Exacq Technologies Inc., headquartered in Indianapolis, Indiana, is a leading developer of open architecture, Video Management System (VMS) solutions for security and surveillance applications. Our exacqVision VMS client-server solutions are scalable from a small single camera solution to large scale corporate or campus systems with thousands of cameras. Real-time and recorded video can be viewed, managed and configured from any location on the network.

For additional information, contact:

Exacq Technologies, Inc.
11955 Exit Five Parkway
Fishers, IN 46037 USA
Phone: +1 317 845-5710
Web: www.exacq.com
E-mail: exacqinfo@tycoint.om

STORAGE SEVER SYSTEM MANAGER

DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

28 20 00 Electronic Surveillance

28 23 00 Video Surveillance

28 23 16 Video Surveillance Monitoring and Supervisory Interfaces

Notes to Specifier:

1. Specifiers may alternately wish to include this specification in the following sections:

28 23 13 Video Surveillance Control and Management Systems
28 23 19 Digital Video Recorders and Analog Recording Devices

2. Where several alternative parameters or specifications exist, or where, the specifier has the option of inserting text, such choices are presented in **[bold text].**

3. Explanatory notes and comments are presented in **colored** text.

Important Note to Security Systems Specifiers

CSI MasterFormat 2016 incorporates numerous significant changes affecting electronic safety and security. This document is written to provide flexibility in using either format, although adoption of MasterFormat 2016 is encouraged. The following is a guide to the MasterFormat numbers relevant and related to the product referenced in this specification.

MasterFormat 2014:

27 20 00 Data Communications
28 05 00 Common Work Results for Electronic Safety and Security
28 13 00 Access Control
28 13 16 Access Control Systems and Database Management
28 16 00 Intrusion Detection
28 16 33 Intrusion Detection Control, GUI, and Logic Systems
28 23 00 Video Surveillance
28 23 13 Video Surveillance Control and Management Systems
28 23 16 Video Surveillance Monitoring and Supervisory Interfaces
28 23 19 Digital Video Recorders and Analog Recording Devices
28 23 23 Video Surveillance Systems Infrastructure
28 23 29 Video Surveillance Remote Devices and Sensors

MasterFormat 2016:

27 15 01.xx Video Surveillance Communications Conductors and Cables
27 20 00 Data Communications
28 05 00 Common Work Results for Electronic Safety and Security
28 05 xx Power Sources for Electronic Safety and Security
28 05 xx Servers, Workstations and Storage for Electronic Safety and Security
28 05 xx Storage Appliances for Electronic Safety and Security
28 05 xx.xx Network Video Recorders
28 05 xx Cyber Requirements for Electronic Safety and Security
28 05 xx Communications Equipment for Electronic Safety and Security
28 05 xx Systems Integration and Interconnection Requirements
28 05 xx.xx Electrical
28 05 xx.xx Information
28 10 00 Access Control
28 10 xx Access Control Software
28 20 00 Video Surveillance
28 2x 00 Video Management System
28 30 00 Security Detection, Alarm, and Monitoring
28 3x 00 Intrusion Detection
28 3x xx.xx Intrusion Detection Interfaces to Security Monitoring and Control

STORAGE SERVER SYSTEM MANAGER

1. GENERAL

1.1 SUMMARY

1.1.1. Section includes a software package to continuously monitor the health of digital video storage servers and the cameras connected to them.

1.1.2. Related Requirements

28 23 13 - Video Surveillance Control and Management Systems

28 23 19 - Digital Video Recorders and Analog Recording Devices

28 23 29 - Video Surveillance Remote Devices and Sensors

1.2. REFERENCES

1.2.1. Abbreviations

1.2.1.1. HDD – Hard Disk Drive

1.2.1.2. IP - Internet Protocol

1.2.1.3. LDAP – Lightweight Directory Access Protocol

1.2.1.4. NVR – Network Video Recorder

1.2.1.5. VMS - Video Management System

1.3. SUBMITTALS

1.3.1. Product Data

1.3.1.1. Manufacturer’s printed or electronic data sheets

1.3.1.2. Manufacturer’s installation and operation manuals

END OF SECTION

2. PRODUCTS

2.1. DESCRIPTION

2.1.1. The Storage Server System Manager (“storage manager”) shall be a software package installed on a dedicated server and providing the following functionality for compatible storage servers reachable via Internet Protocol:

2.1.1.1. The system shall provide a browser-based dashboard to view and monitor health and events related to storage servers and the cameras connected to them, including:

2.1.1.1.1. Camera Events

2.1.1.1.1.1. Video loss – Analog or IP video signal lost.

2.1.1.1.1.2. Video Motion – Camera has detected motion.

2.1.1.1.1.3. Camera Disconnected – Network cannot connect to analog or IP camera.

2.1.1.1.1.4. Camera Analytics – An analytics event defined on the camera has been detected.

2.1.1.1.1.5. Recording Alarm – An event that triggers when the system writes the video from a stream to disk.

2.1.1.1.2. Storage Server Events

2.1.1.1.2.1. Security Integration Connection Alarm – An error in connecting to the Security Integration panel.

2.1.1.1.2.2. Archive Alarm – Failure on archiving target, such as bad mount point.

2.1.1.1.2.3. Archive Task Alarm – Archive task failed.

2.1.1.1.2.4. Auto Export – A user exported video from the server using the exacqVision client.

2.1.1.1.2.5. Button Press – Button input on server pressed.

2.1.1.1.2.6. Content Age Alarm – Video deleted before configured retention period

2.1.1.1.2.7. Core Throttling – Server load requires that video frames be discarded to compensate.

2.1.1.1.2.8. Device Failure – Capture card malfunctioned.

2.1.1.1.2.9. Device Temperature - Capture card temperature not within recommended range

2.1.1.1.2.10. Fan Alarm – Fan has failed on capture board.

2.1.1.1.2.11. Fan Speed Sensor Alarm – System fan not operating at recommended speed.

2.1.1.1.2.12. Input Trigger – Discrete input on a hybrid server (or IP camera with alarm input) activated.

2.1.1.1.2.13. Login Failure – Login attempt failed on server.

2.1.1.1.2.14. Network Activity – Any unexpected network activity on the server’s network.

2.1.1.1.2.15. Power Supply Alarm – Alarm on a server with redundant power supply.

2.1.1.1.2.16. Server Disconnected – Connection to server lost

2.1.1.1.2.17. Server License Error – Invalid license on server

2.1.1.1.2.18. Server License Warning – License will expire in less than 30 days

2.1.1.1.2.19. Soft Trigger – Signal sent from Client to server

2.1.1.1.2.20. Storage Alarm – Drive capacity threshold reached

2.1.1.1.2.21. Storage Hardware Alarm – Server storage malfunctioned

2.1.1.1.2.22. Temperature Sensor Alarm – System temperature not within recommended range

2.1.1.1.2.23. UART Serial Disconnected – A UART serial port is disconnected.

2.1.1.1.2.24. Update Downloading – Software update download in progress.

2.1.1.1.2.25. Update Failure – Server software update failed.

2.1.1.1.2.26. Update Installing – Server software update installing.

2.1.1.1.2.27. Update Pending – Server restarting after software update.

2.1.1.1.2.28. Update Success – Server software update completed.

2.1.1.1.2.29. Voltage Sensor Alarm – System voltage not in recommended range.

2.1.1.1.2.30. Security Integration Health – An intrusion panel that has a health condition active for the device.

2.1.1.2. Provides e-mail notifications of user selected system events and conditions in real time or batch fashion.

2.1.1.2.1. System provides e-mail verification to an e-mail address.

2.1.1.3. Provides a configurable schedule to perform server tasks.

2.1.1.3.1. Schedule server software updates.

2.1.1.3.2. Schedule server configuration backup from a single server or in bulk.

2.1.1.3.3. Schedule server configuration restoration from a single server or in bulk.

2.1.1.3.4. Schedule maintenance for a server or multiple servers.

2.1.1.3.5. Import a license to a server or multiple servers.

2.1.1.4. The system shall allow the configuration of servers for failover.

2.1.1.4.1. Server may be configured as a spare.

2.1.1.4.2. Spare server may be added to a Failover Group.

2.1.1.4.3. Failover Group will include servers covered by the spare to failover to in the case of failure.

2.1.1.4.4. On server recovery, the spare shall failback and return to spare status.

2.1.1.5. The system shall allow the configuration of user and server groups, consisting of monitored systems with identical settings of monitored features.

2.1.1.5.1. Servers may be discovered on the network.

2.1.1.5.2. Servers may be added in bulk.

2.1.1.6. The system shall allow the configuration of users and user groups from an Active Directory or LDAP source.

2.1.1.7. The system shall allow for camera inspection.

2.1.1.7.1. The system shall allow an image from a camera connected to a monitored server to be stored as the reference image.

2.1.1.7.2. The system shall compare a reference image to a current image on demand.

2.1.1.7.3. The system shall allow images that are dissimilar to the reference image to be marked as “bad” until changed and marked as “good”.

2.1.1.8. The system shall allow for password strengthening.

2.1.1.9. Provides color coded status of servers, cameras, and unacknowledged events in the following categories in list or chart format:

2.1.1.9.1. Critical

2.1.1.9.1.1. Server or camera device not detected.

2.1.1.9.1.2. Event occurring and unacknowledged.

2.1.1.9.2. Warning

2.1.1.9.2.1. Health warning on server (such as temperature, storage alarm, archive alarm, CPU fan)

2.1.1.9.2.2. Server license subscription expiring soon

2.1.1.9.2.3. Event unacknowledged but open

2.1.1.9.2.4. Event unacknowledged but closed

2.1.1.9.3. Normal

2.1.1.9.3.1. Server or camera connected and operating

2.1.1.9.3.2. Event acknowledged and closed

2.1.1.10. Allows creation of reports to:

2.1.1.10.1. View and manage a list of unacknowledged events.

2.1.1.10.2. View a list of open events.

2.1.1.10.3. Search for specific events based on various criteria.

2.1.1.11. Allows events to be searched based on various criteria, including event time, event type, and associated cameras and servers.

2.1.1.12. Permits viewing of server licenses.

2.1.2. Database compatibility

2.1.2.1. Postgre

2.1.2.2. Microsoft SQL

2.1.3. The system shall support the following browsers:

2.1.3.1. Microsoft Edge 44 and later

2.1.3.2. Chrome 83 and later

2.1.3.3. Safari 13 and later

2.1.3.4. Mozilla Firefox 76 and later

2.1.4. The system shall operate on all the following operating systems:

2.1.4.1. Windows 10

2.1.4.2. Windows Server 2016

2.1.4.3. Ubuntu Linux 18.04

2.1.5. The system shall run as a service. The system manager shall not require any application to be running to operate.

2.1.5.1. The system shall run on a mobile application at no additional cost.

2.2. HARDWARE REQUIREMENTS

2.2.1. Storage Manager Server

2.2.1.1. The storage manager shall operate on the following minimum requirements:

2.2.1.1.1. Processor: Gen 7 Intel® Core i5

2.2.1.1.2. RAM: 8GB

2.2.1.1.3. Hard drive: 128GB SSD

2.2.1.1.4. Network: 2 x 1 Gbps

2.2.1.1.5. Operating system: Windows 10 or Server 2016 or Ubuntu Linux 18.04

Note: The above minimum requirements are for less than 50 servers, with up to five simultaneous client connections. The following is recommended for larger installations. This configuration will accommodate 500 or more servers, with up to 25 simultaneous client connections:

Processor: Gen 7 Intel® Xeon® E3 Xeon or better

RAM: 16GB

Hard drive: 250GB SSD

Network: 2 x 1 Gbps

Operating system: Windows Server 2016 or Ubuntu Linux 18.04

Email host: SMTP email server

2.2.2. Client PC

2.2.2.1. Minimum requirements

2.2.2.1.1. Processor: Gen 7 Intel® Core i3

2.2.2.1.2. RAM: 4 GB

2.2.2.1.3. Network: 1 x 1 Gbps

2.2.2.1.4. Browser: Microsoft Edge 44, Chrome 83, Safari 13, Mozilla Firefox 76

END OF SECTION

PART 3 EXECUTION

3.01 INSTALLERS

A. Contractor shall comply with all Manufacturer installation guidelines.

B. Contractor personnel shall comply with all applicable state and local licensing requirements.

3.02 STORAGE

A. Hardware shall be stored in an environment where temperature and humidity are in the range specified by the hardware manufacturer.

END OF SECTION