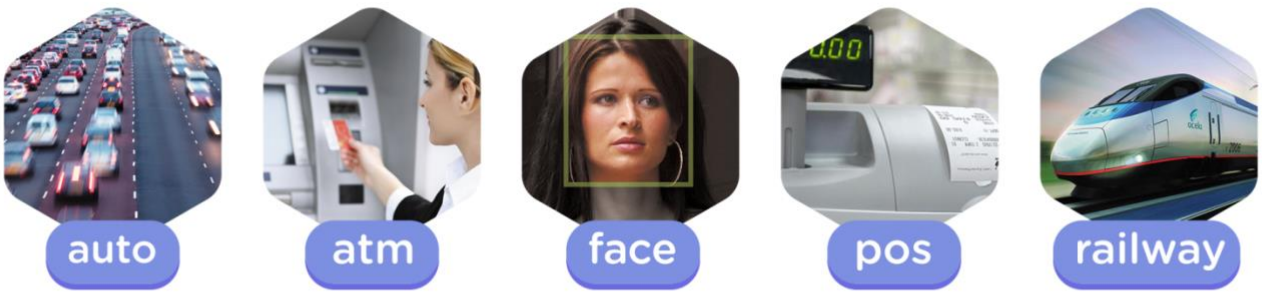
Intellect
PSIM Software

Specifications

Product version 4.11.1

Document version 2.3



CONTENTS

1 Data Sheet

Functionality	Axxon Intellect Enterprise
Total number of servers in the distributed system	Unlimited
Total number of cameras in the system	Unlimited
Total number of cameras per server	Unlimited
Total number of audio channels in the system	Unlimited
Total number of audio channels per server	Unlimited
Number of remote clients	Unlimited
Number of servers which simultaneously transmit video images to a client	Unlimited
Number of camera views displayed simultaneously on a client's screen	Unlimited
Number of PTZ devices used	Unlimited
x64 version	Available for video.run and vmda.run
Synchronous playback of video footage by several cameras	+
Playback with fast or slow motion in forward or reverse	+
Video compression algorithms	• MJPEG • Motion Wavelet
Video decompression algorithms	• MJPEG • Mpeg4 • H.264 • H.264 SVC • H.265 • Motion Wavelet • Mxpeg
Video export	• AVI
Frame export	• JPEG • BMP
Available video image resolutions	Resolutions supported by the video cameras
Hardware video decompression	Nvidia CUDA
Taking video directly from a camera for	+
Multi-streaming support	+
Stream selection for archive recording including different streams for alarm recording and continuous recording	+
Stream selection for analytics	+
Green Stream	+
Archive size	Unlimited

Archive depth limitation	+
SolidStore file system	+
Network archiving support	+
Edge storage support	+
Backup Archiving	+
I/O management	+
Webserver Monitoring	+
Web reports service	+
Failover functionality	+
Health check functionality	+
System restart service	+
LDAP support and Active Directory support	+
Micro-module architecture	+
Alarms notifications	• Sound • Phone • E-mail • SMS
User management	Multilevel access to system
Events online protocol	+
Macros (event management)	Fully featured event management
Scripts (advanced scenario responses)	+
Schedules	+
Interactive and multi-layer map	+
Scene (frame merge)	+
Base video analytics	• Motion detection • Changed background • Blind detection • Tampering detection • Image quality loss • Abandoned object • Face capture
Advanced video analytics	• Line crossing • Motion in the area of interest • Loitering • Entrance to the area of interest • Exit from the area of interest • Object appearance in the area of interest • Object disappearance in the area of interest • Stop in the area of interest • Abandoned object
Embedded video cameras analytics	+
Base audio detection	• Noise detection • Signal detection
Two-way audio	+
Advanced audio detection (Audio-analytics)	• Car alarm detection • Glass breakage detection • Aggression detection
Forensic Search	+
Fisheye video dewarping	+

Video capture cards support	• FS series • FX series • WS series • Stretch series
IP device support	IP cameras and IP video servers from various manufacturers— more than 8000 devices.
Onvif support	• Profile G • Profile S • Profile T
Automated device discovery	+
POS integration	• Event database integration • Title view • Title search
Integration with access control and fire alarm systems	++
Face recognition	+
LPR recognition	+
Traffic control	+
4-eyes rule for authentication	+
iOS, Android and Windows client	+
API/SDK	IIDK

2 General SMP description

The Security Management Platform, or SMP, is designed for the deployment of industrial scalable, flexible (adaptable) integrated security systems, based on digital video surveillance and audio monitoring systems.

The SMP shall have the following core functionality:

1. Integration of digital video surveillance and audio monitoring systems with existing data systems, various security equipment, and auxiliary software of other developers, using integrated open interfaces for data exchange.
2. Compatibility with diverse security hardware and data systems, in particular: fire and security alarm and access control systems, video cameras, data analysis systems, and video analytics systems for tracking and recognition of objects (events).
3. Single-source registration and processing of events plus generation of notifications and system responses based on flexible macros.
4. Open programming platform that allows integration with necessary applications through an SDK and complete control over all parts of the subsystem, as well as handling events and sending commands (reactions).
5. Single-source registration and processing of events received from subsystems, plus generation of notifications and system responses based on flexible macros for subsystem reactions.
6. Unlimited capacity for scaling, task-based customization, and reallocation of resources in the event of changes in the number or quality of monitoring tasks with diverse hardware at guarded sites.
7. Support for failover clusters, that ensures the system's operability if a core subsystem component fails.

8. Remote interaction between core components of the subsystem, with automatic replication of internal databases (containing system configuration settings and data about events recorded in the system) that are part of the SMP.
9. Creation of a single, central database of system settings.
10. Software and hardware monitoring of the functioning of the system's central components.
11. Multilevel hierarchical mapping of the guarded site on an interactive map, to provide:
    11.1. Automatic switching and recursive search for relationships on the map
    11.2. Active graphical representations of devices, allowing for device control via a functional shortcut menu
12. Event log maintenance
13. Support for generating reports based on events
14. Automatic notifications by:
    14.1. SMS (Short Message Service)
    14.2. Email
    14.3. V-dial auto dialing service
    14.4. Audible/voice notification
15. Centralized administration (Administrator Workstation) of system components and user rights/privileges.
16. The system shall be fault-tolerant: if one or more main servers becomes inoperative, the configuration shall be temporarily transferred to a backup server.
17. The system shall be highly configurable, allowing for the basic functionality of the SMP to be expanded by means of custom programs and macros.
18. It shall be possible to switch the localization language of the system interface.
19. Modules developed specially for 64-bit operating systems shall be supported.
20. Authentication Support with Kerberos and SAML

3 Main SMP components

The SMP shall consist of the following core components:

1. Video/audio surveillance subsystem
2. Monitoring and access control subsystem
3. Fire and intrusion alarm subsystem
4. Perimeter security subsystem
5. POS (monitoring of cash desk transactions) subsystem
6. Recognition of vehicle license plate numbers
7. Facial recognition and search subsystem
8. Subsystem for recognition of registration numbers on rail cars and tank cars
9. ATM Protection Subsystem
10. Event Manager/Protoidentification Subsystem
11. Time and Attendance Subsystem
12. Access Manager/Visitor Management Subsystem
13. Web Report Subsystem

4 SMP software database

1. The internal database of SMP server components (servers and administrator workstations) shall be maintained in MS SQL Server 2008 R2, MS SQL Server 2012, MS SQL Server 2014, MS SQL Server 2016, MS SQL Server 2017 format;
2. The SMP database must support the following:
    2.1. Saving data on registered system objects and their settings
    2.2. Saving data on the accounts of departments and users, and on user privileges
    2.3. Saving data on registered system events
    2.4. Saving data on changes in the hardware and software configuration of the SMP
    2.5. Saving data on changes in the list of registered system object and their settings

2.6. Saving data on network names and IP addresses of SMP components and settings for their interaction

2.7. Replicating data stored on different system components

3. The database shall allow synchronizing databases of SMP server components (database synchronization shall allow storing data either centrally, on a single server component, or in a distributed manner, with replication of data from the databases of different SMP server components). Database synchronization shall provide parallel operation with server databases and automatic updating of them after they are modified.
4. A separate database of video captions should be maintained with loop recording.

5 Basis of SMP component licensing

1. Software licensing shall be implemented in hardware and in software.
2. The hardware component of DRM (digital rights management) shall be based on one of the following:

   2.1. Dallas codes from video card cryptochips

   2.2. Dallas codes from Guardant dongle drivers

   2.3. Hardware ID keys
3. When HID-based DRM is used, it shall be possible to change portions of the computer's hardware without breaking license support. The following hardware shall be coded into the license parameters:

   3.1. Motherboard

   3.2. CPU

   3.3. HDD

   3.4. RAM

   3.5. GPU

   3.6. NIC

4. The software component of DRM shall include an activation code, which shall link the hardware component of DRM with the software: The software functionality that is available for use shall depend on the configuration of the SMP installation, and shall be encoded in the activation key.
5. When extending SMP configuration (for example, when installing a new functional subsystem), the activation key must be replaced with a new one (corresponding to the updated SMP functionality) to activate the newly installed subsystem.
6. In a distributed system, a single activation key is used for all computers in the system.
7. If there is no key file SMP shall operate in demo mode within two month since the intellect.exe file creation date, from 8 AM till 12 midnight. An inscription showing that the system is running in demo mode is to be displayed in the splash screen on system start-up as well as in the information window of the Main control panel.

6 SMP components

a. Main components of the video/audio surveillance subsystem:

The video/audio surveillance subsystem shall consist of the following core components:

1. Server
2. Administrator workstation
3. Client Workstation

b. Optional components of the video/audio surveillance subsystem:

1. Videogate
2. Archive Server
3. Web Server
4. RTSP Server

5. Failover Server
6. ONVIF Server
7. RS-RTP Server
8. Data gate

c. Server

1. The Server shall receive and process video signals arriving from analog and IP video cameras. It provides several options: audio signal receipt and processing, PTZ unit control, security services, and custom auto functions (macro commands and scripts).
2. The Server shall record video through Motion Wavelet, Motion JPEG, MPEG-4, H.264 and H.265 video compression, in the following modes:
    2.1. continuously
    2.2. real time (for specified events)
    2.3. alarm recording triggered by an alarm event or by the Operator's command, with pre-history/post-history (pre-event recording/post-event recording) support
3. The Server shall support the ONVIF standard.
4. The Server shall support recording video archives to local disks.
5. The Server shall support recording video archives to network disks.
6. The Server shall support recording video archives to USB drives.
7. The Server shall guarantee the capacity to compress camera video streams for storage on the Archive Server (intra-frame coding for Motion Wavelet and MJPEG and inter-frame coding for H.264, H.265 and MPEG4).
8. The Server shall allow Clients to view video recordings, with support for searching the video archive by time, event, and video camera;
9. The Server shall allow Clients to view recorded video from multiple video cameras simultaneously;
10. The Server shall measure the recording time of archive video.

11. The Server shall be able to perform Motion Wavelet or MJPEG compression of video when serving data to a Videogate or Video Surveillance Monitor.
12. The Server shall be able to perform multistreaming, i.e., process multiple video streams from cameras and then use different video streams to record video to archives constantly or by alarm triggering, to display video on a Video Surveillance Monitor and to send video to remote clients.
13. In a distributed system, the Server shall be able to synchronize the system time with the synchronization source in the distributed system or be able to itself serve as the synchronization source.
14. The Server shall allow selecting the video stream to be displayed on the Video Surveillance Monitor based on the resolution that is requested by the Monitor.
15. Server must be enabled to show the current disk for storing archive.
16. Server shall provide interaction with *Manitou* software.
17. The server must provide interaction with *VideoIntellect* software: sending video to *VideoIntellect* software via RTSP and receiving video stream analysis results from *VideoIntellect* software.

d. Administrator workstation

1. The administrator workstation shall perform VMS remote administration functions, as well as administration for specialized platforms: The Videogate, remote Archive Server, Web Server, Logging Server, and administrator workstation shall perform one or more of the above-listed functions simultaneously.
2. The administrator workstation shall allow for processing audio and video received from IP devices.

e. Videogate

1. The Videogate shall route video signals between Servers and Clients located in different subnets.
2. The Videogate shall allow for multisequencing Client-requested video streams.

3. The Videogate shall allow for video compression (intra-frame coding for Motion Wavelet and MJPEG and inter-frame coding for H.264, H.265 and MPEG4).
4. The Videogate shall monitor the bit rate of video stream transmission over the local network from the Server to the Videogate, with display of a warning on the Client workstation if the streaming bandwidth falls.
5. The Videogate shall provide for archiving of the video streams that pass over it:
   5.1. Recording the archive of video streams which are recorded on the Server.
   5.2. Recording the archive of all video streams.
   5.3. Recording only the video streams requested from the Clients.
6. The Videogate shall support receiving/transmitting video streams to another Videogate or Archive Server.
7. The Videogate shall compress video streaming to the Video Surveillance Monitor by means of the Motion Wavelet and MJPEG codecs. It shall be possible to keep original video format. Compression shall be performed at the side of a video source.

f. Archive Server

1. The Archive Server shall create backup copies of video recordings, from the main Server archive onto other disks.
2. The Archive Server shall support recording video archives to local disks.
3. Encryption on recorded/archived video with Advanced Encryption Standard (AES128)
4. The Archive Server shall support recording video archives to network drives.
5. The Archive Server shall support recording video archives to USB drives.
6. The Server shall guarantee the capacity to compress camera video streams for storage on the Archive Server (intra-frame coding for Motion Wavelet and MJPEG and inter-frame coding for H.264 and MPEG4).
7. The Archive Server shall adjust the bit rate of data transmission over the local network.
8. The Archive Server shall set the frequency of backups of the video archive.

9. The Archive Server shall support loop recording of data to connected drives.
10. The Archive Server shall support video archive viewing from Client VMS workstations.
11. The Archive Server shall control the backup process in two ways:

11.1. Manually using special interface objects.

11.2. Automatically, by using the software's built-in programming capabilities (time periods, macros, and scripts).

12. The Archive Server shall request data from the Server regarding archive indexes every 30 seconds to ensure steady video archive backups.
13. The Archive Server shall be able to create an archive backup from another Archive Server, thus ensuring multilevel backup (for example, level 1: the Archive Server stores 25 fps for 30 days, level 2: Archive Server No. 1 stores 12 fps for 60 days, level 3: Archive Server No. 2 stores 1 fps for 180 days).
14. The Archive Server shall be able to receive a video stream from the Videogate.
15. The Archive Server shall be able to manage local network bandwidth consumption.
16. The Archive Server shall compress the video stream when writing to archives by means of the Motion Wavelet and MJPEG codecs. Compression shall be performed at the side of the Archive Server.
17. The Archive Service shall support recording audio in sync with video.

g. Web Server

1. The Web Server shall allow Clients to perform video surveillance through an Internet browser over TCP/IP.
2. The Web Server shall provide the following HTTP server functionality:

2.1. Access control through authorization.

2.2. Working as a gate for transferring video data using HTTP protocol.

2.3. Video monitoring and camera control through a web browser over TCP/IP.

2.4. Control of camera movement through a web browser over TCP/IP.

2.5. Setting the layout of Video Tiles: 1, 4, 6, 9 tiles per screen.

2.6. Viewing the archives stored on the Server for each camera, through the Client Video Surveillance Monitor.

2.7. Limiting access rights for viewing the video feed from the cameras, controlling camera movement, and viewing Server archives.

2.8. Displaying the video signal parameters (frame rate (fps) and frame size (KB) in the Video Surveillance Monitor.

3. Web server must perform functions of HTTPS server.
4. The Web Server shall act as a Mobile Server so that mobile devices running on iOS can access video surveillance functions.
5. The web server surveillance monitor shall be placed on an HTML page.
6. The Video Surveillance Monitor and control elements for video cameras and PTZ units shall be driven by a Java applet for display in an Internet browser.
7. The Web Server shall require that users perform authentication when connecting.
8. The Web Server shall support user login via Windows account credentials.
9. The Web Server shall allow configuration of a port number for connecting to the HTTP Server.
10. The Web Server shall allow configuration of a maximum number of simultaneous connections to the HTTP Server.
11. The Web Server shall support listening via web browser to the audio signal from microphones that are connected to Cameras.
12. Web server supports video stream pruning when the bandwidth between the Client and Web server is not enough.
13. Web server supports transmitting and receiving audio signals to and from iOS mobile clients.
14. Web server supports user rights differentiation, i.e. the user is not allowed to watch video from cameras he has no access to.

15. The surveillance monitor of Web server must support viewing the server archive, the backup archive as well as the video gate archive by administrator's choice.
16. Web server must not allow controlling camera from the surveillance monitor of Web server regardless of user rights.
17. Web server must enable configuration of video stream to be displayed in the surveillance monitor of Web server.

h. RTSP Server

1. RTSP Server must be able to send video (with or without sound) to the Clients via the RTSP protocol:
   1.1. Live video.
   1.2. Server archive.
   1.3. Videogate archive.
   1.4. Long-term archive.
2. The RTSP Server shall allow for splitting the transmitted signal between different RTSP ports.
3. The RTSP Server shall allow transmitting video in Multicast mode with or without authorisation.
4. The transmitted video stream is to be compressed using the H.264, H.265, MPEG4 or MJPEG codec.
5. RTSP Server must support video acquisition via the Videogate.
6. RTSP Server must be able to send subtitles added to the video by the integrated security system.
7. RTSP Server must support the compatibility mode with VLC Media Player.
8. The RTSP Server must support selection of the network interface that is to be used to broadcast RTSP Server.

i. Failover Server

1. The Failover Server shall ensure that the distributed system works without downtime.

2. If communication is lost with a Server of the distributed system, this mode shall ensure that the configuration created on the server is transferred to a Failover Server.
3. When communication is restored, the configuration shall be restored on the main Server.
9. The Failover Server shall support recording to video archives on local disks.
10. The Failover Server shall support recording to video archives on network disks.
11. The Failover Server shall support recording to video archives on USB drives.
12. SMP shall allow limitation for number of failovers running simultaneously.

j. ONVIF Server

1. ONVIF Server must support transferring (via the ONVIF protocol) of live and archive video that is to be received on Clients with the option to listen to audio, playback embedded archive, control PTZ, transfer metadata, support sensors and relays.
2. ONVIF Server must support transferring of video data via ONVIF2.X in the H.264, H.265, MJPEG and MPEG4 formats.
3. ONVIF Server must support Digest authentication.
4. ONVIF Server must support TopicFilter for sent messages.
5. ONVIF Server must support Message Content Filter for sent messages.
6. ONVIF Server must support metadata transferring.
7. ONVIF Server must support filtering events in the metadata stream the same way as filtering sent messages.
8. ONVIF Server must support ONVIF ImagingService.
9. ONVIF Server must support transferring of the archive from the embedded storage of IP devices.
10. ONVIF Server must support operation in the multistream mode.

k. RS-RTP Server

1. The RS-RTP Server must allow the third-party software controlling cameras, PTZ, sensors and relays configured in SMP via the GB28181 protocol.

2. The RS-RTP Server must allow the third-party software viewing live and archive video.

3. The RS-RTP server must restrict access to the functions mentioned above depending on the user rights.

l. Data gateway

1. The data gateway must provide routing of data transferred between Servers and Clients located in different subnets.

m. Client Workstation

1. Client Workstations are used as operator workstations and shall provide remote video surveillance and audio monitoring: video and audio monitoring, sensor status control, control of cameras and PTZ units, etc.

7 SMP component interaction

1. Interaction between SMP components shall be configurable.
2. Database replication and event exchange must be supported.
3. SMP component interaction must be configurable from the administrator's workstation.

8 Core user functions (configurable by the administrator) to be performed by the video/audio surveillance subsystem:

Core user functions (configurable by the administrator) that the video/audio surveillance subsystem shall perform:

1. Video surveillance functionality
2. Audio monitoring functionality
3. Mapping guarded objects
4. Event registration functionality

5. Notification functionality
6. System health monitoring
7. Management functionality
8. Integration of the distributed video surveillance and audio monitoring system

a. Video surveillance functionality

1. Display of video from multiple cameras (from one or more Servers) simultaneously in a split-screen image displayed on a single monitor (display).
2. An appropriate video stream for display in the Video Surveillance Monitor shall be automatically requested from the server based on the size of the video in the Video Surveillance Monitor (Green Stream).
3. Prioritized automatic selection of displayed video images from alarm or active cameras to bring the required scenes into Operator focus (selection of images depending on set parameters).
4. Configuration of number of Viewing Tiles and their layouts. Shall support the following layouts: 1x1, 2x2, 3x3, 4x4, 5x5, 6x6, 7x7, etc.
5. Priority camera window magnification (Video Tile), magnified Viewing Tiles slideshow option for a selected camera.
6. Color-coding a Viewing Tile (camera window) to indicate its status: “armed”, “alarm”, “recording”, etc.
7. Remote access to audiovisual streams from any workstation, with both local and remote archive recording options.
8. Video recording can be performed:
   8.1. Continuously (extended recording)
   8.2. Real time (for specified events)

8.3. On alarm or by Operator’s command with a pre-event (pre-history) recording option

9. Pre-event video recording
10. Freeze-frame by Operator’s command selection plus viewing snapshots without interruption of recording
11. Display of information in the Video Surveillance Monitor window
    11.1. Current time
    11.2. Current date
    11.3. Camera No (ID)
12. On-demand video recording
13. Real time viewing of images from video cameras
14. Priority-oriented viewing of critical video stream based on alarm detection
15. Web interface-based surveillance
16. Audio- and video-archive management
17. Viewing of recorded video with search and retrieve options (time/event type/camera ID criteria)
18. Synchronized playback of footage recorded by multiple cameras
19. Recorded time calculation
20. Timestamp-based footage search
21. Video image processing:
    21.1. Digital zooming
    21.2. Contrast adjustment
    21.3. Image sharpening
    21.4. Masking
    21.5. Dynamic outlining
    21.6. Deinterlacing
    21.7. Rotation by a predetermined angle of 90, 180 or 270 degrees.

22. Management of end devices using:
    22.1. Third-party programmable interface panel
    22.2. Universal control panel for end devices;
    22.3. Mouse control device
    22.4. Joystick control device
23. Viewing on all workstations of video footage from all System servers over TCP/IP
24. Storage and export of single frames and video sequences
25. Integrated use of various types of multi-zone detection tools:
    25.1. Main motion detection tool
    25.2. Motion
    25.3. Focus loss
    25.4. Video signal stability
    25.5. Background change
    25.6. Camera blinding
    25.7. Camera blocking
    25.8. Abandoned items
    25.9. InfraredFace detection
26. Detection zone(s) masking
27. Pixelation of face/privacy masking in video footage.
28. Adjustable privacy masking (permanent/removable) and masking color (from light grey to black) which allows the administrator to mask certain camera areas in any moment and for all users with the option to temporarily remove them
29. Image de-interlacing
30. Analog video-signal output
31. Deletion of video from the archive through the Video Surveillance Monitor interface.
32. Recorded/exported video signature with the hashing protocol hashing SHA-2
33. Display dewarped video from fisheye cameras.

34. It shall be possible to get video stream directly from the camera while displaying video signal on Video Surveillance Monitor. If camera operates in multistreaming mode (including multicast transmission of video streams), it shall be possible to choose a required video stream for display.

b. Audio Monitoring Functionality

1. Audio monitoring
2. Audio and video synchro recording
3. Sound-activated audio recording
4. Manually activated audio recording
5. Export of audio recordings

c. Mapping guarded objects

1. Guarded object virtual subdividing.
2. Multilevel hierarchical object mapping to obtain:
   2.1. Automatic switching and recursive layer/relationship search
   2.2. Graphical representation of active objects on the map (on different levels) for simple device control via the functional shortcut menu.

d. Event registration functionality

1. Support maintenance of an event log.
2. Warn the operator about alarms in an alarm window, which opens above all other windows in case of an alarm event on a specified device.

e. Notification functionality

1. Automatic notification using:

1.1. SMS (Short Message Service). SMS is used for sending short messages to cell phones about alarm events registered by the subsystem. A short message shall be sent automatically upon registration in the subsystem of any of the events specified in the corresponding macro.

1.2. Email. The Email Message Service (Email) is used for sending email messages about alarm events registered by the subsystem to remote system users. An email shall be sent automatically upon registration in the subsystem of any of the events specified in the corresponding macro.

1.3. V-dial auto dialing service. The Voice Message Service shall transmit voice messages over telephone lines. The Service shall automatically dial up the specified phone numbers and play the audio files. The following dialing options shall be available: “until connection”, “until answer”, “until digital acknowledgment of message reception”.

1.4. Audible/voice notification. The voice notification service shall be used for audio notification of Operators of a VMS about the alarm events registered at the site. This service shall allow voice notification of remote workstations through the following devices: Headphones (speakers) connected to a sound card or IP device. The service shall provide automatic transmission of the voice notification to the specified device IP address and perform audio file playback.

1.5. SNMP Service. Shall allow creating an SNMP service for forwarding messages about messages recorded in the subsystem to the SNMP agent. This ability shall be implemented through the use of an SNMP Trap system object.

1.6. The SNMP Service shall:

1.6.1. Receive messages about events registered in the subsystem

1.6.2. Convert messages regarding events into SNMP format

1.6.3. Transmit messages in SNMP format (SNTP Trap) over TCP/IP to the SNMP agent

1.7. BACnet Service. It shall be possible to send information to third party systems via BACnet.

f. SMP healthmonitoring

The SMP shall implement the following methods for monitoring system health:

1. Software monitoring of operability/uptime
   1.1. Restarting a module if no response is received from the module
   1.2. Restarting the core if no response is received from the module
2. Watchdog - a device used for hardware-based performance monitoring of system modules.

g. Management functionality

1. Macros and scripts shall allow implementing special custom functions (performed according to an individual algorithm).
2. The system shall provide generation of macro events in case of appearing or not appearing of a chain of events in a defined time interval.
3. User virtual objects can be added – reactions, events, states can be set in order to be used in macros and scripts.

h. Integration of the distributed video surveillance and audio monitoring system

1. Remote interaction of the system and automated replication of internal databases (containing system setup parameters and data about the events registered by the system) between Servers and remote administrator workstations that are part of the distributed digital video surveillance system.

2. Generation of the integrated database of system setup parameters and registered events, followed by their processing in compliance with standard and specialized adjustable algorithms, including generation of notifications and system reactions.
3. Software-implemented optimization of video data flows within the distributed video surveillance system, whenever throughput capacity of the communication links is not sufficient.

9 Technical characteristics of the Video Surveillance and Audio Monitoring Subsystem

The Video Surveillance and Audio Monitoring Subsystem shall feature the following characteristics:

1. Shall have two installation options:
    1.1. As an MS Windows application
    1.2. As an MS Windows service
2. The maximum number of video capture channels for processing video signals in live mode and/or for multiplexing shall be limited only by the Server's hardware (CPU and RAM).
3. The maximum number of simultaneously output analog video signals shall be limited by the number of video capture cards (equipped with analog video outputs) used on the Server.
4. Maximum number of (analog) PTZ units used – 64.
5. The maximum number of remote workstations connected to the Server to obtain video signals shall be limited only by the number and parameters of the transmitted video signals, video surveillance system architecture, and network bandwidth.
6. The maximum number of Servers, the video signals from which are simultaneously transmitted to remote workstations, shall be limited only by the number and

parameters of transmitted video signals, video surveillance system architecture, and network bandwidth.

7. The maximum number of video images displayed simultaneously on the screen of a remote workstation shall be limited only by video image characteristics and network capacity.
8. The maximum video stream amount transmitted via a Videogate shall be limited only by the Videogate hardware parameters and network capacity.
9. The following video capture cards shall be supported: FS-5, FS-6, FS-16, FS-8, FS15, FS115, FX2, FX4, FX8, FX16, FX116, FX416, FX HD4, WS-7, WS16, WS-17, WS216, VRC6004, VRC6008, VRC6416, VRC7008L, VRC6404HD, DS-4016HCI(R), SC590N4, SC330Q16, SC330D16.
10. The following types of video cards shall be supported: Nvidia GeForce GT520 1GB RAM or more productive.
11. The following audio cards shall be supported: standard audio cards, MidiMan Delta, Comart Hera, Olkha 9R; the range of sampling frequencies shall be determined by the audio card features and software: 0 – 48,000 Hz

10 Types of installation of Video Surveillance and Audio Monitoring Subsystem software

The software Video Surveillance and Audio Monitoring Subsystem shall allow the following types of installation:

1. A full-featured version with Server, Administrator Workstation, and Operator Workstation functionality
2. A version with minimal functionality, which shall provide functionality only for Operator Workstations

11 Integration of Video Surveillance and Audio Monitoring Subsystem software

1. Integration of the distributed Video Surveillance and Audio Monitoring System shall be provided by data exchange between software Cores.
2. A fully functional software Core shall be the core software component of the system. Functional modules, forming the main software for the functional subsystems, shall interact with the system's software Core.
3. The functional software modules shall support direct interaction with hardware and also serve as a source of data on the status of guarded sites. The software Core of the subsystem shall process the data coming in from various functional modules and provide for their integration.
4. The executable files corresponding to the functional subsystems shall be automatically launched by the Core, according to the SMP configuration.
5. To simplify integration with joint data systems, auxiliary software, or extension functional modules, the software shall offer an alternative IDK/SDK interface for data exchange between functional modules and the software Core.
6. There shall be an ActiveX control that is similar in every way to the Video monitor interface object and allows managing cameras, viewing the archive and using other functions of the Video surveillance monitor.
7. There shall be the HTTP API that allows sending commands and receiving data from SMP by HTTP requests.

12 Purposes and process of configuration of Video Surveillance and Audio Monitoring Subsystem software components

The software components of the video surveillance and audio monitoring system shall be configurable so as to allow:

1. Creation and configuration of system objects corresponding to the functional modules (functional groups) of the software
2. Network-based configuration of SMP components
3. Configuration of video surveillance and audio monitoring functions
4. PTZ configuration.
5. Configuration of the user interface
6. Administration of user rights and privileges

a. Network-based configuration of SMP components

1. Interaction among Servers, Remote Administator Workstations and Remote Operator Workstations shall include replication of databases (only for Servers and Remote Administator Workstations) and exchange of events.
2. Configuration of interaction among components of the video surveillance system shall be performed from the Administration Server or, if there are dedicated subnets, from a node Server or Remote Administator Workstations.
3. For each component of the SMP, it shall be possible to specify a list of components with which that component performs exchange of data about the system configuration parameters.
4. For each component of the SMP, it shall be possible to specify IP addresses for other components of the SMP with which it is necessary to exchange configuration parameters and events.
5. It shall be possible to both change IP addresses for SMP components simultaneously and to change each IP address separately.
6. For each component of the SMP, it shall be possible to specify a list of components with which the component is to perform event exchange.
7. For each component of the SMP, it shall be possible to specify a list of events that are to be forwarded to other SMP components.

b. Configuring Video Subsystem

i. Hardware and software components of the Video Surveillance and Audio Monitoring Subsystem

1. Hardware portion of the video subsystem

The video subsystem hardware shall include the following components:

1. Servers and IBM PC–based Remote Workstations.
2. Network video hubs (WaveHub, LinuxHub)
3. Analog and IP video cameras
4. Audio capture devices
5. TCP/IP

2. Software portion of the video subsystem

The video subsystem software shall include:

1. Components for configuring video capture cards
2. Components for digitized video signal compression and decompression
3. Components for digitized video signal recording
4. Components for digitized video signal transmission to Workstations
5. Components for displaying video signal on the monitor.

ii. Configuring video capture cards

1. Video capture cards shall be configured by video signal digitization and processing settings, which comply with:
   1.1. Signal format (PAL or NTSC)
   1.2. Frame rate
   1.3. Frame resolution

1.4. Brightness

1.5. Contrast

1.6. Color depth

1.7. Color rendition format

1.8. Processing priority (for FS5, FS6, FS8, and FS16 cards)

1.9. Write priority

2. It shall be possible to imitate video stream transmission to a virtual video capture device via playback of the finished video (video recording).

iii. Configuring IP devices

1. IP devices shall be configured via the Web Server or other software supplied together with the device or via the software of the Video Surveillance and Audio Monitoring Subsystem.
2. Video signal compression and processing settings (format, frame rate, frame resolution, brightness, contrast, color depth, color rendition format) shall be performed via the Web Server or other software supplied together with the device.
3. The software of the Video Surveillance and Audio Monitoring Subsystem shall receive and process (via detection tools) video images, as well as write and transmit video signals from IP devices to client workstations.
4. The software of the Video Surveillance and Audio Monitoring Subsystem shall be integrated with the video standards and IP device manufacturers supported by Axxon DriversPack.

iv. Video signal compression and decompression

1. The following algorithms shall be used for compressing video signals from video capture cards:

1.1. Motion Wavelet

1.2. H.264

2. To compress video signals from IP devices, standard or manufacturer-designed algorithms shall be used.

2.1. MxPEG

2.2. MJPEG

2.3. H.264

2.4. H.265

2.5. MPEG4

2.6. Motion Wavelet

3. To decompress video signals, the following algorithms shall be used:

3.1. FfmpegAllInOneDecoder

3.2. H264FfmpegDecoder

3.3. H264DecodeBalancer

3.4. H263IppDecoder

3.5. H264InterlacedIppDecoder

3.6. H264IppDecoder

3.7. MPEG2IppDecoder

3.8. MJPEGIpp

3.9. MPEG4IppDecoder

3.10. H264Svc2Avc

3.11. MxPEG Mobotix

3.12. Motion Wavelet

3.13. Bosch

3.14. Hikvision Decoder

3.15. StreamLabs

3.16. VWV

3.17. H264SvcTEx

3.18. MediaSdkDecoder

4. The key frame rate must be configurable in use of the Motion Wavelet compression algorithm.
5. The criterion for including pixel blocks in delta frames must be configurable in use of the Motion Wavelet compression algorithm.

v. How to record digitized video signals

1. The video archive shall be located on local Server disks or on network drives. As the disk space allocated to the archive is filled up, the archive shall be written over in "ring" order, so that the earliest video is erased first during overwriting.
2. Before archiving video to the Server archive, the video signal shall be compressed by the software. The video signal shall be compressed to reduce the size of the video recordings.
3. The software shall be capable of auto video recording initiated by cameras (triggered by alarms [main motion detection tools] and video image detection tools), as well as by Operator command.
4. Pre-event (pre-history), post-event (video recording of event aftermath), and Hot (higher frame rate) recording shall be supported for more effective post-event analysis of evidence footage.
5. The video archive shall be kept in a folder determined by the software, on a selected system disk.
6. The contents of the folder shall be named in the format "DD-MM-YY HH", i.e., "DATE TIME". These subfolders shall contain the archive files for the specified hour.
7. The extension of the video recording file shall indicate the ID of the camera from which the archive has been recorded.
8. The software shall support three methods for initializing video recording:

   8.1. Forced, by the Operator’s Command

8.2. Automatically, if an alarm event is detected

8.3. Automatically, when a macro/script/program is triggered

9. The process for setting up video signal archiving shall include the following stages:

9.1. Select the disks for video archive storage.

9.2. Switch off/on auto alarm recording.

9.3. Set the video stream frame rate.

9.4. Configuration of video recording in hot mode

9.5. Configuration of video recording in pre-event mode

9.6. Configuration of video recording in post-event mode

9.7. Assign the queue of video signal processing in recording mode.

10. The software shall provide an audio and video synchro recording option. Audio signal recording shall begin at the start time and end at the end time of video signal recording.
11. The software shall provide an audio and video synchro recording option. Recording of the audio signal shall be sound-activated (start when the incoming audio signal exceeds a threshold value).
12. The software shall support viewing the video archive from the internal storage of IP devices (NVR video recorders).
13. The software shall support receiving video and audio archives from mutually unconnected Servers by means of removable disks. When replicating an archive, recordings for a specified period shall be copied from the Source Server to the Destination Server.
14. The software shall support creation of a backup video archive, with or without accompanying audio.
15. The priority of commands to start and stop writing of video shall be configurable.

vi. Types of Video Surveillance Monitors

Depending on the video signal transmission method chosen in the Video Surveillance Subsystem, the following Video Surveillance Monitors shall be made available

1. Video Server Surveillance Monitor.
2. Video Surveillance Monitor for Remote Workstations connected to the video server over a TCP/IP-based local network.
3. Web Server video surveillance module, displayed in web browsers on Remote Workstations connected to the Server by the HTTP-based Web Server module.
4. Client-side Video Surveillance Monitor on iOS.

vii. Video Surveillance Monitor functionality

1. The Video Surveillance Monitor shall:
    1.1. Display video signals.
    1.2. Archive forward or backward playback.
    1.3. Change the sequence of displaying video signals (surveillance windows layout, selection of video signals to be displayed in the surveillance windows, windows slide show, etc.).
    1.4. Process the displayed signals (deinterlacing, zooming, image sharpening and changing contrast).
    1.5. Export and printing of selected frames, export of video and audio, and export of a time interval in the archive
    1.6. Control detection tools, including camera alarm detection tools (main motion detection tools).
    1.7. Control video recording.
    1.8. Control PTZ units and microphones.
    1.9. Deletion of video from archive.

1.10. Displaying transformed fisheye video signal.

2. The Video Surveillance Monitor shall support configuring the display of camera tiles :
   2.1. Active Camera mode. Only the active camera tile is shown in the Monitor window.
   2.2. Alarm Cameras mode. The Monitor window shall display the tiles of video cameras on which an alarm has been registered.
   2.3. List mode. The camera panes shall be displayed in the Monitor window according to the selected layout (1x1, 2x2, 3x3, 4x4, 5x5, 6x6, 7x7, etc.).
3. The Video Surveillance Monitor shall allow rotating through camera layouts, with the help of toolbar buttons, in one of two ways:
   3.1. Manually. Buttons allow moving to the previous or next camera pane.
   3.2. Automatically. Video camera panes are automatically cycled through, at a set interval.
4. The Monitor shall display three modes for configuring overlay function:
   4.1. Mode 1. Camera video is processed as a single stream.
   4.2. Mode 2 (recommended). Camera signals shall be processed independently of one another.
   4.3. Do not use. Camera signals are not processed by the video card.
5. The Video Surveillance Monitor shall enable setting the priority for PTZ control. Priority settings for PTZ control are:
   5.1. Control is forbidden (Forbidden). This item forbids PTZ control by the object in question.
   5.2. Low (Low priority). PTZ control is last in the queue, after the “normal” and “high” priorities. This priority shall be last in the queue for PTZ control.
   5.3. Normal (Normal priority). The PTZ is controlled after a device with “high” priority. It is higher in the queue for PTZ control than any device with “low” priority.
   5.4. High (High priority). This item shall be set as first in the queue for PTZ control. This priority shall be highest in the queue for PTZ control.

6. If the same PTZ is controlled from several workstations by interface objects of the same type with the same PTZ control priority, then the following rules shall apply:
    6.1. Any user can control a PTZ, when no other user with the same control priority is controlling the unit at that moment.
    6.2. If a user with a higher-priority interface object delegates control to a user with a lower-priority interface object, then this procedure shall be delayed. The priority delay time shall be set by the subsystem utility.
7. The Video Surveillance Monitor shall be able to function in panoramic video display mode, for creating and using panoramic video imagery composed from the fields of view of multiple cameras.
8. The Video Surveillance Monitor shall superimpose captions with configurable size, color, and content on top of video.
9. The Video Surveillance Monitor shall support selecting a video stream for display for each camera.
10. The Video Surveillance Monitor shall allow configuring pruning of displayed video.
11. The Video Surveillance Monitor shall allow configuring the compression of the video signal that is displayed.
12. The Video Surveillance Monitor shall allow selecting backup and external archives for viewing.
13. The Video Surveillance Monitor shall support selection of a videogate for obtaining a video signal to display.
14. The Video Surveillance Monitor shall support the ability to select a videogate for obtaining archive video from a backup archive.
15. The Video Surveillance Monitor shall allow including automatic selection of the most appropriate video stream (Green Stream).
16. The Video Surveillance Monitor shall allow export of the archive from the external storage into the file on a disk similar to the export of main archive.
17. The video monitor must support background export of the main archive of the Server, the Videogate archive and the Long-term archive including:

17.1. Export of the video archive for the specified period in the format of the *SPM* file system or in the asf, avi, flv, mkv or mp4 with the possibility of changing the encoding format (codec).

17.2. Scheduled export.

17.3. Export when connecting USB, CD or DVD storage.

17.4. Export with added subtitles.

17.5. Option to limit the size of the exported file.

17.6. Option to copy AxxonPlayer to the export folder.

18. Option to select the export folder.

viii. Mutlistreaming configuration

1. It shall be possible to select a video stream from a camera for each of the following purposes:
   1.1. Display both locally and on remote clients.
   1.2. Recording to archive (continuous).
   1.3. Recording to archive (alarms).
   1.4. Video analytics.
2. A single video stream can be used for several purposes, but one and only one video stream is used for each purpose.

ix. Captioning

1. It shall be possible to apply captions on live or archive video playback in Video Surveillance Monitor as well as background export from Video Surveillance Monitor (optional).
2. The following caption parameters shall be configurable:
   2.1. Captions database depth.
   2.2. Captions font.
   2.3. Captions color.
   2.4. Words highlighting.

c. Configuring Audio Subsystem

i. Audio Subsystem components

The audio subsystem shall include software modules and hardware devices for the receipt, transmission, digitization, processing, recording, and playback of audio signals originating from microphones of the Video Surveillance and Audio Monitoring Subsystem.

1. The audio subsystem hardware may optionally include:
    1.1. Video capture cards
    1.2. Standard sound cards
    1.3. Multi-channel sound cards
    1.4. Audio capture IP devices
    1.5. Microphones
    1.6. Loudspeakers and headphones
2. The audio subsystem software shall include:
    2.1. Components for configuring the audio signal digitizing devices
    2.2. Components for recording digital audio signals
    2.3. Components for transmitting digital audio signals to Remote Workstations and remote servers
    2.4. Components for playback of digital audio signals

ii. Video capture cards

1. Video capture cards, used as audio capture devices, shall support reception and digitization of audio signals. Video capture cards shall not support audio signal output to headphones or speakers.

2. Digitization of audio signals by video capture cards shall be performed in parallel with digitization and processing of video signals. The processes for processing audio and video signals by a video capture card shall be independent.
3. Support for receiving and digitizing audio signals on video capture cards shall depend on the Server's hardware and software configuration: on the type of video capture cards and the activation key parameters.

iii. Standard sound cards, microphones, speakers, and headphones

1. Standard sound cards shall be supported as audio capture and audio output devices. They shall receive and digitize audio signals, reconvert digitized audio signals, and feed them to speakers and headphones.
2. The software shall support an audio signal sample rate range that corresponds to a standard sound card and is restricted to a frequency of 48 kHz.

iv. Multichannel audio capture devices

1. Multichannel audio capture devices shall be PCI cards or external hardware/software modules for digitization and processing of two or more audio signals.
2. The audio subsystem shall be compatible with the following multichannel audio capture devices:
   2.1. MidiMan Delta
   2.2. Comart Hera
   2.3. Olkha 9R
   2.4. Echolot USB-32
3. Multi-channel audio capture devices shall reproduce sound and digitize audio signals in parallel, or sound shall be reproduced by standard sound cards. The audio signal sampling rate range shall depend on the audio capture device type.

v. IP devices

1. The audio subsystem shall support audio signal reception, digitization, processing, and playback using audio capture IP devices. Microphones built into IP cameras and IP servers, or external analog microphones connected to IP servers, may be used for audio signal receipt, digitization, and processing. External IP loudspeakers or headphones, connected to IP servers may be used for audio signal playback.
2. The audio signal sampling rate range shall depend on the IP device type used as an audio capture device. The audio subsystem sampling rate range available for the installed card shall be limited to a maximum value of 48 kHz.
3. In synchro recording mode, audio recordings shall be combined with video recordings and stored in the Server archive.
4. When audio signals are recorded by Operator command or by sound activation, audio recordings shall be separately stored in the audio archive.
5. Once the archive disk(s) is (are) full, the archive shall be overwritten.
6. It shall be possible to set audio delay for synchronous playing back or recording archive.

vi. Transmission by the audio subsystem of digitized audio signals to Remote Workstations and Servers

1. The audio subsystem shall allow transmitting audio signals to Remote Workstations on IBM-compatible PCs connected to a Server over a local TCP/IP-based network, as well as to remote servers.
2. Both real-time and archive audio signals shall be transmitted to Remote Workstations.

vii. Configuring audio playback

1. Playback of audio in the audio subsystem shall be performed by a special software object. The software object shall comprise speaker objects if the object has multiple

channels. It shall be possible to send sounds from a microphone to a speaker through a software module, macro, or script.

viii. Configuring voice notifications

1. Voice notification upon registration of an alarm event by the main motion detection tools shall be configurable.
2. When a camera's motion detection tool is triggered, an audio file in the Wav subfolder in the software's root folder shall be played. The files shall have the extension .wav and have the name cam_alarm_N, where N is the camera's ID.
3. It shall be possible to add custom audio files.

ix. Configuring audio switches

1. The audio subsystem shall support sending the audio signal arriving from any audio source (microphone) to any sound receiver (speaker) for playback.

x. Setup of video signal transmission to IP devices

1. The software shall be able to transmit audio signals from microphones to IP devices and to play them back with speakers or headphones connected to IP devices.

d. PTZ configuration

1. To expand the zone of video surveillance through mechanical PTZ, PTZ units must be used.
2. PTZ units shall be controlled by means of the following interface objects:
   2.1. Video Surveillance Monitor
   2.2. Telemetry panel
   2.3. PTZ controller
3. PTZ control shall be performed through the following devices:
   3.1. Mouse and standard keyboard (during use of the Video Surveillance Monitor and Telemetry panel interface objects)

3.2. Specialized devices designed specially for PTZ control, such as PTZ controllers and joysticks

4. To ensure that operation of PTZ units is consistent when multiple users are active, it is necessary to designate priorities to be applied when controlling PTZ units by means of the objects listed in paragraph 2 objects.
5. The priority levels for PTZ control shall be as follows:
   5.1. Control forbidden (Forbidden). If this value is selected, control of the PTZ device via the object shall be forbidden.
   5.2. Low (Low Priority). If this value is selected, control of the PTZ device shall be performed with last priority, after control by devices with the Standard and High priorities. This priority shall have the lowest level of priority in PTZ control.
   5.3. Standard (Standard Priority). If this value is selected, control of the PTZ device shall be performed after control by a device with High priority. This priority shall have a higher level of priority in PTZ control than a device with Low priority.
   5.4. High (High Priority). If this value is selected, control of the PTZ device shall be performed with the highest priority. This priority shall have the highest level of priority in PTZ control.
6. If a single PTZ unit is being controlled from multiple workstations via interface objects of the same type with the same PTZ control priority, control of the PTZ device shall be allocated as follows:
   6.1. Each user shall be able to control the PTZ unit when it is not being controlled by another user via an interface with the same PTZ control priority.
   6.2. If control is being transferred from a user managing the PTZ unit via an interface object with higher priority to a user managing the same PTZ unit via an interface object of lower priority, transfer of control shall be delayed. The delay in transfer of control in this case shall be configurable by a subsystem utility.
7. The number of PTZ units connected to the Server shall be indicated in the activation key.
8. During PTZ configuration, it shall be possible to specify the speed of focus and zoom in/out for the camera lens.
9. It shall be possible to specify a list of presets.

10. It shall be possible to control PTZ units via the following PTZ controllers:
    10.1. BOSCH 12c-KBD-Digital
    10.2. Axis T8310
    10.3. Lilin PIH-800III
    10.4. Panasonic WV-CU950
    10.5. Samsung SSC-2000
    10.6. Samsung SPC-7000
    10.7. Everfocus EKB-200
    10.8. VIDEOTEC DCZ
11. Control of PTZ units shall be possible with the help of the Operator Query Pane.
12. It shall be possible to map commands for PTZ control to joystick keys.
13. It shall be possible to map commands for PTZ control to mouse buttons and their combinations.
14. Setting the speed of performing the following commands by the PTZ device:
    14.1. Zooming
    14.2. Changing the focus of the camera lens using the mouse
    14.3. Changing the focus of the camera lens using the joystick
    14.4. Point&Click
15. It should be possible to work with PTZ cameras that support positioning in absolute coordinates to track objects on the map.

e. Rights and privileges administration

1. The SMP shall support the following types of users:
    1.1. Administrator
    1.2. Operator, who may optionally be granted some rights for administration, control and viewing
2. The administrator must possess full administration rights for all SMP computers.

3. Any other registered user of the system is an operator, who may optionally be granted the rights for administration, control and/or monitoring of particular components of subsystems.
4. To register an Operator, a user account shall be created, with this user's rights and privileges for administration, control and/or monitoring. A password shall be assigned to each Operator at the time of registration, and shall be used for authorization at software start and exit. An Operator may, optionally, be forbidden from quitting the software.
5. An account shall not be created for the Administrator. No authorization based on the system administrator's password shall be performed when the software is started. The administrator password shall be used to access the system configuration dialog box and the settings panels of system objects, to change the current user, and to quit the software.
6. A Person system object shall be created for each user account. Each Operator shall have his (her) own user account, which shall hold all the data about the Operator's rights and authorization password.
7. User name, surname and patronymic shall be entered in different fields. Full name of the Operator shall display in the "User" system objects tree.
8. A photo assigned via Access Manager or Face recognition and search interface modules shall be displayed on the "User" system object settings panel.
9. The account shall also indicate to which department the Operator belongs. A Department system object shall be created for each department account.
10. The Department and Person objects shall form an account hierarchy of two levels.
11. The administrative functions shall include:
    11.1. Creation or removal of system objects
    11.2. Editing the settings of the system objects
    11.3. Moving the system objects across the object tree

12. By default, the Operator shall be entirely forbidden from using administration functions, but shall have complete permission to use control and monitoring functions at all sites for which the functions are provided. There shall be support for forbidding an Operator from administering one or more objects, restricting the available functions for object management, and limiting monitoring features.
13. When an Operator receives administration rights for a system object, he (she) also receives the control and monitoring rights for that object at the same time.
14. When the operator has the rights for control functions, he (she) should also be able to use the buttons, menu items and other interface elements allowing to control the corresponding objects (cameras, microphones, telemetry, event log, etc).
15. Monitoring functions shall be limited to Operator viewing of the interface components (user screens, surveillance monitors, Long-term archiving window, microphone indicators, etc.).
16. To rule out unauthorized shutdown of the surveillance system, the SMP shutdown function can be protected by a password. The following methods for SMP shutdown shall be implemented:
    16.1. Shutdown by the password of any registered Operator
    16.2. Shutdown by the password of the current authorized user only.
    16.3. Shutdown by the administrator password.
    16.4. An Operator cannot shut the system down.
17. By default, the system is set for shutdown by any registered Operator's password, regardless of the current authorized user.
18. Hiding of all interface components can be forbidden. Thus the user's computer will always display the Video Surveillance Monitor with the set of interface objects that has been determined by the SMP administrator.
19. By default, the Operator shall be allowed to hide all on-screen user interface components at the same time.

20. SMP functionality shall allow forbidding the Operator from playing back video archives with the use of the Video Surveillance Monitor (video archives on the Server and Long-term archive).
21. By default, the Operators shall be allowed to play back archives.
22. SMP functionality shall support setting a limit on the number of hours of video that Operators can view.
23. By default, it shall be forbidden for Operators to delete entries from the archive through the Video Surveillance Monitor interface.
24. It shall be possible to allow Operators to protect archive files from overwriting or remove protection.
25. Operators shall not be allowed to protect archive files from overwriting or remove protection by default.
26. It shall be possible to forbid Operators from frames export and printout and video archive export.
27. Operators shall have permissions to export and print frames and export archive by default.
28. The user rights accounts in the SMP shall be stored separately from the Operator accounts. It shall be possible to assign identical rights to multiple Operators. Each Operator shall have a single set of rights only.
29. The SMP shall support Windows account–based authorization of users.
30. The SMP shall support import of data from LDAP address books into the SMP database. Data import shall be performed using macros.
31. Import or synchronization of an LDAP address book shall not affect users who have been manually created in the SMP prior to or after import.
32. The SMP shall allow synchronization of LDAP imported users with Windows Active Directory. There shall be an unambiguous correspondence between user permissions in the SMP and security groups in Active Directory, as well as users in the SMP and users in Active Directory.
33. The SMP shall support changing the Operator's password in the following cases:

33.1. When requested by the Operator

33.2. When the Operator's password expires

33.3. When the Operator logs into the system for the first time

34. Logging in into the system by the four-eyes rule, i.e. with confirmation of user logging in by a supervisor shall be provided.
35. It shall be possible to combine existing user permissions to create new permissions.
36. Double step verification is available for administrators and operators to access the system via sms and/or email

f. Main interfaces

1. The system shall be based on a tree-like structure of object layout (object tree). The object tree shall be arranged as a multi-level list of embedded objects.
2. The top-down embedded objects structure shall reflect the object hierarchy, where lower-order (child) objects are created only under higher-order (parent) objects.
3. The objects tree shall be viewable in expanded form, where embedded groups (branches) can be viewed or, if not currently needed for monitoring, hidden.
4. The SMP shall support distributing the activation key, which governs the system configuration, to all computers on the distributed Security Management Platform.
5. The SMP shall support verification of the settings of all created objects, as well as restoration of the correct object configuration if it is changed. Restoration shall occur from a configuration template, which can be created at any time based on the current settings.
6. The SMP shall support MS SQL database backup creation.
7. The SMP shall include a utility to play video and audio archives, and to convert them to standard formats: AVI, MPEG, DivX, MP3, etc.
8. Besides video and audio playback, the utility shall be able to perform:

   8.1. Conversion of video and audio files

8.2. Copying of files from the archive to another folder, without loss of data

8.3. If video and audio were synchronized at the time of recording, the converted file will contain sound.

9. A utility shall allow configuring the SMP by editing keys in the Windows Registry.

10. The utility shall provide the following functionality:

10.1. Configuration of SMP start

10.2. Enabling of SMP debug mode

10.3. Extended configuration of the Video Surveillance Monitor

10.4. Extended configuration of events logging

10.5. Extended configuration of video signal processing by Servers

10.6. Extended configuration of distributed architecture

10.7. Changing computer names and IP addresses in the configuration database:

10.8. Compressing the MS Access database

10.9. Limiting the amount of RAM used by the MS SQL server

10.10. Extended setup of audio or video recording to an archive

10.11. Re-indexing audio and video archives

10.12. Selecting the analog video out mode

10.13. Testing the operability of video capture cards

10.14. Extended setup of PTZ devices

10.15. Display of versions of SMP modules

10.16. Configuration of the Client to automatically connect to backup video servers if connection with the main Server is lost

10.17. Enabling support for PureVideo/CUDA during decompression of video signals from IP devices. In this case, the video card's CPU can perform decompression, reducing the load on the Server's CPU.

11. The SMP shall include a utility to check the authenticity of frames exported into BMP or JPG format.

12. The SMP shall include automatic search for connected IP devices.
13. The SMP shall include a utility for measuring video processing performance.
14. The SMP shall include a utility for correcting the creation and modification dates of the video archive.
15. The SMP shall include a utility for editing templates for databases and external settings files.
16. The SMP shall include a utility for creating user dialog boxes.
17. The SMP shall include a utility for converting, selecting a template for, and creating backup copies of databases.
18. The SMP shall include a utility for reading Matrix codes.
19. The SMP shall include a utility for configuring audio signal digitalization devices that installed on the Server.
20. The SMP shall include a utility for verification of the settings of all created objects, as well as restoration of the correct object configuration if it is changed.
21. Restoration shall be made from the configuration template.
22. It shall be possible to create a configuration template at any time based on the current settings.
23. The SMP shall include a utility for re-indexing archive files.
24. The SMP shall include a utility for creating a query file to replicate the archive from non-connected Servers, by using removable disks.
25. The SMP shall include a utility for viewing video and archives from fish-eye cameras.

13 Quick access to interface objects

1. The Video Surveillance and Audio Monitoring Subsystem for quick access to interface objects shall support connecting a special keyboard and controlling the following core subsystem functions:
    1.1. Video surveillance

1.2. Audio monitoring

1.3. Archive

1.4. Telemetry

1.5. Event log

1.6. Macros

1.7. Dry contacts/relays

2. The Video Surveillance and Audio Monitoring Subsystem shall support the following models of special keyboards:

2.1. PROMAG KB-840

2.2. PROMAG KB-950A

2.3. Any USB or PS/2 connectible keyboard including Posiflex KB-4000 programmable POS keyboard.

14 Clusterization and virtualization

To improve the redundancy and fault-tolerance of Video Surveillance and Audio Monitoring Subsystems including IP cameras, the subsystem shall support the following:

1. Clusterization through Windows Server Clustering
2. Clusterization through the software's own mechanisms (N+1, where N represents the functioning servers and 1 is the server that should automatically replace any functioning server that goes offline)
3. Installation and startup on virtual (guest) operating systems

15 Analytics

a. Videoanalytics

1. Video detection tools shall provide video analysis and recognize various events that occur in the field of view. Event recognition capabilities shall depend on the detection tool type.
2. The Video Surveillance Subsystem shall provide for the following detection tools:
   2.1. Main motion detection tool
   2.2. Motion
   2.3. Focus loss
   2.4. Video signal stability
   2.5. Background change
   2.6. Camera blinding
   2.7. Camera blocking
   2.8. Abandoned items
   2.9. Infrared
   2.10. Face detection
3. By default, only the main motion detection tool (which recognizes camera alarms) is used in the subsystem. All other video image detection tools can be optionally enabled.
4. The main motion detection tool recognizes any motion that occurs in the field of view of armed cameras and generates alarms.
5. The motion detection tool shall recognize moving objects within the monitored area. Detected moving objects shall be dynamically outlined. The motion shall be detected by calculating gradients between consequent frames.
6. The focus detection tool shall notify the operator about camera tampering which results in focus loss or degradation of camera sensitivity. The high-frequency component of the video signal shall be analyzed to check for the presence of distinct contours.

7. This software detection tool shall react to any change in video camera position. The detection tool's operation shall be based on a comparison between each frame's parameters and the average parameters. It shall use high-frequency filtration to detect the objects' contours, if they are sufficiently distinct.
8. This detection tool shall be capable of reacting to changes in the scene background due to physical tampering of the CCTV camera. Its algorithm shall be based on the calculation of the root-mean-square deviation of the overall scene intensity with respect to the average value.
9. The lens blinding detection tool shall recognize attempts to blind the camera lens. Its operation shall be based on comparing the histograms of the received frames with the sample blind frame histogram (pure white).
10. The lens blocking detection tool shall recognize attempts to block the camera lens. Its operation shall be based on analysis of the broadening of the frame histogram, relative to the histogram median of the reference closing frame (gray).
11. A face detection tool shall recognize the presence of "human face" elements within an area under surveillance. When a human face is detected in a frame:
    11.1. The face shall be dynamically outlined in a frame.
    11.2. If the facial recognition subsystem is installed, support recording of the clip with the face as a .bmp file.
12. The abandoned items detection tool shall be capable of recognizing objects that have been lost (or disappeared) in the guarded area. If the presence/absence time of a motionless object exceeds the pre-defined time value, a rectangular border shall outline the critical object. The special algorithm shall analyze the changes in averaged frames at different points of time. The detection tool shall be capable of recognizing abandoned objects and the objects that are found within a scene. This shall be done by the motion detection tool, which allows registering object appearance in the frame.

13. The infrared detection tool shall be used for thermal imagers/infrared cameras. The infrared detection tool shall recognize moving objects within the monitored area. Detected moving objects shall be dynamically outlined. The motion shall be detected by calculating gradients between consecutive frames.
14. The sensitivity of all types of detection tools shall be configurable.

b. Forensic Search of archives

1. The Forensic Search subsystem is a set of tools for searching video recordings in the archive by using video image metadata. Forensic Search shall be performed according to the parameters of objects in a video camera's field of view, for example, according to the object's direction of motion.
2. Video metadata shall be obtained with the help of the tracking detection tool. When the Tracker object is activated, information only about the objects that have triggered the activation shall be written to the trajectory database. Correspondingly, if tracking detection tools are configured, Forensic Search shall support finding only video for which the detection tools were activated.
3. The following tools, which should be accessible in the Video Surveillance Monitor, shall be present in the Video Surveillance Subsystem for Forensic Search:
   3.1. Line crossing (straight or fragmented)
   3.2. Motion in an area
4. Line crossing detection tool – a detection tool which shall be triggered when the trajectory of an object crosses a virtual line in a video camera's field of view.
5. The following settings shall be configurable in the triggering conditions for the line crossing detection tool:
   5.1. Line type
      5.1.1. Straight
      5.1.2. Polyline

5.2. Type of object for which the detection tool shall be triggered:

5.2.1. Any object. The detection tool shall be triggered for any object that crosses the line.

5.2.2. Person. The detection tool shall be triggered for any person that crosses the line.

5.2.3. Vehicle. The detection tool shall be triggered for any motor vehicle that crosses the line.

5.3. Direction of motion

6. The area motion detection tool is a tracking detection tool that is triggered when an object(s) performs certain actions in a virtual area within the camera's field of view.
7. The following settings shall be configurable in the triggering conditions for the line crossing detection tool:

7.1. Type of object for which the detection tool shall be triggered:

7.1.1. Any object. The detection tool shall be triggered for any object that crosses the line.

7.1.2. Person. The detection tool shall be triggered for any person that crosses the line.

7.1.3. Vehicle. The detection tool shall be triggered for any motor vehicle that crosses the line.

7.2. Type of detection tool:

7.2.1. Motion in a specific area. The detection tool shall be triggered by any motion in the area.

7.2.2. Area entry. The detection tool shall be triggered by movement of an object into the area.

7.2.3. Exit from area. The detection tool shall be triggered by movement of an object from the area.

7.2.4. Appearance in an area. The detection tool shall be triggered by the appearance of an object in the area.

7.2.5. Disappearance in an area. The detection tool shall be triggered by the disappearance of an object in the area.

7.2.6. Stopping in an area. The detection tool shall be triggered by the stopping of an object in the area.

7.2.7. More than 10 seconds in area. The detection tool shall be triggered by an object that spends more than ten seconds in the area.

7.2.8. Abandoned object. The detection tool shall be triggered upon discovery of an abandoned object in the area.

8. Archive search shall be made of all cases listed above when a detection tool has been triggered, except for when triggered by an object in an area or disappearance of an object from an area.
9. If a camera is installed on a mobile object, software image stabilization and error reduction for the detection tool shall be available.
10. It shall be possible to arm and disarm tracking detection tools.
11. The possibility to use the following additional object types to trigger the detection shall be supported:
    11.1. Human;
    11.2. Group of humans;
    11.3. Car;
    11.4. Noise;
    11.5. Item carried into the area;
    11.6. Object carried out of the area.
    11.7. Other.
12. Detector shall trigger on any object classified using neural network.

c. Systems for on-board analytics

The video surveillance subsystem shall support systems for on-board analytics on cameras and video capture cards integrated in latest DriversPack.

16 Event logging

1. The Video Surveillance and Audio Monitoring Subsystem shall log registered events.
2. Logging of registered events shall be performed both locally and on servers on the distributed system that have been previously defined by the Administrator.
3. The event log shall be capable of being displayed on screen in an interface window.
4. The event log shall allow selecting the type of object for which an event can be registered.
5. By default, if the Administrator does not specify any type of object, the event log shall record all events for all subsystem objects.
6. The interface window of the event log shall allow viewing archive video from the list of messages.
7. When an object is selected, the event log shall allow viewing that subsystem object on an interactive map of the guarded site.
8. The event log shall allow creating a printed form for event reporting.
9. The Video Surveillance Subsystem shall support setting a time limit for storage of an event archive in the event log database.
10. It shall be possible to filter event list in the Event Viewer using preset filters.
11. The Video Surveillance Subsystem shall have a specialized event log made for operators. The specialized event log shall provide:
    - 11.1. Display in the interface window of events that have been registered by subsystem objects
    - 11.2. Assignment of a status (type) to registered events (at least three types)

11.3. Addition of comments to events

11.4. Writing of events to the archive

11.5. Search of events in the archive

11.6. Viewing of event video

11.7. Possibility to postpone event processing for a set period of time once.

11.8. Escalation of events to the superior interface.

11.9. Generating events of the specified type.

11.10. Creating reports on the facts of event processing by operators.

11.11. Creating reports on registered events.

11.12. Finding the position of the event source object on the map.

11.13. Confirming the event type assignment with a password.

17 Interactive map

1. The Video Surveillance and Audio Monitoring Subsystem shall allow creating an interactive map of the guarded site.
2. The interactive map shall allow using graphical diagrams (blueprints) of the guarded territory to navigate among the Video Surveillance and Audio Monitoring Subsystem components.
3. The interactive map shall allow controlling the subsystem objects from the functional shortcut menus of the graphical symbols (icons) on the map, which indicate the states of the corresponding objects.
4. An object can be added to the map in one of the following forms:
   4.1. .bmp, .jpg or .png image.
   4.2. .bmp, .jpg or .png image with an indicator.
   4.3. .svg vector image.
   4.4. Text.
   4.5. Line.
   4.6. Polygon with up to 51 vertexes.

4.7. Ellipse.

5. Several different icons of the same object can be added to one or more layers of an interactive map.
6. The Interactive Map shall allow using a set of plans (layers) of photos, maps, blueprints, and drawings (in BMP format), without limitation on the size or resolution of the drawings.
7. The Interactive map shall allow to set the substrate color, even when the layer drawing is not selected.
8. It shall be possible to configure rules for switching to layers with alarm devices on multilevel interactive maps as well as to any layer including the previous.
9. The following ways of displaying the layer with an alarm device shall be present on the interactive map:
   9.1. When an alarm occurs, the Interactive Map window shall open above all other active windows, showing the layer that contains the alarm device.
   9.2. The link symbols recursively lead to the layer containing the alarmed device.
10. The object signature must contain an object ID before or after the object name when placing it to the map layer.
11. There must be possibility to disable the object ID in the signature on the map.
12. Signature position relative to the object icon shall be selected: above, below, to the right, to the left, none.
13. When multiple layer interactive maps are in use the feature to switch between layers (within the same map or on other maps in the system) must be enabled.
14. If an object is in several states simultaneously, then the device symbol or color shall change in accordance with these states in some time.
15. When the object is marked on the map, all its states shall be displayed next to it as diminished icons.
16. It shall be possible to disable displaying diminished icons of object states.
17. It shall be possible to set the order of object display on the map when graphical symbols of objects overlap.

18. There must be an option to display the specified number of recent events of the selected object in the Interactive Map window.
19. There must be an option to link map coordinates to geographic coordinates.
20. There must be an option of complex tracking of objects transferring their coordinates to the integrated security system using PTZ cameras that support absolute coordinate control.
21. There must be an option to display the minimap of the layer to simplify navigation on the map layer.
22. There must be an option to search for an object on the map.
23. It shall be possible to control the groups same type objects via the functional menu on Map.
24. It shall be possible to display camera angle on Map (for cameras providing the absolute coordinates to SMP).

18 Technical support for users

1. The SMP shall include a utility to collect information about the configuration and status of the hardware, Windows OS, and the Security Management Platform.
2. The utility shall generate an archive that can be used by the developer's technical support department.

19 Report subsystem

1. The Report subsystem shall be designed for the following purposes:
   1.1. Compiling, and sending for print, reports about events and reactions to events registered in the SMP.
   1.2. Viewing the video archive starting from the time of the event registered in the report.
2. The Report subsystem shall support the following functionality:

2.1. Selecting objects (or groups of objects) from those included in the report (objects shall include hardware and software modules)

2.2. Selecting the events to be included in the report for each object selected.

2.3. Creating the report templates.

2.4. Creating the screen reports.

2.5. Creating the printed reports.

2.6. Exporting the printed report to a file.

2.7. Viewing the video archive from the screen report form using the Video Surveillance Monitor or the built-in utility.

2.8. Using the cameras of the ATM subsystem (automatic teller machine monitoring subsystem) using the X.25 protocol.

20 Basic hardware and software requirements

1. The SMP shall be developed for use on non-proprietary IBM PC–compliant hardware.

a. Operating system requirements

1. The SMP shall be compatible with 32- and 64-bit licensed versions of Microsoft Windows:

1.1. Windows Server 2008 R2 SP1 x64;

1.2. Windows 7 SP1 x86, x64;

1.3. Windows Storage Server 2008 R2 SP1 x64;

1.4. Windows Small Business Server 2011 SP1 x64;

1.5. Windows Home Server 2011 SP1 x64;

1.6. Windows Server 2012 x64;

1.7. Windows 8 x86, x64;

1.8. Windows 8.1 x86, x64;

1.9. Windows Server 2012 R2 x64;

1.10. Windows 10 x86, x64;

1.11. Windows Server 2016 x64.

b. List of TCP ports used by the Security Management Platform

1. SMP modules shall function over the TCP ports described in the table (Tab. b—1 – Tab. 19.2—6). If in the **Connecting to the module** column there is the "-" sign, that means connection to the INTELLECT.EXE.

Tab. b—1 List of TCP ports used by SMP modules

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Connecting to the module
1	ARCHIVER.RUN	Archive	21007	-
2	ARCHPANEL.RUN	Backup archive panel	22118	-
3	ATM	ATM	21090	-
4	AUDIO.RUN	Microphone	21008	-
5	AUDIO.RUN	Microphone	20903	VIDEO.RUN
6	AUDIO.RUN	Microphone	20904	VIDEO.RUN
7	AUDIO.RUN	Backup audio archive	20911	-
8	CAM_TITLE.RUN	Captioner	21077	-
9	CAM_TITLE.RUN	Captioner	20900	VIDEO.RUN
10	CONFCHEKUTIL.RUN	Configuration check	22220	-
11	DIALOG.RUN	Operator query panel	21058	-
12	DRS.RUN	Data replication service	22175	-
13	EVENT_COUNTER.RUN	Event counter	22153	-
14	EVENT_VIEWER.RUN	Event viewer	21055	-
15	IIDK_TEST.EXE	IIDK interface	21030	-
16	JAVA.EXE	Web-server 2.0	22212	-

17	KEYB.RUN	Keyboard	21005	-
18	LDAPIMPORT.RUN	LDAP service	22252	-
19	LIVEPLAYER.RUN	Live sound switch	22199	-
20	MAP.RUN	Map	21051	-
21	MC_CLIENT.RUN	Intercom Control Monitor	22179	-
22	MESSAGE.RUN	Alarm Message Window	21056	-
23	MMS.RUN	Mail Message Service	21031	-
24	OPERATORPROTOCOL.RUN	Operator protocol	22215	-
25	PLAYER.RUN	Audio player	20910	AUDIO.RUN
26	PLAYER.RUN	Audio player	21060	-
27	SLAVE.EXE	Computer	21111	-
28	SMS.RUN	Short Message Service	21035	-
29	STREAMINGSERVER.RUN	rtsp Server	22228	-
30	TELEMETRY.RUN	Telemetry Controller	21010	-
31	TELEMETRY_PANEL.RUN	Telemetry control panel	22101	-
32	TITLEVIEWER.RUN	Search by captions	20978	CAM_TITLE.run
33	TITLEVIEWER.RUN	Search by captions	22112	-
34	VIDEO.RUN	-	20900	-
35	VIDEO.RUN	Video Capture Device	21050	-
36	VIDEO.RUN	Video stream archiever	20901	-
37	VIDEO.RUN	Video stream gate	20902	-
38	VMDADB.RUN	VMDA metadata storage	22219	-

39	VMS.RUN	Voice Message Service	21032	-
40	VNS.RUN	Voice notification service	21004	-
41	WEBSERVER.RUN	Web-server	21034	-
42	WINDOW.RUN	External window	21053	-
43	OPCIE.RUN	HTML Interface	22141	-
44	Manitou.run	Manitou software	22302	-
45	QueuesManager.run	Queues Manager	22322	-
46	display_manager.run	Display Manager	22323	-
47	SipPanel.run	SIP_PANEL	22331	-
48	StreamTerminal.run	SIP_TERMINAL	22332, 22537	-

Tab. b—2 List of TCP ports used by ATM protection modules

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	VIDEOSRV.EXE	IIDK interface	21030	-
2	VIDEOSRV.EXE	VideoServer	20900	VIDEO.RUN
3	VIDEOSRV.EXE	ATM machine	22174	-
4	VIDEOSRV_C.RUN	ATM-Intellect Pro	22001	-

5	VIDEOSRV_E.RUN	Search in archive	22003	-
6	VIDEOSRV_M.RUN	Monitoring	22222	-
7	VIDEOSRV_R.RUN	Monitoring reports	22223	-
8	VIDEOSRV_S.RUN	ATM-Intellect Workstation	22002	-
9	VIDEOSRV.EXE	ATM-Intellect Pro	7777	VIDEOSRV.EXE
10	EVENTATM.EXE (Integration with ATM through XFS)	-	8888	VIDEOSRV.EXE
11	TELLMEDLL.DLL (Integration with ATM through the SKS software)	-	8888	VIDEOSRV.EXE
12	VMON_ITV.DLL (Integration with ATM through the “Gold Crown” software)	-	8888	VIDEOSRV.EXE
13	STATEUPS.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
14	BATDISCH.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
15	POWEROFF.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
16	POWERON.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
17	VPIPECLIENT.EXE (Internet FPSU operation)	-	7777	VIDEOSRV.EXE
18	VPIPECLIENT.EXE (Internet FPSU operation)	-	8555	VPIPESERVER.EXE
19	VIDEOSRV.EXE	ATM-Intellect Pro	7777	VPIPESERVER.EXE
20	VIDEOSRV.EXE	ATM-Intellect Workstation	7777	VIDEOSRV.EXE
21	VIDEOSRV.EXE	ATM-Intellect Workstation	7777	CPDVAlarmServer.exe
22	CPDVNETSERVER.EXE	CPDV	24345	VIDEOSRV.EXE

23	CPDVNETSERVEREX1.EXE	CPDV	7755	VIDEOSRV.EXE
24	VIDEOSRV.EXE	Agent of Control	7777	VIDEOSRV.EXE
25	STATEUPS.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
26	BATDISCH.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
27	POWEROFF.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
28	POWERON.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
29	forward.run	Data gateway	22327	-

Tab. b—3 List of TCP ports used by Transport Flow Control modules

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	DT_SERVER.RUN	Traffic Detector	22151	-
2	DT_SERVER.RUN	Traffic Detector	20900	VIDEO.RUN
3	DT_SERVER.RUN	Traffic Detector	22152	-
4	DT_VIEWER.RUN	Traffic Monitor	22152	-
5	ITV_VEHICLE_DETECTOR.RUN	Vehicle Detector	22182	-
6	LPRDB.RUN	External Plates DB	22100	-
7	RADAR.RUN	Speed traps server	22157	-
8	ROSSI_FLOW.RUN	Potok recognition server	22119	-
9	TRAFFIC_PROCESSOR.RUN	Vehicle Processor	22181	-
10	URMLPR.RUN	LPR channel	22137	-

11	URMLPR.RUN	LPR channel	20900	VIDEO.RUN
12	VEHICLE_TRACER.RUN	Vehicle Tracer	22187	-

Tab. b—4 List of TCP ports used by Face search and recongnition modules

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	FACE_MONITOR.RUN	Face Monitor	21919	-
2	FACE_RECOGNITION_PROXY.RUN	Face Search Server	22207	-
3	FACE_RECOGNITION_WEB_PROXY.RUN	Web access to face search	22214	-
4	FIR_MONITOR.RUN	Recognized Faces Monitor	22135	-
5	FIR_MONITOR.RUN	Recognized Faces Monitor	20985	FIRSERVER.RUN
6	FIR_MONITOR.RUN	Recognized Faces Monitor	20900	VIDEO.RUN
7	FIRSERVER.RUN	Face Recognition Server	22136, 10000	-
8	WEBVIEWER.RUN	Web-interface viewing module	22216	-
9	FACE_CLIENT.RUN	Face recognition and search interface	22297, 20985	FIRSERVER.RUN via 20985

Tab. b—5 List of TCP ports used by POS modules

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	ALERTNURSES.RUN	Alert nurse	22196	-
2	POS.RUN	POS terminal	21012	-
3	POSAGGREGATOR.RUN	POS Replicator	22245	-
4	POSVIEWER.RUN	Receipt viewer	22111	-
5	POSVIEWER.RUN	Receipt viewer	20977	POS.RUN

6	McMixer.run	McMixer	22321	-

Tab. b—6 List of TCP ports used by ACFA, AM/Pass&ID, EM/Photoidentification, T&A modules

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	abc.run	ABC	22031	-
2	abc_cr.run	ABC control reader *	22235	-
3	agency_person.run	Visitor Management System	21057	-
4	aiu.run	"777 ROVALANT" system *	22145	-
5	aiu3.run	Rovalant 777 ISS *	22217	-
6	anson.run	Anson ACS *	22267	-
7	APDA.run	Tempo Reale ACS *	22188	-
8	apollosdk.run	ApolloSdk	22204	-
9	Bagulnik2.run	Bagulnik2 *	22195	-
10	biosmart.run	BioSmart *	22236	-
11	bolid.run	"Bolid" (COM server)	21025	-
12	castle.run	Castle server	22183	-
13	castle_cr.run	CASTLE control reader *	22231	-
14	chrysantemum.run	PRHK *	22198	-
15	DB_Import.run	Data import	21022	-
16	Dunai2.run	Dunai 2 *	22255	-
17	dunai3.run	Dunai 3 *	22255	-
18	Elsys.run	Elsys *	22206	-
19	forsec.run	ForSec *	22166	-
20	forteza.run	Forteza *	22237	-
21	Galaxy.run	Galaxy Dimension	22189	-
22	galaxy2.run	Honeywell ACS/SGPS	22239	-
23	gate_cr_z2.run	Z2 control reader *	21222	-
24	Hid.run	VertX / Edge ACS	22220	-
25	hunter.run	HUNTER PRO SFA	22256	-
26	intrepid.run	Intrepid Interface Module	22172	-
27	Intrepid2.run	Intrepid Grunt	22229	-
28	Intrepid3.run	Intrepid II System	22240	-
29	keyking.run	KeyKing ACS	22244	-
30	keywatcher.run	KeyWatcher ACS *	22258	-
31	keywatcher_interface.run	KeyWatcher ACS Interface *	22259	-
32	kodos.run	Kodos server *	22130	-

33	kodos_cr.run	KODOS control reader *	22155	-
34	kronverk.run	Kronverk *	22139	-
35	ksu_cr.run	KSU control reader *	22338	-
36	legos2.run	"Octagram" ACS/SFA *	22190	-
37	Magistrator.run	Magistrator *	22161	-
38	nac.run	"NAC" ACS *	21020	-
39	nc.run	HoneyWell N1000	21052	-
40	ncg9.run	Controller NCG-9	22266	-
41	net.run	"Net" system *	22185	-
42	nskat.run	SKAT ACS *	22248	-
43	opc_wrapper.run	OPC Wrapper	22263	-
44	Optex.run	Optex System	22232	-
45	orion.run	Bolid (SDK Orion) *	22173	-
46	paradox.run	Paradox SFA/ACS	22192	-
47	parsec_pr_x08.run	PR-x08 control reader *	22226	-
48	Paxton_NET2.run	ACS Paxton NET2	22233	-
49	pelco.run	PELCO	22234	-
50	perco.run	"Perco" ACS *	21019	-
51	PercoS20.run	Perco S20 controller *	22246	-
52	PhotoIdentification.run	Photo Identification	22163	-
53	pl.run	Polon Alfa System	22242	-
54	pnet3.run	ParsecNET 3 ACS/SFA *	22264	-
55	ravelin.run	Gate Parking ACS	22227	-
56	RifString.run	RifString system *	22197	-
57	Rosslare.run	Rosslare ACS *	22203	-
58	rovalant_a6_a16.run	"ROVALANT (A6, A16)" system *	22165	-
59	rubeg8_isb.run	Rubeg 8 ISS *	22256	-
60	rubezh.run	Rubeg SFA *	22261	-
61	rubicon.run	Rubicon SFA *	22209	-
62	rusguard.run	"RusGuard" ACS *	22250	-
63	salto.run	SALTO Server	22208	-
64	satel.run	"Satel"	21998	-
65	securiton.run	"Securiton" ACS *	22247	-
66	sintegral.run	Strelec-Integral SFA *	22257	-
67	sphinx.run	Sphinx server	22177	-
68	strelec.run	"Strelec" SFA *	22162	-
69	topol.run	Topol PSS *	22241	-
70	trombon.run	Trombone SFA	22224	-
71	tss2.run	"TSS" ACS/SFA *	22218	-
72	unipos.run	"UniPos" 7002	22184	-
73	nipos5xxx.run	UniPos ACFA 5100-5200	22211	-

74	vers_rs.run	VERS ACS*	22126	-
75	WorkTime.run	Work Time Accounting	22133	-
76	xabc.run	Fortecia ACS *	22260	-
77	zline.run	"ZLine" FSA *	22243	-
78	account_manager.run	Access Manager	22291	-
79	event_manager.run	Event Manager	22287	-
80	dsc.run	"DSC" FSA	22292	-
81	IntellectToNextBridge.run	ACFA Intellect - Axxon Next Bridge	22293	-
82	rubezh_global.run	"Rubezh Global" FSA *	22294	-
83	satel2.md	"Satel INTEGRA" FSA	22296	-
84	Unicard.run	"Unicard" ACS	22298	-
85	zk.run	"ZK Teco" ACS	22299	-
86	glx2.run	"Galaxy Dimension v.2" FSA	22300	-
87	sintegral_web.run	"Strelec Integral Web Api" ACS *	22301	-
88	XTralis2WayProtocol.run	"ADPRO" PID	22303	-
89	Chomtech.run	"Chomtech" ACS	22304	-
90	Rbg08.run	"Rubezh-08" ACS *	22305	-
91	topol3.run	"Topol-3" PID	22306	-
92	nedap_retail.run	"Nedap retail" FSA	22307	-
93	WinPak.run	"HoneyWell WinPak" ACFA	22308	-

94	fs80cr.run	BioSmart FS80 control reader	22309	-
95	evs_sk.run	"EVS" ACS *	22310	-
96	acfa_emulator.run	Virtual Access Server	22311	-
97	pvscr.run	PVS control reader	22312	-
98	bsveins.run	"Biosmart UniPass" ACS *	22313	-
99	RubezhGlobal.run	Third-party integration for R3 protocol of the Rubezh company. Not included to ACFA-Intellect.	22314	-
100	an.run	OPC Wrapper	22315	-
101	nedap_aeos.run	"Nedap AEOS" ACS	22317	-
102	parsec_pr_p08.run	Parsec PR-P08 control reader	22318	-
103	suprema_cr.run	Suprema BioMini control reader	22319	-
104	UfdVolna.run	"Volna Alpha" PID	22320	-
105	SCardDriver.run	PCSC Wrapper control reader	22324	-
106	NoderEe12.run	"Aritech FP2000" FSA	22325	-

107	LockerBox.run	"LockerBox" ACS *	22326	-
108	suprema_2.run	"Suprema 2" ACS	22328	-
109	NoderEw1.run	"Noder EE12" ACS	22329	-
110	hikvision.run	"HikVision" ACS	22330	-
113	suprema_realscan.run	Suprema Realscan control reader	22333	-
114	stalt.run	"Stalt-SV" ACS *	22334	-
116	percoS20v2.run	"PERCo-S-20" ACS *	22340	-
117	dingo.run	Dingo *	22346	-
118	snmpwrapper.run	SNMP Wrapper Parent object	22277	-
119	MorphoLite.run	MorphoAccess SIGMA Lite	22345	-
120	ratek.run	Ratek *	22352	-

* These integrations shall not be included into the English version of ACFA subsystem.

21 Requirements for extension modules

a. Connected modules

The SMP shall support connecting additional modules to perform the following functions:

1. Based on a face photo, search for times when the face appears in the guarded area.
2. Automatic identification by comparing faces in the video frame with reference images stored in a database.
3. Monitoring and access control subsystem.

4. Integration of fire and security alarm hardware.
5. Integration of perimeter security hardware.
6. Automated monitoring of transport flows.
7. Monitoring of checkout transactions in retail establishments.
8. Automated monitoring of rail car movements and loading/unloading.
9. Workplace time and attendance tracking.
10. Pass and ID office configuration.
11. ATM protection.
12. Generation of reports from data in the databases of the connected modules.
13. Photoidentification.

b. Requirements for Face Search module

The Face Search module shall support:

1. Finding a person's face in a video frame
2. Saving captured faces to a database
3. Search for faces in the database based on a face photo

c. Requirements for Facial Recognition module

The Face Recognition module shall support:

1. Finding a person's face in a video frame
2. Obtaining the biometric parameters of faces
3. Comparing the face in a video frame with reference images via biometric parameters
4. Keeping a database of faces for recognition
5. Creating a photo and video archive

d. Requirements for Access Control integration modules

The Access Control integration modules should support:

1. Combining access control with other security systems at the same control centers of the distributed system.
2. Programming Access Control system reactions to event, including events that occur in other security subsystems.
3. Providing a high degree of automation of the mechanism for managing access rights.
4. Combining users into groups.
5. Monitoring the system status and operability.

e. Requirements for Fire and Security Alarm integration modules

Fire and Security Alarm integration modules should support:

1. Processing of information from control panels, alarm sensors, and other notification devices
2. Control of actuators, audio and light alarm devices, etc.

f. Requirements for modules for Perimeter Security System integration

Modules for Perimeter Security System integrations shall support:

1. Processing of information from perimeter security sensors as well as sensors installed at the entrance to the object whose perimeter is secured
2. Control of actuators, security notification devices, entry/exit control devices (turnstiles and boom barriers)

g. Requirements for Transport Flow Control modules

Modules for automatic control of Transport Flow Control shall support:

1. Recognizing license plates.

2. Matching recognized license plates with numbers found in the database connected to the Auto Intellect software.
3. Measuring vehicle speed.
4. Measuring overall transport flow movement and information on the movement of each individual vehicle.
5. Single-source registration and processing of events plus generation of notifications and system responses based on flexible macros.
6. Creating a photo and video archive.
7. Support scalability of the software.

h. Requirements for POS modules

Point-of-Sale (cash desk/checkout) transaction control modules shall support:

1. Real-time synchronized viewing of surveillance video with superimposed receipt contents and cash register events
2. Synchronized viewing of surveillance video with receipt contents and cash register events
3. Custom queries for searching the video archive based on receipt contents and system events
4. Integration with popular POS terminals
5. Support for creating, viewing, and processing summary and detailed events based on cash register events, within the web report subsystem

i. Requirements for modules for Automated Monitoring of Train Car Movement

Modules for train car number recognition shall support:

1. Automatic monitoring of dispatch of production from a site by rail
2. Tracking of rail movement at weighing and sorting stations

3. Automated receipt of rail cargo and shipment monitoring
4. Monitoring of car weight and liquid level in tank cars

j. Requirements for Report Generation module

The web report subsystem should forma site, on a LAN or on the Internet (depending on the security system requirements), that is implemented on the basis of the Security Management Platform. Administration and use of the subsystem shall be performed exclusively through a web interface.

The web interface of the report subsystem should allow for the following:

1. Configuring differentiated access of users to POS reports and reports from the workplace time and attendance module.
2. Configuring automated functioning of the report subsystem.
3. Configuring reports of POS events (configuration of POS event statuses, etc.).
4. Compilation and export of summary and detailed reports of POS events.
5. Compilation and export of summary and detailed reports of workplace time and attendance.
6. Viewing the video archive starting from the registration time of the event selected in the report.
7. Viewing of data from the cash register corresponding to a selected POS event.
8. Assigning statuses to registered POS events.
9. Compiling and exporting reports for saturation of the observed area.
10. Compiling and exporting reports for the number of visitors to the observed area.
11. Compiling and exporting reports for events from Transport Flow Control modules.
12. Photo-based face search

k. Requirements for Time and Attendance module

The Time and Attendance module shall support the following functions:

1. Viewing the personnel structure of the company for each department and getting information for each employee.
2. Generating schedules and work plans of varying durations and assigning these to an employee or entire department.
3. Tracking employee accountability and overtime documents.
4. Calculating the total time worked for each employee of a unit and presenting the results as a table.
5. Creating a report with the total time worked by employees.

l. Requirements for Access Manager/Pass and ID office module

The Access Manager/Pass and ID office module shall provide for the following:

1. Monitoring compliance with the access regime for employees and visitors to the site via automated access control systems as well as their movements around the site, in accordance with their access levels.
2. Configuring the rights of users to edit and view departments and employees.
3. Creating and configuring access levels both for each employee individually and for entire departments.
4. Creating templates and stamps for electronic passes for employees and visitors to the guarded site.
5. Synchronization of added photos with face search and recognition modules.

m. Requirements for ATM protection modules

ATM protection modules should support:

1. Recording video:

1.1. in continuous mode

1.2. when motion detection is triggered

1.3. when ATM protection sensors are activated (vibration sensor, safe door opening sensor, temperature sensor, fire sensor)

2. Synchronizing ATM transaction data and sensor readings with the video archive.
3. Viewing video archive stills and transaction data on a remote monitoring workstation.
4. Receiving, processing, and recording sensor alarms and messages from an ATM's control computer.
5. Sending alarm messages, video stills, and transaction data to a remote monitoring workstation using pre-existing X.25 and TCP/IP communication lines of the ATM.
6. Searching for information in the video archive based on ATM events and sensor alarms.
7. Remote centralized monitoring of the status of the ATM protection system, in real time.
8. Remote monitoring of the status of ATM hardware.
9. Creating reports for ATM transactions and events, sensor alarms, and hardware and communication line status.

n. Requirements for Event Manager/Photoidentification module

The Event Manager/Photoidentification module should provide for the following:

1. Displaying photos and information about user in the Event Manager/Photoidentification window while the access request.
2. Displaying image from camera in the Event Manager/Photoidentification window while the access request.
3. Possibility to create the template of the pass which is displayed in the Event Manager/Photoidentification window for each of readers.
4. Possibility to choose objects by events of which the displaying of Event Manager/Photoidentification window is performed.

5. Configuring actions available for operator in the Event Manager/Photoidentification window while the access request.
6. Maintaining, storing and displaying the operator action log.

22 Requirements for Operator interface

The program interface shall contain the following components:

1. Main Control Panel
2. Video Monitor
3. Fisheye Camera Monitor
4. Audio Player
5. Telemetry control window
6. Custom Dialog Box
7. Long-term Archiving Panel
8. Alarm Notification Window
9. Event Log
10. Operator Log
11. Map
12. Video Surveillance Monitor for web browsers
13. Panoramic Viewing Tile
14. Live audio switch

a. Main Control Panel

i. Purpose

The Main Control Panel is the core of the interface for controlling SMP.

ii. Functions

The Main Control Panel shall provide access to the following functions of the Program:

1. Start and quit the Program.
2. Configure the Program.
3. Control the display of various interface windows of the Program.
4. Display technical messages about the Program's functioning.
5. Perform macros by manual command.
6. Display information about the current version of the Program.

iii. Requirements for the interface

The Main Control Panel shall be located in the upper-right corner of the screen.

When inactive, the pane shall automatically disappear from the screen. To use the pane again, one of the following actions must be performed:

1. Move the cursor to the upper-right corner, after which the Program's Main Control Panel shall appear on the screen.
2. Hold the F8 key on the keyboard. In addition to display of the Control Panel, a Run menu shall also open.
3. Left-click the icon in the Windows task bar. In addition to display of the Control Panel, a Run menu shall also open.

The interface elements of the Main Control Panel for SMP are described in the table (see Tab. a—1).

Tab. a—1. Interface elements of the Main Control Panel

Name	Element type	Function
Information window	Text box (cannot be edited)	The information window displays hints for how to use the program, as well as error messages
Interfaces	Button	Allows selecting and displaying interface windows on the desktop. The **Hide all** option allows hiding all active visible windows of the Program.
Run	Button	This button allows accessing different functions for managing the Program: starting, quitting, and configuring the program; manual execution of macros; display of debugger windows, as well as display of information about SMP including: • version of SMP and installed extension modules; • equipment installed; • license key limitations to the number of objects.

b. Video Surveillance Monitor

i. Purpose

The Video Surveillance Monitor is designed to display and manage Video Tiles.

ii. Functions

The Video Surveillance Monitor shall provide access to the following functions of the Program:

1. Display video imagery from video surveillance cameras.
2. Manage video surveillance modes.
3. Process of video from video cameras.
4. Manage footage from video cameras.
5. Working with archives, including archive viewing and export.
6. Display information about the status of video cameras.
7. Protecting important archive recordings against loop recording.
8. Creating bookmarks – several recordings protected against loop recording; a comment can be added.
9. Viewing bookmarks.

iii. Requirements for interface

The Video Surveillance Monitor consists of a field for displaying viewing tiles and a toolbar, which shall contain the elements described in the table (Tab. b—1).

Tab. b—1 Description of interface elements in the Video Monitor

Name	Element type	Function
Changing the number of displayed tiles	Button group	Change the number of displayed Viewing Tiles on a Video Monitor
Switching layouts	Button	Switching layouts
Flipping through video tiles	Button group	Flipping through video tiles
Current date and time	Text box (cannot be edited)	Display current date and time
Functional shortcut menu	Menu	Access functions including arming (disarming) video cameras, processing video imagery, controlling video recording, exporting and printing stills, etc.

For ease of use of the Video Surveillance Monitor and Viewing Tiles, keyboard combinations ("hot keys") shall be reserved, as described in the table (Tab. b—2).

Tab. b—2. Hot keys for the video monitor

Key combinations (hot keys)	**Action**	**Notes**
0 .. 9 Num (number pad)	Select the active Viewing Tile	The number of the Viewing Tile is the number of the relevant keyboard key. To select a Viewing Tile with a two-digit number, press both of the numbers in quick succession.
F1 .. F8	Select number of Viewing Tiles to display	F1: 1 tile F2: 4 tiles F3: 9 tiles F4: 16 tiles, etc.
Ctrl + R Ctrl + T	Controlling video recording	Ctrl + R: start recording Ctrl + T: stop recording

Key combinations (hot keys)	**Action**	**Notes**
Shift + LeftClick/RightClick	Scale Viewing Tile contents	Shift + LeftClick: zoom in by one step Shift + RightClick: zoom out by one step
Tab	Switch from the active Viewing Tile to archive mode and vice versa	
Ctrl + / Ctrl + Spacebar Ctrl + * Ctrl + Left/Right	Control archive playback (playback control panel)	Ctrl + /: play Ctrl + Spacebar: stop Ctrl + *: pause Ctrl + Left/Right: previous/next frame (while paused)
Ctrl + A/D	Arming (disarming) a video camera	Ctrl + A: arm camera Ctrl + D: disarm camera
Ctrl + E/P	Working with individual frames	Ctrl + E: export (save) frame Ctrl + P: print frame

Key combinations (hot keys)	Action	Notes
Ctrl + W	Increase imagery contrast	Sets contrast to maximum. To return to the previous value, press the key combination again.
Ctrl + S Ctrl + H	Add (remove) camera mask	Ctrl + S: show camera mask Ctrl + H: hide camera mask

c. Audio Player

i. Purpose

The audio player is designed for Operator interaction with the audio monitoring subsystem, which supports audio monitoring and recording at system sites.

ii. Functions

The audio player shall provide access to the following functions of the Program:

1. Play back the audio component of events.
2. Record the audio component of events.
3. Play back audio recordings triggered by alarm events.
4. Save recorded audio components of events as audio files in standard Windows format.

iii. Requirements for interface

The upper portion of the interface window shall include a list of microphones that can be managed from the audio player. For each microphone there shall be a status indicator and real-time indicator of microphone signal strength.

The Audio Player window shall contain buttons for controlling recording (arming and disarming a microphone) and a button for starting/stopping playback of audio from the microphone, as well as a list of recordings made from the selected microphone on the specified day.

The start and end time, as well as duration, shall be given for each audio recording.

Selection of a date for viewing accessible recordings shall be present.

Beneath the list of audio recordings, there shall be a panel for controlling playback of recordings.

There shall also be buttons for controlling playback of the selected recording and a button for exporting the recording to a file.

d. Integrated Telemetry Window

i. Purpose

The Integrated Telemetry Window is designed to control PTZ units connected to the System (such as a camera's PTZ unit).

ii. Functions

The Integrated Telemetry Window shall provide for:

1. Controlling PTZ units.

2. Controlling lens zoom.
3. Configuring video camera lens zoom.
4. Selecting and specifying custom settings for PTZ units.

iii. Requirements for interface

The necessary elements of the interface for the Integrated Telemetry Window are described in the table (Tab. d—1).

Tab. d—1. Interface elements of the Integrated Telemetry Window

Name	Element type	Function
Minimize	Button	Minimize the Integrated Telemetry Window (minimizes the client portion of the window, leaving only the window's title bar).
Camera	Drop-down list	Select the camera whose PTZ unit the user wants to control.
Speed	Allowable values	Set the relative speed of motion of the video camera when controlling the PTZ unit for that camera.
Control	Button group	Controlling the orientation of the camera lens
Zoom	Button group	Controlling lens zoom.
Focus	Button group	Configuring video camera lens zoom.
Presets	Button group and drop-down list	Selecting and specifying custom settings for PTZ units
Size	Button	Change the size of the Integrated Telemetry Window

e. Custom Dialog Box

i. Purpose

The Custom Dialog Box allows controlling different devices and modules of the System.

ii. Functions

The Custom Dialog Box shall provide:

1. Control of various devices and modules of the System
2. Access to custom System functions

iii. Requirements for interface

The Custom Dialog Box shall display a custom-configurable set of items created by the Program administrator during setup.

f. Long-term archiving Panel

i. Purpose

The Long-term archiving panel allows controlling and managing the Long-term archive on the Failover Server.

ii. Functions

The Long-term archiving Panel shall allow:

1. Monitoring the status of the Long-term archive.
2. Performing manual backup of video recordings.
3. Performing automatic backup of video recordings.
4. Selecting video cameras for which backups will be made.

5. Setting a time interval for performing backup of video recordings (separately for each camera).

iii. Requirements for interface

Above the panel there shall be **Monitoring** and **Schedule** tabs. The **Monitoring** tab provides access to surveillance and manual management of the Long-term archive. The **Schedule** tab is for configuring automatic functioning of the Long-term archive.

The **Monitoring** tab shall contain the elements described in the table (Tab. f—1).

Tab. f—1 Interface elements of the Long-term archiving Panel

Name	Element type	Function
Start	Button	Start backup
Stop	Button	Stop backup
Archiving period	Text box (can be edited)	Boxes for setting the time interval for backup
Video camera	Table	Selecting video cameras and backup status
Select all	Button	Simultaneous selection (de-selection) of all video cameras

The **Schedule** tab has a table for configuring automatic backups.

g. Alarm notification window

i. Purpose

The alarm notification window informs the Operator when the System has recorded different types of alarms and information events.

ii. Functions

The alarm notification window shall provide:

1. Automatic notification of the Operator when the System has recorded information events
2. Automatic notification of the Operator when the System has recorded alarm events
3. Ability for the Operator to process the information events and alarms that have been recorded by the System

iii. Requirements for interface

By default, the alarm notification window is not displayed. It is displayed only when the System has recorded information events or alarms, and appears above all other windows in the user interface of the Program. The alarm notification window is displayed even if all elements of the user interface of the Program are hidden.

The necessary elements of the interface for the alarm notification window are described in the table (Tab. g—1).

Tab. g—1. Elements of the interface for the alarm notification window

Name of interface element	Element type	Notes
Alarm	Button	Event name
Date and time	Text box (cannot be edited)	Date and time of event
Source	Text box (cannot be edited)	Object that is the source of the event
Area	Text box (cannot be edited)	Approximate area (zone) in which the event source object is located
Notes	Text box (cannot be edited)	Additional information about the event

Name of interface element	Element type	Notes
Control of event processing	Button group	Interface elements for accepting or declining events
Navigation	Button group	Group of interface items for navigating between events

h. Event log

i. Purpose

The event log displays data about events recorded by the System (with support for filtering the data displayed, based on event type).

ii. Functions

The event log shall:

1. Display the list of all events, recorded by the System.
2. Displaying the list of events registered in the system according to the preset filter.
3. Show the following information about the displayed event: source, event name, area, date and time of event, and additional event information.
4. Save and print a report about recorded events.
5. Switch to the location on the Map of the event source object.
6. Allow playing back video from the source video camera for the event from the Event Log child window.

iii. Requirements for interface

All displayed events should be presented in a table of events with the columns described in the table (see Tab. h—1).

Tab. h—1. Description of the interface of the Event Log Window

Column name	Notes
Source	Object that is the source of the event
Event	Event name
Zone	Approximate area (zone) in which the event source object is located
Notes	Additional information about the event
Date	Date and time of event
Time	
Card	Card code for events related to access. This column can be disabled while configuring the program object.

There shall be the following features:

1. A checkbox in the Event viewer interface window intended to display the filter list preset while configuring the system. Activation of one or more filters shall be performed by setting the checkboxes next to their names.
2. There shall be a dynamic filter by each column.
3. Additionally, the icon across from the name of the event source object shall indicate the current status of the object.
4. Each event in the table shall have a functional shortcut menu, opened by right-clicking the line with the name of the event in the table or by pressing the keyboard combination Ctrl + P. The specific contents of the functional shortcut menu shall depend on the type of event source object.

i. Operator log

i. Purpose

The operator log window is made for processing events registered by objects in the security system and for searching for events in the archive.

ii. Functions

The operator log window shall provide:

1. Display in the interface window of events that have been registered by security system objects
2. Assignment of a status (type) to registered events
3. Addition of comments to events
4. Writing of events to the archive
5. Search of events in the archive
6. Viewing of event video
7. Displaying an event source object on the map
8. Escalating non-processed events to the operator protocol of a higher level
9. Creating reports on events in the archive
10. Creating events on system objects manually

iii. Requirements for interface

A description of the interface elements required for the operator log window is given in the table (Tab. i—1).

Tab. i—1 Description of interface elements in the operator log window

Name	Element type	Description
Current events tab		
Event control panel		
Notes	Text box (can be edited)	Comments field

Name	Element type	Description
Apply to all	Check box	When the check box is selected, the type assigned to the event will be assigned for all events on the **Current events** tab.
Set bookmark	Check box	Enables automatic creation of a bookmark in the archive when the operator processes the event. The name of the bookmark should be the comment.
Status	Button group	Button for assigning event type (status)
Escalation	Button	Events escalation to the operator protocol of a higher level
Postpone	Button	Allows postponing event processing once for the period specified while configuring the Operator protocol
Log in to archive	Button	Go to archive for viewing and exporting event video
Find on map	Button	Go to map layer on which the event source is located
Checklist	Checkbox list	The list of actions that must be performed for the event processing.
Event cell		
Alarm still	Image	Alarm still with a caption containing the name and number of the camera.
Buttons for switching frames	Buttons	Switching frames from several cameras (if several cameras are attached to an object).
Event information	Text box (cannot be edited)	Event information: ▪ Name of event in the system

Name	Element type	Description
		▪ Object that registered the event ▪ Time until the event is assigned the "Unprocessed event" status ▪ Date and time of event registration ▪ Additional settings or is escalated
Search event archive tab		
Department	Dropdown list	The list of departments which the operator belongs to. If the value is not selected, then all operators registered in the system are displayed.
Operator	Drop-down list	Operator selection list
Region	List	Region selection list
Object	Drop-down list	Object selection list
Start date	Button	Button for setting the beginning of the time period
End date	Button	Button for setting the end of the time period
Event types	Check box group	Types of events to be searched for
Search	Button	Button to start search
Go to archive	Button	Button for going to the archive to view event video
Create report tab		
List of objects	Check box group	The list of objects by events of which the report can be generated
List of events	Check box group	The list of events by which the report can be generated
Start date	Button	Specifying the date after which events get into the report

Name	Element type	Description
End date	Button	Specifying the date after which events do not get into the report
Combine similar responses	Check box	Enables showing the event in the report only once and not for each operator individually.
Generate	Button	Showing report on the screen
Create event tab		
Comment	Text field	Specifying description of the event
Date/time	Button	Specifying event date and time
Type	Drop-down list	Selecting the type of event source object
Object	Drop-down list	Selecting the event source object
Generate	Button	Creating event

In the lower part of the **Search event archive** tab, there is a table that contains the search results.

A description of the table of the event log is given in the table (Tab. i—2).

Tab. i—2 Description of event log table

Column name	Description
Type	Event type icon
Source	Object that is the source of the event
Init. event	Initial event
Operator	Operator who processed the event
Date/Time	Date and time when the event was registered
Notes	Operator comments

j. Map

i. Purpose

The map is for observing and managing System devices (video cameras, microphones, sensors, and relays) as well as for performing macros.

ii. Functions

The Map shall:

1. Generate a multi-layer interactive map (visual blueprint) of the monitored site.
2. Provide interactive monitoring of the status of all System devices on the Map.
3. Draw virtual lines to divide the secured facility/location into regions and areas.
4. Support for automatic switching and search for recursive alarm connections between Map layers.
5. Control actuator devices of the System on the Map.
6. Perform macros.

iii. Requirements for interface

The appearance of the Map shall depend on the layout of the monitored site and be configured during Program setup.

System devices shall be depicted in symbolic form on the Map. The status of each device shall be shown. Access to device functions shall be performed through a functional shortcut menu for the device, opened by right-clicking the depiction of the device on the Map.

If the Map has several layers, there shall be a button for switching between the Map layers.

In addition, the button for switching between Map layers shall indicate the presence of alarms that have been registered by the devices on the corresponding Map layer.

k. Video Surveillance Monitor for web browsers

i. Purpose

The Video Surveillance Monitor for web browsers is designed for remote video monitoring of sites through a web browser over TCP/IP. Remote video monitoring through a web browser shall not require installation of SMP on the Operator's workstation (however, the browser used shall support Java).

ii. Functions

The Video Surveillance Monitor for web browser shall provide for the following:

1. Remote video surveillance without installing SMP on the Client.
2. Changing the number of Viewing Tiles displayed simultaneously in the Video Surveillance Monitor through the web browser.
3. Arming and disarming video cameras.
4. Managing detection tools.
5. Video recording
6. Working with video archives.
7. Controlling PTZ units.

iii. Requirements for interface

The Video Surveillance Monitor for web browsers consists of a field for displaying Viewing Tiles and a toolbar, which shall contain the elements described in the table (Tab. k—1).

Tab. k—1 Description of interface elements in the Video Surveillance Monitor for web browsers

Name of interface element	Element type	Function
Changing the number of displayed windows	Button group	Changing the number of displayed tiles
Archive	Button	Switching to archive playback mode
Date and time	Text box (cannot be edited)	Display current date and time
Camera	Menu	Selection of a video camera and access to some functions The functional shortcut menu can be accessed by left-clicking the number of the video camera in the

The color of the frame of the Video Surveillance Monitor and the text of the name of the video camera shall indicate the camera's current status.

l. Panoramic Viewing Tile

i. Purpose

The Panoramic Viewing Tile is for creating and using panoramic video imagery. The Panoramic Viewing Tile is functionally divided into two parts: a video surveillance toolbar and a field for displaying video.

ii. Functions

In use of the Panoramic Viewing Tile, the following modes for processing video shall be supported:

1. Movement of video in the window for video display
2. Correction for perspective
3. Restoration of video to a specified aspect ratio
4. Turning

5. Cropping
6. Video zoom in/out

iii. Requirements for the interface

The Panoramic Viewing Tile consists of a field for displaying viewing tiles and a toolbar, which shall contain the elements described in the table (Tab. l—1).

Tab. l—1 Description of interface elements in the Panoramic Viewing Tile

Name of interface element	Element type	Function
Processing	Button group	Video image processing
Date and time	Text box (cannot be edited)	Display current date and time

m. Fisheye Camera Monitor

i. Purpose

The Fisheye Camera Monitor is intended for viewing video streams and archive video from fisheye cameras.

ii. List of functions

The Fisheye Camera Monitor shall support the following Program functions:

1. Support dewarping of video into one of the following formats:
   1.1. Single View (virtual PTZ)
   1.2. Panorama 360°
   1.3. Panorama 2*180°
2. Access to selection of any particular dewarping format shall depend on the camera position and dewarper type.

3. Viewing in a dewarped format of the video stream received from fisheye cameras
4. Viewing in a dewarped format of archive video generated with use of the video stream received from a fisheye camera.

iii. Interface requirements

The Fisheye Camera Monitor window consists of a field for displaying Dewarp Windows. Each Dewarp Window, in addition to video, shall display the current date and time as well as the name of the camera whose video is used for dewarping.

Each Dewarp Window shall contain a button for jumping to the archives. The transition to/from archives shall be made simultaneously for all dewarp windows of a single camera.

n. Live sound switch

i. Purpose

The Live sound switch shall send the audio signal received from any audio source (microphone) to any sound receiver (speaker) for playback.

ii. List of functions

The Live sound switch shall ensure transmission of an audio signal received from any audio source (microphone) to any sound receiver (speaker) for playback.

iii. Interface requirements

The interface elements in the sound switch window are given in the table (Tab. **n**–1).

Tab. n–1 Description of interface elements of the Live sound switch

Element name	Element type	Function
Execute	Button	Send signal from audio sources to receivers

Element name	Element type	Function
Speakers	List	Specify list of audio receivers to be used for playback
Microphones	List	Specify list of audio sources whose signal is to be sent to speakers

o. HTML interface

i. Purpose

The HTML Interface window is designed for displaying specified web-page or other files, including text and images.

If there is video displaying or sound playing back on the web-page, it will be also available in the **HTML interface** window.

ii. List of functions

The HTML Interface window performs the following functions:

1. Display web-pages located as locally on computer, as in the Internet.
2. Display images and text files.
3. Display video data and play back sound from the displayed web-page.

iii. Interface requirements

View of the HTML Interface window entirely depends on settings.

By default the list of cameras that can be armed/disarmed must be displayed in the HTML

Interface window after creating the corresponding object.

The table describes hotkey combinations available at working with the HTML interface:

Hotkey/ hotkey combination	Performed action
Backspace	Back
Alt+left arrow	
Shift+Backspace	Forward
Alt+right arrow	
F5	Update page
Ctrl + + or -	Zoom in/out page

p. Display manager

i. Purpose

The display manager is used to control video walls and attract the attention of the Operator.

ii. Functions

The display manager provides:

1. Control over Video Monitors added to the screens of various computers.
2. Creating, editing and deleting layouts of the Video Monitor.
3. Creating temporary layouts of the Video Monitor.

iii. Interface requirements

The interface of the Display manager must contain the following elements:

Element name	Element type	Function
The **Screen activation** group		
Computer	Dropdown list	Select the computer to which the required screen is assigned to
Screen	Dropdown list	Select the screen
Activate	Button	Activate the selected screen
The **Setting and activation of monitors** group		
Monitor	Dropdown list	Select the **Monitor** object
Layout	Text field	Search for layout by name
Layout	List	Add, delete and change the layout order
Camera	Text field	Search for camera by name
Camera	List	Select cameras for layout
Apply	Button	Apply changes in the layout
Cancel	Button	Cancel changes and switch to the previously saved layout
Show	Button	Show the layout on the selected Video Monitor without saving it
Clear	Button	Delete all cameras from the layout
Refresh	Button	Refresh images in the preview windows of cameras on the layout
Layouts	Button	Select the standard layout in the list
Layout creation panel	Set of surveillance windows	Layout creation

q. State Statistics

i. Function

State statistics shall perform monitoring of the number of objects in the specified states.

ii. List of functions

State statistics provides the following functions:

1. Displays the table showing the number of objects of the selected type that are in a particular state at the current time.
2. Displays the graph showing the number of objects of the selected type that were in particular states for the last 15 minutes.
3. Displays the graph showing the number of objects of the selected type that were in particular states for the specified period of time.

iii. Interface requirements

The State statistics interface shall contain the following elements:

Element name	Element type	Function
The **Table** tab		
Object	Column	Shows object type
State	Column	Displays the state of the object with the specified color indication.
Quantity	Column	Displays the number of objects in the corresponding state.
The **Graph** tab		
Key	Text field	Shows explanation of the color cod on the graph.
Graph	-	Displays the object state graph for the last 15 minutes.
The **Retrospective** Tab		
Calendar	Calendar	Set the time period to the minute.
Key	Text field	Shows explanation of the color cod on the graph.
Graph	-	Displays the object state graph for the selected time period.