Smart Fence Energiser

Microprocessor-Based Non-Lethal Security System

The energiser should be powered by an intelligent microprocessor that enables automated monitoring, diagnostics, and fault detection. It ensures high performance, reliability, and precision control, while maintaining non-lethal energy output levels to deter intruders without causing harm.

High Voltage Output: 1.0 kV to 9.9 kV

The system should deliver adjustable high-voltage pulses between 1.0 kV and 9.9 kV. This flexibility allows it to be used for different perimeter sizes and threat levels, providing an effective physical deterrent.

Output Energy: 4.8 Joules

The energiser should release 4.8 Joules of energy per pulse, strong enough to deter threats while conforming to non-lethal standards. This energy level strikes a balance between effectiveness and safety.

Pulse Synchronisation for Safety

Pulse synchronisation ensures that electrical discharges are timed precisely, minimizing the chance of dangerous electrical interference with other systems and ensuring that humans or animals who come in contact receive non-lethal shocks.

Robust and Flexible Design

The device should be designed to withstand harsh environmental conditions (heat, rain, dust). The enclosure must be durable, and its internal electronics should be protected from external damage, offering long-term performance with low maintenance.

Built-in Alarm for Tampering or Faults

The system should have integrated sensors to detect tampering (e.g., cutting wires) or operational faults (e.g., grounding issues). These alarms should instantly notify the control center for prompt action.

TCP/IP Connectivity Without a Converter

The energiser must support native Ethernet communication using the TCP/IP protocol. This avoids the need for external adapters or converters, simplifying integration into modern security systems and networks.

Remote Control via Command & Control Software

Authorized personnel should be able to control and monitor the system from any remote location using secure command and control software. Functions include arming/disarming, voltage adjustments, log monitoring, and status alerts.

Open Integration Platform for Third-Party Systems

The energiser should support API or communication protocols that allow easy integration with third-party security systems, including CCTV, access control, or emergency alert systems.

Lightning and Surge Protection

The system should be protected against voltage spikes from lightning or power surges using built-in protection circuits. This ensures uninterrupted performance and reduces the risk of hardware damage.

Intelligent Power Saving

The energiser should automatically enter power-saving modes during inactivity or off-peak hours. This feature extends battery backup duration and reduces energy consumption, making the system eco-friendly and cost-effective.

Onboard LCD and Keypad

A user-friendly LCD panel and keypad should allow for local configuration and monitoring. Operators should be able to view system status, logs, alerts, and make basic configurations without external tools.

Inbuilt Configurable Temperature Management

The system should monitor its internal temperature using sensors. It must allow configurable temperature thresholds and trigger alerts or actions like fan activation to prevent overheating.

Custom Over-Temperature Triggers & Alerts

If the temperature exceeds the set threshold, the system should automatically take action — e.g., activate a cooling fan, shut down components, and send alerts to the central command system for operator intervention.

Smart Rack System Integration

The energiser must be compatible with smart rack solutions used in data centers or critical infrastructure. It should support power and network integration in a rack-mounted environment for centralized control.

Power Supply: 170-270 V AC

The device should operate reliably across a wide input voltage range (170–270V), providing resilience against voltage fluctuations commonly found in various regions.

Compliance and Certification Requirements

Compliance with Safety & EMC Standards:
- IEC 60335-2-76:2018 / IS 302-2-76:1999
- IS 9000 (Part 6)
- IEC 61000-4-2:2008 (Electrostatic Discharge Immunity)
- IEC 61000-4-3:2006 + A1:2007 + A2:2010 (Radiated Electromagnetic Field Immunity)
- IEC 61000-4-4:2012 (Electrical Fast Transients)
- IEC 61000-4-5:2014 + A1:2017 (Surge Immunity)

Software OEM Certification Requirements

- CMMI Level 3 Certification: To assure high maturity and process capability.
- ISO 9001:2015 Certification: Indicating compliance with quality management systems.
- Certification must be at least 6 months old from the bid date to ensure the vendor’s maturity and operational stability.