Security Management System
Configuring TCP-IP MODBUS Inputs (23.01.18.01)

Introduction

The ‘Security Management System’ software supports capturing alarms from ‘external 3rd party systems’ through TCP/IP MODBUS interface.
This document describes the configuration for the same.

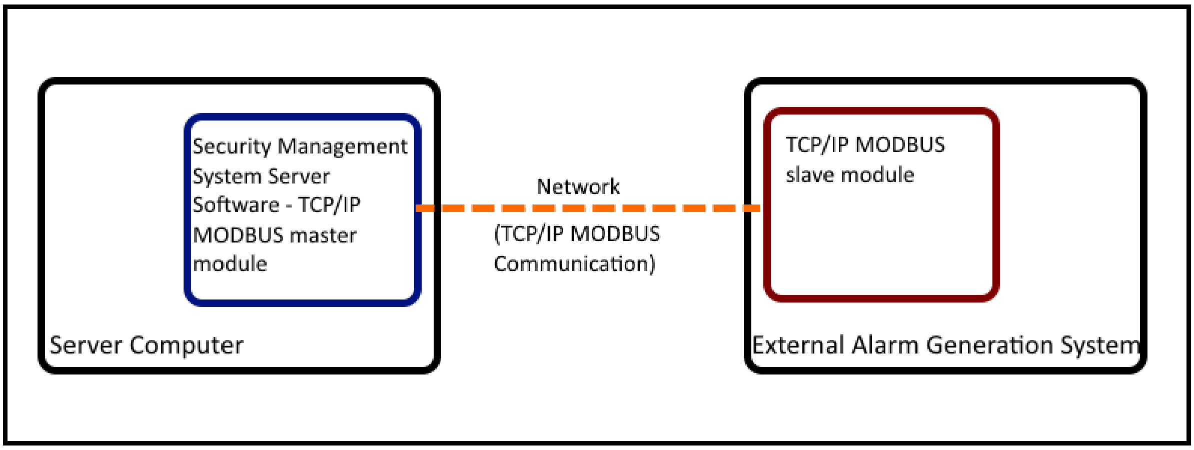
Note – The target ‘external 3rd party system’ should support TCP/IP MODBUS interface. Please confirm the same from the target external 3rd party system manufacturer.

The ‘external 3rd party system’ works as ‘TCP/IP MODBUS slave’ and the ‘Security Management System server software’ works as ‘TCP/IP MODBUS master.
The ‘alarm indication’ from the ‘external 3rd party system’ is captured as an alarm in the ‘Security Management System server software’ through TCP/IP MODBUS protocol.

Compatibility Check - 'External 3rd party system'

Note – it is important to perform the 'compatibility check ' for the 'External 3rd party system'; and to get confirmation from the 'External 3rd party system' manufacturer for the same

[A] Integration type 1 – Direct communication


Security Management System Server Software - TCP/IP MODBUS master module
Server Computer
Network
(TCP/IP MODBUS Communication)
TCP/IP MODBUS slave module
External Alarm Generation System

(a) The 'External Alarm Generator System' supports 'TCP/IP MODBUS' communication
(b) The 'Security Management System Server Software – TCP/IP MODBUS master module' directly communicates with the 'External Alarm Generator System', through MODBUS protocol

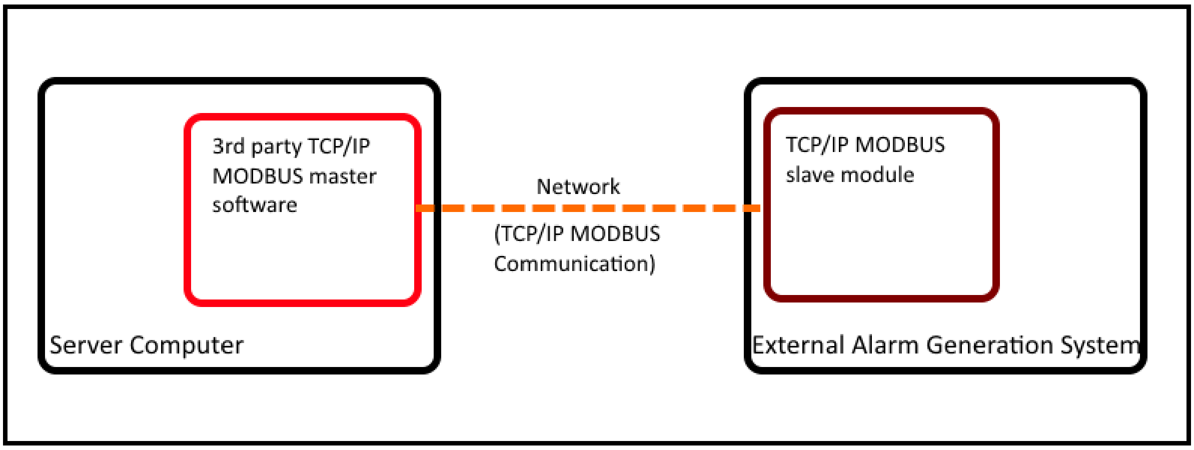
1. Compliance checklist

Please confirm following points from the 'External Alarm Generator System' manufacturer

(a) The 'External Alarm Generator System' supports 'TCP/IP MODBUS' communication
(b) The 'External Alarm Generator System' functions as 'TCP/IP MODBUS slave'

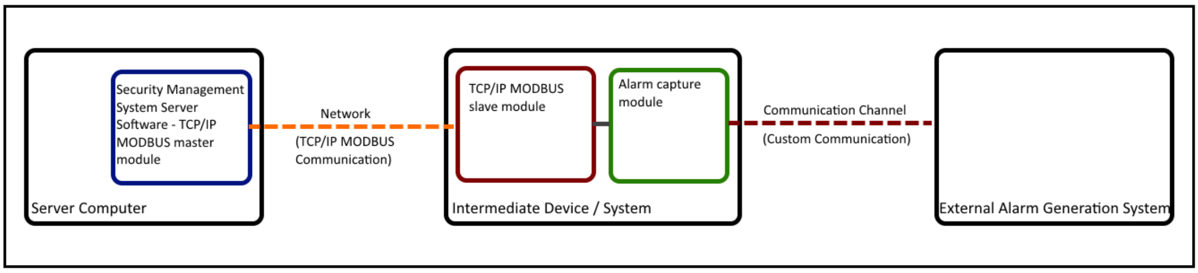
2. Confirmation tests

Please confirm from the 'External Alarm Generator System' manufacturer that following tests can be performed and the target results can be achieved


3rd party TCP/IP MODBUS master software
Server Computer
Network
(TCP/IP MODBUS Communication)
TCP/IP MODBUS slave module
External Alarm Generation System

(a) Configure the 'External Alarm Generator System', to expose alarm states for all target alarms through TCP/IP MODBUS slave module
(b) Install '3rd party TCP/IP MODBUS master software' on the Server Computer
(c) Configure the '3rd party TCP/IP MODBUS master software' to capture alarm(s) generated from the 'External Alarm Generator System'.
(d) For each of the target alarms expected to be generated by the 'External Alarm Generator System', 'Alarm OFF state' should be displayed in the '3rd party TCP/IP MODBUS master software'.
(e) Generate each of the target actual alarms in the 'External Alarm Generator System'. 'Alarm ON state' should be displayed in the '3rd party TCP/IP MODBUS master software'.

[B] Integration type 2 – Communication through intermediate device / sub-system


Security Management System Server Software - TCP/IP MODBUS master module
Server Computer
Network
(TCP/IP MODBUS Communication)
TCP/IP MODBUS slave module
Alarm capture module
Intermediate Device / System
Communication Channel
(Custom Communication)
External Alarm Generation System

(a) The 'External Alarm Generator System' does NOT support 'TCP/IP MODBUS' communication
(b) Hence 'Intermediate Device / System' is added to the solution.
(c) The 'Intermediate Device / System' functions as a 'converter', to 'convert' the input 'alarm state' from the 'External Alarm Generator System' to TCP/IP MODBUS output.
(d) The 'Intermediate Device / System' communicates with the 'External Alarm Generator System', through custom communication over custom communication channel
(e) The 'Intermediate Device / System' also functions as 'TCP/IP MODBUS' slave
(f) The 'Security Management System Server Software – TCP/IP MODBUS master module' communicates with the 'Intermediate Device / System' TCP/IP MODBUS slave module, through MODBUS protocol

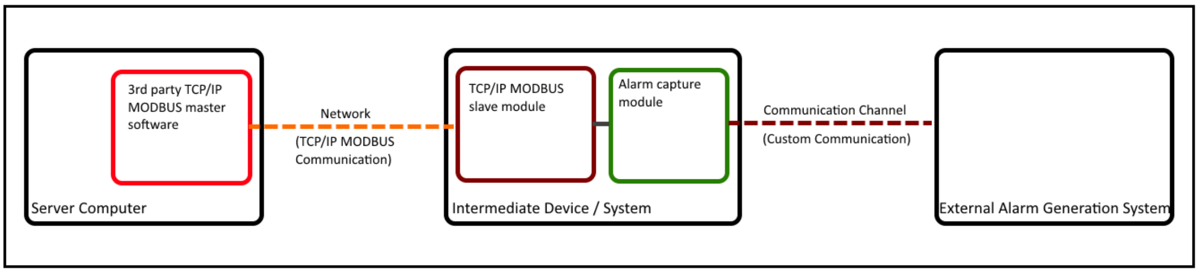
1. Compliance checklist

Please confirm following points from the 'Intermediate Device / System' manufacturer

(a) The 'Intermediate Device / System' can capture alarms generated from the 'External Alarm Generator System', through custom communication over custom communication channel
(b) The 'Intermediate Device / System' can also function as 'TCP/IP MODBUS slave'
(c) The 'Intermediate Device / System' can reflect/expose the 'Alarm state' for each of the alarms captured from the 'External Alarm Generator System', as 'Alarm state' output from its 'TCP/IP MODBUS slave'.

2. Confirmation tests

Please confirm from the 'Intermediate Device / System' manufacturer that following tests can be performed and the target results can be achieved


3rd party TCP/IP MODBUS master software
Server Computer
Network
(TCP/IP MODBUS Communication)
TCP/IP MODBUS slave module
Alarm capture module
Intermediate Device / System
Communication Channel
(Custom Communication)
External Alarm Generation System

(a) Configure the 'Intermediate Device / System', to capture all target alarms from the 'External Alarm Generator System'
(b) Configure the 'Intermediate Device / System', to expose alarm states for all target alarms through TCP/IP MODBUS slave module
(c) Install '3rd party TCP/IP MODBUS master software' on the Server Computer
(d) Configure the '3rd party TCP/IP MODBUS master software' to capture alarm(s) exposed from the 'Intermediate Device / System'.
(e) For each of the target alarms expected to be generated by the 'External Alarm Generator System', 'Alarm OFF state' should be displayed in the '3rd party TCP/IP MODBUS master software'.
(f) Generate each of the target actual alarms in the 'External Alarm Generator System'. 'Alarm ON state' should be displayed in the '3rd party TCP/IP MODBUS master software'.

Configuration

The configuration involves following steps –

1. Step 1 – Information gathering and confirmation tests

   (a) Creating list of 'alarms' from the 'external 3rd party system' to be captured in the 'Security Management System' software

   (b) Listing 'TCP-IP MODBUS communication' information for each of these alarms. This information is part of technical details of the target system and would be available from the target 'external 3rd party system' manufacturer.
   The 'TCP-IP MODBUS communication' information includes –
   i. 'device IP address'
   ii. 'device port number'
   iii. 'device unit ID'
   iv. 'target alarm input type'
   v. 'target alarm input address'
   vi. 'target alarm - Input value - Normal state'
   vii. 'target alarm - Input value - Alarm state'

   (c) Testing 'TCP-IP MODBUS communication' from 3rd party MODBUS master software

2. Step 2 – Alarm capture in the 'Security Management System server software'

   (a) Configuring the 'Security Management System server software' to connect to the target 'external 3rd party system' and to capture one or more alarms

3. Step 3 – Alarm rules in the 'Security Management System server software'

   (a) Configuring the 'Security Management System server software' to define 'alarm rule' to perform target actions (eg move one or more PTZ cameras to pre-configured presets) when an alarm is received from the 'external 3rd party system'.

Note – the steps listed above are related to single 'external 3rd party system'. Same steps need to be followed for each 'external 3rd party system', if more than one 'external 3rd party system' exist.

Configuration Step 1 – Information gathering and confirmation tests

This step involves information gathering and confirmation tests, which are outside the 'Security Management System' software.
The sub-steps in this step ensure that technical details related to the target 'external 3rd party system' are available and target 'external 3rd party system' TCP-IP MODBUS interface is tested and confirmed.

(a) Creating list of 'alarms' from the 'external 3rd party system' to be captured in the 'Security Management System' software

This sub-step involves listing all 'alarm conditions' in the target 'external 3rd party system'

In this document, 2 'alarm conditions' are used as example –

i. Fire alarm 1
ii. Gauge 1 high pressure

Note – these 2 'alarm conditions' are for example only. There can be any 'alarm conditions' depending on the deployment solution design.

(b) Listing 'TCP-IP MODBUS communication' information for each of these alarms. This information is part of technical details of the target system and would be available from the target 'external 3rd party system' manufacturer.
The 'TCP-IP MODBUS communication' information includes –

i. 'device IP address' - IP address of the target 'external 3rd party system'
ii. 'device port number' – TCP port number of the target 'external 3rd party system'
iii. 'device unit ID' – MODBUS unit ID of the target 'external 3rd party system'
iv. 'target alarm input type' – MODBUS input type
v. 'target alarm input address' – MODBUS input address
vi. 'target alarm - Input value - Normal state' – MODBUS input value in normal state
vii. 'target alarm - Input value - Alarm state' – MODBUS input value in alarm state

The 'target alarm input type' value would be one of the following options -

i. 'Coil (0x01)'
ii. 'Discrete Input (0x02)'
iii. 'Holding Register (0x03)'
iv. 'Input Register (0x04)'

Please create a table listing the 'TCP-IP MODBUS communication' information.

Following is the table created for example in this document –

Sr. No.	Alarm description / Name	TCP-IP MODBUS device communication information						
		Device IP address	Device port number	Device unit ID	Target alarm - Input type	Target alarm - Input value - Normal state	Target alarm - Input value - Alarm state	Target alarm - Input address
1	Fire alarm 1	192.168.1.51	502	1	Discrete Input (0x02)	0	1	10023
2	Gauge 1 high pressure	192.168.1.51	502	1	’Input Register (0x04)	0-100	>100	10024

(c) Testing ‘TCP-IP MODBUS communication’ from 3rd party MODBUS master software

Example of ‘3rd party MODBUS master software’ is ‘MODBUS poll’ application, which can be downloaded from –
https://www.modbustools.com/modbus_poll.html

Notes –

i. This is a suggestion and NOT a mandatory software. Any other suitable software can be used, instead of this suggested software for the tests
ii. This is a 3rd party software. Please refer to the license agreement from the manufacturer, and confirm, before using this software.
iii. Free version of this software is available with limitations, but should be ok for the target tests

The test involves –

i. Connecting to the target ‘external 3rd party system’ from the ‘3rd party MODBUS master software’
ii. Configuring the ‘3rd party MODBUS master software’ to display the current values for the target inputs
iii. Confirming the current values for the target inputs are as listed in the table, for ‘normal state’ (‘no-alarm state’)
iv. Generating alarm(s) in the target ‘external 3rd party system’ and confirming the current values for the target inputs are as listed in the table, for ‘alarm state’

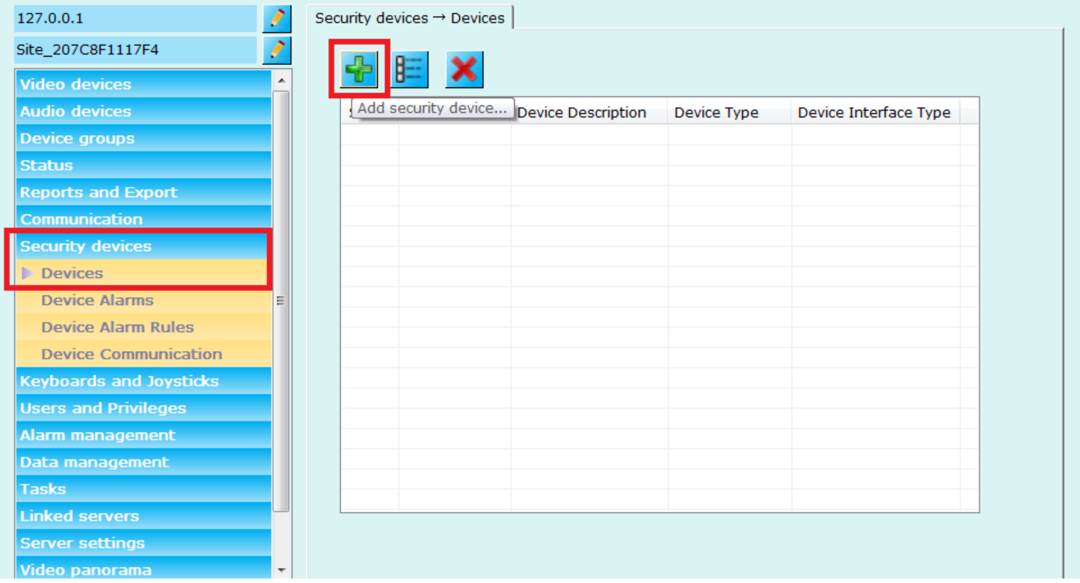
Note – it is important to test the external 3rd party TCP-IP MODBUS device from 3rd party MODBUS master software, before configuring the ‘Security Management System’ software for alarm capture.

Successful tests from 3rd party MODBUS master software ensure that communication details of the ‘external 3rd party TCP-IP MODBUS device’ are correct and the ‘external 3rd party TCP-IP MODBUS device’ is configured properly and is in healthy state

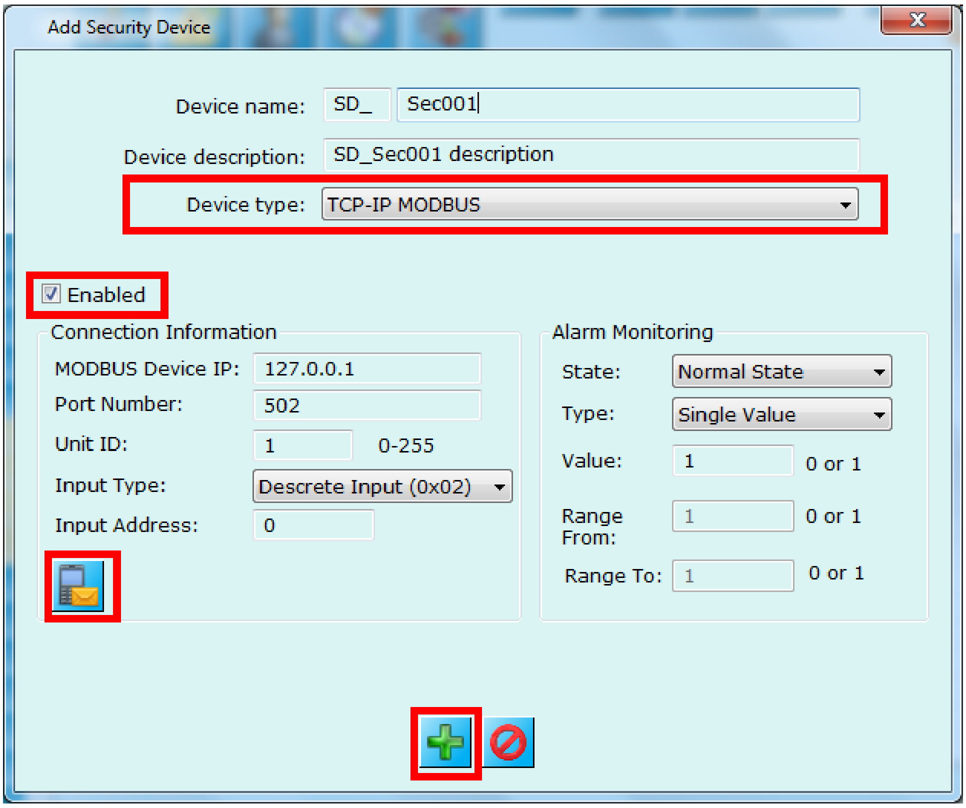
Configuration Step 2 – Alarm capture in the 'Security Management System server software'

Note – this section describes the sub-steps to configure a single 'TCP-IP MODBUS' input alarm in the 'Security Management System server software'.
Please follow same set of sub-steps, for each of the target 'TCP-IP MODBUS' input alarms.

1. In the 'Security Management System server software', please navigate to the 'Security Devices' link in the left navigation menu bar. Please navigate to the 'Devices' sub-link under it.



2. Click on the 'Add Security Device…' button which will pop up the 'Add Security Device' dialog box.



Device name: SD_ Sec001

Device description: SD_Sec001 description

Device type: TCP-IP MODBUS

☑ Enabled

Connection Information

MODBUS Device IP: 127.0.0.1

Port Number: 502

Unit ID: 1 0-255

Input Type: Descrete Input (0x02)

Input Address: 0

Alarm Monitoring

State: Normal State

Type: Single Value

Value: 1 0 or 1

Range From: 1 0 or 1

Range To: 1 0 or 1

(a) Type the 'Device name' - it can be any valid string useful for identifying the target alarm from the target 'external 3rd party system'

(b) Type the 'Device description' – it can be any valid string which provides short description for the target alarm from the target 'external 3rd party system'

(c) Select 'Device type' as 'TCP-IP MODBUS'.

(d) Please select the 'Enabled' chech-box

(e) Please specify in the MODBUS 'connection information' -'MODBUS Device IP', 'Port Number', 'Unit ID', 'Input Type', and 'Input Address'.
Note – this information should match exactly with data from the target row of the 'TCP-IP MODBUS communication' information table created as described in section 'Configuration Step 1 – Information gathering and confirmation tests' of this document

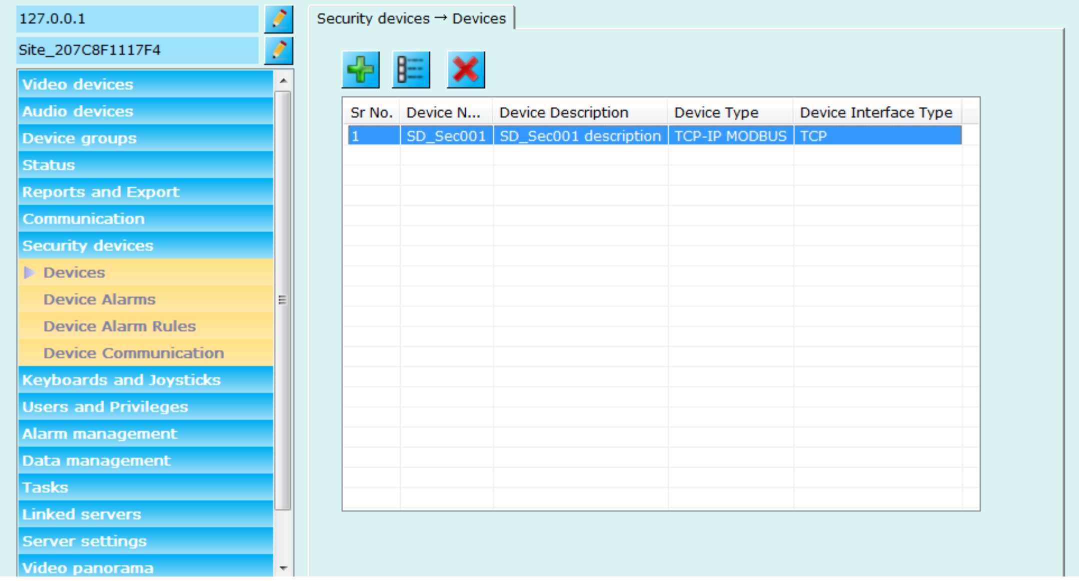
Please use the 'Test connection' button available below the 'Connection Information' section; to test the connection with the target device.
It should display 'success' message, which confirms that the 'Security Management System server software' is able to connect to the target device

(f) Please specify 'Alarm Monitoring' information.
i. Please select the 'State' – 'Normal State' or 'Alarm State'. This selection depends on the data from the target row of the 'TCP-IP MODBUS communication' information table created as described in section 'Configuration Step 1 – Information gathering and confirmation tests' of this document.
ii. If 'Target alarm - Input value - Normal state' details are available, please select 'Normal State' option.

If 'Target alarm - Input value - Alarm state' details are available, please select 'Alarm State' option.
Please select the 'Type' option – 'Single Value' or 'Value Range', depending on the data available for the target alarm.
iii. Depending upon the 'Type' option selection, either 'Value' OR 'Range From and Range To' GUI will be enabled. Type the values to complete specifying the 'Normal State' or 'Alarm State' for the target alarm

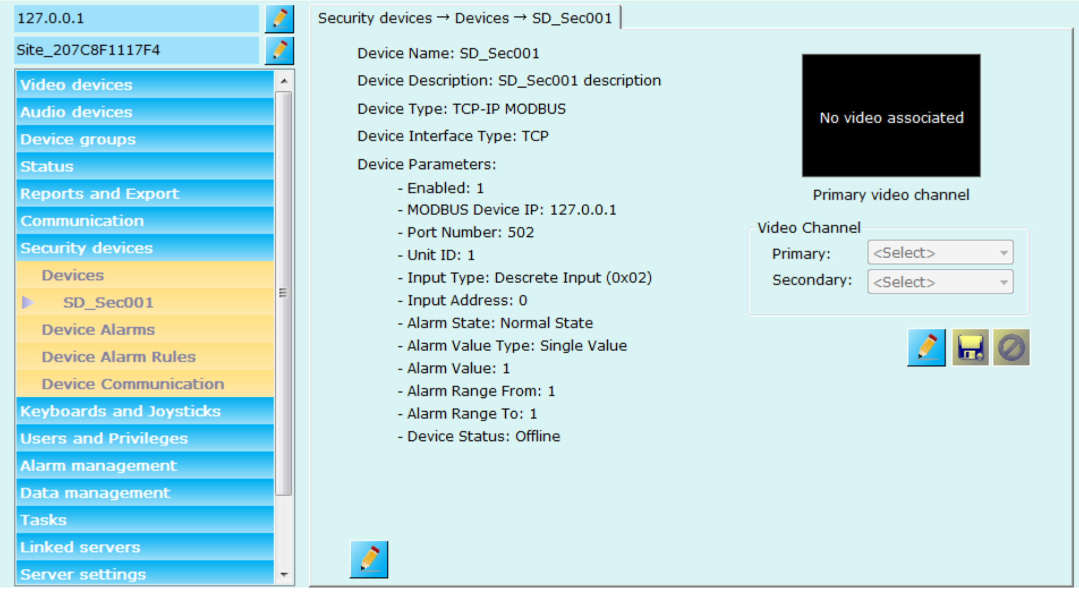
(g) Click on the 'Add' button to finish adding the alarm and to close the 'Add Security Device' dialog box

3. The newly added configuration will be displayed in the 'Security Devices' list



Sr No.	Device N...	Device Description	Device Type	Device Interface Type
1	SD_Sec001	SD_Sec001 description	TCP-IP MODBUS	TCP

4. Please select the entry from the list and click on 'View device details' button (or double-click on the target entry) to view details.



Device Name: SD_Sec001
Device Description: SD_Sec001 description
Device Type: TCP-IP MODBUS
Device Interface Type: TCP
Device Parameters:
- Enabled: 1
- MODBUS Device IP: 127.0.0.1
- Port Number: 502
- Unit ID: 1
- Input Type: Descrete Input (0x02)
- Input Address: 0
- Alarm State: Normal State
- Alarm Value Type: Single Value
- Alarm Value: 1
- Alarm Range From: 1
- Alarm Range To: 1
- Device Status: Offline

Video Channel
Primary: <Select>
Secondary: <Select>

Please configure 'Primary video channel' and 'Secondary video channel' using edit and save buttons below the GUI for the same.

After the configuration is completed, please generate the target alarm in the target 'external 3rd party system', and confirm that the alarm is captured in the 'Security Management System server software'.

Configuration Step 3 – Alarm rules in the 'Security Management System server software'

The section 'Configuration Step 2 – Alarm capture in the 'Security Management System server software' completes the configuration for capturing target alarm from the target 'external 3rd party system'

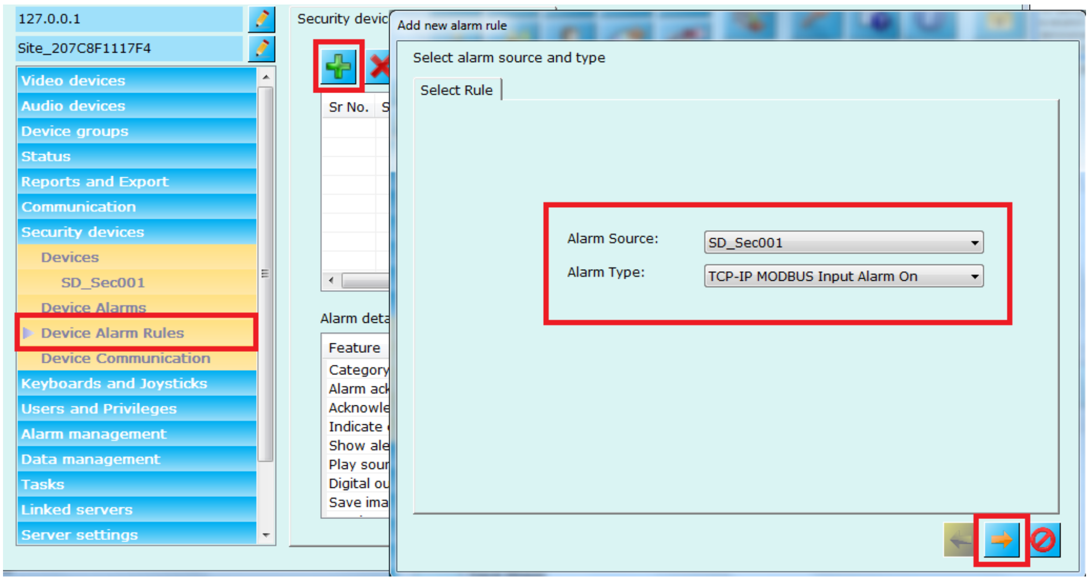
This section involves configuring the 'Security Management System server software' to define 'alarm rule' to perform target actions (eg move one or more PTZ cameras to pre-configured presets) when target alarm is received from the target 'external 3rd party system'.

The sub-steps in this section are not mandatory, but are expected to be used in most of the deployment situations.

Note – one 'Device Alarm Rule' needs to be defined for every target alarm from the target 'external 3rd party system'; for which specific actions are required to be configured in the 'Security Management System software'

1. In the 'Security Management System server software', please navigate to the 'Security Devices' link in the left navigation menu bar. Please navigate to the 'Device Alarm Rules' sub-link under it.

2. Click on the 'Add' button. This will pop up 'Add new alarm rule' dialog box.



Alarm Source: SD_Sec001
Alarm Type: TCP-IP MODBUS Input Alarm On

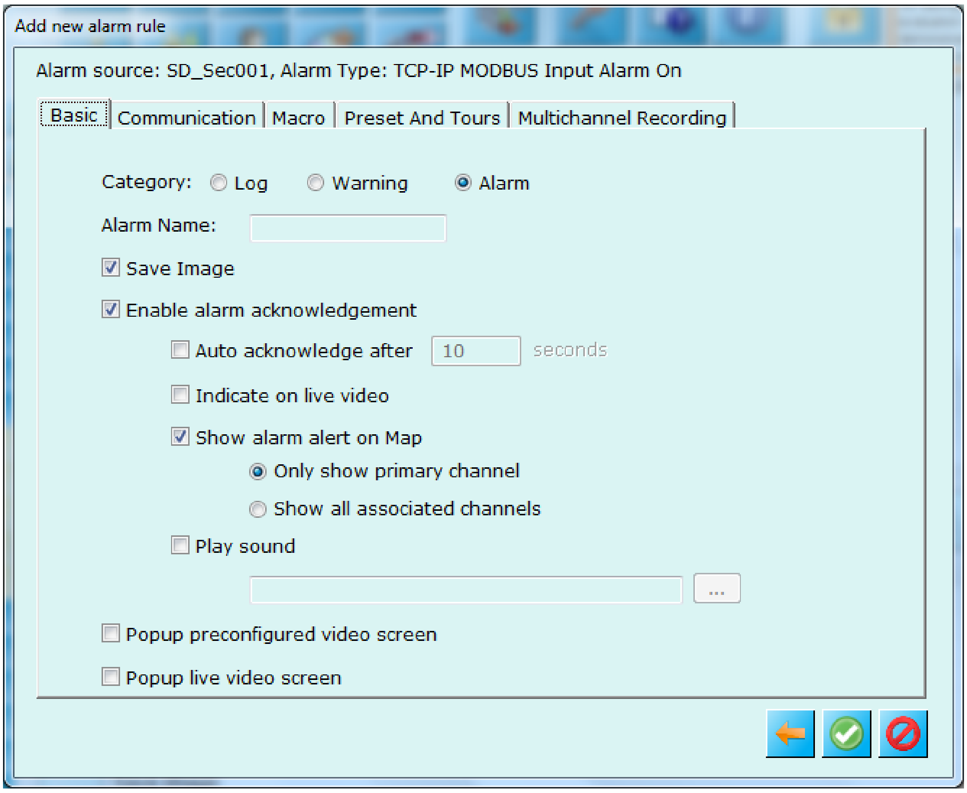
3. Please select the 'Alarm Source'. This is the 'Device name' specified in the 'Add Security Device' dialog box, as described in section 'Configuration Step 2 – Alarm capture in the 'Security Management System server software' in this document.
   Please select 'Alarm Type'. In all normal cases, this would be 'TCP-IP MODBUS Input Alarm On'.

   Note – following is the list of 'Alarm types' associated with 'TCP-IP MODBUS inputs' –

i. ‘TCP-IP MODBUS Input Alarm On’
ii. ‘TCP-IP MODBUS Input Alarm Off’
iii. ‘TCP-IP MODBUS Input Online’
iv. ‘TCP-IP MODBUS Input Offline’

In all normal cases, ‘device alarm rule’ is configured only for ‘TCP-IP MODBUS Input Alarm On’ alarm type. However depending on the project requirements and the solution design; ‘device alarm rules’ may be required to be configured for other alarm types too

4. Click on the ‘Next’ button. This will display the GUI to configure various actions, which will be processed, when the target alarm from target source is received by the ‘Security Management System software’



Add new alarm rule

Alarm source: SD_Sec001, Alarm Type: TCP-IP MODBUS Input Alarm On

Basic | Communication | Macro | Preset And Tours | Multichannel Recording

Category: ○ Log ○ Warning ● Alarm

Alarm Name:

☑ Save Image

☑ Enable alarm acknowledgement

□ Auto acknowledge after 10 seconds

□ Indicate on live video

☑ Show alarm alert on Map

● Only show primary channel

○ Show all associated channels

□ Play sound

□ Popup preconfigured video screen

□ Popup live video screen

Please configure the actions, as per the requirement.

E,g. to move one or more PTZ cameras to pre-configured preset positions, when target alarm from target source is received; please use the ‘Presets and Tours’ tab and specify the settings.

5. Click on the ‘Ok’ button to complete the ‘Device alarm rule’ configuration and to close the ‘Add new alarm rule’ dialog box.