Independent Watchdogs with Dump-Load/Crowbar Protection and Detune-on-Fault Architectures for High-Energy Rotating-Field Systems

Docket: NTL-PROV-018
Inventors: [Inventor Names]
Assignee: [Assignee / Organization]
Date: February 1, 2026

Abstract

Disclosed are apparatus, systems, methods, and non-transitory computer-readable media for safety hardening of rotating-field and resonant electromagnetic systems using an *independent watchdog* and a fault-mitigation stack comprising one or more of dump loads, crowbar circuits, contactors, and detune-on-fault commands. In various embodiments, a primary controller operates a rotating-field device (including generator-mode operation) and a separate watchdog subsystem independently monitors hazard indicators such as bus overvoltage, overcurrent, overspeed, loss-of-load signatures, and thermal derivatives. Upon detecting a fault or loss of primary controller heartbeat, the watchdog triggers rapid protective actions including engaging a dump load, activating a crowbar, opening a contactor, and/or commanding an active detuning governor to collapse coupling efficiency.

In one embodiment, the watchdog is implemented with independent power, clocking, and threshold comparators, enabling fail-safe response even if the primary controller is compromised. The disclosed architectures provide a layered safety system suitable for high-energy experiments and products requiring rapid response and auditable fault handling.

Technical Field

The present disclosure relates to safety systems for high-energy electromechanical platforms, and more particularly to independent watchdog controllers, dump-load and crowbar protection circuits, contactor management, heartbeat monitoring, and detune-on-fault safety architectures for rotating-field and resonant electromagnetic systems.

Background

Rotating-field systems and resonant electromagnetic devices can produce rapid transients in voltage, current, temperature, and mechanical state. Safety mitigations implemented only in a primary controller can fail due to software faults, timing faults, EMI, or component failure. Additionally, certain hazards (e.g., load disconnect in generator mode, bus overvoltage) may require response faster than a typical supervisory control loop.

Conventional safety approaches include fuses, circuit breakers, and thermal cutoffs. While useful, these may not respond optimally to fast transients or may not coordinate safely with a resonant device state. A layered safety architecture that includes an independent watchdog capable of initiating fast protective actions is needed.

Summary

This disclosure provides a multi-layer safety architecture comprising:

- **Independent watchdog:** separate monitoring logic and/or hardware with independent power and clocking.
- **Fast fault detection:** analog comparators and/or digital logic for overvoltage, overcurrent, and heartbeat loss.
- **Mitigation stack:** dump loads, crowbars, contactors, and detune-on-fault commands to collapse coupling and absorb energy.
- **Latched safe state:** a safe state requiring explicit recovery procedure, optionally including operator acknowledgement.

Brief Description of the Drawings

Drawings may be provided later. For purposes of this specification:

- **FIG. 1** depicts a primary controller and an independent watchdog supervising a rotating-field driver and power stage.
- **FIG. 2** depicts a dump-load network and crowbar coupled to a DC bus.
- **FIG. 3** depicts heartbeat monitoring and timeout behavior.
- **FIG. 4** depicts a fault ladder with escalating mitigation (detune, dump load, crowbar, contactor open).
- **FIG. 5** depicts a recovery procedure and revalidation gates.

Definitions and Notation

Unless otherwise indicated:

- A *watchdog* refers to an independent subsystem that monitors safety conditions and can initiate protective actions.
- A *heartbeat* refers to a periodic signal from a primary controller indicating normal operation.
- A *dump load* refers to a controllable load configured to absorb electrical energy (e.g., resistor bank).
- A *crowbar* refers to a protection circuit that clamps a bus (e.g., via SCR or MOSFET) to prevent overvoltage.
- A *contactor* refers to a switching element that disconnects energy sources or loads.
- A *detune-on-fault command* refers to a command that collapses coupling by detuning a commutation schedule or drive waveform.

Detailed Description

1. Layered Safety Architecture

In one embodiment, the system includes:

- a primary controller operating a rotating-field driver and optionally a load interface;
- an independent watchdog that monitors hazard indicators;
- a fault mitigation stack including dump loads, crowbar, contactors, and detune-on-fault.

In one embodiment, the watchdog has independent power and clocking and can function even if the primary controller is reset, hung, or corrupted.

2. Fault Detection

Non-limiting hazard indicators monitored by the watchdog include:

- bus overvoltage (absolute threshold or dV/dt);
- overcurrent (absolute threshold or dI/dt);
- loss-of-load signature (falling load current with rising bus voltage);
- overspeed or unsafe acceleration;
- thermal derivative dT/dt exceeding a threshold;
- heartbeat timeout of the primary controller.

In one embodiment, the watchdog uses analog comparators for fast thresholds and digital logic for pattern-based detection (e.g., loss-of-load).

3. Heartbeat Monitoring

In one embodiment, the primary controller emits a periodic heartbeat pulse. The watchdog resets a timer on receipt. If the timer exceeds a timeout τ, the watchdog assumes fault and triggers mitigation.

4. Mitigation Actions

Upon fault detection, the watchdog may execute one or more actions, alone or in sequence:

- **Detune-on-fault:** command a detuning governor to inject phase slip/noise and collapse coupling.
- **Dump-load engagement:** switch a dump load across the DC bus to absorb energy.
- **Crowbar activation:** clamp the bus voltage to prevent overvoltage.
- **Contactor open:** disconnect energy sources or isolate the device.
- **Driver disable:** force gate-disable signals low and/or assert a hardware kill line.

In one embodiment, mitigation is escalated based on severity (e.g., warning detune first, then dump load, then crowbar and contactor open).

5. Latched Safe State and Recovery

In one embodiment, after mitigation, the watchdog places the system in a latched safe state. Recovery may require:

- bus voltage below a safe threshold;
- temperatures below safe thresholds;
- operator acknowledgement and a revalidation checklist;
- restarting primary controller and rearming watchdog.

6. Embodiments

Non-limiting embodiments include:

- watchdog implemented on a separate microcontroller, FPGA, or analog logic board;
- redundant sensors and comparators for critical thresholds;
- independent battery-backed watchdog supply;
- tamper detection causing immediate detune and dump-load engagement.

Claims (Draft)

Note: The following claims are an initial, non-limiting claim set intended to preserve multiple fallback positions. Final claim strategy should be reviewed by counsel.

Independent Claims

1. **(System)** A safety system for a rotating-field device comprising: a primary controller configured to operate the rotating-field device; an independent watchdog configured to monitor at least one hazard indicator; and a mitigation subsystem comprising at least one of a dump load, a crowbar circuit, a contactor, or a detune-on-fault interface, wherein the independent watchdog is configured to initiate at least one mitigation action in response to the at least one hazard indicator satisfying a trigger condition.

2. **(Method)** A method of protecting a rotating-field system, the method comprising: monitoring hazard indicators using a watchdog subsystem; detecting at least one of bus overvoltage, overcurrent, loss-of-load, overspeed, thermal runaway, or loss of heartbeat; and responsive to detecting the hazard, executing a mitigation action comprising engaging a dump load, activating a crowbar, opening a contactor, disabling a driver, and/or issuing a detune-on-fault command.

3. **(Non-transitory medium)** A non-transitory computer-readable medium storing instructions that, when executed by one or more processors of a watchdog, cause the watchdog to: monitor a heartbeat signal from a primary controller; detect a heartbeat timeout; and upon the timeout, assert a hardware kill line and engage a dump load and/or detune-on-fault command.

Dependent Claims (Examples; Non-Limiting)

4. The system of claim 1, wherein the independent watchdog has an independent power supply and independent clocking.

5. The system of claim 1, wherein monitoring comprises using an analog comparator to detect bus overvoltage.

6. The system of claim 1, wherein the mitigation action comprises commanding a phase-slip detuning governor.

7. The method of claim 2, wherein executing the mitigation action comprises escalating through a ladder of detune, dump load, crowbar, and contactor open.

8. The system of claim 1, wherein the independent watchdog enters a latched safe state until an operator acknowledgement is received.

9. The non-transitory medium of claim 3, wherein the watchdog logs a fault event and associated sensor values to a run artifact.

10. The system of claim 1, wherein the hazard indicator comprises rising bus voltage concurrent with falling load current.

11. The system of claim 1, wherein the mitigation subsystem comprises a pre-charge circuit and a contactor management interface.

Additional Embodiments and Fallback Positions (Non-Limiting)

- Dump loads may be implemented as resistor banks, water-cooled loads, or pulsed load absorbers.
- Crowbar circuits may be implemented using SCRs, MOSFET clamps, or other fast clamping devices.
- The watchdog may support periodic self-test routines, including comparator threshold tests and heartbeat validation.
- The watchdog may coordinate with an energy-accounting pipeline by marking fault windows and excluding them from analysis.

End of Specification (Draft)