



Section 28 16 00 Intrusion Detection

FiberPatrol RAMS (FPRAMS) Remote Alarm Management System Version 3.10

Architectural and Engineering Specifications

TECHNICAL SPECIFICATIONS
DIVISION 28 – ELECTRONIC SAFETY AND SECURITY
SECTION 281600 – INTRUSION DETECTION
PART 2 – PRODUCTS

2.01 GENERAL

- A. All equipments, software and media used shall be standard components, regularly manufactured, and regularly utilized in the manufacturer's system.
- B. All systems and components shall have been thoroughly tested and proven in actual use.
- C. All systems and components shall be provided with the availability of a technical support phone number from the manufacturer. The phone number shall allow for immediate technical assistance for either the dealer/installer or the end user.
- D. All equipment and media shall be provided with an explicit manufacturer warranty.

2.02 SYSTEM DESCRIPTION

- A. The system shall be a network-enabled software platform for security system integration and alarm management.
- B. The system shall promote integration of perimeter intrusion detection and video surveillance across multiple remote sites.
- C. The system shall be built on a client-server architecture model.
- D. The system shall combine automated alarm processing with user-driven site management and remote system administration.
- E. The system shall provide an open interface document for integration with and into other security platforms.
- F. The system shall meet or exceed performance criteria provided by the FiberPatrol Remote Alarm Management System (FPRAMS) as manufactured by Optellios, Inc., 11 Penns Trail, STE 300, Newtown, PA 18940, U.S.A.

2.03 SYSTEM ARCHITECTURE

- A. The system shall include a central server to coordinate system operation.
- B. The central server software shall be based on Microsoft Windows service architecture for unattended operation.
- C. The central server shall maintain a database of configuration information and alarm records.
- D. The system shall include client software enabling operators to interface with the central server.
- E. The client software shall be a Microsoft Windows application with a graphical user interface.
- F. The central server shall be able to advertise its network address to the clients.
- G. The central server shall support multiple simultaneous client connections.
- H. The client software configuration shall control which sites a client can monitor and / or manage.
- I. The client software shall support Microsoft Windows integrated role-based security.
- J. The client software shall be able to automatically reconnect to the central server when network connection is re-established after a disruption.

2.04 SUBMITTALS

- A. System software installation CD

- B. System operation manual
- C. System configuration as-built

2.05 SYSTEM PERFORMANCE

- A. The system shall be capable of automated alarm processing, including
 - 1. Graphical alarm annunciation on site map display.
 - 2. Audible alarm annunciation.
 - 3. Automated alarm recording into alarm database.
 - 4. Activating PTZ presets for one or more cameras associated with the reported alarm location.
 - 5. Displaying on-screen live video from one or more cameras associated with the reported alarm location in client application.
 - 6. Alarm notification to mobile clients via email or text message (SMTP server required).
 - 7. Alarm notification to other alarm management platforms based on supported protocols.
 - 8. Application of zone masking schedules.
- B. The system clients shall provide
 - 1. Graphical representation for each monitored site, containing active links to intrusion detection systems, perimeter detection zones, security cameras and 3rd party sensors.
 - 2. Means to annotate and acknowledge / clear alarms.
 - 3. Multi-camera live security video display on demand with on-screen PTZ controls.
 - 4. Simultaneous multi-camera video playback referenced to past alarms.
 - 5. Alarm database tools for alarm reloading, detail viewing, sorting, grouping, and report generation.
 - 6. Alarm history tools for alarm review and perimeter security assessment.
 - 7. Equipment operating status and network connection status indicators.
 - 8. System configuration tools.
- C. The system clients should provide user authentication including
 - 1. Integrated Microsoft Windows security with support for Windows domain security.
 - 2. Multiple access levels for role-based security administration.
 - 3. Assess rights configuration tools.
 - 4. Operator logon, logoff, and impersonation.

2.06 SYSTEM COMPATIBILITY

- A. The system is compatible with
 - 1. Microsoft Windows XP Pro SP2
 - 2. Microsoft Windows 2003 Server SP1
 - 3. The system requires Microsoft .NET framework 2.0
- B. The system shall be capable of broadcasting alarm information using the following protocols
 - 1. FiberPatrol Alarm Protocol
 - 2. ICD-0100 and ICD-0101 from SEIWG

3. CAP v1.1 and V1.2 from OASIS
- C. The system in its off-the-shelf configuration shall support the following security equipment
1. Standard relay contacts for input and output
 2. Intrusion Detection Systems
 - a. Optellios FiberPatrol
 3. Digital Video Recorders
 - a. American Dynamics Intellex Digital Video Management System
 - b. Integral Technologies MasterControl and DS Xpress Digital Video Solution
 - c. Pelco Digital Video Recorder
 - d. Dedicated Micros Digital Sprite DVR
 - e. Vicon ViconNet Network Video Recorder
 - f. WebGate DS Series DVR
 - g. DVTel Latitude Network Video Management System
 - h. Cisco Broadware
 - i. Honeywell FUSION III
 4. Video Matrix Switchers
 - a. Pelco CM6700
 - b. Pelco CM6800
 - c. Pelco CM9700
 5. IP Cameras
 - a. SONY
 - b. Axis Communication
 6. Alarm Management Platforms
 - a. Lenel OnGuard 5.12.110
 - b. Lenel OnGuard 6.0.148
 - c. Other alarm management platforms via supported standard alarm protocols
- D. The system manufacturer shall have available integration support services for integrating additional and future models of security equipment and communication protocols.

2.07 SYSTEM SERVER

- A. The system server shall include
1. System Server Computer
 2. System Server Database
 3. System Server Services
 4. System Server Service Manager
- B. System server shall support server clustering and replication for high availability.
- C. The system server software shall be pre-installed, configured, and tested by the manufacturer.
- D. The system server software for reinstallation shall be provided on a compact disk.
- E. System Server Computer shall have the following specifications (or equivalent)
1. Hardware Specifications

The contents of this document are subject to change without notice.

- a. Processor: 2.20 GHz AMD Athlon 64 X2 Dual Core
- b. Mother Board: ABIT KN9 ULTRA, 200 MHz Bus Clock
- c. Hard Disk Drive: 74 GB SATA, 10,000 RPM
- d. Memory: 1024 MB, DDR2 533 (PC2 4200) Dual Channel
- e. Display Adapter: Radeon X1650 Series
- f. Network Adapter: NVIDIA nForce GigaBit Networking Controller
- g. Uninterruptible Power Supply recommended

2. Software Specifications

- a. Operating System: Windows XP Pro SP2 or Windows 2003 Server SP1
- b. .NET Framework: V2.0
- c. SQL Server: Microsoft SQL Server 2005 Express

3. Mechanical Specifications

- a. Width: 19 inches (483 mm)
- b. Depth: 19 inches (483 mm)
- c. Height: 3RU (5.25 inches, 133 mm)
- d. Weight: 30 lbs (13.6 kg)

4. Network Specifications

- a. Multicast enabled
- b. ICMP enabled
- c. Static IP address required.
- d. The following TCP-IP ports shall be used by system server
 - i. (optional) 25 notification
 - ii. (optional) 123 time service
 - iii. (reserved) 4120, 4121
 - iv. 4122 alarm proxy
 - v. 4123 camera control
 - vi. 4124 data
 - vii. (optional) 4125 - 4129 protocol translation
 - viii. (reserved) 4130 - 4135

F. System Server Database

- 1. The following database software shall be pre-installed
 - a. Microsoft SQL Server 2005 Express
 - b. Microsoft SQL Server Management Studio Express
- 2. System server database shall be set up using mixed mode security
- 3. System server database shall be pre-configured with information provided by customer, including
 - a. Intrusion Detection System information
 - i. Model and serial number
 - ii. IP address and port
 - iii. Physical location (e.g. GPS) of the unit
 - b. Site perimeter information
 - i. Perimeter definition
 - ii. Perimeter zone definition
 - iii. Perimeter zone status (enabled/disabled)
 - iv. Perimeter zone schedules (optional)
 - v. Zone camera preset assignments (if applicable)
 - c. CCTV system information (if applicable)
 - i. DVR/NVR and camera brands and models

The contents of this document are subject to change without notice.

- ii. IP address, port, and login credentials for DVR/NVR/IP cameras
- iii. Physical locations (e.g. GPS) of security cameras

G. System Server Services

1. The following System Server Services shall be pre-installed
 - a. Alarm Proxy Service (port 4122) for alarm report aggregation, filtering, distribution, and automated alarm processing
 - b. Data Service (port 4124) for database operation and client remote access
 - c. (optional) Camera Service (port 4123) for enabling remote access to serial camera control devices, such as Video Matrix Switchers
 - d. (optional) Relay Service (port 4128) for enabling remote access to contact closure interfaces
 - e. (optional) Notification Service for sending alarm messages via an SMTP server provided by customer
 - f. (optional) Protocol Translation Service (ports 4125-4129) for re-broadcasting alarm reports using 3rd party alarm protocols
 - g. (optional) WMI Service for sending alarm reports via WMI technology
2. All services shall be configured as follows
 - a. Startup Type: Automatically
 - b. Logon Account: NT AUTHORITY\NetworkService
 - c. Recovery: Take No Action for all
 - d. Dependency: Data Service only – SQL Server (SQLEXPRESS)
3. The Camera Service shall require a connection between the system server and Video Matrix Switchers via RS232 serial ports or equivalent.
4. Service events shall be stored in system event log under a dedicated key.
5. Proxy Service shall support alarm zone masking
 - a. Alarm received from the masked zone shall be marked as “Disabled” status
 - b. Alarm received from the masked zone shall not trigger any automated action.
 - c. Alarm zone masking shall support a one-time schedule
 - d. Alarm zone masking shall support the following re-occurring pattern
 1. Daily
 2. Weekly
 3. Monthly
 4. Yearly
 - e. Re-occurring alarm zone masking shall support termination, including
 1. A fixed Date Time
 2. Number of occurrences
 3. Manual termination

H. System Server Service Manager shall enable a system administrator to

1. Start and stop any pre-installed services
2. Configure any pre-installed services, including
 - a. TCP/IP connection Parameters
 - b. Service specific parameters
3. View service event log in real time.
4. View details of any service event
5. Download, view, modify and upload the system database

6. Back up and restore the system database
7. View current client connection status
 - a. Number of active client connections
 - b. Client IP address
 - c. Client security token
8. Enable limited user access using access key-based feature control

2.08 SYSTEM CLIENT

- A. System client shall be a Windows application with a graphical user interface that enables an operator to communicate with the System Server.
- B. System Client software shall be able to operate at any location, provided it has a network connection through the appropriate ports to the System Server and (if applicable) to the CCTV system and / or other integrated components.
- C. System Client software installation
 1. System client software installation shall require the current logon user to have system administrative privilege.
 2. System client software installation shall support Microsoft Windows Installer Engine 3.1 or above.
 3. System Client software shall provide an MSI package for silent installation.
 4. System Client software installation package shall include the Microsoft .NET framework, Microsoft Installation Engine, Video SDK, and other required components.
- D. Recommended Hardware Configuration
 1. Processor: 2.2 GHz or better
 2. Hard Disk Space: minimum 100 MB required for software installation
 3. Memory: 1024 Megabytes Minimum, 2048 MB recommended
 4. Display Adapter: Radeon X1650 Series, 250 MB Video Memory or equivalent recommended
 5. Minimum Display: minimum 1024x768, 1280x1024 or above recommended.
 6. Network: 100 Megabit minimum, Gigabit recommended
- E. Software Specifications
 1. Operating System: Windows XP Professional SP2 or Windows 2003 Server SP1
 2. .NET Framework: V2.0
- F. Computers running system clients shall not run other programs, with the exception of standard anti-virus software from a reputable company. It is recommended that the computer running the system client software be tested for compatibility.
- G. Role-Based Security
 1. Role Based Security shall be based on windows active directory user group.
 2. Role Based Security shall support the following roles, each with its own set of accessible features:
 - a. Administrator
 - b. Supervisor
 - c. Operator

The contents of this document are subject to change without notice.

- d. Guest
 - 3. Role Based Security shall support operator logon, logoff, and impersonation.
 - 4. Role Based Security shall be able to be enabled / disabled by authorized personnel.
 - 5. Role Based Security feature access list shall be configurable.
 - 6. Role Based Security shall support windows domain active directory.
- H. Event Logging
 - 1. System Client shall log events in system event log under a dedicated key.
 - 2. System Client Event Log shall have a maximum log size of 512kB.
 - 3. System Client Event Log shall have a minimum of 7 days entries stored.
- I. System Client shall provide the following features:
 - 1. GPS-enabled interactive perimeter map
 - 2. Remotely add/remove/modified zone masking schedule
 - 3. Role-based security and feature control
 - 4. System event log
 - 5. On-the-map alarm display
 - 6. Audible alarm annunciation
 - 7. Web browser enabled alarm monitoring
 - 8. Remote alarm acknowledgement / clearing
 - 9. Alarm history / assessment tools
 - 10. Alarm report generation
 - 11. Site configuration report generation
 - 12. Sensor status remote monitoring
 - 13. Sensor signal and communication remote monitoring
 - 14. Remote FiberPatrol sensor settings adjustment
 - 15. (Optional) Automated multi-camera preset activation
 - 16. (Optional) Multi-camera live alarm video
 - 17. (Optional) Live video on-demand
 - 18. (Optional) Video referencing, search, and playback
 - 19. (Optional) Universal on-screen camera PTZ control
- J. System client shall be able to automatically reconnect to the system server when network connection is restored following a disruption.
- K. System client shall include a client configuration tool
 - 1. Client configuration tool shall be protected by an access code, which shall be
 - a. saved in a machine-specific encrypted form
 - b. able to be changed by authorized personnel
 - 2. Client configuration tool shall be able to
 - a. Enable/Disable automatic server discovery
 - b. set the IP address and port of the system server
 - c. set which sites this client can monitor/manage
 - d. set default alarm database downloading filter
 - e. enable / disable role-based security
 - f. change feature access list for each role
 - g. set default map and library path
- L. System client shall require a valid license key to communicate with system server
 - 1. A valid license key shall be required for each instance of system client software

The contents of this document are subject to change without notice.

2. A valid license key shall be issued by the manufacturer and shall contains the following information
 - a. License serial number
 - b. Private key for validation
 - c. Licensed customer name
 - d. Client software edition indicator
 - e. Feature control list
 - f. (Optional) trial time period and/or max number of usage
3. A unique valid license key shall be required for a client to communicate with the system server. Concurrent duplicate use of the same license key shall be rejected by the server.

2.10 PRODUCT AVAILABILITY

- A. The system as described herein is manufactured by

Optellios Inc.
11 Penns Trail
STE 300
Newtown, PA 18940
U.S.A.
phone: 267.364.5298
fax: 267.364.5357
email: info@optellios.com

2.11 WARRANTY AND SERVICE

- A. The hardware and media shall be free of defects in workmanship and material under normal operating conditions for a period of one year from the date of shipping.
- B. Any hardware or media shown defective in workmanship or material during the warranty period shall be repaired, replaced or adjusted free of charge.
- C. Local or locally represented service organization shall maintain trained and certified manpower adequate for the service needs of the installed system.
- D. Warranty and general service shall be provided locally by

Optellios Inc.
11 Penns Trail
STE 300
Newtown, PA 18940
U.S.A.
phone: 267.364.5298
fax: 267.364.5357
email: info@optellios.com

END OF SECTION