

CERTIFIED SYSTEM FOR INTEGRATING FIRE SAFETY EQUIPMENT

INFORMATION SHEET

TELBUD SA

ARGUS SIUP

ARGUS SIUP – the latest Fire Protection Equipment Integration System

The new ARGUS SIUP Fire Protection Equipment Integration System from TELBUD SA offers a range of unique hardware and software solutions.

The system is based on advanced industrial computers and industrial panel PCs, which run the Argus PSIM management software.

The system's distributed architecture allows its components to be deployed in various parts of the protected premises.

Wall-mounted cabinets are used to house the components; **these are connected via a dedicated SIUP system LAN**, including a fibre-optic ring. An RS-485 bus ring is also used to connect to remote input/output modules.

The following types of units may be used in the system: the ZJC central unit, the ZSK client station, the ZTO operator terminal, the ZKI interface concentrator, the ZUK communication devices and the ZMW input/output modules.

The equipment and number of individual units are determined and designed on a case-by-case basis, depending on the needs of the specific site.



TELBUD SA
ul. Krauthofera 23
60-203 Poznań
+48 61 866 88 48
telbud@telbud.pl
www.telbud.pl

1. GENERAL CHARACTERISTICS OF THE ARGUS SIUP SYSTEM

Fire Protection Equipment Integration System (SIUP) – The ARGUS SIUP computerised security management system is a hardware and software solution with a distributed network architecture, designed specifically for the monitoring and control of fire protection systems. The system is based on PSIM (Physical Security Information Management) class management software. Argus PSIM software is used as standard, but for installations that must be compatible with the previously manufactured ARGUS RV-C system in accordance with National Technical Assessment No. CNBOP-PIB-KOT-2018/ 0057-1002 (e.g. in the case of the expansion of existing installations), it may alternatively operate under the control of Argus RV software.

The system can integrate all fire protection installations and devices located in one or more dispersed premises, including, amongst others:

- fire alarm systems (SSP),
- audible warning systems (DSO),
- fixed fire-extinguishing systems (SUG),
- smoke and heat control systems,
- fire ventilation systems,
- gravity smoke extraction systems,
- fire compartmentation elements (doors, curtains, gates),
- fire lifts for rescue teams,
- emergency and evacuation lighting systems,
- CO and LPG detection systems,
- other installations and equipment used or controlled during a fire alarm.

ARGUS SIUP also allows for the integration of technical security systems not directly related to fire response, such as: closed-circuit television (CCTV), access control (AC) and intrusion and hold-up alarm (IHA) systems, and can monitor the operation of other equipment and installations affecting the security of the premises (power supply, communications, HVAC, BMS, etc.). The integration of SIUP with these systems improves the operator's situational awareness and supports their decision-making in any emergency situation.

The system supports any number of signals. It can integrate any subsystems via Ethernet TCP/IP network interfaces and RS-232, RS-422 or RS-485, utilising a variety of communication protocols, open OPC standards or software development kits (SDKs, APIs) provided by manufacturers, as well as via binary and analogue input/output modules.

The ARGUS SIUP system can be used in remote centres for the monitoring, control and management of security (including fire safety) at geographically dispersed sites, which are connected to the centre via a dedicated or leased WAN, typically operating as a corporate network.

2. SYSTEM ARCHITECTURE AND COMPONENTS

The Fire Protection Equipment Integration System – the ARGUS SIUP computerised safety management system – features a distributed architecture, with its components working together within a dedicated SIUP LAN. The system comprises the following basic components:

• ZJC – the central unit (server) module, which is based on an industrial computer. Depending on the type of software required for a specific system application, either the Argus PSIM or Argus RV system software is installed on the computer, along with communication drivers for the integrated devices. This software performs the functions of data collection, processing, archiving and visualisation, as well as the control and management of the entire system. The enclosure can house a single server (ZJC-S), two servers operating in a redundant configuration (ZJC-DR), or a server and a computer acting as a client workstation for the system (ZJC-DK). An industrial LCD touchscreen monitor, used for visualisation and operator control, may be optionally installed (built-in) on the cabinet door. The cabinet can then serve as a ZTO operator terminal.

• ZSK – a certified client station enclosure built using an industrial computer (as for the central unit), running the Argus PSIM or Argus RV visualisation (client) application software, as appropriate. Visualisation is displayed on external industrial LCD touchscreens or via a keyboard and mouse. An industrial touchscreen monitor, which is installed on the cabinet door, may also be used optionally for visualisation and operator control. The cabinet can then serve as a ZTO operator terminal.

• ZTO – an operator terminal enclosure based on an industrial panel PC with an LCD touchscreen or, optionally, on an industrial computer and an industrial LCD touchscreen monitor built into the enclosure door. The terminal operates using the Argus PSIM visualisation application software, accessed via a web browser, or Argus RV, as appropriate, in the same way as the client station in the ZSK. It functions as a certified operator workstation which, once the Argus PSIM or Argus RV server system software has been installed, can simultaneously operate as a redundant or independent central processing unit of the system. The ZJC, ZSK and ZKI enclosures, which are fitted with an industrial LCD touchscreen integrated into the door, can also serve as ZTO operator terminals.

• ZKI – an interface concentrator unit, which is an intelligent system component that facilitates communication with integrated devices via network and serial interfaces, as well as through binary and analogue input/output modules, independently of the central unit. It is based on an industrial computer running the system software's communication drivers. Functionally, the concentrator enables the implementation of distributed telemechanics for monitoring and control, executing locally programmed data acquisition algorithms and acting as data buffers between the monitored systems and the individual servers of the ARGUS SIUP system. If the Argus PSIM or, where applicable, Argus RV client software is installed on the concentrator's computer, an industrial LCD touchscreen monitor may be built into the cabinet door to enable local operation and visualisation. The cabinet can then simultaneously serve as a ZTO operator terminal.

• ZUK – enclosures for communication equipment used to connect the system's integrated devices and operator stations to the SIUP LAN. Depending on requirements, various types of communication components may be used within the system in a range of configurations, including:

- network switches, which enable the creation of an extensive SIUP LAN and the connection of various devices to it via twisted-pair copper cable or fibre-optic cable;
- LTE and Wi-Fi routers for wireless and wired communication, which may be used in particular for remote communication with the SIUP installation, including remote monitoring of the system's operation by operational and maintenance services, as well as for communication between geographically remote SIUP components and for establishing connections with mobile devices via secure VPN channels;
- PoE injectors, which supply power to PoE-compliant devices via Ethernet lines;
- media converters used to convert the Ethernet signal between a copper cable on an RJ45 port and a fibre-optic (FO) cable;
- interface converters and separators/repeaters, which allow the communication interfaces available in individual SIUP units to be adapted to the interfaces on connected devices and enable reliable data transmission between the system and integrated devices over longer distances;
- serial port servers, which allow devices equipped with RS-232, RS-422 and RS-485 serial transmission ports to an Ethernet network and access to them via the software of the central unit, a certified client station, an operator terminal or an interface concentrator – access may be achieved via virtual COM serial ports associated with physically existing ports, or by transmitting data using the UDP or TCP protocols;
- encryption modules utilising industrial IIoT (Industrial Internet of Things) gateways with built-in microcomputers based on RISC architecture, on which a programming application runs that communicates with integrated devices via serial and network interfaces and carries out encrypted data transmission with the central unit on the SIUP LAN;
- binary and analogue input/output modules used to monitor power supply status and environmental conditions within enclosures, and for 'hard-wired' connections to integrated devices.

All the types of communication equipment listed above can also be installed in ZJC, ZSK, ZTO and ZKI enclosures.

• ZMW – enclosures for remote binary and analogue input/output system modules of the DCM-100 series (already used in the certified ARGUS RV-C system), which can be connected to an interface concentrator, a central unit, a certified client station or an operator terminal via an RS-485 bus ring configured in such a way that a single break in the ring does not result in a loss of communication.

All enclosures are fitted with a complete set of power supply, communication and protection devices. They are available in various designs and with different equipment configurations, which are designed and configured individually for each installation.

The equipment installed within them is powered by 24 VDC from internal buffer power supplies, which operate in conjunction with a 2x12V battery pack with a capacity sufficient to maintain the voltage for a minimum of 30 minutes following a loss of the main 230V/50Hz mains supply. Exceptions may include:

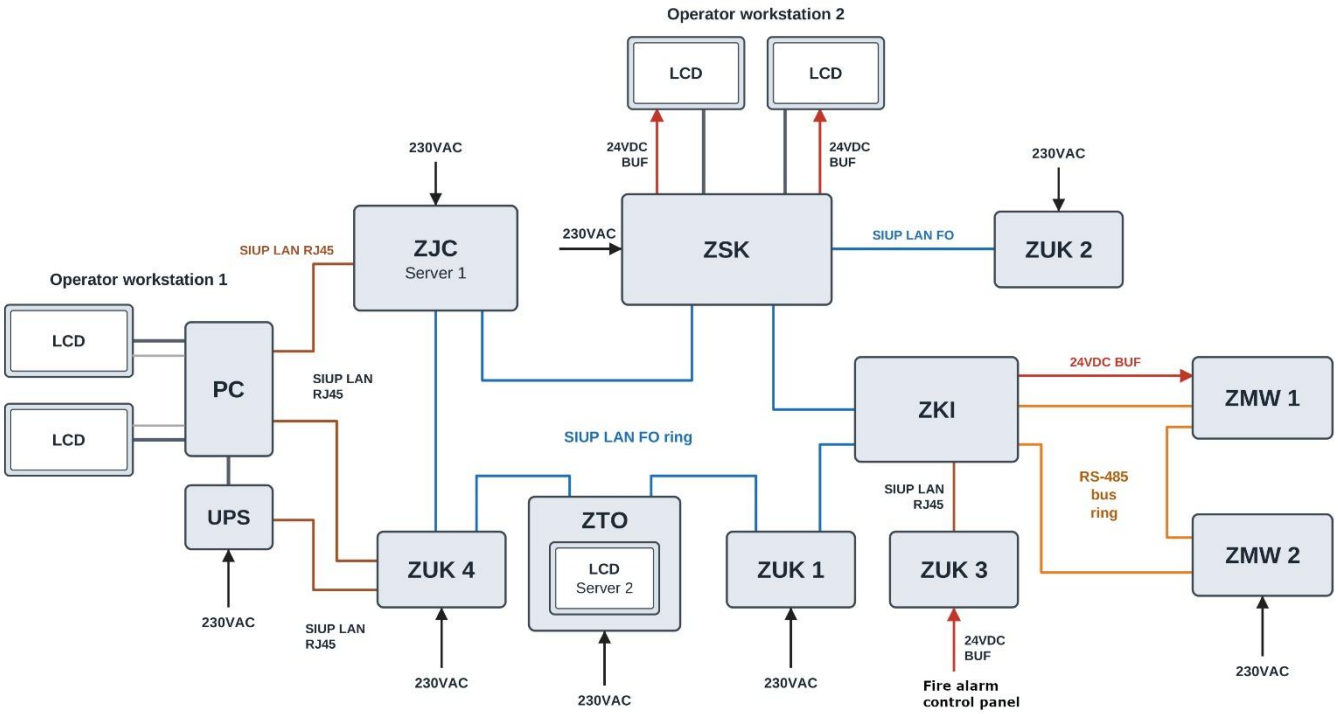
• ZUK communication equipment enclosures fitted with low-power components, which may be powered by 24 VDC from dedicated power outputs available in the connected fire alarm control panels;

• enclosures for remote DCM-100 series (ZMW) input/output modules, which may be powered from external fire-rated power supplies (including those located within the enclosures of other system components – e.g. concentrators).

Depending on the buffer power supply used, the condition of the battery bank and the status of the 230V/50Hz mains supply, the supply voltage to SIUP devices may vary within the range of 20 to 29 VDC. DC/DC converters may be used to power devices requiring a different voltage level.

All units, with the exception of the ZMW, are connected via a dedicated SIUP LAN. The ZJC, ZTO and ZKI units are connected redundantly via a SIUP fibre-optic LAN ring, in which a single break does not result in a loss of communication. ZSK client station units and ZUK communication devices located near the control centres of integrated subsystems, as end nodes of the SIUP LAN, may operate in a ring configuration or be connected to it in a star topology via a single fibre-optic cable or an RJ45 twisted-pair cable.

The method of connecting the system components is shown in the figure below.



Example of connections between ARGUS SIUP components

To enable the integration of fire protection equipment in geographically remote locations, connections between ARGUS SIUP system components may be established via a dedicated or leased WAN. Dedicated SIUP VLAN channels with guaranteed bandwidth should be allocated within the network. It is recommended that the network provide redundancy for SIUP communication links. The use of such a network in the system under implementation should always be preceded by a risk analysis.

3. SYSTEM SOFTWARE

Each of the two types of software (Argus PSIM and Argus RV) used in the ARGUS SIUP security management system is an advanced PSIM-class integration platform based on client-server architecture. It allows the system to be operated simultaneously from multiple operator workstations.

The Argus PSIM software is a proprietary solution for a network-based system integration software platform, which was developed and is being further developed by TELBUD S.A. using the latest Microsoft .NET technologies. Operation of the system is based on a visualisation application running in a web browser. The use of Microsoft Blazor technology enables high functionality, ease of use and application responsiveness. The application of the MVC and MVVM design patterns allows for the creation and installation of selected software modules. The use of WebAPI and SignalR technologies ensures high performance and enables simultaneous communication between multiple services and the system server. Building the system using ASP.NET technology enables faster implementation of new solutions whilst ensuring automated communication with the database. Argus PSIM is built on a PostgreSQL database with the Timescale package, and the Entity Framework library is used to communicate with it.

The Argus RV software, previously used in the ARGUS RV-C system, is developed by TELBUD S.A. on the basis of the advanced SYNDIS RV dispatch software platform from Mikronika. This platform is widely used to manage extensive power systems throughout Poland, as well as beyond its borders. The software utilises a high-performance Oracle database, ensuring adequate speed and operational reliability. The use of solutions that have been tried and tested in critical situations over many years of operation, combined with comprehensive cyber security mechanisms, communication protection and software self-monitoring, real-time operation with a resolution of up to 1 ms, and no limitations on the number of monitored signals and devices, guarantees reliable, stable and secure system operation.

The system software is compatible with both Windows and Linux operating systems. It comprises two core applications: a server and an operator monitoring visualisation application (client), enabling the creation of multiple monitoring workstations and the assignment of different access rights to them.

The server runs the system database and background processes for communication with on-site devices. The software records events occurring in the monitored systems, stores them in the database, and transmits control signals to the monitored devices. In each version of the system software (Argus PSIM and Argus RV), two databases are available: an editing database and a transaction database, which allow changes to be made to the software application without interrupting site monitoring. The database reload mechanism enables the visualisation of changes made in the editing database, which are transferred to the transaction database upon reload.

The server application operates without requiring manual intervention. It starts automatically as a system process. Whilst the application is running, it is possible to perform a range of administrative functions, including:

- data archiving,
- creating backups,
- database maintenance,
- tracking the progress of data transmission sessions.

The visualisation application displays events in the form of lists and graphically on facility maps and synoptic screens. A fully graphical, vector-based presentation of the status of all monitored elements on facility maps allows for easy monitoring and control of equipment. The application can operate on workstations with multiple monitors and display information on a video wall.

The system software application performs, amongst other things, the following basic functions:

- collecting information from monitored systems,
- processing information and storing it in a database,
- visualising the status of monitored systems on maps,
- signalling alarms and visualising event messages in the event log,
- managing alarm handling procedures,
- transmitting control commands to monitored systems,
- synchronising data between servers,
- exchanging data between client applications,
- database management – archiving, creating backups, organising the database, restoring the database in the event of a failure,
- managing operator permissions as well as communication, security and configuration integrity.

The system software can be configured by the user, which allows the application to be adapted independently to changes made to facilities and significantly simplifies its expansion to include further monitored facilities and devices.

4. OPERATOR CONTROL

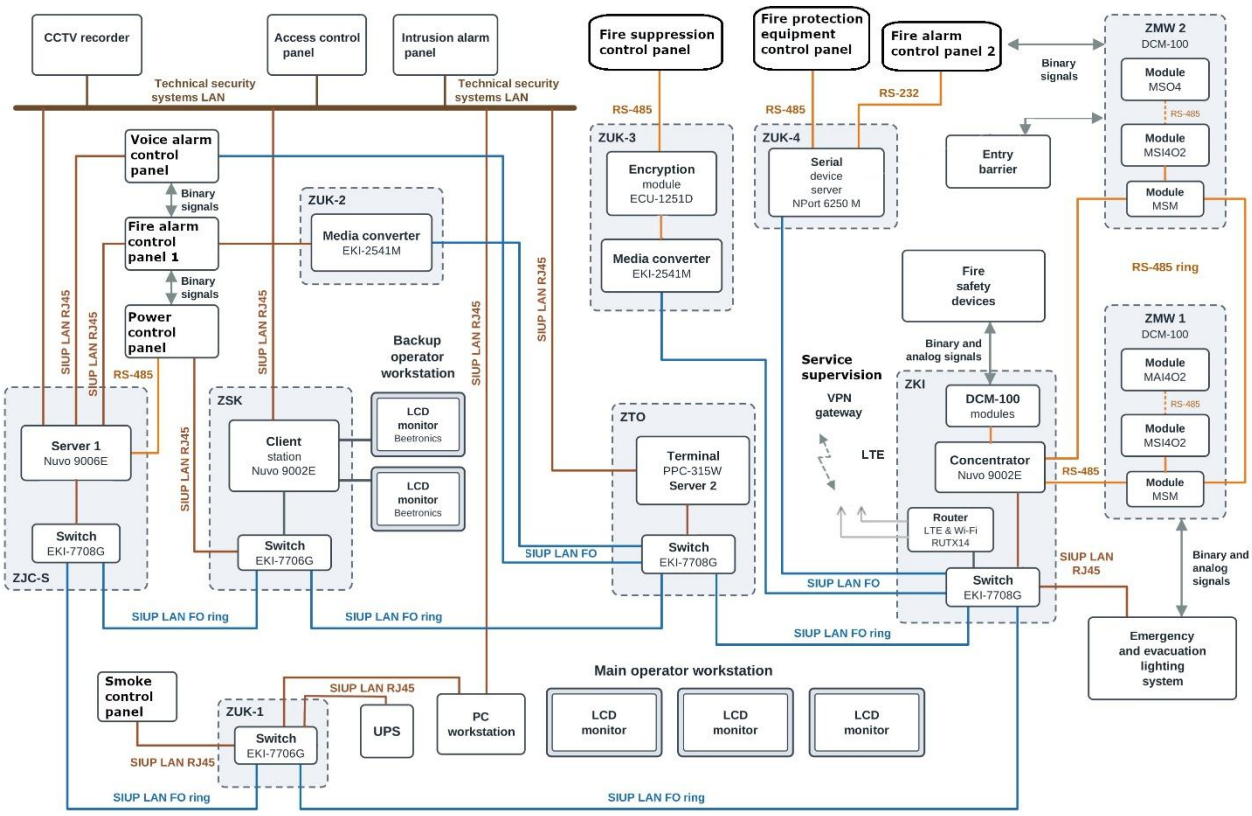
Operator control of the system can be carried out from certified client stations and operator terminals located in ZJC, ZSK, ZKI and ZTO buildings, as well as from PC workstations, via a client visualisation application. This is a web browser-based application. On certified client stations and PC workstations, visualisation can be displayed on one or more monitors with a resolution of at least Full HD (1920x1080), although the use of monitors with a screen size of at least 24" is recommended. Basic operator stations, whose speed and as operational reliability is crucial to the system’s functioning, they should be fitted with at least two monitors.

As PC workstations are not construction products and are not subject to certification in the same way as other system components, it is recommended that the system be equipped with at least one certified client workstation or operator terminal.

5. SYSTEM CONFIGURATION OPTIONS

The ARGUS SIUP system is configured individually for each installation. Depending on the chosen configuration, it can operate with a single server, two servers in a hot standby configuration, or in an expanded multi-server system. The number of individual system components, including servers, operator terminals, concentrators, input/output modules, communication devices and operator stations, depends on the specific requirements of the project in question. Depending on requirements, various system configurations may be used: ranging from the simplest, comprising only a central unit (ZJC), or even just an operator terminal (ZTO) on which both the ARGUS PSIM and Argus RV server and client applications run simultaneously, to the most complex, consisting of multiple servers and other components forming a hierarchical structure. Data exchange between the elements of such a structure is carried out via the SIUP LAN.

The figure below shows a diagram of an example configuration of the ARGUS SIUP system.



Block diagram of an example configuration of the ARGUS SIUP system

If the server (ZJC) and the operator console are located in a remote fire safety management centre for geographically dispersed sites, the ARGUS SIUP system configuration must take into account connections via a dedicated or leased WAN, or communication via an LTE mobile network within a separate, private APN. The recommended system configuration for such installations is to install an interface concentrator (ZKI) at each site, which communicates with the central server via the encrypted TLS system protocol. The concentrator's role is to mediate the acquisition of data from local fire protection devices and the transmission of control commands to them. For communication between the concentrator and the server, it is recommended to use routers that form part of the ARGUS SIUP system.

In premises with permanent staff, the concentrator may alternatively be replaced by a local server (ZJC-S) working in conjunction with a certified client station (ZSK) or a PC workstation, a server and client station in a single unit (ZJC-DK), or an operator terminal (ZTO) with server functionality, which will additionally enable local management of devices integrated on-site, regardless of the connection to the control centre.

To enable remote operators to verify fire alarms, remote sites (particularly unmanned ones) should be equipped with a CCTV surveillance system which, once integrated with the ARGUS SIUP system, will allow camera footage to be transmitted to the operator's console at the control centre.

6. EQUIPMENT USED IN THE SYSTEM

The ARGUS SIUP system is built using a range of devices, which are specified in the National Technical Assessment and selected on a case-by-case basis depending on the required system configuration and functionality for individual implementations. The system utilises industrial devices powered by a DC voltage within a wide range (typically 24V), including:

• NEOUSYS TECHNOLOGY's Nuvo 9000 series industrial computers, specifically the Nuvo-9002/9006, Nuvo-9531, Nuvo-9501 and Nuvo-9160GC, which are used as central processing units, certified client stations and interface hubs. They can run on the Windows 10 IoT Enterprise operating system or higher, or on Linux. Depending on their function, they are equipped with server and client application software, or communication driver software for the Argus PSIM system, or alternatively Argus RV. Thanks to their support for the latest 12th-generation Intel® processors (Alder Lake Core™) Intel® Core™ i9/i7/i5/i3, Intel® Pentium® and Celeron® processors with 35/65W TDP, and up to 64 GB of DDR5 RAM (depending on the model), the Nuvo 9000 Series computers offer sufficient performance even for the most demanding and complex applications. They can be equipped with a high-speed NVMe SSD installed in an M.2 Gen4x4 slot and/or – depending on the model – one or two SATA HDD/SSD drives operating in RAID 1. The computers feature, amongst other things, 2 or 3 independent video output ports (VGA, HDMI, DP), 2, 4 or 6 Ethernet ports (including optional PoE ports), 2 RS-232/422/485 serial ports and multiple USB ports (including one USB-C). Depending on the model, the computers may be equipped with one or two PCIe slots and a MezIO™ expansion slot, into which additional communication modules and I/O devices can be installed.

• Advantech's TPC and PPC series of industrial LCD touchscreen panel PCs, functioning as operator terminals running Windows 10 IoT Enterprise or later, or Linux, with the Argus PSIM or Argus RV client application software. The terminal can also operate with the full Argus PSIM or Argus RV server software, acting as a standalone or redundant central system unit. Depending on the series, type and model, the panel PCs are designed to support 8th generation Intel® Core™ i3/i5/i7 processors (TPC-

3xx series, TPC-B510), 11th generation (PPC-3xx series, TGL versions), or 13th generation (TPC-B520, PPC-3xxSW RPL, PPC-4xx), or Atom™ x6425E/Celeron® J6412 (EHL versions), or Adler Lake N97 (PPC-3xxSW ADL), working with DDR4 or DDR5 RAM up to 32 GB or 64 GB. They can be fitted with a standard 2.5" SATA SSD and/or an M.2 SSD with a SATA interface. If the computer is fitted with two drives, they can operate in RAID 1. The computers are equipped with, amongst other things, a video output port (DP or HDMI), two Ethernet ports, RS-232 and RS-232/422/485 serial ports, and several USB ports.

• Beetronics HB9M series industrial LCD touchscreen monitors with Full HD resolution (1920x1080), which can be built into the doors of ZJC, ZSK, ZKI and ZTO enclosures and work in conjunction with Nuvo computers installed in these enclosures, acting as operator terminals. They are designed for continuous operation and professional use. The front panel has an IP65 protection rating. The monitors are fitted with a speaker, feature HDMI, DisplayPort, VGA, USB-C and USB-A connectors, and can be powered by a DC voltage ranging from 9 to 36 VDC. They operate within a wide temperature range: from -20°C to 70°C. Monitors with screen sizes ranging from 10‘ (10HB9M), through 12’, 15‘, 17’, 19‘ and 22’, up to 24" (24HB9M) can be used in the system. At present, a 27-inch monitor from this series is not available, but should the manufacturer launch such a model, it may also be used. Monitors from this series may also be used at operator workstations in certified client stations (e.g. ZSK) either as free-standing (desktop) units or mounted on the wall.

• Managed network switches:

- Advantech’s EKI-7700 series in E (Fast Ethernet) and G (Gigabit Ethernet) variants,

- Moxa’s latest EDS-4000/G4000 series, which complies with the IEC 62443-4-2 and IEC 62443-4-1 cybersecurity standards specifying requirements for safety functionality and secure product design and development,

- Moxa’s EDS-505A/508A, EDS-G506-4PoE, EDS-G509, EDS-510A, EDS-510E and EDS-G512E/G518E series.

The EDS 4000 series switches with the LVB designation feature PoE-compliant Ethernet ports. For the construction of the SIUP LAN system ring, it is recommended to use fibre-optic switches from a single manufacturer, which increases the reliability of the communication network and reduces the connection recovery time in the event of a failure of one of the ring components to 20 ms. It is permissible to operate Advantech and Moxa switches simultaneously within the ring using a redundancy mechanism based on the RSTP (Rapid Spanning Tree Protocol), which enables the network topology to be reconfigured within a few seconds.

• LTE and Wi-Fi routers: Routers from the RT900, RTM and RTX series by TELTRONIKA Networks, used for wireless and wired communication, including: RUT901, RUT906, RUT955, RUT956, RUTM50, RUTX09, RUTX10, RUTX11, RUTX12, RUTX14 and RUTX50. These devices provide high performance, critical mobile communications with connectivity redundancy via Dual-SIM, communication over Wi-Fi networks and wired LAN and WAN networks (they can function as network switches), and are capable of receiving real-time location and time signals from GPS. By connecting a range of external antennas, effective detection and reception of radio signals of sufficient quality are ensured.• Injectory PoE: Anybus AWB4006.

• Media converters: Advantech EKI-2541M/MI and 2541S/SI series, and EKI-2741; Moxa IMC-21 series (IMC-21A/21GA).

• Interface converters, isolators and repeaters:

1. Devices from CEL-MAR's ADA series, including: RS-232/RS-232: ADA-1010, RS-485/RS-485: ADA-4040, RS-232/RS-485 and RS-422: ADA-1040, ADA-4010, ADA-1044h (RS-232 – 4xRS-485), RS-232/1-Wire: ADA-101W, RS-485 and 422/1-Wire: ADA-401WA and WP (Modbus RTU protocol), RS-232/Ethernet: ADA-13110MG, RS-485 and RS-422/Ethernet: ADA-13040MG, RS-232/FO (multimode fibre): ADA-7010, RS-485 and RS-422/FO (multimode fibre): ADA-7040, RS-485 and RS-422/RF (wireless network). All converters feature galvanic isolation of the interfaces from one another and from the supply voltage. Converters with a 1-Wire interface are used to connect environmental sensors, which can be used in particular for measuring temperature and humidity (e.g. DHT22) in SIUP installations and within building premises (e.g. in server rooms, POUP and PTUP).2. Urządzenia Advantech serii ADAM, w tym: RS-485 (RS-422)/RS-485 (RS-422): seria ADAM-4510, RS-232/RS-485 (RS-422): serie ADAM-4520/4522, ADAM-4521.

3. Moxa TCC 120/120I series devices.

4. The MSM module from Mikronika's DCM-100 series of I/O bus isolators can also be used as a standalone RS-485 isolator.

• Serial port servers enabling the connection of devices with RS-232, RS-422 and RS-485 serial ports to an Ethernet network: Advantech's EKI-1511 and EKI-1521/1522/1524 series, Moxa NPort 5100/5200A series (5110A, 5130A, 5150A, 5210A, 5230A, 5250A), Moxa 6100/6200 series (6150, 6250, 6250-M-SC, 6250-S-SC), which provide encrypted data transmission whilst also functioning as encryption modules, and are available in versions with a port for single-mode fibre (S-SC) or multi-mode fibre (M-SC), thereby eliminating the need for media converters, CEL-MAR ADA-13110MG and ADA-13140MG. Depending on the type and model, these devices allow the connection of one, two or four RS-232, RS-422 or RS-485 ports.

• Encryption modules built around IIoT gateways based on miniature embedded computers for industrial applications with RISC Cortex-A8 architecture, running the RT-Linux operating system. They are equipped with communication drivers for devices connected via serial and network interfaces, similar to those found on interface concentrators. The system can utilise modules from the following series: Advantech ECU-1051 and ECU-1251 – the ECU-1251D model is additionally equipped with 4 inputs and 4 binary outputs with galvanic isolation – and Moxa UC-2100. The modules feature 1 or 2 configurable RS-232/422/485 serial ports and 1 or 2 LAN ports. Depending on the type, model and configuration, the modules can also operate over Wi-Fi, whilst built-in SIM slots enable communication via LTE mobile networks. They communicate with the central unit by encrypting data using the AES protocol, which is then encapsulated into TCP or UDP packets.

• Binary and analogue input/output modules comprising two product groups:

- Mikronika's DCM-100 series modules, specified in National Technical Assessment No. CNBOP-PIB-KOT-2018/0057-1002 for the ARGUS RV-C system, which have been expanded and upgraded for use with the ARGUS SIUP system,

- Moxa ioLogic E1200 series modules.

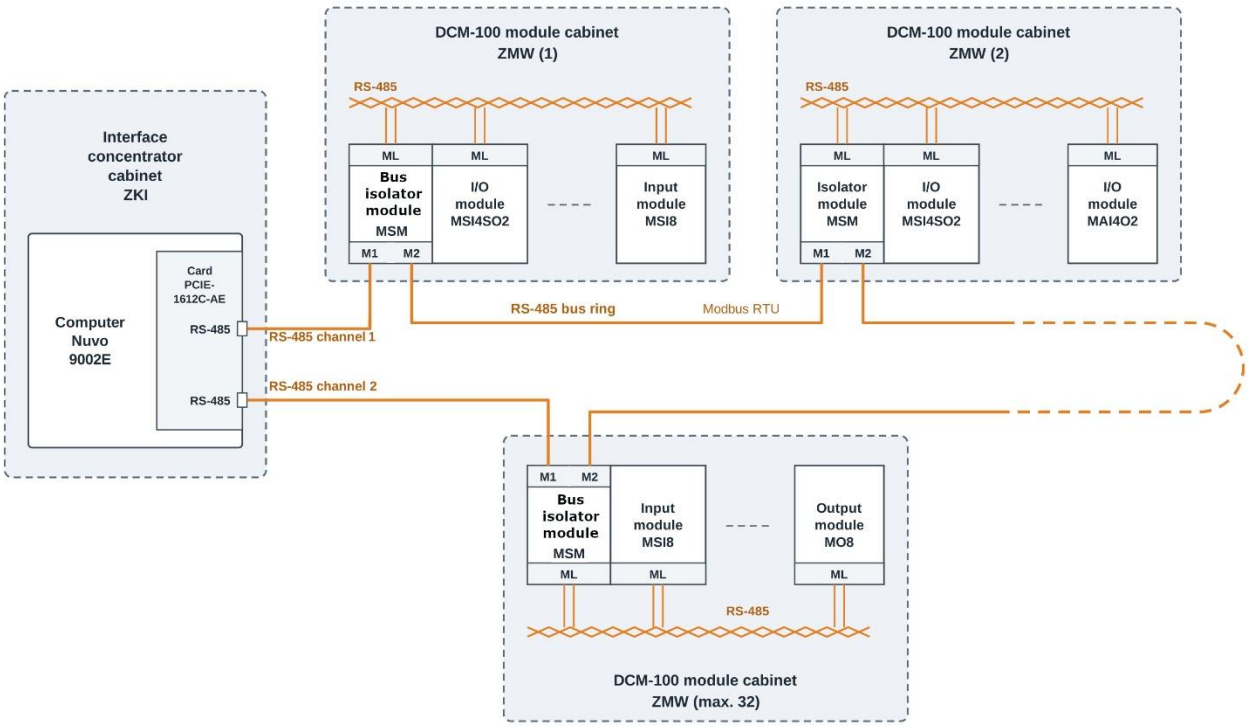
Both groups of modules provide galvanic isolation of inputs and outputs. In addition to the above-mentioned modules, the Argus Control BMP-PoE input/output module from Telbud may also be used;

this module can be powered via PoE in accordance with the IEEE 802.3af Class 0 standard and also features a 1-Wire port for connecting sensors that measure environmental parameters.

DCM-100 Series Modules

The DCM-100 industrial series modules form part of a control and monitoring system for applications requiring continuous monitoring of input and output circuits. The system architecture is based on groups of modules mounted on a shared DIN rail and connected via a local RS-485 bus. These groups are linked via the main RS-485 bus as 'slave' devices working in conjunction with a 'master' management device – which may be a central processing unit, an operator terminal, a certified client station, an interface concentrator, or an encryption module. The local bus and the sections of the main bus chain connected to it are galvanically isolated from one another via a dedicated isolation module, installed at the start of each group. For groups of modules housed in separate ZMW enclosures, the bus is connected in a ring configuration. To form the ring, the 'master' management device must utilise two galvanically isolated RS-485 interfaces.

The method for connecting modules installed in separate ZMW enclosures is shown in the figure below.



An example block diagram showing the connection of DCM-100 series modules installed in ZMW enclosures

Each group may contain up to 32 input/output modules (excluding the isolator module), and up to 32 groups of modules may be connected to a single bus ring, provided that the total number of I/O modules does not exceed 128. The number of rings is limited only by the number of isolated RS-485 ports available in ARGUS SIUP system devices.

Communication with the DCM-100 series modules is carried out via the Modbus RTU protocol using communication driver software installed on the computers of the management devices; data transmission can be encrypted if required.

The upgraded DCM-100 series comprises the following modules:

• MSM – an RS-485 bus isolator module, which is installed at the start of each group of modules and divides the bus into three galvanically isolated sections: the local bus of the module group and two sections of the bus chain connecting adjacent groups. This module can also be used independently of the input/output modules as a separator for any RS-485 interface lacking galvanic isolation.

• MSI4SO2 – a digital input/output module with line continuity monitoring; it features four 24 VDC inputs with status detection for: supervision, alarm, short circuit and open circuit, as well as two NO/NC relay outputs with circuit continuity detection when a 24 VDC voltage is applied. Compared to the module used in the ARGUS RV-C system, this module is not equipped with an RS-485 local bus isolator and features voltage-configurable dual inputs, allowing two control contacts (e.g. limit switches for fire dampers) to be connected to a single input. The circuit continuity check option can be disabled via software for individual inputs and outputs.

• MSI8 – an 8-input 24 VDC digital module with status detection: supervision, alarm, short circuit and open circuit, with the same parameters as the inputs in the MSI4SO2 module.

• MI8 – a module with 8 binary 24 VDC inputs with detection of the following states: alarm, supervision.

• MSO4 – a module with 4 NO/NC relay outputs with circuit continuity detection when a 24 V DC voltage is applied, with parameters identical to those of the outputs in the MSI4SO2 module.

• MO8 – a module with 8 relay outputs, including 4 NO/NC outputs and 4 configurable NO or NC outputs.

• MAI4O2 – analogue input/output module, featuring 4 inputs and 2 outputs, each of which can be software-configured to the 4–20 mA or 0–10 V standard.

DCM-100 series modules can be installed in ZKI concentrator enclosures, ZJC central units, ZTO operator terminals, ZSK certified client stations and ZUK encryption modules, as well as in separate ZMW enclosures. The MSM bus isolator module can be installed in any enclosure where galvanic isolation of the RS-485 interface is required.

ioLogic series modules

The ioLogik E1200 series of industrial I/O modules features a built-in two-port Ethernet switch, which enables data to flow between local area networks or allows the next ioLogik module to be daisy-chained. These modules can be used to create distributed control systems that communicate over a LAN using various communication protocols, including Modbus TCP, EtherNet/IP, Moxa AOPC and SNMP. The modules are designed for DIN-rail mounting.

The ioLogik E1200 series comprises a range of modules differing in the type and number of inputs and outputs. A wide selection of input/output types and versions, including binary inputs (DI), binary outputs (DO) of the 'Sink' and 'Source' types, relay outputs, analogue inputs and outputs (AI/AO) of 0–10 VDC, 0–20 mA and 4–20 mA, RTD inputs for resistive temperature sensors PT50, PT100, PT200, PT500, PT-1000, and inputs for type J, K, T, E, R, S, B and N thermocouples (TC), enables the construction of data acquisition and control systems for a wide variety of devices. There are currently 10 module types available: E1210 (16 x DI), E1211 (16 x DO), E1212 (8 x DI, 8 x DO), E1213 (8 x DI, 4 x DO, 4 x DIO), E1214 (6 x DI, 6 x Relay), E1240 (8 x AI), E1241 (4 x AO), E1242 (4 x DI, 4 x DIO, 4 x AI), E1260 (6 x RTD) and E1262 (8 x TC). The ioLogik E1200 series modules can be installed in all system component enclosures that are connected to the SIUP LAN.

Argus Control Module

The Argus Control BMP-POE-1000 module from Telbud features 8 configurable digital inputs and 2 relay outputs. The inputs can be configured as NC, NO, 2EOL and 3EOL. An input configured as 2EOL or 3EOL for a 2- or 3-parameter line can monitor up to three binary signals, e.g. signals from the NC outputs of a PIR motion detector: alarm, tamper and masking. Line parameterisation is carried out by connecting appropriate resistors to the individual outputs. Each relay output has NO and NC contacts, which can be used to control any devices with a voltage of up to 230 VAC. The module is also equipped with a 1-Wire port, which can be used to connect sensors for measuring environmental parameters, including, in particular, DHT22 temperature and humidity sensors.

7. POWER SUPPLY SYSTEMS

The primary power source for the enclosures in the ARGUS SIUP system is the 230 V, 50 Hz on-site mains supply. The enclosures utilise 24 VDC buffer power supplies operating in conjunction with a 2 x 12 V battery pack, which serves as a backup power source.

The following types of buffer power supplies may be used in the system:

• certified Pulsar EN54M series fire-rated power supplies (EN54M-2A7/3A7/5A7/10A7), providing a supply voltage within the range of 20.0 V to 27.6 V depending on the state of the battery pack, designed to operate within a temperature range of -5 to 75°C,

• Merawex ZSPM series certified fire power supplies (ZSPM-75/150/200/320) with an output voltage of 21.0 V to 28.8 V (depending on the condition of the battery pack),

• certified Merawex ZM-AZ/PZ series emergency power supplies (ZM24V6A/12A/24A), with an output voltage of 21.6 V to 26.4…28.8 V (depending on the condition of the battery pack and the setting for the voltage per battery cell),

• Mean Well DRC series power supplies with a rated output voltage of 27.6 VDC (DRC 40B/60B/100B/180B).

The power supplies are fitted with independent outputs for signalling a 230V/50Hz mains power failure, as well as a general failure or the discharge/failure of the rechargeable battery pack (ZM-AZ and DRC). The separately protected outputs of the fire-rated power supplies can be used to power ARGUS SIUP system devices located outside the enclosure, such as industrial LCD monitors or DCM-101 and DCM-100 series input/output modules in separate enclosures.

YUASA NP-series AGM industrial rechargeable batteries are used as the standard backup power source, with a capacity selected to match the power supply unit's output and the required backup time. Equivalent batteries from other manufacturers with comparable specifications may also be used.

The type and power rating of the power supply, as well as the battery capacity, are selected on a case-by-case basis to match the supply voltage range, the total power drawn by all loads, and the required backup time.

For equipment requiring a supply voltage other than that provided by buffer power supplies, Mean Well DDR series DC-DC converters may be used in the system:

• DDR-15, DDR-30 and DDR-60 with an input voltage range of 9–36 V DC,

• DDR-120 and DDR-240 with an input voltage range of 16.8–33.6 V DC.

8. OPERATOR STATION EQUIPMENT

• Equipment for operating client stations in ZJC, ZSK and ZKI facilities

Beetronics industrial LCD monitors with screen sizes of 15/17/19/22/24/27 inches and Full HD resolution (1920x1080) are intended for operating the system from client stations located in ZJC and ZSK enclosures. These may be touchscreen monitors from the TS7 and TS7M series, or the HB9M series, or standard monitors from the HD7 and HD7M series, which are operated via a keyboard and a wired USB mouse. All monitors are fitted with a speaker, and the front panel has an IP65 protection rating. They are designed for continuous operation and professional use.

The TS7, TS7M, HD7 and HD7M series monitors are designed for wall mounting or desktop use. They feature HDMI and VGA sockets for connection to the video outputs of Nuvo computers. They can be powered by a DC voltage ranging from 9 to 33 VDC and operate within a temperature range of -20°C to 60°C.

In addition to the standard options of wall mounting or desktop placement, the HB9M series monitors can also be built into the doors of ZJC, ZSK, ZKI and ZTO enclosures in the ARGUS SIUP system, forming an integral part of these enclosures and serving as operator terminals. They offer better specifications than the TS series monitors – more connectors (HDMI, DP, VGA, USB-C and USB-A) and a wider range of supply voltages (9 to 36 VDC) and operating temperatures (-20°C to 70°C).

Other monitors with similar specifications may be used in the system, in particular those powered by a DC voltage within a range corresponding to the voltage supplied by the buffer power supplies in the ZJC, ZSK, ZKI and ZTO enclosures.

• PC workstations

Workstations used to operate the ARGUS SIUP system should be designed for continuous 24/7 operation. Operation and visualisation are carried out via the Argus PSIM client application, which is made available by the central unit via a web browser.

Workstations should support multi-monitor operation (up to four monitors) with a resolution of at least Full HD (1920x1080) and be equipped with a wired keyboard and mouse. It is recommended to use LCD monitors with a screen size of at least 24", designed for continuous operation. In the case of workstations with multiple monitors, one of them typically displays the current event log, whilst the

others display maps, overview screens and, where applicable, CCTV camera feeds. The user can dynamically split the monitor screen between the synoptic display and the event list. The workstation software can also integrate with visualisation systems on a graphic wall comprising large-format monitors.

The equipment and required specifications of workstations depend on the functions performed and the method of operating the system's client application.

The minimum specifications that the system's workstations should meet are:

- Intel Core i5-12600 processor, 3.30 GHz, 18 MB, 6 cores, 65 W, ECC,
- 16 GB DDR5 4800 UDIMM RAM, NECC,
- 512 GB SSD,
- an additional dedicated NVIDIA T1000 4 GB graphics card or equivalent – only for workstations handling the visualisation of CCTV camera footage,
- 2 x 1 GB RJ45 Ethernet ports,
- a wired USB keyboard,
- a wireless mouse,
- Windows 10 Pro operating system or higher.

Due to the required reliability and operational certainty, it is recommended to use branded workstations from recognised manufacturers such as Dell, HP, Lenovo, etc.

Workstations, together with their display monitors – in particular the primary workstation located in the fire protection equipment control room (POUP) – should be powered from the 230V/50Hz mains supply via a UPS capable of maintaining the power supply for the time required by the entire system, for no less than 30 minutes. UPS units equipped with an Ethernet port must be used, enabling the monitoring of the UPS and battery status via the SNMP protocol.

9. SYSTEM SECURITY

System functions are accessible once the operator has logged in (using a unique ID and password). Access to individual functions is subject to specific permissions granted by the system administrator. To limit the possibility of unauthorised manipulation, the system has built-in functions that enforce periodic password changes in accordance with password creation rules – the syntax of which is determined by the administrator. Two accounts are configured by default: the operator and the administrator.

To ensure the safety of equipment control, the system software is equipped with two-stage control mechanisms featuring confirmation. The execution of critical control actions may also require additional authorisation from the operator, or even approval by a supervising operator.

In large-scale systems requiring multiple operator workstations, operational safety can be enhanced by utilising the functionality for workstation supervision by senior operators. This functionality includes, in particular, mechanisms for monitoring operator activity, with the option of dynamically taking over their authorisation to handle events.

The system's digital security is ensured by the isolation of the SIUP LAN communication network and the encrypted transmission of data between servers, interface concentrators and operator workstations, as well as through the use of system communication components enabling the encryption of connections with integrated devices (encryption modules and serial port servers with encrypted transmission). The system software also allows for the creation of secure VPN connections.

Security mechanisms available in the Windows operating system, including in particular Windows Defender, are also utilised to protect the system. The system software allows for the management of system security using Active Directory services.

10. CABINETS FOR INSTALLING SYSTEM COMPONENTS

Wall-mounted cabinets from ZPAS's SWN range are used for installing system components. These cabinets are available in various dimensions: heights of 300, 400, 500, 600, 800 or 1000 mm, widths of 200, 300, 400, 500, 600, 800 mm wide and 115, 150, 210, 250 or 300 mm deep – depending on the cabinet size. The specific cabinet size is selected on a case-by-case basis depending on the type of installation and its equipment in a given system application. The cabinets have an IP65 protection rating in accordance with EN 60529. The protection rating of ARGUS SIUP system enclosures depends on the method of cable routing and the cable glands used. The minimum protection rating for the enclosures is IP30.

Enclosures housing devices with higher power consumption, such as ZJC, ZSK, ZKI and ZTO, may be optionally fitted with a thermostat-controlled fan, which is activated when the set temperature inside the cabinet is exceeded.

The cabinets may be optionally fitted with ventilated grilles with a filter (e.g. GV200) and a fan (e.g. LV200) with a thermostat (e.g. KTS 111) featuring a normally open (NO) contact that activates forced ventilation once the set temperature is exceeded.

The cabinets may also be fitted with limit switches to signal when the door is open, the status of which is monitored by the system.