Designing and Fabrication of Advanced Army Camp Security System

Mr. Prabhat Singh, Mr. Rohit Patel – Student, Department of Mechanical Engineering, Shri Ramswaroop Memorial College of Engineering and Management, Lucknow, India – 226025

Keyword

RFID
Layered
Integration
Real- time
Alert
pitfalls
robust
Threat analysis
Unauthorized

Abstract

This paper presents a multi-layered electronic security system designed for comprehensive protection of confined areas. The system integrates three distinct security layers an electric fencing system serving as an original physical and cerebral interference, an RFID- grounded landmine security system aimed at precluding unauthorized access while allowing passage for authorized labor force, and an RFID- grounded alarm landmine system furnishing early warning of intrusions. The electric hedge delivers non-lethal electric shocks upon contact, discouraging unauthorized entry. The RFID landmine system utilizes radio frequence identification to separate between sanctioned labor force carrying specific markers and implicit pitfalls, widely enabling or disabling the detonator. Completing this, the RFID alarm landmine system emits a loud audible alert upon driving, furnishing an early warning medium. The community of these three layers creates a robust 360- degree, real- time security result able of discovery, assessment, waking, and response against ground pitfalls at fixed spots. This integrated approach enhances security by combining deterrence, controlled access, and early warning capabilities.

1. INTRODUCTION –

A army camp is an arising military installation that supports the military operations of a deployable unit and provides the necessary support and services for nonstop operation that's why Camp security is a member of the Army security system which is grounded on trouble analysis, concerned with defensive procedures and physical way taken to help unauthorized access to outfit, installations, tackle and information, as well as labor force and property, while securing operations from terrorism, sabotage, damage, abuse, and theft. The Camp security program is each about how different rudiments work together to produce a well- rounded approach to security issues. It exemplifies the successful integration of detector technology and RFID tagging for enhanced military protection and underscores the significance of invention in securing our fortified forces. This system offers a comprehensive, 360- degree security in real- time, allowing them to descry, estimate, alert, and respond to ground pitfalls at designated locales. The main thing of a security system for any area and installation, is to ensure a concentrated grounded security. This helps to minimize the pitfalls of sabotage, theft, terrorism, trespass, and other felonious conditioning.

PROBLEM DEFINITION

To develop a system which is able of performing following

Conduct:

1. Full dimension
2. Layered
3. Integration
4. Enduring

2. LITREATURE REVIEW

Researchers [1-2], analyze that how deployed forces rely on efficiently established and operated military camps to extend their operational reach and sustain combat power. However, the challenges of construction, complexities of military camp lifecycle, maintenance, military camp security, harsh environment necessitate through proper planning and resource management to mitigate vulnerabilities, hazards and resource waste to achieve mission success across diverse military operation.

Research [3], based on army tactics techniques and procedures(ATTP)which provides comprehensive guidance for establishing the frame work for robust physical security programs emphasizing the integration of prevention and protection measures and outlining the policies, planes and procedures necessary to enhance the security of personnel, equipment and property, thereby supporting the protection warfighting function through coordinated policies advanced planning and technical solution across diverse operational environments.

Research [4], examines rapidly deployable electronic security system (ESS) for military camps [2014], equipped with advanced electronic security system to enhance perimeter security through integrated deterrence, detection, assessment, delay, response capabilities ensuring robust protection for operation, equipment and personnel across diverse global environments.

Researchers [5-6], observe the functionalities of PIR and ultrasonic sensors, GSM based communication and microcontroller-based technology for military security system. These-study proposes the development of an enhance military security system by utilizing PIR sensors to detect intrusion and GSM technologies to provide robust perimeter security, intrusion detection and autonomous response capabilities, thereby significantly improving safety and operational efficiency through real time detection and user authentication.

Researcher [7], have created an design-aided research and affective design theories to develop an innovative, user-centric fencing system for facility locations delivering a desirable, intuitive and visually appealing solution that simplifies installation and operations without heavy machinery.

Researcher [8,9,10], recognized the RFID tags serves as crucial component contains directional and locational information ensuring precise determination of the user. To address safety concerns RFID tags are shield for protection. While this solution effectively combines internal and external security system technologies. The operational process involves obstacles detection by sensors, standoff distance, activation of buzzers. This technology is used in project to avoid unauthorized access to restrict area, accidental detonation of landmine by friendly forces and enabling targeted detonation against unauthorized threats, early warning of threats. thereby improving perimeter security, reducing collateral damage and advancing strategic defenses capabilities in military operations.

3. BASIC THEORY

3.1 Army Camp Security System

A solid physical security system starts with a strong foundation, where birth security and protection measures are set up. This foundation takes into account original pitfalls, specific vulnerabilities of the point, the number and types of critical means, and the coffers at hand. To tidily avoid the implicit pitfalls, this security system demanded to be adaptable and commensurate to any increases in original pitfalls. Our Camp security system measures correspond of both active and unresistant systems, bias, and security labor force that work together to guard an asset or installation from implicit pitfalls. These systems and measures encompass —

1. Electric Fencing system.
2. Integrated electronic RFID grounded alarm landmine security system.
3. Electronic RFID grounded landmine security system.

3.1.1 High Voltage Electric Fencing System

There are 3 types of fencing are authorized, which are used in protecting restricted areas- chain link, barbed wire, and barbed tape or concertina. The type used for construction depends primarily on the threat and the degree of permanence. It may also depend on the availability of materials and the time available for construction. Fencing may be erected for other uses besides impeding personnel access; it can hindering observation, reduce the effectiveness of standoff-weapon systems, and serve as a barrier to hand-thrown weapons.

Generally, we use Electric fencing which act as a psychological and physical barrier which is used to deter people from crossing boundaries. This system works by delivering a deep, uncomfortable, but generally a non-lethal electric shock when contact is made. This system basically consists of a power generator that converts battery power into very high-voltage pulses, line of current carrying wires that carries the current, and the grounding rods or poles that complete the electrical circuit. When a person touches the wire and is also in contact with the ground, they complete the circuit and receive the shock. The shock is designed to be startling and unpleasant, teaching the subject to avoid future contact. Electric fences are used for security purposes in some commercial and residential settings. The effectiveness of this electric fence relies on proper installation, adequate voltage, and the subject's understanding that contact will result in a repulsive experience.

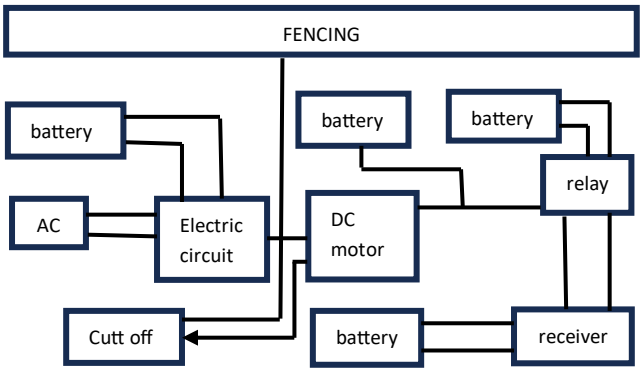

Fig-3.1.1(a): Electric Fencing System

3.1.2 Integrated Electronic RFID landmine security system

While the word "RFID landmine" credibly sounds like an futuristic weapon. It plays very crucial role to understand that current conversations and researches around this concept primarily revolve around upgrading landmine safety and detection, rather than creating a new type of explosive devices.

The combination of Radio Frequency Identification (RFID) technology with landmine is being marked for several potential benefits. One key application is to developing "smart" landmines that can differentiate between friendly forces and external threats. By adjusting authorized personnel with RFID tag, a landmine equipped with an RFID reader could be designed to deactivate landmine when a tagged person approaches it, thus prevent the accidental detonations of landmines. contrarily, the absence of a valid RFID tag could serve as a trigger mechanism.

Besides this, It is important to point that the deployment of such "smart" landmines raise an ethical and practical considerations, such as reliability, security against unauthorized alterations and the capable for unintended consequences. The aim of current research appears to be on capitalizing RFID's identification and tracing capabilities to enhance the safety and management of landmines, rather than creating a new, more dangerous type of explosive.

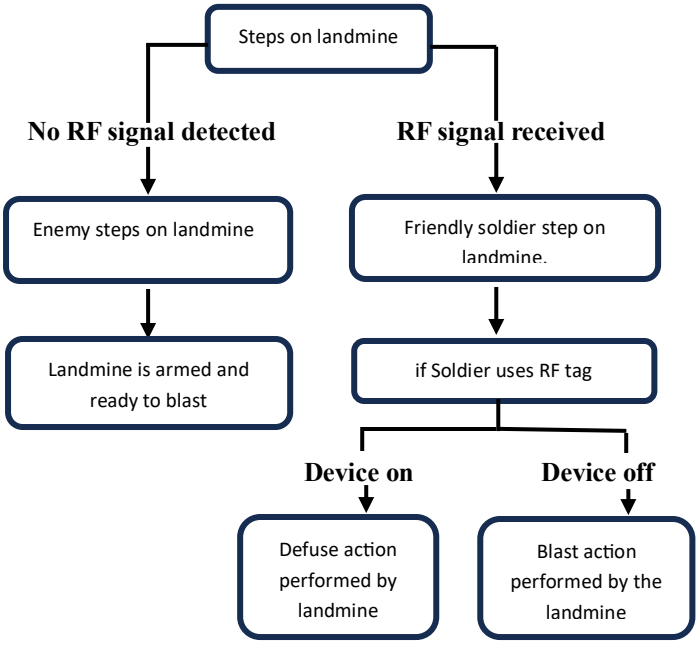

Fig-3.1.2: Flow chart

3.1.3 Integrated Electronic RFID Based Alarm Landmine Security system

An RFID based alarm landmine is a type of landmine that could be designed not to detonate and not to cause immediate destruction, but rather than to emit an loud alarm signal, basically a bang or an piercing whistle, when triggered. The primary purpose of this landmine is to alert patrolling forces to the presence of any dangerous threat or any movement around the restricted area. These devices deliver as an early warning system, which allowing friendly forces for a timely response and conceivably preventing potential threats. While not directly lethal, the sudden and loud noise that can be perplexing and psychologically impactful. RFID based Alarm landmines are employed in conjunction with RFID based landmines and with other security systems to create a layered based defense system. Their use raises ethical considerations, as even non-lethal devices can contribute to a climate of fear and restrict civilian movement in affected areas.

Fig-3.1.3(a): Alarm Landmine

4. METHODOLOGY

1. **Deterrence:** Discouraging potential threats from attacking by increasing their perceived risk of being caught
2. **Detection:** Identify and verify unauthorized activities or intrusions in real-time.
3. **Assessment:** Evaluating the nature, scale, and intent of detected unauthorized activities.
4. **Delay:** Measures implemented to impede an aggressor's progress towards an asset or to protect the asset from threats, categorized as active (triggered) or passive (always in effect).
5. **Response:** Actions taken by personnel to evaluate threats, relay information, and neutralize unauthorized activities, requiring supportive defensive and detection systems.

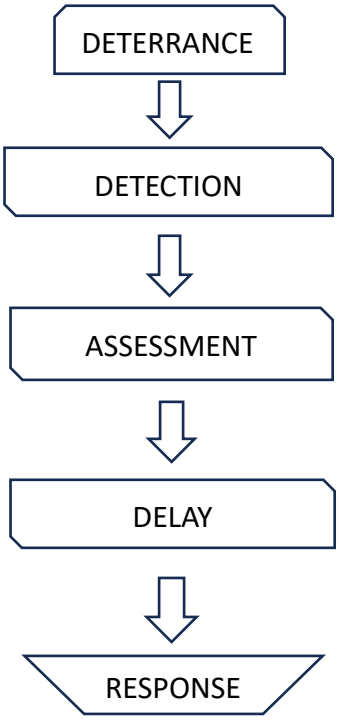

Fig-4: Methodology

5. WORKING

This system based on multilayered security, which have 360-degree, real-time capability to detect, assess, alert, and act against ground threats at fixed sites. The different security layers are as follows-

5.1. High Voltage Electric Fence

The first layer is electric fence, which act as an barrier that uses electric shocks to deter dangerous animal or unauthorized people around the camp. As shown in fig[3.1.1(b)] our electric circuit has contain-

1. **Transformerless Power Supply (Capacitor and Bridge Rectifier):** This stage takes the incoming AC mains voltage and converts it into a low-voltage DC. The capacitor is likely used for capacitive reactance to limit the current (since there's no transformer for voltage step-down and isolation), and the bridge rectifier converts the AC waveform to a pulsating DC.
2. **Oscillator Transistor:** This transistor generates a high-frequency AC signal. This high frequency is crucial because it allows for more efficient voltage multiplication using capacitors and diodes.

3. **Step-Up Transformer, Voltage Multiplier Diodes and Capacitor:** The step-up transformer increases the amplitude of the high-frequency AC signal generated by the oscillator. The voltage multiplier using diodes and capacitors takes the stepped-up AC voltage and further increases the DC voltage to a very high level. Common voltage multiplier circuits include Cockcroft-Walton multipliers. Each stage of the multiplier adds roughly twice the peak AC voltage to the DC output.
4. **High-Voltage Storage Capacitor:** This capacitor stores the high DC voltage generated by the voltage multiplier. It acts as a pool, that collect charge and releasing it in pulses.
5. **Motor, Relay, and Receiver:** This part describe a control mechanism for enabling or disabling the high-voltage output: The receiver detects a signal send by transmitter and transfer This signal to relay which acts as an electrically controlled switch. When the receiver gets the "on" signal, it activates the relay, and relay send this signal to motor which feasibly connects the high-voltage storage capacitor to the fencing circuit. While, when it receives the "off" signal, the relay disassociate the high voltage with help off motor.
6. **On/Off Push Button:** This provides a manual way to trigger the release of the stored high voltage to the fencing, bypassing the remote control system.
7. **Fencing and Electric Shock:** The fencing acts as one terminal of the high-voltage circuit. When an unauthorized being touches the fencing and makes contact with the ground (or another part of the circuit), it completes the electrical circuit. Due to which The high voltage stored in the capacitor has been discharged through the body, causing an electric shock.

2. Electronic RFID landmine security system

The second layer of security contain Integrated Electronic RFID Based Landmine Security system, as shown in above fig[3.1.3(a),3.1.3(b)] this system contain:

How the System Works:

2.1 Army Personnel Approach:

1. The transmitter in the army personnel's shoe comes within range of the mine's receiver.
2. The transmitter activates and sends a signal.
3. The mine's receiver detects this signal.
4. The receiver then turns OFF the relay.
5. The relay, now OFF, turns OFF the pressure switch (presumably by interrupting the circuit controlling it).
6. With the pressure switch OFF, the electrical power to the detonator is cut.
7. Therefore, if the army personnel steps on the mine (activating the pressure switch), the detonator will not receive power and the mine will not explode.

2.2 Terrorist Steps on the Mine:

1. The terrorist's shoe does not have the specific transmitter.
2. The mine's receiver does not receive the activation signal.
3. The relay remains in its default ON state.
4. The pressure switch remains in its default ON state (allowing the flow of electric power).
5. When the terrorist steps on the mine, they activate the pressure switch.
6. Since the pressure switch is ON, the electrical power flows to the detonator.
7. The detonator initiates the explosion.

3. Integrated Electronic RFID Based Alarm Landmine Security system

The Third layer of security contain Integrated Electronic RFID Based Alarm Landmine Security system, as shown in above fig[3.1.3(a)] this system contain:

3.1 Transmitter (Simulated Mine):

1. **Power Source:** Provides the necessary electrical energy to operate the transmitter. This could be a battery.
2. **LEDs:** used as visual indicators – perhaps to show the device is armed, triggered, or has low power.
3. **On/Off Switch:** Allows for activation and deactivation of the simulated mine.
4. **Transmitter (RFID Tag/Beacon):** Emits a radio frequency signal at a specific frequency. This signal carries an identification code.
5. **Pressure Button (Trigger):** When pressure is applied (simulating someone stepping on the mine), it activates the transmitter to send its RFID signal.
6. **Charging Module:** If the power source is a rechargeable battery, this module allows for recharging.

3.2 Receiver (Alert Unit):

1. **Buzzer:** Produces an audible alarm to indicate a potential intrusion.
2. **LEDs:** Likely used as visual indicators – perhaps to show the receiver is active, has received a signal, or has low power.
3. **On/Off Switch:** Allows for activation and deactivation of the receiver unit.
4. **Receiver (RFID Reader):** Constantly listens for RFID signals at the specific frequency emitted by the transmitter. When it gets the correct signal, it triggers the alert.
5. **Power Source:** Provides the necessary electrical energy to operate the receiver. This could be a battery or a wired connection.

How it Works:

1. The transmitter is placed at a designated area and it is turned on.

2. The receiver (alert unit) is positioned at a monitoring location and turned on.

3. When an unauthorized being steps on the pressure button of the RFID alarm landmine mine, it activates the transmitter.

4. Then this transmitter emits an RFID signal with its unique identification code.

5. Further, The receiver detects this specific RFID signal.

6. Once the receiver receives the signal, it activates the buzzer (sound alert) and potentially lights up the LEDs, indicating a potential intrusion.

6. APPLICATIONS OF SMART LANDMINE

1. Used in Armed forces
2. Used In battlefield
3. At military camps for security purposes
4. Used in Borders

7. RESULT AND DISCUSSIONS

1. Advanced technology
2. Improved signature
3. It is more efficient than normal landmine
4. Accuracy is more
5. Enhanced safety
6. Cost savings
7. Neutralizing is easy

8. CONCLUSION

The proposed multi-layered security system, incorporating electric fencing and innovative RFID-based landmine technologies for both deterrence and early warning, represents a significant step towards creating more secure and intelligent army camp defenses. Further research and development focusing on robustness, ethical considerations, and practical implementation will be essential to realize the full potential of these technologies in safeguarding critical assets and personnel.

9. REFRENCES

[1] James H. Raymer and Robert S. Walsh, “base camps”, headquarters department of the army Washington DC-27january 2017.

[2] Mr. Bart Durst* and Ms. Pam Kinnebrew U.S. Army Engineer Research and Development Center Vicksburg, MS 39180-dec 2004.

[3] “Army Tactics, Techniques, and Procedures”, Headquarters Department of the Army Washington, DC, 3 August 2010

[4] Senstar selected to secure NATO’s deployable Military camps-19 june 2015.

[5] Varun Suthar, Darshan Panwar, Varnish v., Varshitha N., Natraj Urs H.D., “Military Base security system using Arduino”, ISSN: 2454-132X (Volume 6, Issue 3) Reva university, Bengaluru - March 2020.

[6] Shanker Bharti, Prof. Anil Khandelwal, Prof. Amit Shrivastav, “Implementation of Military camp security system using GSM, microcontroller and pir sensor, (volume 4, Issue6)-august 2016.

[7] McKinley, Matthew H, “Re- energizing the fence: designing a desirable Electric fence system”, Massey university, New Zealand – June 2009.

[8] Prakhar Pandey, T Dakshayani, Umang S Patre, Himanshu Sahu, “Smart Landmine and restraining shoes”, Department of Electrical and Electronics Engineering, Shri Shankaracharya Technical Campus, Chhattisgarh Swami Vivekanand Technical University (VOLUME 11 Issue V) May 2023.

[9] Rajesh Kumar Patnaik1*, Rakesh Kumar Patnaik*2, N. Nagasai Srinivas*3, Associate Professor, EEE, “smart landmine future of battlefield ”, GMR Institute of Technology1&3, DNR College of Engineering & Technology2-15 Aug 2024.

[10] Milind Yerpude*1, Vinit Nikure*2, Kapil Shahare*3, Harsh Kumbhare*4, Satyam Dangre*5, Himanshu Dhurde*6, Prof. Y.A. Deodhe *7“anti-blast landmine system”, 1,2,3,4,5,6 Student Of Department Of Electronics & Telecommunication Engineering, RTMNU, Priyadarshini J.L.College Of Engineering, Nagpur, Maharashtra India. *7 Professor Of Department Of Electronics & Telecommunication Engineering, RTMNU, Priyadarshini J.L. College Of Engineering, Nagpur Nagpur, Maharashtra India (volume-07) issue-2 February-2025

[11] A. Bartczak, K. Fortuniak , E. Maklewska, E. Obersztyn, M. Olejnik, G. Redlich, “Camouflage as the Additional Form of Protection during Special Operations” , The Institute of Security Technology (Moratex)-July 2009.