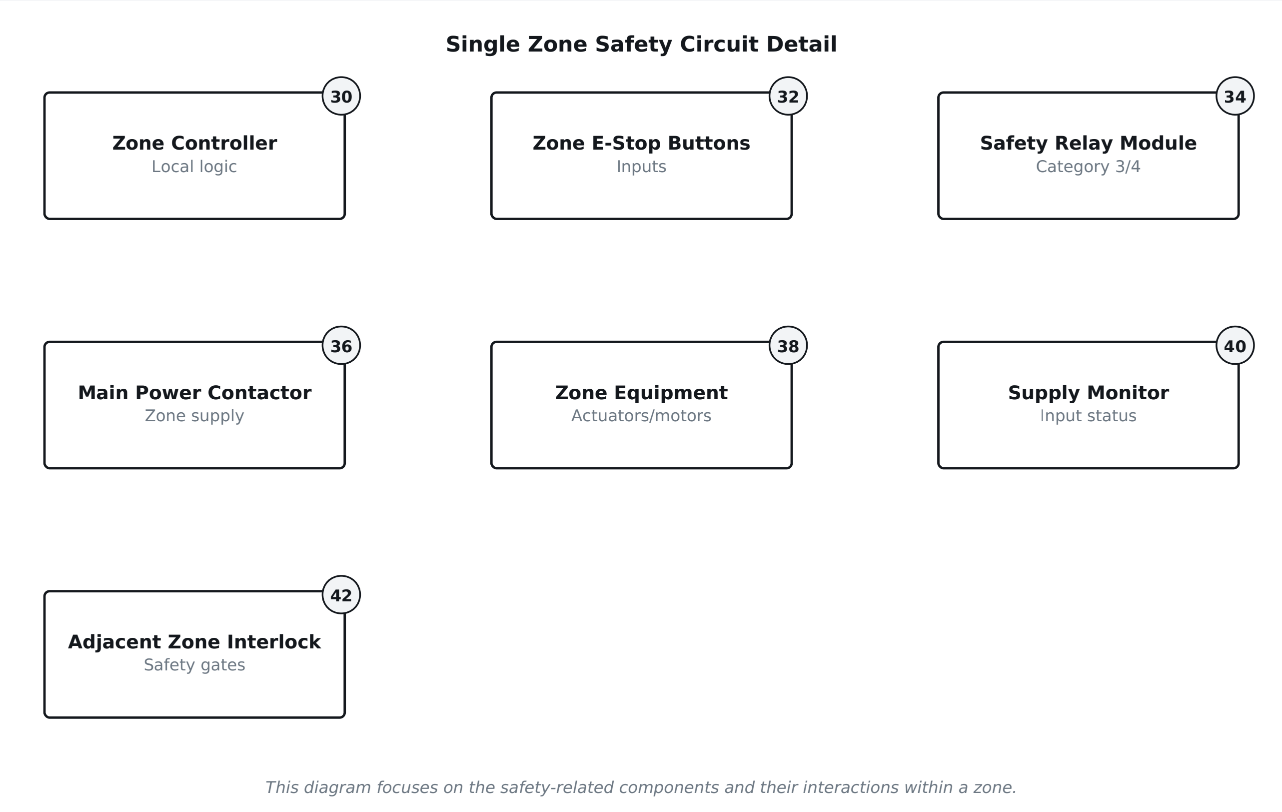

FIG. 2 A detailed block diagram of the safety circuit within a single operational zone. PNG

OpenTechnical Publication OT-2026-000000058. Published September 15, 2026 at 11:56:47 UTC. https://opentechnical.org/p/OT-2026-000000058