

GUARDDO

GUIDE

Technical specifications.....3

Data security.....4

Disk space.....5

Front panel.....6

Rear panel.....7

First system start-up.....8

Arming the system 9

Disarming the system from the “Guard” mode.....10

Operation of indicators.....11

Security mode errors.....12

Remote GSM control.....13

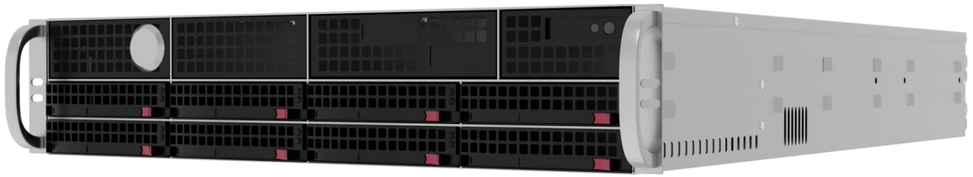
Remote triggering.....14

Contacts.....15

TECHNICAL CHARACTERISTICS

Samurai device is designed for irretrievable erasure of information from HDD/SSD hard disks.

Supply voltage	220B
Consumption power	up to 75W
Battery voltage	10-14B
E/m field strength at triggering	450kA/m
Current consumption in “Guard” mode	max. 0.1A
Current consumption in charging mode	not more than 6A
Power unit charging time	up to 40 sec
Number of digital sensors to be connected	up to 6 pcs
Voltage at inputs	0...+25B
Voltage is considered as low level	less than 0.5V
Voltage is considered as high level	more than 1.5V
Triggers by radio keyfob	up to 1000m



The system is equipped as standard with an event logger, which can only be read out by the service center. The date and time are stored in the logger:

- sensor actuation
- key fobs (RF cards) attachment
- change of security modes
- disappearance and resumption of supply voltage

DATA SECURITY

To avoid irretrievable data loss, use the system only after reading this manual completely.

The main method of arming/disarming is by proximity cards or keyfobs.
Data destruction is performed:

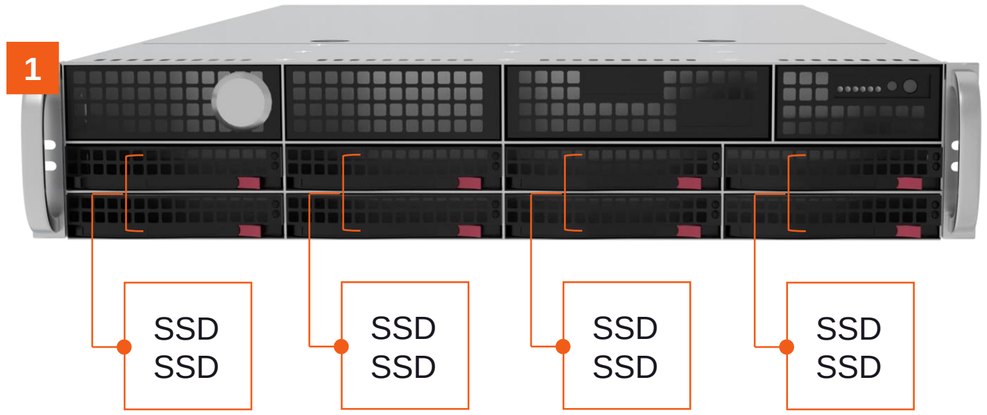
- Remotely by SMS messages
- Manually by wired button
- By radio keyfob

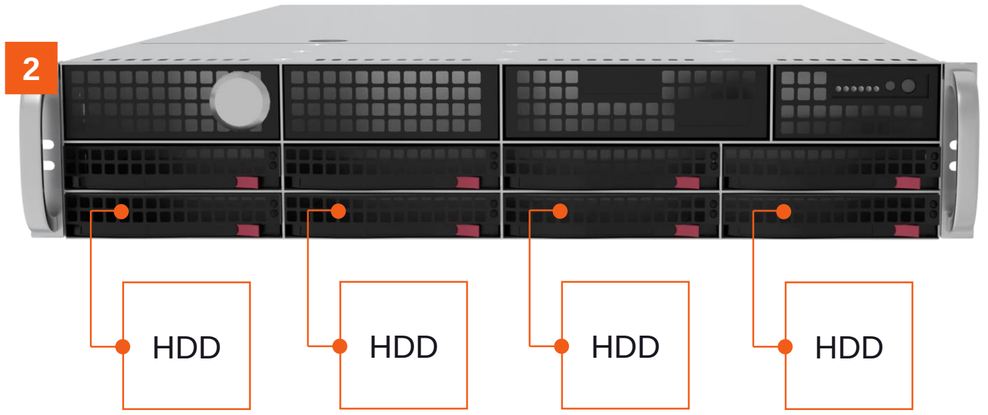


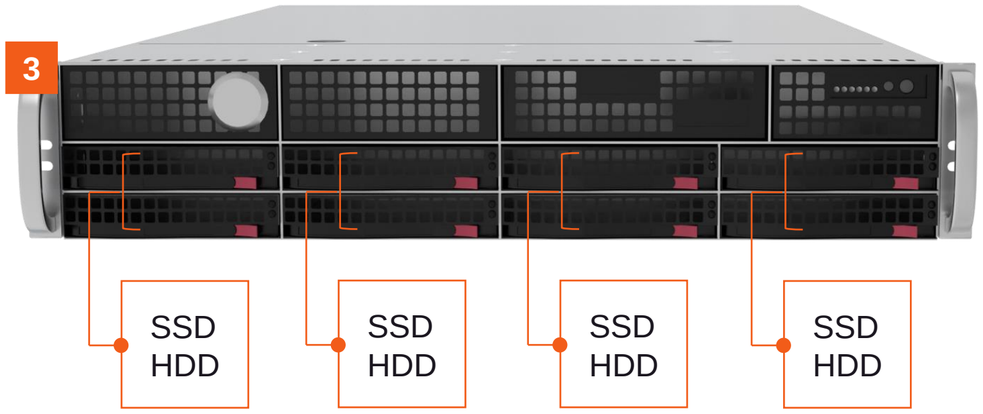
The system is designed for round-the-clock power supply from the mains voltage ~220V. In case of power failure, the guaranteed autonomous operation time is 24 hours.

DISK SPACE

The data destruction system works with any combination of disks.

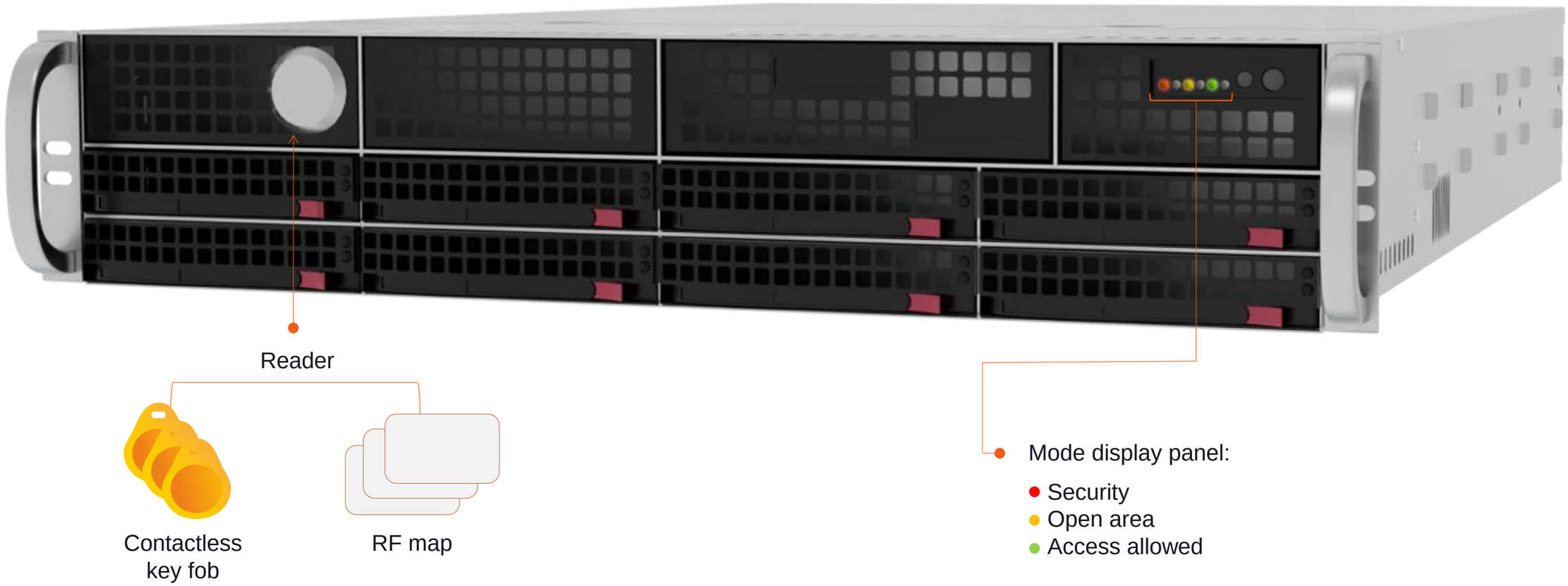






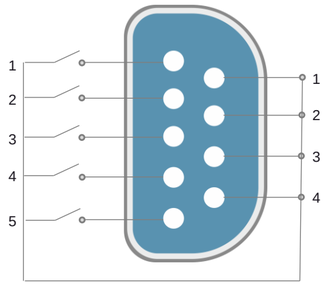
FRONT PANEL

The standard package includes 3 proximity fobs or RF cards of the customer's choice. The maximum possible number of proximity fobs and cards is 6.



REAR PANEL





Wired button 1 (DB-9 connector). There can be up to 5 wired buttons

GSM antenna

~220V

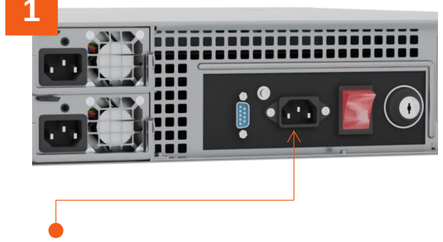
Mains power switch



Backup power supply lock keys

FIRST SYSTEM STARTUP

1



Connect the power lead to the connector on the rear panel.

2



Turn the key of the backup power lock to the “ON” position:

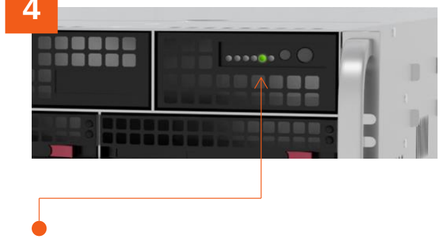
- The “ON” position removes the key from the power lock.
- The “OFF” position does not remove the key from the power lock.

3



Press the key. When the power switch key is in the ON position and the key is removed from the lock, the power switch key prevents the power from being turned off (protection against unauthorized disconnection).

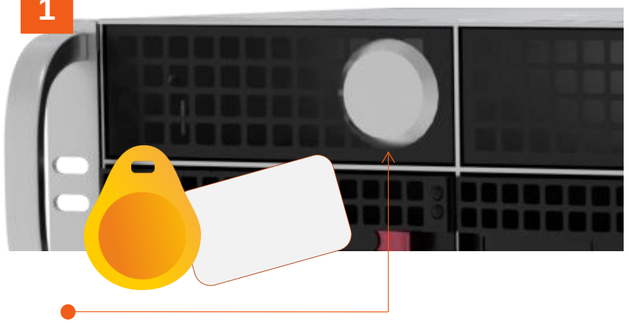
4



The green light on the front display panel will illuminate.

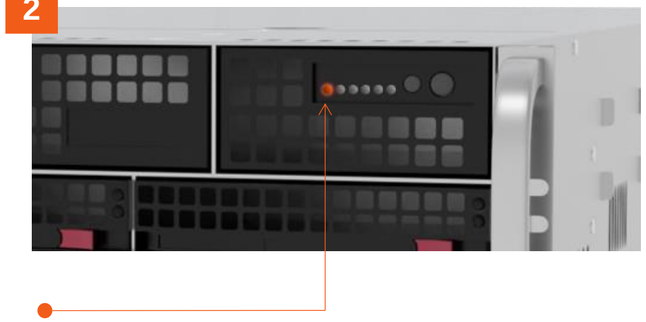
ARMING THE SYSTEM

1



To arm the system, place the proximity keyfob or RF card to the reader on the front panel. The red LED will blink for 10-30 seconds (the power unit is charging).

2



“Guard” - the red light will be on permanently.

3

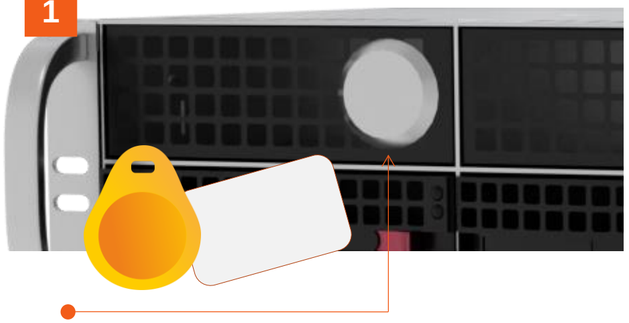


For safety reasons (unauthorized disconnection of power supply) it is recommended to remove the key from the lock on the rear panel of the device.



DISARMING THE SYSTEM

1



When the proximity keyfob or RF card is touched again to the reader on the front panel, the green LED will light up - the system will enter the “Access Allowed” mode.



Functionality check

1

When checking the device performance, no more than 2 consecutive checks are allowed. After that, a time pause of at least 10 minutes is required to prevent overheating of the device.

2

If at least one of the sensors is defective, the system will automatically enter the “Open Zone” mode. In this mode, the yellow LED will blink for 1 minute, then the system will switch to the “Guard” mode with open zone.

3

Remove the system from Guard mode. If the Open Zone mode does not turn on, insert protected disks into the system or check for power and proper connections.

INDICATOR OPERATION

1



The system is armed and the power pack is charging. The red indicator flashes for 10-30 seconds.

2



The system has entered the armed mode. The red indicator is constantly lit

3

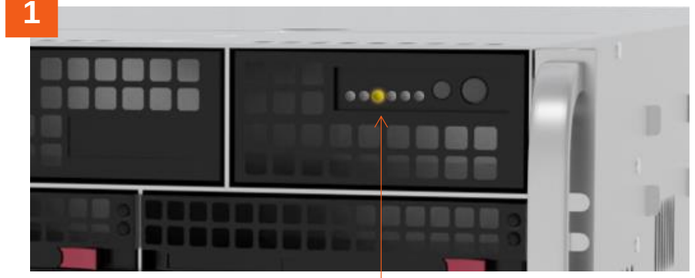


The system is disarmed. The green LED is permanently illuminated.

ARMED MODE ERRORS

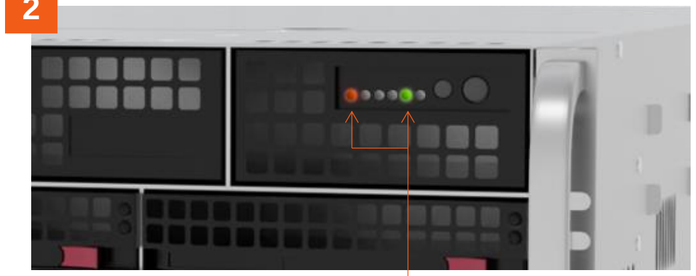
In case of error write or call support. Contacts on the last page.

1



The system goes into armed mode, the sensor is faulty. The number of flashes between pauses indicates the number of the faulty sensor. The yellow indicator flashes for 1 minute.

2



The system goes into armed mode, the power supply unit is defective. Both red and green LEDs are blinking continuously.

REMOTE GSM CONTROL

Call the number of the SIM card installed in the GSM module from the telephone to be used as the owner's telephone (M1). The GSM module will detect the number, establish connection and you will hear a greeting:

1

StarLine welcomes you! Enter password 1! Enter 4 digits of the first password. For example - 1234. After successful entry, you will hear a confirmation beep and a request to enter the second password, also consisting of 4 digits.

2

Enter password 2! Enter the 4 digits of the second password. For example - 4321. After successful entry, you will hear an audible confirmation. The M1 telephone number and passwords will be stored in the GSM module memory, and a confirmation SMS message with the recorded data will be sent to the M1 telephone.

Telephone numbers can be changed or deleted from the GSM module memory by means of SMS commands sent from the owner's telephone (M1). In order to write a new number or change an already programmed one, the following format commands are used:

SMS command format					
Command code	0	0	0	0	phone number
	0	0	0	1	for phone M1
	0	0	0	2	for phone M2
	0	0	0	3	for phone M3
	0	0	0	4	for phone M4

Examples of commands	
change the phone number of the M1 owner	00011100+79115623881
record/change the M2 phone number	00020000+79011231111

Deletion of phone numbers M2, M3, M4	
Delete M2 phone	00021100
Delete M3 phone	00031100
Delete M4 phone	00041100

To delete phone numbers, the same commands are used as for recording, but the “phone number” parameter is not specified.

SMS command 07 is used to request the list of telephone numbers stored in the module memory.

To activate the device triggering, send the 81 command from the M1 telephone or the 81001234 command from the M2, M3 or M4 telephone, where 81 is the command code, 00 is the separator and the last 4 digits are the password 1, which you set during initial configuration.

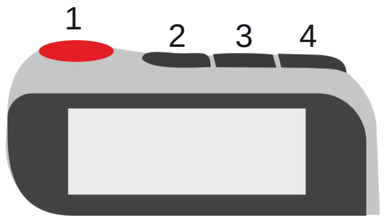
REMOTE TRIGGERING

1 PUSH BUTTON

- Remote triggering is performed manually by a wired button 1 (DB-9 connector), remote from the central unit via twisted pair cable at a distance of up to 200m.
- To destroy data from disks, press and hold the wired button for 1-2 seconds.

2 ON RADIO CHANNEL

- The radio communication range is up to 1000 m in line-of-sight conditions. The range of the radio keyfob may decrease depending on the installation location and orientation of the radio control board and antenna, radio frequency interference, weather conditions and radio keyfob battery voltage. The system is equipped with the function of visual and audible confirmation of command execution. The maximum number of keyfobs is 6.
- The command to destroy data corresponds to successive pressing of buttons 3 and 1 on the keyfob. Pressing button 3 must be long (8-10 seconds), pressing button 1 - short (2-3 seconds).
- To activate from the keyfob, press button 2 until a beep, and then press button 1 briefly.



CONTACTS

Click on the app icon and you will have a support chat open up





