Table of Context

The intended audience of this Guide is the advanced user of Windows XP/Vista/7/8 operating system who has knowledge of the manuals for all devices of the Orion Integrated Security System
The aim of the Guide is to explain how to configure and operate the Orion Pro Suite software product. The Guide information is intended both for the administrators and operators of the Orion Pro System.

1. About the System

The Orion Integrated Security System (hereinafter called Orion ISS) is the combination of hardware and software solutions to build intrusion (detection) and fire alarm systems (IFS), fire extinguishing systems, access control system (ACS), and video surveillance system as well building automation systems.

The Orion Pro Suite is a software platform of the Orion ISS designed to provide comprehensive security for banks, small and large industrial facilities, commercial buildings, warehouses, residential buildings, cottages, hotels, parking areas, and education facilities.

The Orion Pro Suite offers capabilities to provide simultaneous online monitoring and control of multiple sites and facilities with maintaining event records in the log.

Using the Orion Pro Suite, the user can predefine system responses to the certain events to secure assets from emergency situations.

The Orion Pro Suite software offers integration of practically unlimited inputs (loops or addressable zones) and relay outputs to monitor and control appliances and access points.

System Features:

- Supports the following Orion ISS devices: S2000, S2000M, S2000-K, S2000-KS, S2000-BI, S2000-BKI, S2000-2, S2000-4, S2000-BIOAccess, Signal-20, Signal-20 ver.02, Signal-20P, Signal-20M, Signal-10, S2000-KDL, S2000-KDL-2I, S2000-KDLS, S2000-Adem, S2000-SP1, S2000-KPB, S2000-ASPT, S2000-PT, Potok-3N, S2000-BI mod.01, Rupor, Rupor mod.01, Rupor-200, S2000-IT, UO-4S, S2000-PGE, BBPS-12 RS, BBPS-12-2A RS, BBPS-24-2A RS, S2000-PP, S2000-Ethernet, and UOP.
- Provides advanced control and integrating capabilities:
  - Connection of system devices to several COM/USB ports on one PC
    - Connection of up to 127 S2000 (S200M) network control panels to one COM/USB Port, each network control panel can accommodate up to 127 monitoring and control modules (devices), or up to 127 monitoring and control modules can be connected to one COM/USB port
    - Up to 32 biometric to one COM/USB port
    - Up to 10 electronic keyboxes to one COM/USB port
    - Up to 10 key cylinder sections to keybox
    - Up to 127 Heliotron dot-matrix display to one COM Port
  - Connection of devices via the Ethernet network
    - Connection of system devices via the S2000-Ethernet module, one S2000-Ethernet module can accommodate one S2000/S2000M (where up to 127 monitoring and control devices can be connected) or up to 127 monitoring and control devices
    - Connection of biometric readers
  - Connection of up to 32 video cameras to one PC-based workstations
  - Deployment in the system network as many workstations as required
- A modular architecture and scalability: the system consists of individual software clients that can be used on a single computer or several networked computers. Due to the flexible configurability, each software client allows customizing each workstation for a specific task.
- Expandability: supports either a single workstation or multiple TCP/IP networked workstations, possibility of purchasing one workstation with further system expansion by purchasing additional software modules
- Flexibility: a wide range of configuration options, programmable response scenarios, expandability capabilities make system function in accordance with requirements and specifics of protected sites.
- Reliability: workstations with Operative Tasks remain functional even after network disconnection, enhancing a security level at a site.

Main Capabilities of the Orion Pro System:

- Displaying the status of each IFS and ACS entity on premises maps
- Tracking employee routes and locations with resolution power up to an access zone
- Displaying video from IP cameras, IP Servers, video servers (video encoders) and DVR recorders in the System Monitor module
- Recording video images as well storing and playing video recordings using the Video Archive module
- Gathering and displaying ADC statistics of addressable sensor in a special software module, as well as displaying it on premises maps if required.
- Advanced authorization and access rights delimitation in accordance with a user status in the system
- Time and Attendance monitoring
- Supports local operation of an Operative Task workstation in case of the Central Server disconnection; and failover support for the entire system as well as individual workstations if the main Server is disconnected
- On-line remote configuration of IFS and ACS systems using one or multiple workstations
- Programming system management (response) scenarios (using templates or proprietary macrolanguage) assigning them to the events of system entities (devices and their zones, partitions, partition groups, and access zones) for automatic activation of the scenarios; scheduled or manual activations of the scenarios are also supported
- Merging multiple databases in a single one.
- Database backup and restoration as well as data verification, repair, and removal

1.1 Orion Pro. Brief Overview

The Orion Pro Suite is a software package consisting of application modules with each intended to resolve its own set of tasks as part of the entire system. Due to this, the user has a flexibility to configure each network workstation installing individual modules as required. The client-server approach of the system architecture facilitates the easy scaling up of the system with the flexibility and transparency of the system structure and management remaining at the same level.

1.1.1 Main Network Modules of the Orion Pro Suite

The Orion Pro Suite includes the following network modules:

Orion Pro Central Server

The Central Server is the main software module that is usually installed on a workstation with the physically located Orion Pro Database. The Central Server mediates interactions between the system modules and used DBMS. It supports operations with SQL Database and data flow to system workstations in the network.

The system operation requires one Central Server. If the failover support configuration is used, the system will need more Central Servers.

Orion Pro Central Server Manager

The Central Server Manager offers the following capabilities:

- Configuration of the Central Server
- Creation of new databases and removal of existing ones
- Verification, Updates and repair of existing databases
- Creation of database backups and restoration from backups
- Automatic back-up and restoration using MS SQL Server capabilities
- Cleaning log records and scheduling removal of records using SQL Server tools
- Manual and scheduled re-indexation of the Database using SQL Server tools
- Configuring replication of the database using SQL Server capabilities

Orion Pro System Shell

The System Shell is a module that mediates between Orion Pro network clients. The System Shell must be installed on all workstations of the system.

 **Orion Pro Database Administrator**

The Database Administrator (also called as DBA) is the system client used for configuring the system and controllers:

- Defining physical structures of the system: workstations and devices and cameras connected to these workstation-
- Defining logical structures of the system: partitions, partition groups, access points, and access zones
- Representing system entities on premises maps
- Programming management scenarios (responses) and scheduling system responses to any events
- Creating and maintaining employee profiles
- Management of employees' privileges and working schedules
- Enrollment of credentials and tokens (software passwords, PINs, ibuttons and proximity cards)
- Entering privileges, PINs, token codes, and finger prints to the devices (controllers)
- To be functional, the Orion Pro system requires at least one Database Administrator

 **Orin Pro Scanning Core**

Scanning Core directly provides operations with Orion ISS devices: It monitors and controls the workstation-connected devices at a physical level. The Scanning Core polls devices, fetches events from the communication interface, sends commands to IFS and ICS system components.
To work with cameras (video servers and recorders), biometric readers, and electronic key boxes, the Scanning Core used optional applications such Video System, BioAccess and Keyboxe Driver modules:
To be functional, the system requires one Scanning Core at least.

 **Orion Pro System Monitor**

The System Monitor is a system supervision module. The System Monitor performs the following:

- Displaying real time information coming from one or multiple workstations online;
- Displaying the status of each system entity on interactive maps and management tabs in real time mode;
- Displaying video images from cameras, servers and DVRs as well as playing video recordings
- Tracking employees online with resolving power up to an access zone,
- Managing and controlling loops/zones, partitions, partition groups, access points and other entities of the system using interactive premises maps and management tabs,
- Online operator's control of fire extinguishing using interactive maps,
- Launching response scenarios by system operators,
- Management of Operator privileges
- Online handling and saving history of system alarm events

Orion Pro Operative Task

The Operative Task (OT) is the Combination of Scanning Core and System Monitor installed on one workstation.

 **Orion Pro Report Generator**

This client is used to generate reports on system alarms and events for a time period as defined. It offers flexibly configurable reporting functions due to large amount of report templates and built-in Report Editor. The resulted reports can be exported to the most common formats such as Word, Excel, XML, HTML, PDF, TXT, pictures, etc.

 **Orion Pro Time and Attendance**

The Time and Attendance network client supports time and attendance records of staff at a protected site, as well as analysis and control of labor discipline compliance at this site. The Time and Attendance allows calculating work hours, late and early arrivals as well as specifying absences and their reasons. The resulted reports can be exported to Excel, XML, HTML, or TXT files. Using optional elements, the resulted data can be exported to the **1C: Enterprise 8** application so that clients can be able to maintain their own Time and Attendance as required.

 **Orion Pro Statistics**

The Statistics client support interactive display of the following:

- Data received from smoke analog addressable sensors, heat analog addressable sensors, and humidity analog addressable sensors
- ADC readings from signaling loops
- ADC readings from the zones of BBPS RS power supplies.
- Interactive display of the peak values
- History of readings

 **Orion Pro Site Occupants (LockDown.exe)**

This client allows tracking employee locations in access zones when the Scanning Core starts and the Database is updated in the Scanning Core.
This client also supports report generation and export to Excel, XML, HTML, or TXT format.

 **Orion Pro Personal Card**

This application performs a verification function: it checks an employee's personality against their profile in the database (it provides an operator with an employee's photo and personal data when he/she requests access via an access point)

1.1.2 Orion Pro Utilities

 **Orion Pro Map Editor**

This utility is designed to create and edit premises maps in the BMP format.

 **Orion Pro Employee Import/Export Wizard**

This utility is used to import the employee list to the database from the CSV files

 **Orion Pro GUI Editor**

This utility is used to change displayed color and elements of the System Monitor user graphic interface

 **Orion Pro Simulator (Demon.exe)**

This utility emulates operation of devices to demonstrate the Orion Pro functionality and capabilities (with Orion Pro protocol)

 **Orion Pro RS Configuration**

This utility is used to configure of RS 232 interface

 **Orion Pro Loop Status.**

This unity is used to view a current status and impedance of connected devices' loops.

1.1.3 Additional Software Modules of Orion Pro Suite

The Orion Pro Suite includes the following additional applications:

 **Orion Pro Video System**
The Video System module offers the following:

- Interaction with network cameras, IP video servers, and DVR recorders
- Integration of video subsystem such as Intellect, SecurOS and COM-interface video systems (Fobos, Goal, VideoNet, Video7, CVS, Trassir, Onvif, DVR etc.).

 **Orion Pro Video Archive**
This is used to store and playback video recordings

 **Orion Pro Video Archive Cleaner**
This application is used for automatic cleaning the video archive (storage).

 **Orion Pro BIOAccess Driver** (reserved for the future release).
This application is used to support biometric readers

 **Orion Pro Keybox Driver**
This module is used to control electronic safe boxes for keys (keyboxes)

 **Voice Announcement Module**
This module is used for voiced notification on system events

 **MegaLib Vehicle License Plates Recognition**
MegaLib is intended for the recognition of vehicle license plates.

1.1.4 Additional Configuration Utilities

The following additional utilities can be installed as a part of the Orion Pro Suite:

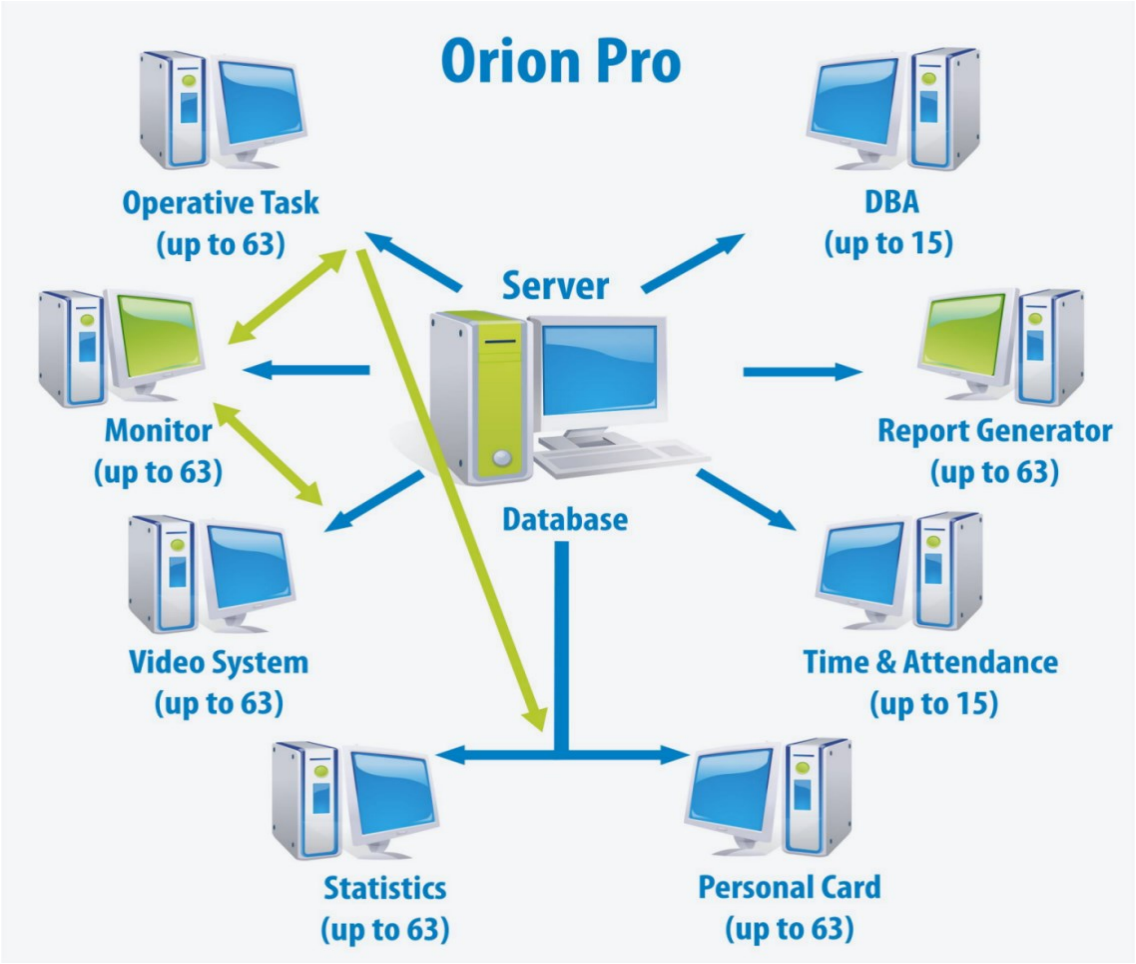
 **PProg Utility**
This utility is used to configure the Database S2000/S2000M panels

 **UProg Utility**
The utility is used to configure devices of the Orion System.

 **BAProg Utitlity**
This utility is used to configure biometric readers.

1.1.5 Orion Pro System Structure

The following figurer shows the flowchart of Orion Pro Network:



Characteristics:

- ✓ Orion Pro Workstations: up to 63.
- ✓ System Video Servers: up to 63.
- ✓ Maximum of devices (alarm monitoring and control modules and panels) connected to one workstation: up to 1,024.
- ✓ Available zones on workstation: up to 16,000.
- ✓ Available partitions for one workstation: up to10,000
- ✓ Access points controllable on one workstation: up to 2,048
- ✓ Maximum number of users for one workstation: up to 32,000.
- ✓ Maximum number of video cameras for one video server – unlimited

1.1.6 Operating System and PC Requirements

Minimum requirements to a personal computer:

- Central Server/Scanning Core Workstation:
  - Intrusion and Fire Protection System:
    - CPU — Intel Pentium IV 3 GHz,
    - RAM — 1 GB,
    - HDD — 30 GB,
  - Including access control systems:
    - CPU — Intel Pentium IV 3 GHz,
    - RAM — 2 GB,
    - HDD — 30 GB,

- Video Server Workstation:
  - For 20 cameras:
    - CPU — Intel Core I5 3.2 GHz,
    - RAM — 3 GB,
    - HDD — depends on resolution and number of cameras
    - Network connection — 1 1 Gbps
  - For 32 cameras
    - CPU — Intel Core I7 3.5 GHz
    - RAM — 3 GB
    - HDD — depends on resolution and number of cameras
    - Сетевое соединение — 1 1 Gbps,
- System Monitor Workstation:
  - Intrusion and Fire System:
    - CPU — Intel Pentium IV 3 GHz,
    - RAM — 1 GB,
    - HDD — 30 GB,
  - Including Access Control Systems:
    - CPU — Intel Pentium IV 3 GHz,
    - RAM — 2 GB,
    - HDD — 30 GB,
  - For 20 cameras:
    - CPU — Intel Core I3 3.1 GHz,
    - RAM — 3 GB,
    - HDD — 30 GB,
    - Network connection — 1 Gbps
  - For 32 cameras:
    - CPU — Intel Core I5 3,2 GHz
    - RAM — 3 GB
    - HDD — 30 GB
    - Network connection — 1 Gbps

Operating system: Microsoft Windows XP SP3 / 2003 Server / Vista / 2008 Server / 7 / 8 32x and 64x

Staring any other none-Orion Pro applications that requires much performance may affect the performance of the Orion Pro System. The installation of any other third-party software on this PC is not recommended.

1.2 Orion Pro Suite: Basic Information

1.2.1 Terms and Definitions, Logical Entities, and Operation Principles

Zone: an arbitrary part of an asset, building, or area protected by one loop, addressable sensor, monitored (supervised) circuit, or monitored output (intrusion or fire). The zone can be related only to a single loop, or addressable sensor, monitored output, and monitored circuit.

Partition: a group of zones supervised and controlled as a single unit. One specific zone can be included in one partition only at the same time.

Partition Group: a group of partitions that can be monitored and controlled as a single unit. One and the same partition can be included in several partitions.

Access Point: any point (door, turnstile, vehicle barrier, etc.) where access control is provided.

Access Zone: a part of area inside or outside a protected site which is associated to an access point (access points) and where a person can gain access in the direction as controlled by an access point.

Time Zone: group of time intervals defining specific time when employees are allowed to access a protected area or to control some components of intrusion and fire protection system.

Access Level: an aggregation of user rights to access individual access points, access zones, and/or to control security system entities.

Management scenario (response): a sequence of system actions performed by the system automatically to control the system modules, devices, etc. The scenario can be initiated by the system in a defined time point or can be launched manually by an operator.

The Orion ISS supports both local (standalone) and centralized (online) control of system elements.
In case of the local control, the device itself is responsible for activating outputs (relay actions) as a response to the status of its zone, as well as for granting access, and arming/disarming of this device zones.

In case of the centralized control, all decisions are taken by a network controller (S2000/S2000M or Orion Pro). In this case, the control actions are provided as a response to the status of logical entities: partitions and partition groups rather than zones.

The partition-based control offers the following advantages over the zone-based control:

- Arming and disarming of partitions requires less user efforts and time, and provides more security against an operator error; when an operator has to arm /disarm huge amount of zone, especially if they belong to different devices, grouping these zone into a partition gives quite tangible benefits.
- A user can arm or disarm only allowed partitions or partition groups in accordance with his/her rights and authority
- Partitions can be armed and disarmed using not only a panel or controller but also other devices such as S2000-K, S2000-KS, S2000-BKI, S2000-2, S2000-4, S2000-2, Signal 20P, Signal-10», S2000-KDL, S2000-KDL-2I, and S2000-KDLS connected to the controller ;

- In addition to an extinguishing control panel or network controller, a network controller-connected S2000-PT device can be used to control fire extinguishing system

- S2000-BI, S2000-BKI, S2000-KS and S2000-PT, Potok, S2000-BKI, S2000-KS, S2000-PT, Potok BKI and S2000-BI mod01 can be used for indication of partition or partition group status;

- Possibility to control system outputs (relays)

The local control offers more reliability. Access control and relay outputs control remain available even in an off-line mode when a network or controller fails.

However it is unlikely to avoid a centralized control approach in case of large integrated systems.

1.2.2 System Devices, Orion and Orion Pro Protocols, Connectivity Options

The Orion Pro-based system can include several workstations with connected devices. Each workstation has an installed Scanning Core interacting with devices at physical level.
The Scanning Core supports the following:

- Connection of system devices to several COM/USB ports on a single PC (workstation)
- Connection of up to 127 S2000 (S2000M) network integrating control panels to one COM/USB Port, where each S2000 (S200M) can accommodate up to 127 monitoring and control modules (devices), or
- Up to 127 monitoring and control modules can be connected to one COM/USB port
- Up to 32 biometric to one COM/USB port
- Up to 10 electronic keyboxes to one COM/USB port
- Up to 10 key cylinder sections to a keybox
- Up to 127 Heliotron dot-matrix displays to one COM Port
- Connection of system devices via the S2000-Ethernet module: one S2000-Ethernet module can accommodate one S2000/S2000M (where up to 127 monitoring and control devices can be connected) or up to 127 monitoring and control devices
- Connection of biometric readers

Further this chapter provides a brief description of the following connectivity:

- COM/USB Port Connection
- Ethernet Connection
- Connection of biometric readers
- Connection of keyboxes
- Network cameras, IP servers, and DVR recorders
- UOP-3 GSM devices

The Orion Pro Scanning Core module can poll and send commands to the following system devices:

- S2000 and S2000M control panels
- Signal-10, Signal-20, Signal-20 ser.02, Signal-20P, and Signal-20M, and Signal 10 intrusion and fire alarm panels
- S2000-KDL, S2000-KDL-2I, and S2000-KDLS multiplex addressable polling loop controllers
- S2000-Adem controller
- S2000-ASPT and Potok-3N fire alarm and extinguishing control panels
- S2000-4 intrusion, fire and access control panels
- S2000-2 access controllers
- S2000-K keypad
- S2000-KS LED keypad
- S2000-BI and S2000-BI mod.01 indication and control modules
- S2000-BKI and S2000-PT indication and control modules
- S2000-SP1 output control modules
- S2000-KPB output monitoring and control modules
- Rupor, Rupor mod 01 and Rupor-200 voice alarm control modules
- S2000-IT telephone communicator
- UO-4S and S2000-PGE devices
- RIP-12 RS, and RIP-12-2A-RS and RIP-24-2A-RS backup battery power supplies
- S2000-PP protocol converter
- S2000-BIOAccess-F4 and S2000-BIOAccess- F8 biometric access controllers
- UOP
- SK24 electronic keybox
- Heliotron dot-matrix display

1.2.2.1 Connecting Devices: Orion Protocol

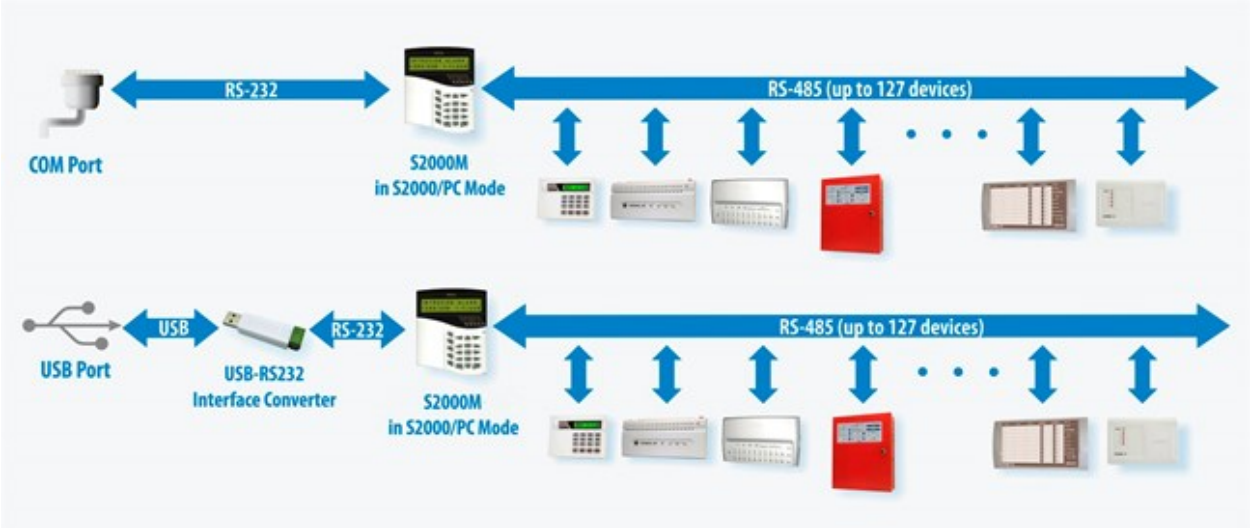
The S2000M can work as an RS-232 / RS-485 interface converter (S2000/PC mode), and switch over to an active mode if a Scanning Core stops polling devices. This mode allows using S2000M as a standby in case of Scanning Core failure.

When the Scanning Core operates normally and polls devices, the network control panel operates as an RS-232 / RS-485 converter automatically switching to a receive/transmit position, with no galvanic isolation of an RS232 output from RS485. If the Scanning Core workstation stops polling devices for some time, the S2000/S2000M panel goes into an active condition, i.e. it starts polling and controlling devices as configured.

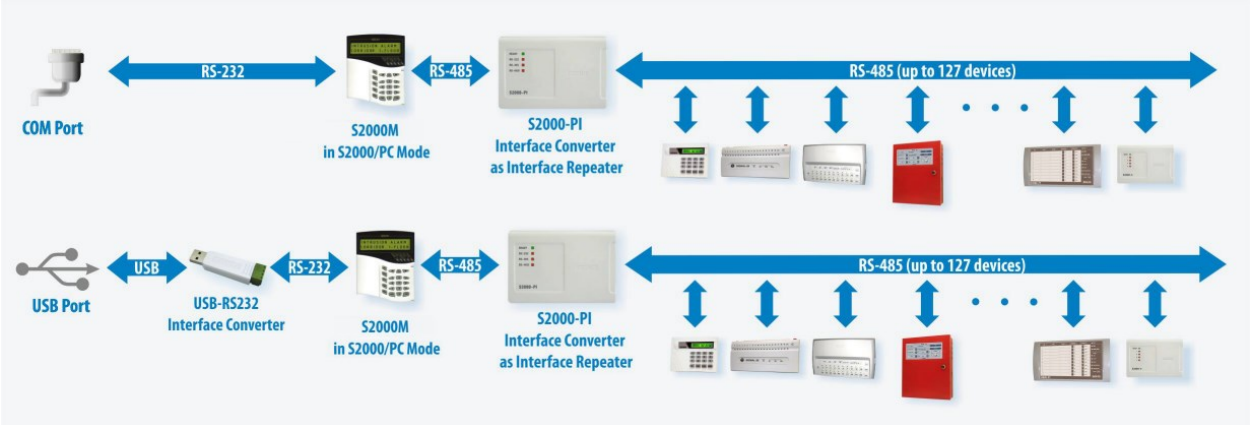
The main limitation of this mode is that when the workstation resumes polling devices, the S2000M panel immediately will start working as an interface converter with Orion Pro missing events occurred in the system while the panel was working as a network controller. All such events will stay in a panel buffer.

When the S2000/S2000M panel works in the S2000/PC mode it can be used for the manual control of the system.

System Configuration with Devices Connected to One COM/USB Port via Orion Protocol (without Galvanic Isolation):

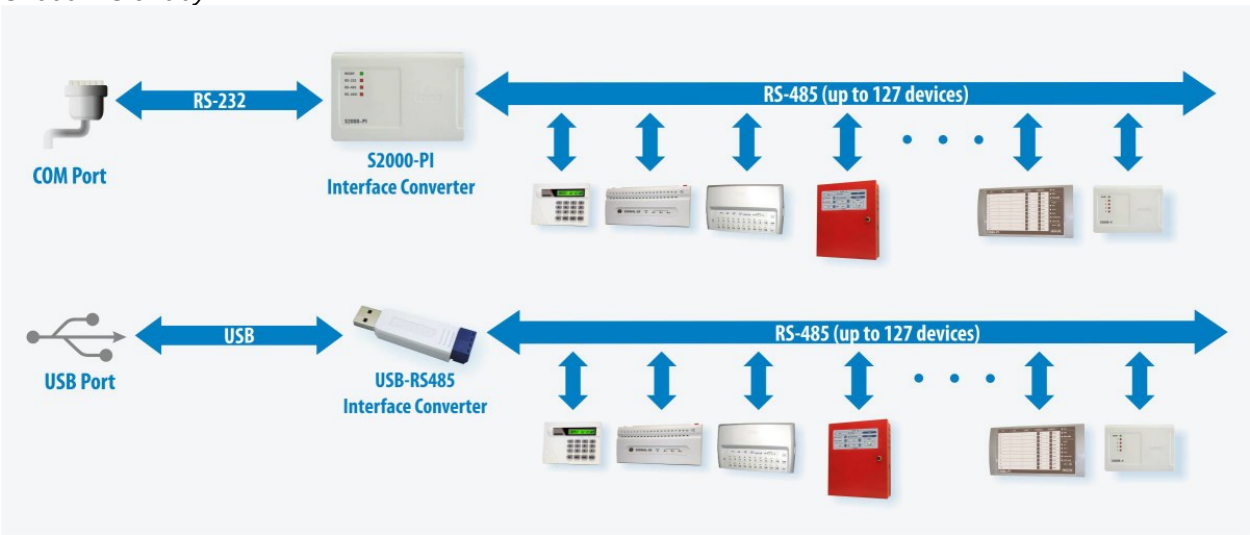


System Configuration with Devices Connected to One COM/USB Port via Orion Protocol (with Galvanic Isolation):



Devices can be connected to a computer without using S2000M as a standby. In this case, when the Scanning Core is disconnected, each device will switch over to a local (standalone) mode, and when the Scanning Core is online again, all events occurred during disconnection will be available in the Orion Pro System.

System Configuration with Devices Connected to One COM/USB Port via the Orion Protocol without S2000M Standby:



1.2.2.2 Connecting Devices: Orion Pro Protocol

Orion Pro protocol allows the Scanning Core to read from and sent commands to the S2000M panel. In this case, the S2000M is always in the active mode. And when workstation recovers after failure, the Scanning Core will receive all events occurred since the moment of a system failure.

To provide the Orion Pro performance with a proper standby support using the S2000M panel, the S2000M configuration has to match the configuration of Orion Pro workstation (configured in DBA) as much as possible. The DBA supports a database export to the S2000M panel.

The size of the S2000M database is quite limited as compared to the Orion Pro database, which prevents backing up a system that has more than 2,048 detection loops (zones) and more than 511 partitions.

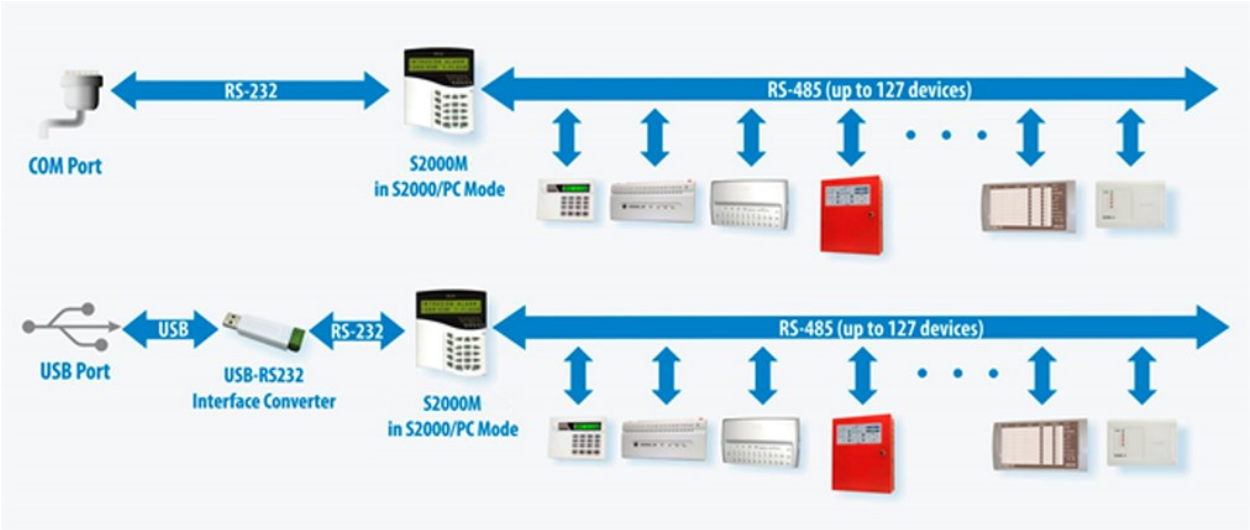
The possible solution is to divide such a system into several parts (subsystems) with each controlled by a dedicated S2000M panel. Since, only one S2000M panel can be connected to the RS-232 (COM Port) of a computer, each S2000M has to be connected to individual COM Port, or alternatively, the RS232 should be converted into the RS485 interface (via S2000-PI converter) where several S2000M panels can be connected. The RS-232 output of each S2000M panel is connected to RS-485 line using the S2000-PI converter. The system devices (modules and controllers) are connected to the RS-485 outputs of S2000M panels. In addition to the connection of multiple S2000M panels to one COM Port, the S2000-PI converter provides a galvanic isolation between a computer and S2000M panels.

Orion Pro operates with all connected S2000M panels, when an Orion Pro workstation is disconnected, each S2000M controls only those devices that connected to its RS-485 output; in other words, the entire system is disintegrated into several small subsystems.

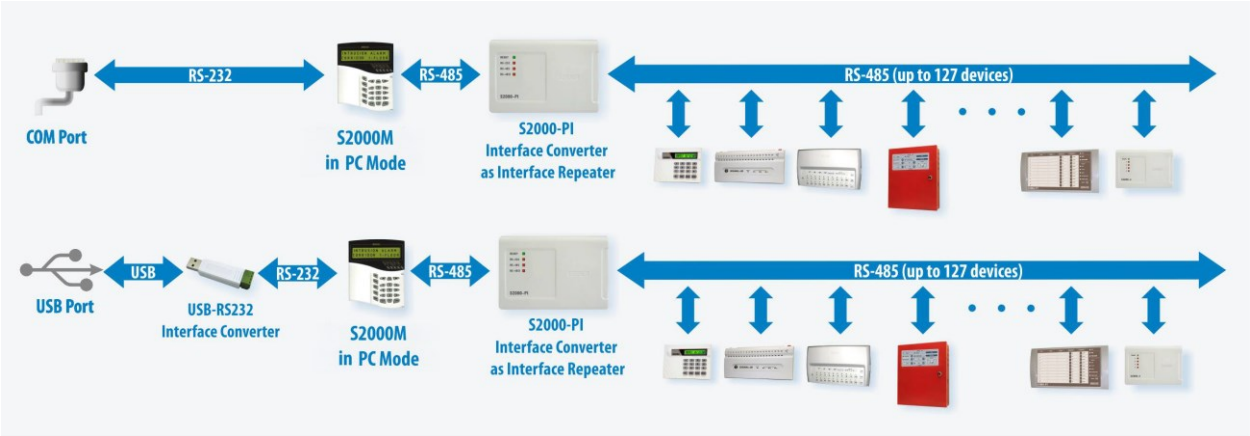
Implementation of the above approach significantly improves the performance of the system. The Scanning Core polls S2000M panels to read the status of systems controlled by these panels. However, the Scanning Core does not polls each device connected to these S2000M panels.

When a system is based on multiple S2000M panels, it is possible to process the sequence of commands simultaneously within the system. The Scanning Core sends the command batch to the S2000M panels. Each S2000M starts processing the sequence of commands related to its system. Thus, multiple Scanning Core commands can be processed within a system at the same time, which in turn also enhances the system performance.

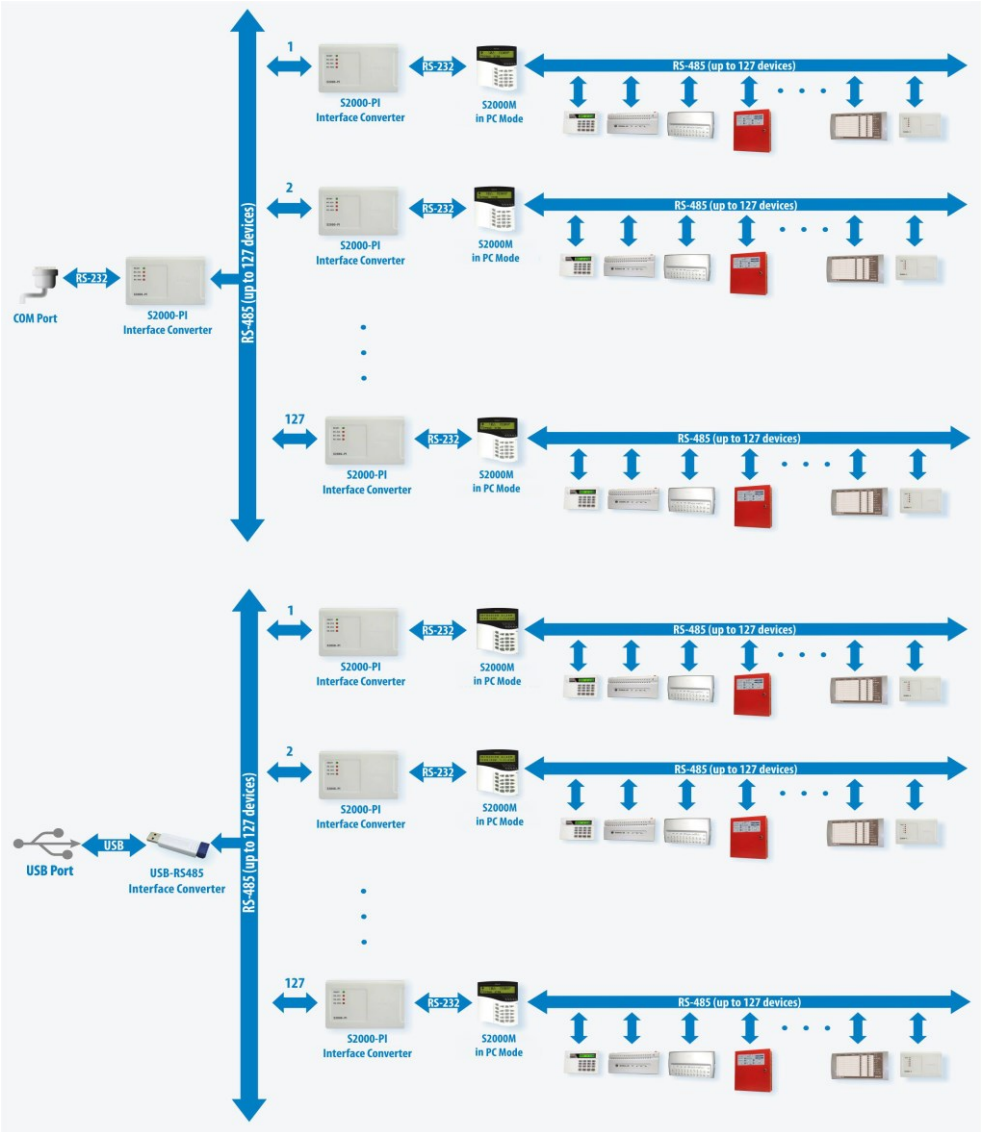
System Configuration with Devices Connected to One COM/USB Port via the Orion Pro Protocol without Galvanic Isolation:



System Configuration with Devices Connected to One COM/USB Port via the Orion Pro Protocol with Galvanic Isolation:



System Configuration with Several Device Branches Connected to One COM/USB Port via the Orion Pro Protocol:



Devices can be connected to one workstation using different protocols: the Orion Protocol to one COM Port and the Orion Pro Protocol to another port

There are the following limitations:

- Devices working with different protocols cannot be connected to the same com port
- The number of ports is limited by the Windows - 255 ports in theory
- USB-RS232 and USB-RS485 interfaces occupy one com-port in the Operating System (OS)

This guide recommends the following:

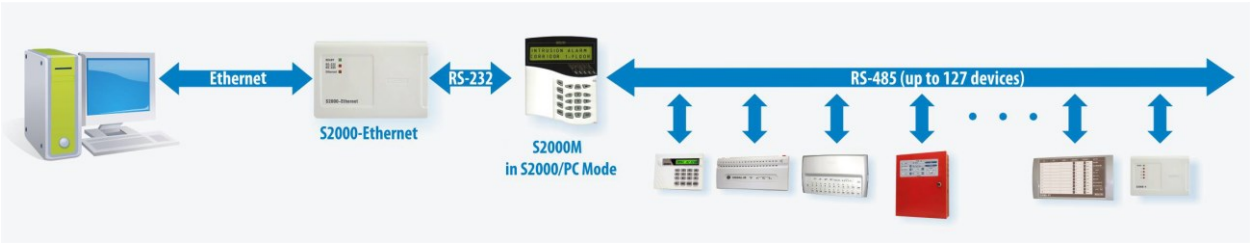
- **Use of Orion Pro protocol**;
- Connect each S2000 panel to its own dedicated COM/USB port (connection of devices via Orion Pro protocol w/ galvanic isolation), if multiple S2000 panels have to be connected to the Scanning Core
- Reduce devices connected to one S2000M panel, if you are not planning 24/7 operation for the Scanning Core. It may need because of the limited capacity of S2000M's event buffer that, in turn is critical for access control systems.

1.2.2.3 Ethernet Connection

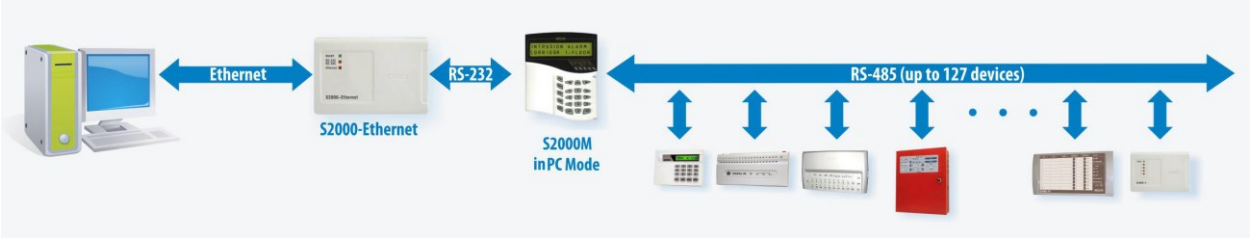
In case of remote location of Orion Pro workstationы and devices, The system devices can be connected via Ethernet (if available) as follows:

Orion Protocol Connection via Ethernet:

Orion Protocol Connection via Ethernet Using S2000M as a Standby:



Orion Pro Protocol Connection via Ethernet:



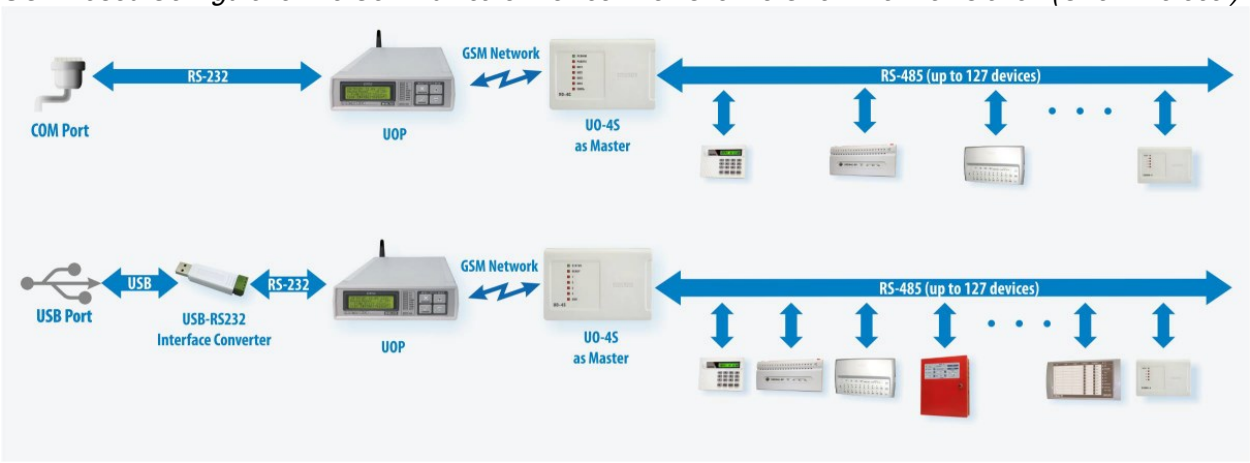
Note:

1. If this configuration approach is used, each S2000 Ethernet takes one COM Port in the Orion Pro Database.
2. The system performance would be slower compared with the configuration when devices are connected directly to a com-port.
3. The S2000-Ethernet can operate in the '*transparent*' mode only (see the manual for S2000-Ethernent).

1.2.2.4 Connecting UOP-3 GSM

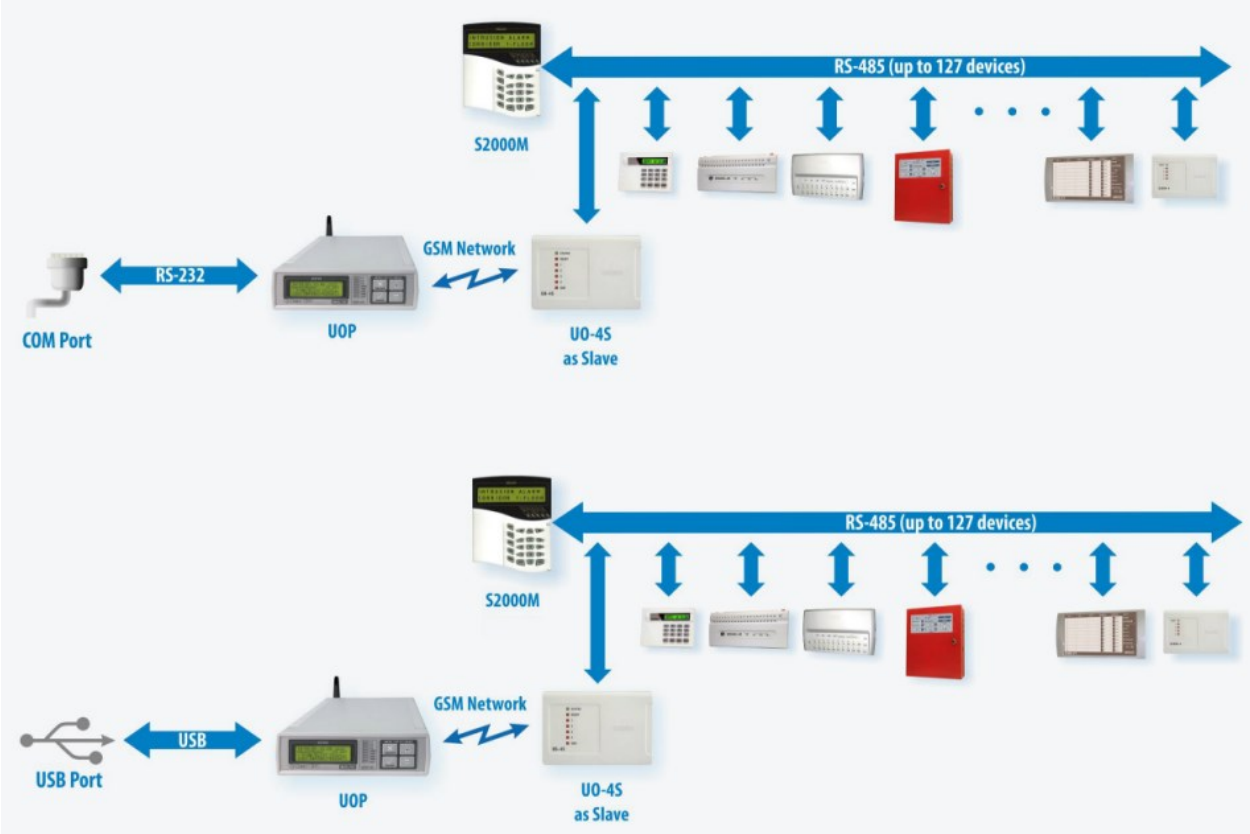
If required, the devices can be connected to one PC com-port using one of the following connection schemes:

UOP Based Configuration to Communicate Device Events to the Orion Pro Workstation (Orion Protocol):



In this case, UO-4S polls the connected devices to transmit device's events to Orion Pro System.

UOP Based Configuration to Communicate Device Events to the Orion Pro Workstation (Orion Pro Protocol):



In this case, the S2000M polls devices and transmit the device events to Orion Pro via the UO-4C.

Note:

1. Only one UOP-3 GSM can be connected to a computer.
2. This type of connection to Orion Pro allows only transmission of device events. Control function of Orion Pro will not be available.
3. If UO-4S is used as a Primary device, only local control is available. If a connection scheme with S2000M is used, the centralized control is available with S2000M used as a Primary unit.

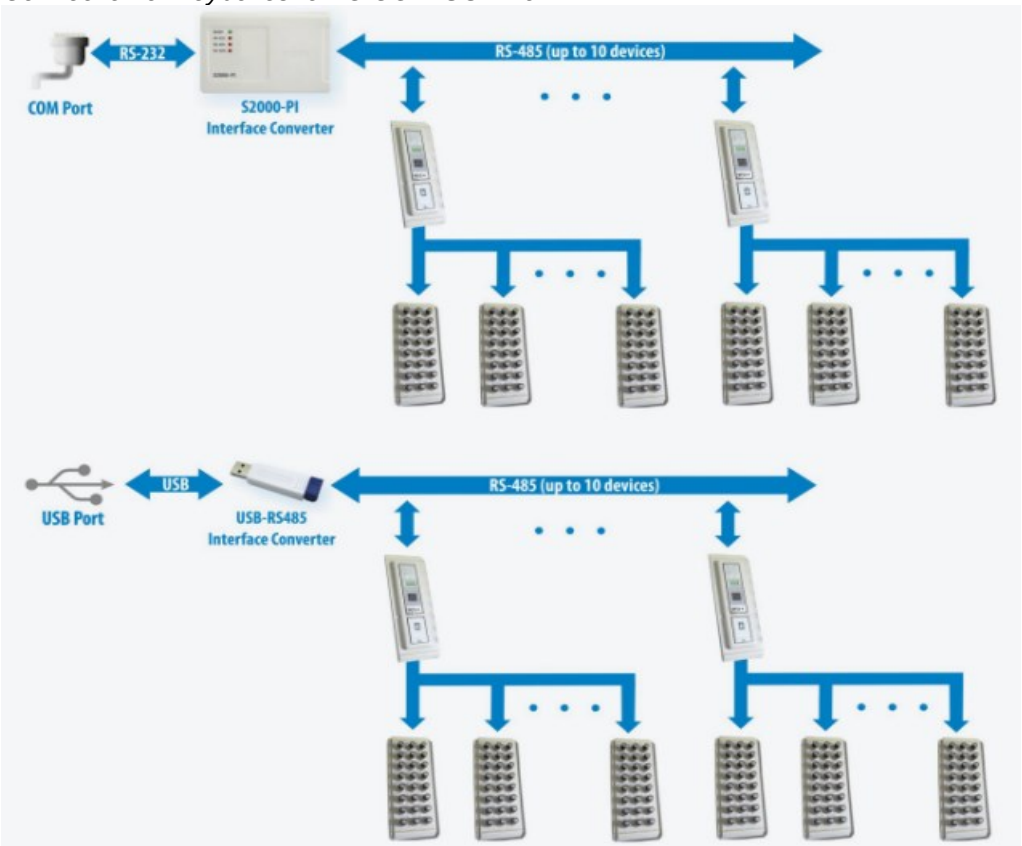
1.2.2.5 Connecting Biometric Readers

Connection of Biometric Readers:

1.2.2.6 Connecting Keyboxes

The Keyboxes are connected to a PC com-port using one of the following schemes:

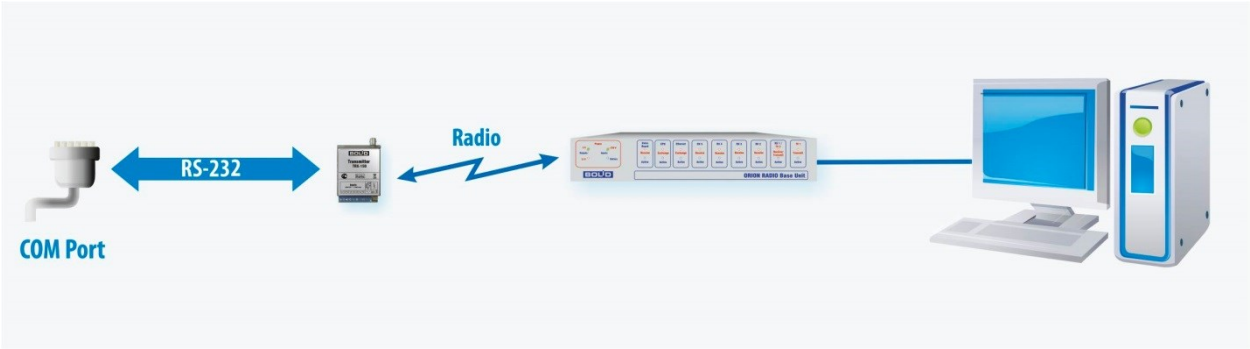
Connection of Keyboxes to PC COM-USB Port



Only a new version of keyboxes support RS-485 connection. The old version supports the connection to PC COM Ports only.

1.2.2.7 Printer Protocol Connection of Orion -Radio and other Systems

Connection of Orion-Radio Transmitter to a PC COM Port:



Note:

1. Only one Orion-Radio transmitter can be connected to a workstation.
2. The device events are transmitted to the Orion Pro workstation. Nothing is transmitted from the Orion Pro workstation.

Other equipment such as Contact GSM-5-RT3 is connected in the similar manner.

1.2.2.8 Connection Configuration of Networked Cameras, IP Servers, and DVR Recorders

One video server supports unlimited number of video cameras (depending on workstation performance and LAN bandwidth) connected as the following configuration:

The list of supported cameras, IP servers, and DVRs is always updated. Please see the actual list of supported video systems at: www.bolid.ru.

1.2.3 Orion Pro System Structure

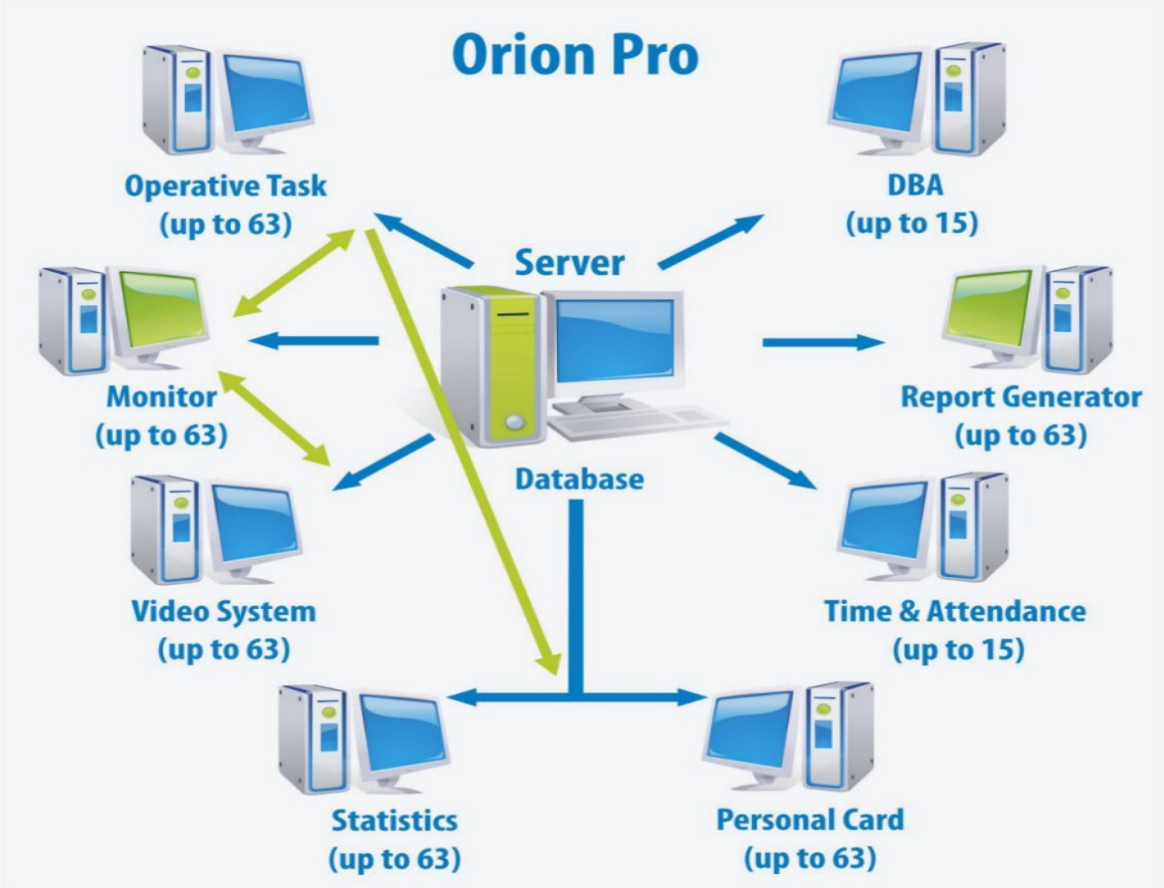
The Orion Pro System structure can have various configurations:

The simplest configuration is when all software modules are installed on the same computer with SQL Server (or MSDE- free version of SQL Server):

- Orion Pro Central Server
- Orion Pro Database Administrator
- Orion Pro Operative Task

  and, if needed:
- Orion Pro Report Generator
- Orion Pro Time and Attendance

In most cases, the software modules are distributed throughout several workstations:



Attention:

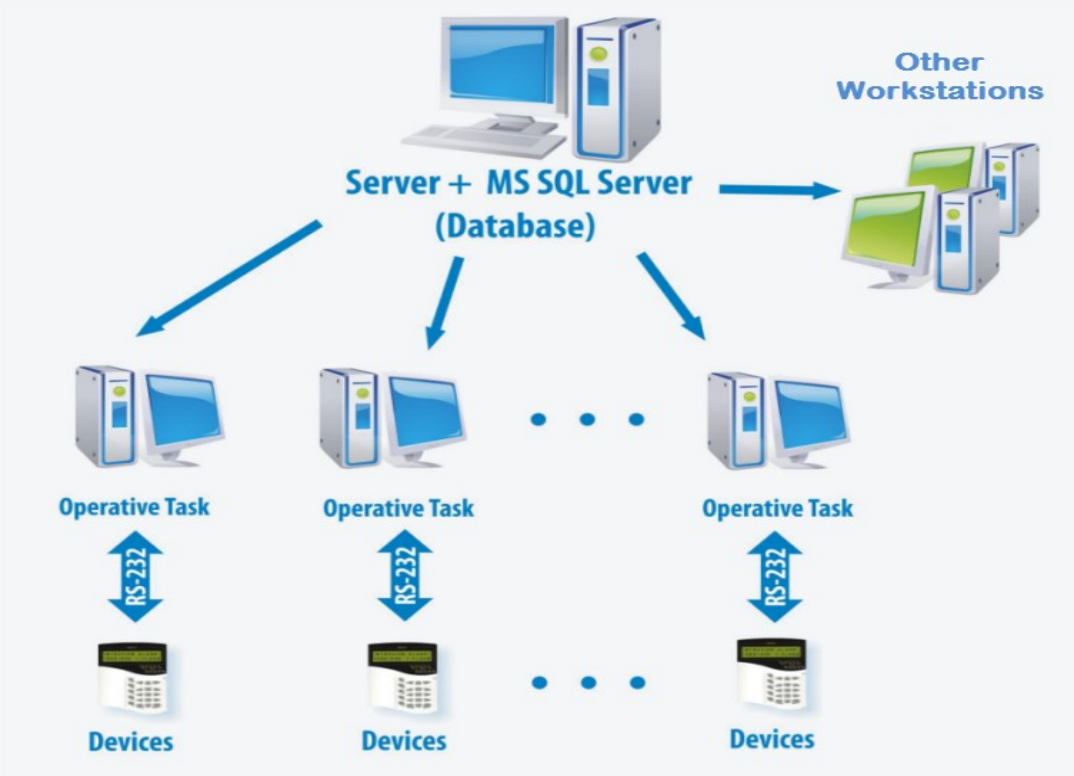
1. All workstations are connected to one network.
2. The Central Server can be installed both on the same workstation where SQL Server installed and on other workstations.
   It is recommended that the Central Server should be installed on the same workstation with SQL Server.
3. To provide better understanding of the system structures, the configuration above shows each module installed on an individual workstation, i.e. one software module is installed on one workstation.
   But in case of field installation, the workstation can have a specific combination of installed workstations. For example, the workstation for a site supervisor can include the System Monitor, Report Generator, Time and Attendance, and Site Occupants modules.
4. The Operative Task includes the Scanning Core and System Monitor. In most cases, both modules are running on the same workstation. But if needed, these modules can be used on separate workstations.

5. The System Shell must be started first on the workstation to launch and run any one of the Operative Task, System Monitor, Scanning Core, Database Administrator, Report Generator, Time & Attendance, Personal Card or Video System modules.
   Operation of other modules does not require the startup of the System Shell

6. The Central Sever, Operative Task (consisting of Scanning Core and System Monitor), Scanning Core, System Monitor, Database Administrator, Report Generator, and Video System are charged-license software. Other software modules are included as free-license software.
   The Central Server, Scanning Core, and Video System are protected with protection keys (dongles).
   The System Monitor, Database Administrator, Report Generator, and Time and Attendance modules are protected with the protection key of the Central Server module, and do not require individual protection keys.
7. The access to software data is protected and managed by software modules

1.2.3.1 System without Failover Support

When such a configuration is used, the Central Sever and MS SQL Server are installed on the same workstation. This workstation as well as some other workstations accommodates the required set of Orion Pro modules



The licensing of this system is provided on the following basis:

- The license key for the Central Server will be inducted to the workstation where the Central Server is installed
- The Scanning Core license key will be inducted to each workstation where the Scanning Core is installed.

(If the Central Server and Scanning Core are installed on the same workstation, two appropriate protection keys must be inducted to this workstation.)

In case of network disconnection, each workstation starts working off-line (local mode).
The workstation where the Central Server is installed will continue operating in the normal mode. The limitations:

- The System Monitor, Report Generator, Time and Attendance, Site Occupants, and Personal Card modules will be unable to receive events (occurred since the disconnection) from Scanning Cores running on off-line workstations.
- The System Monitor and Statistics modules will be unable to obtain the status of entities from the Scanning Cores installed on disconnected workstations.

When the connection fails, each workstation goes to the off-line operation mode.

As for the other workstations, two options are possible depending on whether the local cache is used or not.

The use of local cache is the attribute of each workstation, which is configured in the Database Administrator.

1.2.3.1.1 Workstation with Disabled Local Cache

When disconnected, the workstation with disabled local cache will experience the following:

- ✓ Database Administrator:
  If the workstation with the installed Central Server is disconnected, no changes can be made to the Database, and the software module cannot be started.
  When connection with the Central Server workstation is recovered, the Database Administrator must be restarted, if two or more Database Administrators are used in the system.

- ✓ Scanning Core:
  If the workstation with the installed Central Server is disconnected, all events of devices and cameras connected to the workstation will **not** be recorded to the database, stored anywhere, or shared with any other workstations; the status of the workstation's entities will not be shared (transmitted), and the commands (signals) from other workstation cannot be received as well.
  When connection with the Central Server workstation is recovered, the information will be automatically synchronized with the Database requesting the status of each entity associated to the workstation; the possibility of receiving commands from other workstation will be also recovered.

- ✓ System Monitor:
  If the workstation with the System Monitor is disconnected, it will stop receiving all events, and states of entities form all Scanning Cores on other workstations; the status of such entities will be unknown: the entities of these Scanning Cores cannot be controlled. The System Monitor will continue receiving events and states related to the entities of the Scanning Core installed on the same workstation with this System Monitor; the entities of this Scanning Core will be still controllable.
  When the connection with the Central Server workstation is recovered, the data will be automatically synchronized with the Database with further requesting the status of entities related to Scanning Cores installed on other workstations as well as to the Scanning Core installed on the same workstation where this System Monitor is installed.

- ✓ Report Generator:
  If the Central Server is disconnected, the Report Generator will be unable to start or generate any reports if it was launched before the disconnection.
  When the connection is recovered, the reporting functions will be recovered as well.

- ✓ Time and Attendance:
  If the Central Server is disconnected, the application cannot be launched and generate any reports.
  When the connection with the Central Server is recovered, the Time and Attendance has to be restated or reconnected using the reconnect option in the application.

- ✓ Statistics:
  When the Scanning Core is disconnected, the Statistics module stops receiving the states of entities related to a disconnected Scanning Core. The Statistics module will continue receiving the states of entities from the Scanning Core installed on the same workstation where the Statistics module is installed, as well as from Scanning Cores installed on other workstations, if they are available online.

If the Central Server is disconnected, the history of any system entities will be inaccessible. The Statistics module can be started with limited functions to receive status data on entities related only to Scanning Cores running on on-line workstations and the Scanning Core running on the same workstation where the Statistics module is installed.
When the connection with a Scanning Core workstation is recovered, the software module will reconnect automatically to start receiving status data from this Scanning Core.
If the software module was started at the moment when any Scanning Core workstation was off-line (disconnected), the Statistics software module has to be restarted to recover connection with this workstation.
When the connection with the Central Server is recovered, the history of system entities can be viewed again.

- ✓ **Site Occupants**:
  When the Central Server workstation is disconnected, the application cannot be launched and generate any reports.
  When the connection with the Central Server is recovered, the Site Occupants software module will reconnect automatically to the Central Station.

- ✓ **Personal Card**:
  When any Scanning Core workstation is disconnected, the Personal Card will stop receiving any events from this Scanning Core. The application will continue receiving event from the Scanning Core running on the same workstation where the Personal Card is installed as well as from all other on-line Scanning Cores

  When the Central Server workstation is disconnected, the automatic updates from the Database (when it is changed) will be disabled. The software module can be started, but in can receive events only from Scanning Cores running on connected (on-line) workstations, as well as from the Scanning Core running on the same workstation with the Personal Card.

  When the connection of the Scanning Core workstation is recovered, the Personal Card will automatically reconnect to start receiving events from this Scanning Core.

  When the connection with the Central Server recovers, the information will be automatically updated from the Database; if changed during the disconnection period.

1.2.3.1.2 Workstation with Enabled Local Cache

The workstation with local cache enabled will experience the same as with disabled local cache, except for the following critical issues:

- All events of entities connected to the workstation with installed Scanning Core will be stored in cache if Central Server workstation is disconnected, but when the connection is recovered the above events will be uploaded to the Central Server (Database)
- The Operative Task (Scanning Core and Monitor) and/or Video System can be used even if there is no connection with the Central Server workstation.

Attention!

1. The enabled local cache is recommended only on for workstations with Scanning Cores installed
2. If the failover support is used, the enabled local cache is not recommended.

1.2.3.2 System with Failover Support

One more schema of Orion Pro use is one with used of several database instances. In this case multiple MS SQL Servers have to be used to maintain system operation when the network fails, and to synchronize data between the primary database and its replicas when the network recovers. To support such configuration, multiple instances of the Central Server have to be used with one used as main and others as secondary.

To provide the above system approach, the full version of MS SQL Server must be used. Free versions are not applicable as they do not provide data synchronization (replication).

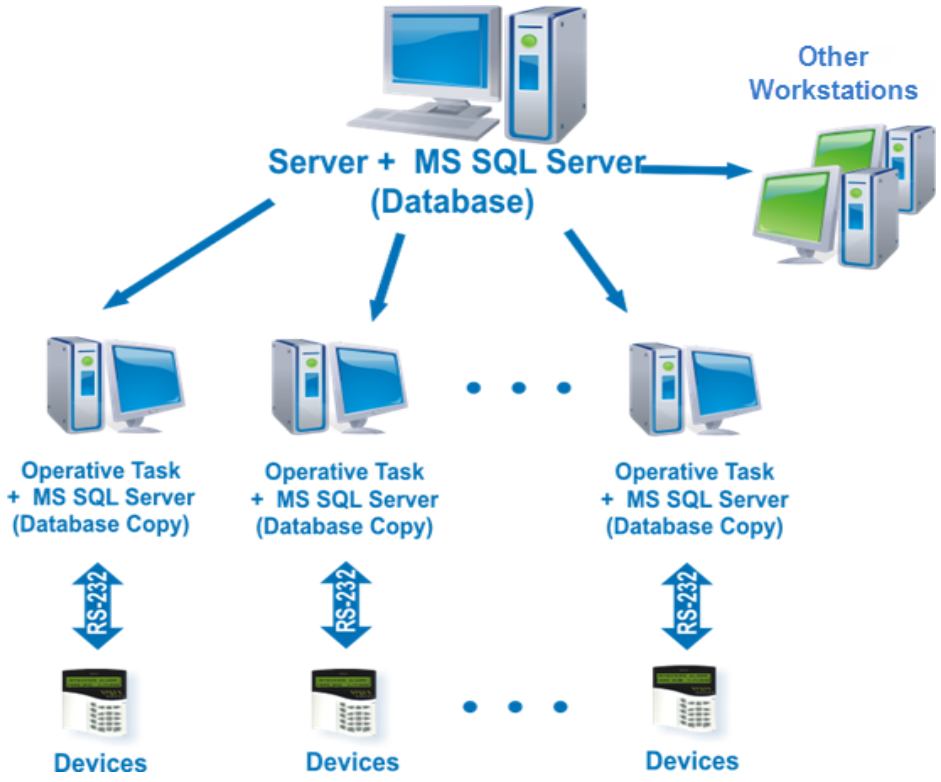
Advantages of failover support:
It is the MS SQL Server that is responsible for the data storage and replication in case of connection failures. The SQL Server has several protection levels and virtually cannot loss any data.
The LAN fails, the system can remain operative, and the available functions would depend on what workstations have been disconnected.

LAN connection loss is an abnormal situation, and the discussion is focused on connection loss across the entire local area network among all workstations. However, the disconnection of the Central Server workstation only and other individual workstation disconnection will be discussed also.

If the system is configured in the line of the described scheme, the Central Server and SQL Server must be installed on one of the workstations. The required set of Orion Pro modules is installed on the above workstation. The secondary Central Servers are installed on some other workstations where SQL Server instances with secondary databases will be installed on each of the workstation.

As said above the off-line status (connection loss) is not a normal situation. Thus, the focus of system performance is case of connection failure will be on saving events occurred since the disconnection connection failure.
Consequently, secondary Central Servers and Secondary SQL Server are usually installed on workstations where Scanning Cores and Video Systems are installed.

But if needed, secondary Central Servers and SQL servers can be installed on other workstations as well, for example they can be installed on a workstation with installed Time and Attendance to enable a responsible employee to generate reports for the periods prior to a connection failure (usually for the previous month) even if there is no network connectivity at the moment.



As the figure shows, one (Central) Server is used as Primary and others as Secondary. In case of network disconnection, each workstation with installed secondary Central Server will switch to this secondary Central Server and continue operation with the Database Copy (secondary Database) of Orion Pro Suite. Each secondary Central Server works with the SQL Server instance that installed on the same workstation.

Synchronization (replication) between primary and secondary SQL servers is configured using the Orion Pro Central Server Manager or SQL Server tools. The recommended replication configuration is when a secondary SQL server copies all data form the primary server, and the primary server copies only event, alarm, and statistics logs.

It should be noted, the Central Server supports only those software modules that are put down in its protection key, so it is necessary to purchase licenses of those software module (Scanning Core, System Monitor, Database Administrator that will be installed together with each such Central Server on the same workstation (or only for those software modules that will be used in case of local network disconnection).

In case of using the failover support scheme, if a local network is disconnected, software modules running on workstations with no secondary Central Server and SQL Server will work without the failover support as described above. But software modules running on the workstations with installed secondary Central Server and SQL Server will work as follows:

- ✓ Scanning Core:
  If the Primary Central Server workstation is disconnected (goes off-line), the Scanning Core will switch over automatically to the Secondary Central Server, all events from the workstation-connected devices and cameras will be recorded to the secondary Database and shared with other on-line workstations; the status of each entity of the workstation will shared with on-line workstations; no commands and requests can be received from off-line (disconnected) workstations or from workstations where a secondary Central Server is not installed.
  When the connection with the Primary Central Server workstation is recovered, the system will be automatically switched over to the primary Central Server, the information will be synchronized with the Database, and the status of each workstation-connected entity will be requested and updated; the workstation will receive commands and queries from other on-line workstation (connected to the primary Central Server or where a Secondary Central Server is installed)

- ✓ System Monitor:
  If the workstation with the installed primary Central Server is disconnected, the System Monitor will stop receiving all events and states from all Scanning Cores on off-line workstations or those where no secondary Central Server is installed, the status of the entities of these Scanning Cores cannot not reported, and the entities cannot be controlled. The Scanning Core running on the same workstation with System Monitor as well as Scanning Cores on on-line workstations where secondary Central Servers installed will share event and states with this System Monitor; the entities of these Scanning Cores still can be controllable.

  When the connection with the Primary Central Server workstation is recovered, the system will be automatically switched over to the primary Central Server, the information will be synchronized with the Database, than the status of each entity will be requested from Scanning Cores installed on other on-line workstations (connected to the primary Central Server or where a Secondary Central Server is installed) and from the Scanning Core running on the same workstation with this System Monitor.

- ✓ Report Generator
  When the Primary Central Server workstation is disconnected, the connection to the available Secondary Central Server has to be set in the Report Generator module to maintain report generation functions (It is recommended that the Report Generator and secondary Central Server should be installed on the same workstation).
  When the network with the Primary Central Server workstation is recovered, the connection with it has to be set in the Report Generator module.

- ✓ Time and Attendance:
  When the connectivity with the Primary Central Server workstation is lost, the connection to the available Secondary Central Server has to be set in the Time and Attendance module to maintain report generation functions (It is recommended that the Time and Attendance module and secondary Central Server should be installed on the same workstation).

When the network with the Primary Central Server workstation is recovered, the connection with it has to be restored in the Time and Attendance module.

- ✓ **Statistics**:

  When a Scanning Core is disconnected, the Statistics module stops receiving the states of entities related to a disconnected Scanning Core. The Statistics module will continue receiving the states of entities from the Scanning Core running on the same workstation where the Statistics module is installed, as well as from Scanning Cores installed on other online workstations.

  If the Central Server is disconnected, the history of any system entities will be inaccessible. To view the history, the Statistics module has to be restarted switching over to a secondary Central Server. Also, the Statistics module can be started with limited functions to receive status data on entities related only to Scanning Cores running on on-line workstations and the Scanning Core running on the same workstation where the Statistics module is installed.

  When the connection with a Scanning Core workstation is recovered, the software module will reconnect automatically to start receiving status data from this Scanning Core.

  If the software module was started at time when any Scanning Core workstation was off-line (disconnected), the Statistics software module has to be restarted to recover connection with this workstation.

  When the connection with the Central Server is recovered, the history of system entities can be viewed again. If the switchover was performed, the module has to be restarted setting a connection to the Primary Central Server.

- ✓ **Personal Card**

  When any Scanning Core workstation is disconnected, the Personal Card will stop receiving any events from this particular Scanning Core. The application will continue receiving event from the Scanning Core running on the same workstation where the Personal Card is installed as well as from all other on-line Scanning Cores.

  When the Primary Central Server workstation is disconnected, the automatic updates from the Database (in case of changing) will be disabled. The software module can be started, but in can receive events only from Scanning Cores running on connected (on-line) workstations, as well as from the Scanning Core running on the same workstation with the Personal Card.

  When the connection of the Scanning Core workstation is recovered, the Personal Card will automatically reconnect to start receiving events from this Scanning Core.

  When the connection with the Primary Central Server recovers, the information will be automatically updated from the Database; if it has any changes occurred during the disconnection period

- ✓ **Database Administrator**

  If the installed Primary Central Server workstation is disconnected, no changes can be entered to the Database, and the software module cannot be started.
  When connectivity with the Primary Central Server workstation is recovered, the Database Administrator must be restarted, if two or more Database Administrators are used in the system.
  If only one Database Administrator is used in the system, changes can be made to the Database using the Database Administrator during the network disconnection

If two or more Database Administrator modules are used in the system, it **is strongly recommended that no** changes should be entered to the Database using the Database Administrator modules.