Instruction manual
MTL Industrial Network Solutions

May 2021
INM CSL RugiCAM-IP MK2 Rev 2

CSL RugiCAM-IP MK2

Intrinsically Safe Network Camera

Powering Business Worldwide

Declaration of Conformity

A printed version of the Declaration of Conformity has been provided separately within the original shipment of goods. However, you can find a copy of the latest version at http://www.mtl-inst.com/certificates

CONTENTS

CSL RugiCAM-IP MK2
Intrinsically Safe Network camera

1 INTRODUCTION

1.1 Description

The CSL RugiCAM-IP MK2 is an Intrinsically Safe (IS) Network Camera ideally suited to Group I Mining applications. It connects directly to compatible IS Ethernet Systems via a wired LAN cable or Wi-Fi (both work concurrently). The small, rugged and cost effective design makes it the ideal choice for many applications:

Petrochem- Drill Rigs, Process Monitoring, Remote Safety Inspections, Hazardous Zone Security….Mining- Conveyor Transfer Points, Bunkers, Fan Sites, Face Roof Supports (Chocks/ Shields)….

The CSL RugiCAM-IP MK2 is an improved version of the popular MK1 model. It features Full HD 1080P resolution and supports video streaming via the H.264 or

H.265 compression standards and/or Motion JPEG with frame rate selectable to reduce network bandwidth. All configuration is by a standard web browser or ONVIF compliant tool (settings can be backed up and restored to file).

The camera body is manufactured from high quality polished 316 stainless steel to suit harsh Group I Mining applications. A 6mm thick toughened glass window provides optimal protection in the harsh environment.

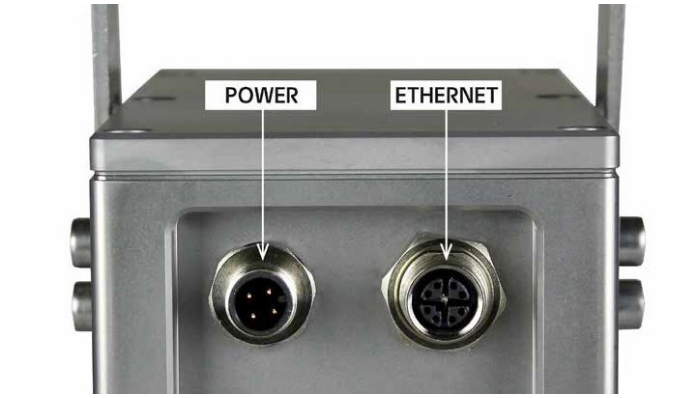
As well as adding H.265 compression and MJPEG support, this new MK2 version also features an enhanced low-light image sensor with wide dynamic range ideal for underground use. The Wi-Fi antenna is integrated into a 'Puck' design on the bottom of the enclosure to improve on the ruggedness of the MK1 external antenna connector arrangement

2 FEATURES

- Intrinsically Safe ATEX / IECEx / QLD Certification
- Ex ia I Ma (M1 mining). Ex ia IIB T4 Ga; Ex ia IIIC T135°C Da (non-mining)
  Ta =-40ºC to +60ºC
- Resolution 1920x1080, 1290x720 (main) + D1, VGA, CIF (sub-stream)
- 1/2.8" SONY Back-Illuminated CMOS Starlight Technology Sensor + HS3516D DSP
- Min. illumination 0.001 Lux + Wide Dynamic Range (WDR)
- Mega-Pixel 4mm f1.6 IR Lens, viewing angle (approx) 78°(H) x 59°(V) x 98°(D)
- H.264 + H.265 Server, MJPEG and Adjustable Frame Rate- Controls Network Bandwidth Usage (30fps max)
- 10/100 IS Ethernet LAN Interface supports up to 100m Cat5e Connection
- Wi-Fi supporting 802.11 b/g/n standards at up to 150Mbps – with integral antenna 'Puck' design
- LED indication (on rear) – Power / LAN
- ONVIF 2.4
- Backup and Restore of Configuration Settings
- 12VDC IS Power Supply Input or PoExTM (Power over IS Ethernet)
- Minimum operating voltage 10VDC
- 300mA operating Current maximum <400mA inrush current
- Rugged IP66 rated polished 316 Stainless Steel Enclosure suitable for harsh environments
- Compact dimensions W:87 x H:95 x D:165 (with WIFI),
  W:87 x H:79 x D:165 (without WIFI)
- Plug & Socket Connections- shortens installation time

NOTE
The unit is certified to operate safely at-40°C while the standard designed operating/storage range is-20°C to +60°C, the unit will function at-40°C. Some aspects of performance are not guaranteed by design at temperature below-20°C (e.g. Wi-Fi range), additionally possible issues with condensation or frosting of the glass window should be considered at low temperatures, both of these depend on the actual installation and environment and may not affect all applications.

3 CONNECTION



12Vdc Power / RS485 X1 4 Pole M12 Connector (M)	**Wire Colour**	**Description**
1	Brown	-
2	White	-
3	Blue	+12Vdc
4	Black	0V

12Vdc Power / RS485 X1 4 Pole M12 Connector (M)	**Wire Colour**	**Description**	**RJ45 Connector**
1	ORG-WHT	Tx+	1
2	ORG	Tx-	2
3	GRN-WHT	Rx+	3
4	GRN	Rx-	4
5	BRN-WH	PoEx-	5
6	BRN	PoEx-	6
7	BLU-WHT	PoEx+	7
8	BLU	PoEx+	8
Shield	Screen	GND	Shield

NOTE
The cable core colours as shown in the diagrams above are for reference if using an MTL supplied cable assembly. Alternatively some cables may have black cores numbered 1-4 corresponding to the M12 connector pin ..

3.1 LED Indications

3.2 Hardware reset

By removing the top cover, it is possible to access the hardwire reset button (shown below). This button needs holding in for about 40 seconds on a power up. Make sure to replace the top cover maintaining the seal.

1.1.1 Installation

The RugiCAM-IP MK2 is an Intrinsically Safe IP Network Camera capable of producing high quality colour video images at up to 1920x1080p at 30fps.

The H.265 compression technique ensure optimal bandwidth usage of the Ethernet network and compatibility with all major video streaming players.

The IP66 rated units are constructed from high quality anodised aluminium, powder coated steel or stainless steel to suit different applications and environments and contains a fully encapsulated camera (or LED) module. The resulting compact and cost effective solution is suited to many HD video monitoring and surveillance applications in and around the Hazardous Area.

The connections are made by multi-pin M12 plug and sockets on the rear of the unit. This allows easy installation and maintenance in the event of a damaged cable assembly.

	WARNING !
	This equipment must be installed, operated and maintained only be trained competent personnel and in accordance with all appropriate international, national and local standard codes of practice and site regulation for intrinsically safe apparatus and in accordance with the instructions contained here

1.1.1 ActiveX installation

In order to view the video using Internet Explorer or the IE Tab add-on (www.ietab.com) for other browsers, an ActiveX Control needs installing first.

Enter the IP address of the camera into the browser to get to the login page, on this page Click File to download the ActiveX:

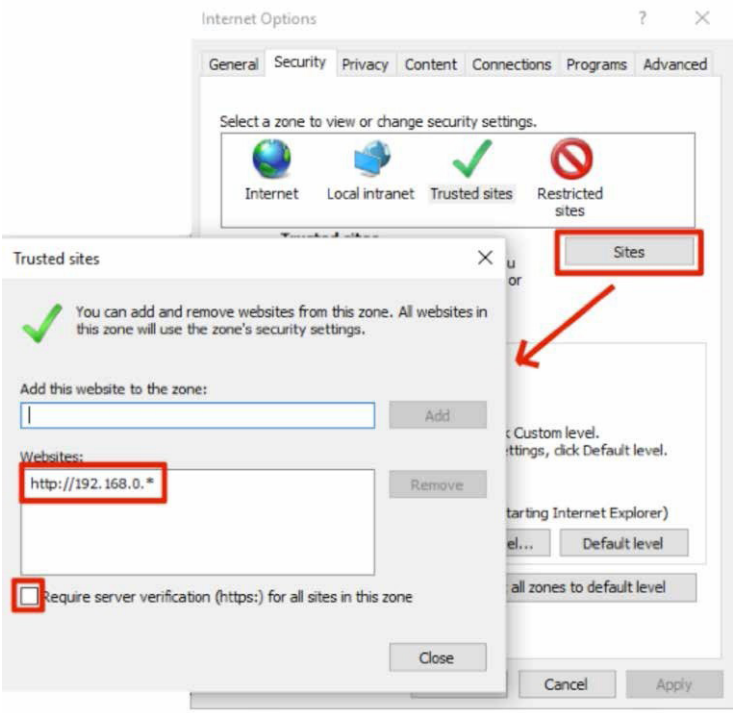
NOTE
The default LAN IP Address of the camera is 192.168.0.168

3.3 Possible Problems

If when installing the ActiveX a window pops up as shown below, then the security setting within the Browser need altering:

Open IE, Go to Internet Options Security Trusted sites.

Click Sites, uncheck Require server verification (https:) for all sites in this zone and add the IP address of camera to Websites.



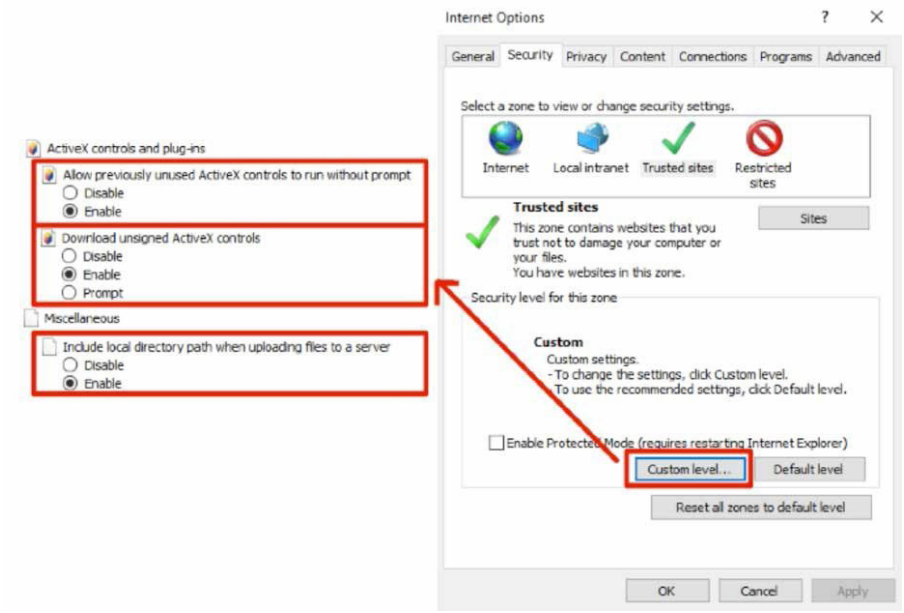
FOR EXAMPLE: HTTP://192.168.0.*

Click custom level;

Under activex controls and plug-ins

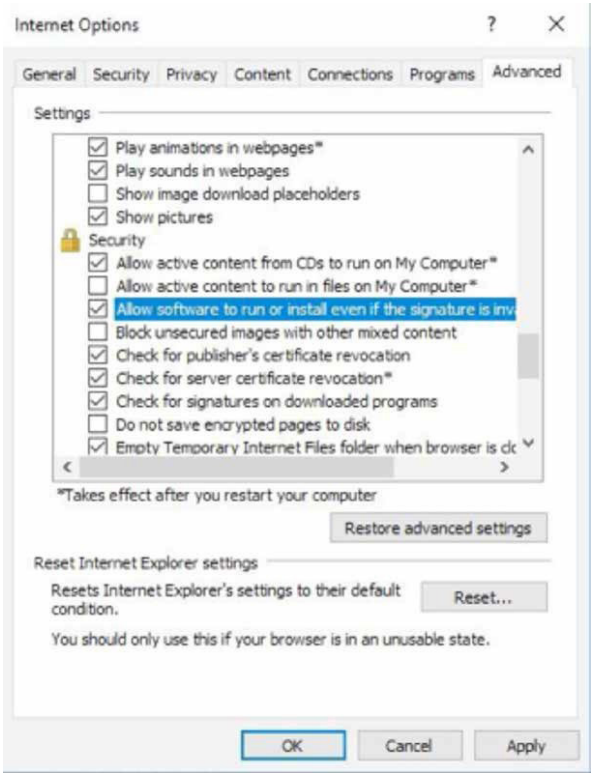
Enable allow previously unused activex controls to run without prompt Set download unsigned activex controls to prompt.

Under miscellaneous



Set Include local directory path when uploading files to a server Under Advanced tab, tick the setting

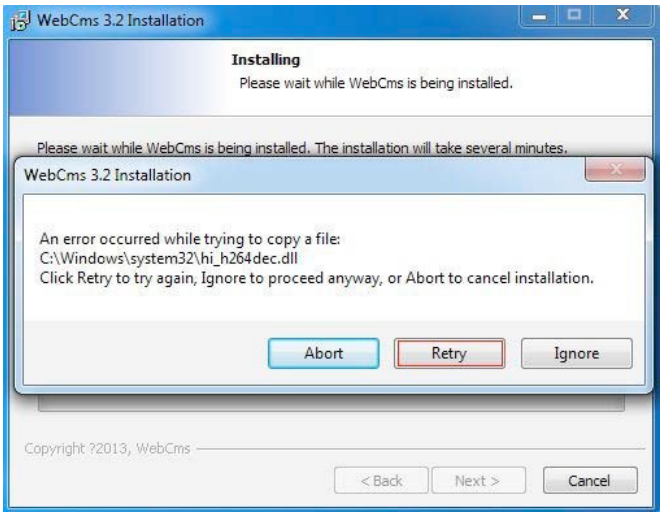
"Allow software to run or install even if the signature is invalid"



On IE interface (after login), reload the page

I

f when installing the ActiveX, the window below appears, Close the Browser and click Retry.



4 LOGIN

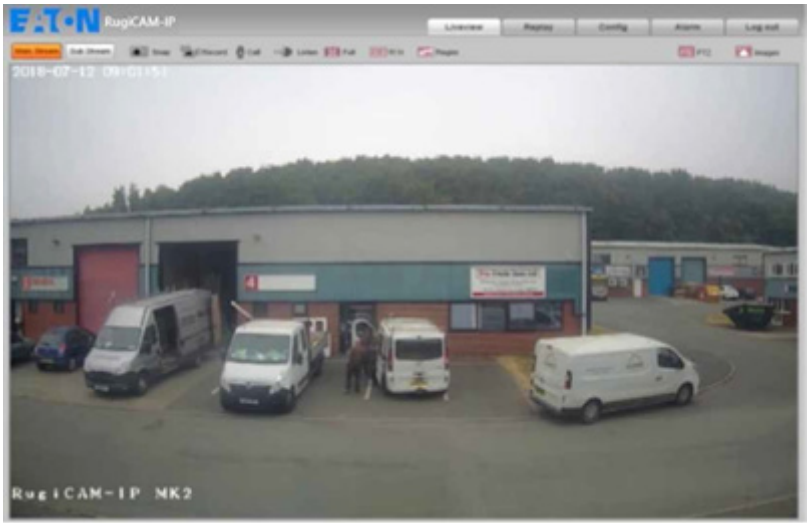
After the ActiveX installation completes, Input the IP address of the camera to get to the login page, then enter the username and password

4.1 Default setting

User Name: admin
Password: admin

Click login to continue to the main interface

5 LIVE PREVIEW



In the Live view interface, there are numerous operations like Snapping, Recording, Playback, Call, Listen, Clear Alarm, Log Search, Local Zoom of Image, Full-screen Viewing, PTZ and Lens Control.

Main Stream

Open up the main stream of camera to get the best quality.

Sub Stream

Open up the sub stream of camera, which is a lower resolution, suitable for problematic networks.

Snap

Takes a snapshot of the current image and saves it in .JPG format automatically to the storage directory of snapped images.

Record

This starts the Manual image recording; it automatically records the current video saving them in 264 format to the storage directory of recorded images. Click again to turn off.

Zoom

This feature allows the manual drag and drop of video display area partially zooming in.

Full

Display the video in full-screen, right click or click Esc to exit full screen mode.

W:H

Click "W:H" to get the real Width and Height ratio of image, avoiding the distortion when stretched to the screen size.

Replay

Click "Replay", the playback window will pop up for searching and playback of recorded videos or pictures. See Section 9

Alarm

When there is an alarm, the warning light will flash, Click Alarm to cancel the alarm message manually, and pop up the log-searching window see Section 10.8.8. The last 512 alarms are stored.

5.1 Snapshot Request

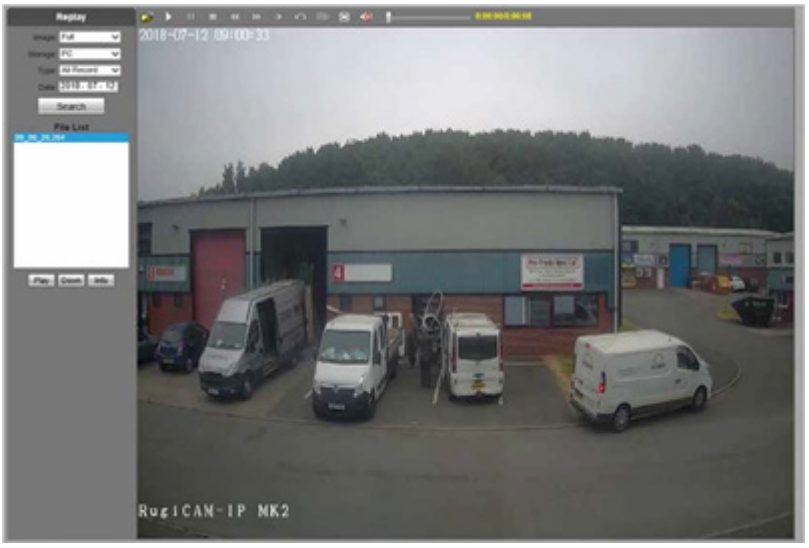
In order to request a snapshot the user can enter the following into the browser

http://<server ipaddr>/cgi-bin/images_cgi?channel=<value>&user=<value>&pwd=<value>

When the camera is set to default the syntax will be as follows:-

http://192 .168 .0 .168/cgi-bin/images_cgi?channel=0&user=admin&pwd=admin

6 REPLAY



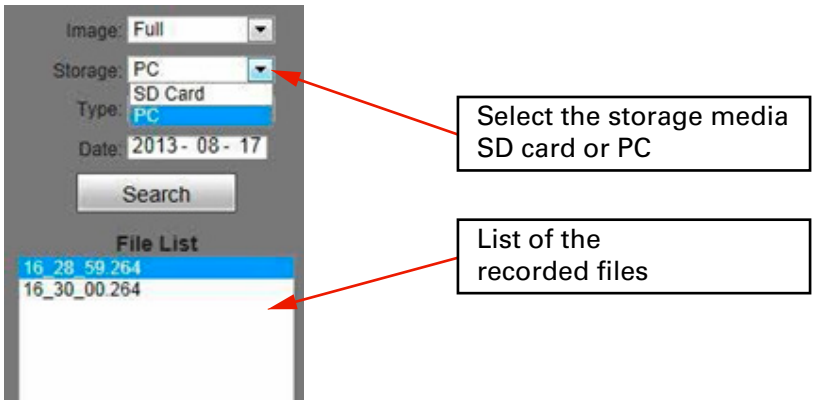
Users can search for recorded video or picture files on the local PC. The files are arranged according to date.

PC
Users can select a specific date to search for files stored on the local PC

Search
Click this button to perform a search for recorded files

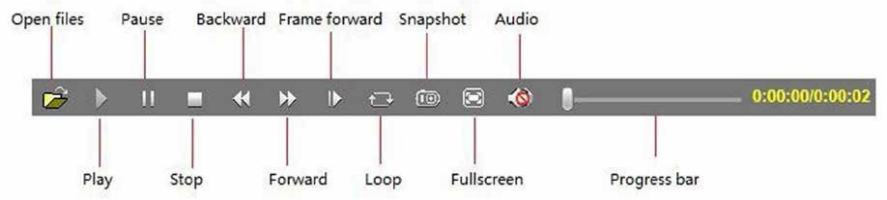
File List

Shows the recorded video or picture files using the selected parameter



Play

Choose the recorded video or picture in file list, right click the file or click the play button to play. The contents of the file are displayed in the window. If viewing a video it can be controlled using the toolbar.



Info

Users can view information about the file

7 SET SYSTEM PARAMETERS

7.1 Local Config

Preview Mode

Users can choose Real time priority or Fluency priority mode according to their needs.

Reset Mosaic

Select this option to make image quality better, but CPU usage rate will be higher at the same time.

Record file packing time

Set packing time of record files for local PC when it is recording.

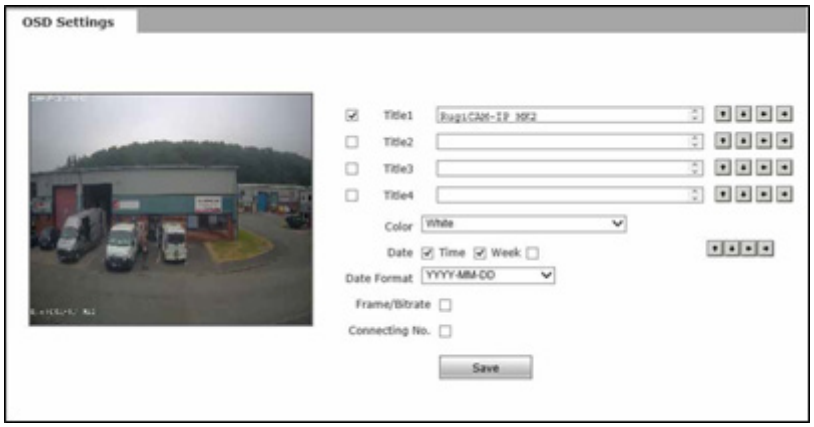
Record file path

Set the storage directory for local records and snapped files.
After you set these parameters, click Save to confirm the settings.

1.1.1 OSD Settings

Title

Enter a name for the video channel so that it can be easily recognisable.



Color

Choose the colour to use for the onscreen text.

OSD

Choose what information to display on the screen. The options are Title, Date, Time or Week.

Date Format

Select the format of the Date to be on the video.

Frame/Bitrate of channels .

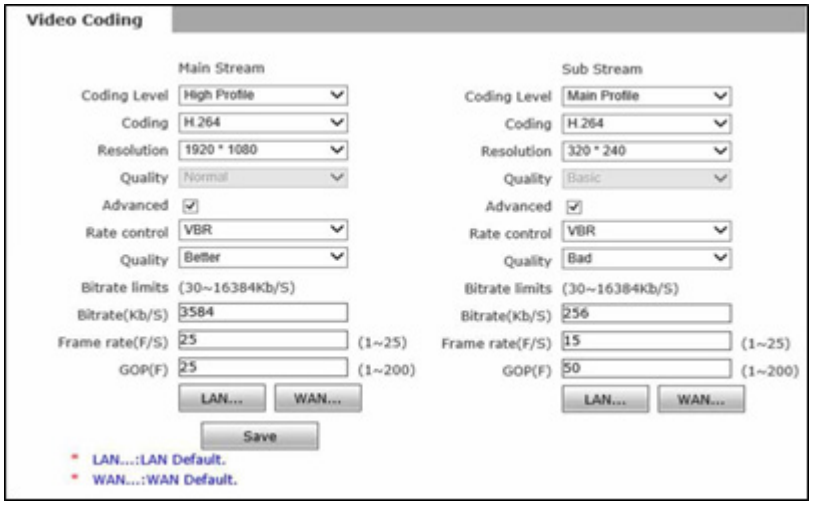
Choose what information to display on the screen. The options are Title, Date, Time or Week.

Position

Use the arrow buttons to adjust the position of video title, Date, Time or Week.

Click save to confirm settings.

1.1.1 Video Coding



Coding Level

Baseline and Main profile and High profile available, for H.264 compression format. Baseline suits low delay and when real time video is required. Then main profile suits the best image quality video. Main Profile is an average of the two.

Coding

H256+, H265, H.264 and MJPEG.

Resolution

Preferred Stream 1920*1080, 1280*720 Alternate Stream 704*576, 640*480, 320*240

Quality

You can choose the right quality according to your need: Fine, Normal, Basic, and the parameters can also be user-defined by choosing [advanced].

Rate control

CBR and VBR are optional
CBR adopts constant encoding bitrate,
VBR adopts variable encoding bitrate.

Quality

Under CBR setting: set the bitrate range via "Image Quality", you can choose self-adaption, it means the bitrate controlled by the software, and also can choose ±10% ±50%, ±10% means the bitrate range from-10% to +10% of the value of bitrate. Under VBR setting: set image quality via "Image Quality", 6 level available, from best to worst.

Bitrate

The range of preferred and alternate stream is 30~16384Kbps.Higher bitrate setting can generate better image quality, but it occupies more bandwidth, please adjust the setting according to your actual bandwidth. Under CBR setting, [Bitrate] is the constant bitrate of encoding. Under VBR setting, [Bitrate] is the variable bitrate of encoding.

Frame rate

Set encoding frame rate per second. Under poor network condition, frame rate can be reduced to control encoding bitrate to make motion images smoother.

GOP (Group Of Pictures)

Adjustable between 1 200 (Preferred Stream), 1 200 (Alternate Stream). Smaller I frame interval means higher bitrate and better image quality. It is recommended to set the I frame interval as above 25.

LAN default value

Main stream

H.264 Coding:
GOP: 25, frame rate: 25, rate control: VBR, image quality: better 720P:2080kps, 1080P:4096kps
MJEPG Coding
GOP: 25, frame rate:25, rate control: VBR, image quality: better 720P:9216kbps, 1080P:10240kbps

Sub Stream

H.264 Coding
GOP: 50, frame rate: 25, bitrate: VBR, 512kbps, image quality: Bad
MJPGE Coding
GOP50, frame rate: 25, bitrate: VBR, 4096kbps, image quality: Bad

WAN default value

H.264 Coding: GOP: 25, frame rate: 5, bitrate: CBR, 384kbps, image quality: Bad
MJPEG Coding: GOP: 25, frame rate: 5, bitrate: CBR, 4096kbps, image quality: Bad

Click save to confirm the setting (camera will restart)

1.1.1 Video Mask

Enable Mask
Enable or disable video masking.

Mask area set
Click and move the cursor to set an image masking area. The image can be masked partially or entirely. The camera supports a maximum of four masked areas.

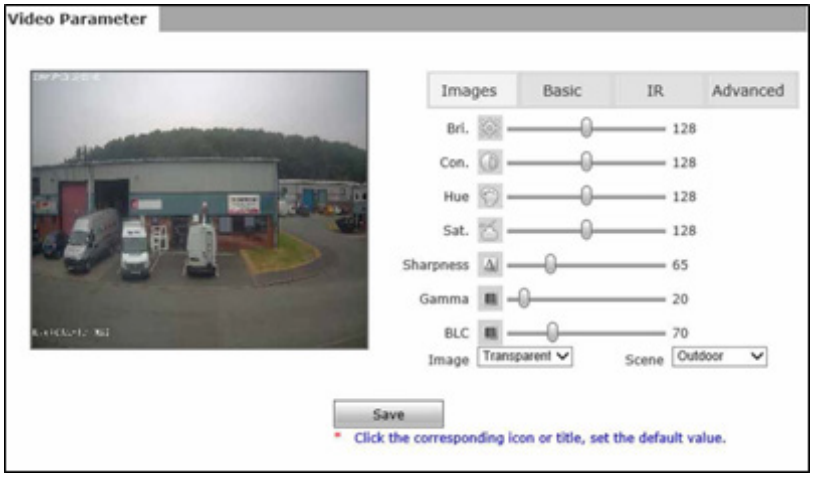
All
Mask the whole image. Clear all masked areas.

Clear
Clear all masked areas.

Click save to confirm the settings

1.1.1 Video Parameter

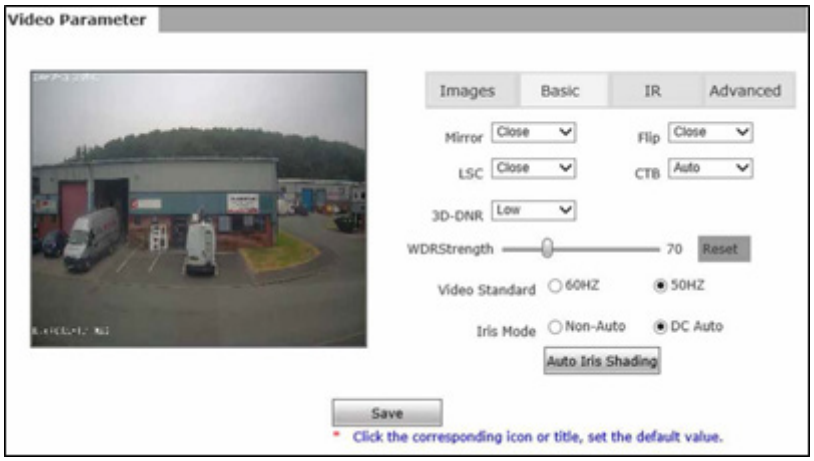
Images



Allows the adjustment of the Brightness, Contrast, Hue, Saturation, Acutance, Gamma of video and Image mode to Transparent or True Color.

Click Save to confirm the settings

Basic



Mirror
Horizontally rotate the video if required.

Flip
Vertically rotate the video

LSC
Lens Shading Correction corrects the phenomenon where the image is darkened or blurred on the periphery

CTB
Colour Temperature Blue automatically increases the colour temperature of the image.

WDR
Wide Dynamic Range enhances the image quality in such area: strong light source (sunlight, lamps or reflectors, etc.) , shadow of high-brightness, backlight.

3D-DNR

3D DNR processes the noise reduction between two frames. It can decrease the noise effect, especially when capturing moving images in low light conditions and delivering more accurate and sharp image.

Video Standard

If flashing lamps are resulting in the image to flicker, ensure that this setting matches the power frequency. 50HZ for PAL systems, 60HZ for NTSC systems.

Iris Mode

Leave at Non-Auto as the RugiCAM-IP only support Non Auto Iris Lens.

Click Save to confirm the settings

IR

IR Mode

This function only for the camera has infrared function, support three kinds of detection mode, suit for different infrared light board and situation.

Time Detection

For this mode, set the time to turn day mode and B/W mode, this mode with first priority.

Video Detection

For this mode, the sensor will detect the value of LUX, and decide turn to B/W mode or not. The larger the value is more sensitive about turn to B/W mode.

IR Detection

For this mode, the photo-resistor will detect the value of LUX, to suit different infrared Light board; we support 3 kinds of wording mode:

Low-level mode

When the device gets a low voltage from Infrared light board, the device will turn to B/W mode

High-level mode

When the device gets a high voltage from infrared light board, the device will turn to B/W mode;

Auto detection mode

When the device powers on, it takes sample of light, then adjusts its mode to day or B/W mode. It also gets the value of voltage from infrared light board; a combination of the two values turns to day mode or B/W Mode.

Black-color (only in the IR Detection mode)
The Video from Black-White to color when the detection becomes effective.

Color-black (only in the IR Detection mode)
The video from color to Black-White when the detection becomes effective.

ICR
Setting the control level of the IR-CUT according to the IR-CUT control level.

IR
This function suit for the camera with IRCUT and infrared light board. e.g. for ICR, when set low level, it means when the device send a low-level voltage to IRCUT module, the IRCUT will turn to B/W mode.

Click Save to confirm the settings

Advanced

Rotation
Support 90 degree and 270-degree rotation.

Gain value
Change the value of AGC can adjust the effect of image in low light-level.

Exposure
Set the value of Shutter to control exposure time.

WB
You can choose Manual WB or AWB mode to adjust white balance, AWB is default open.

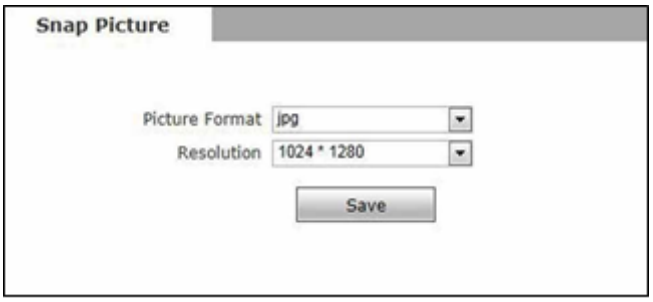
AntiFogging:
Set anti-fogging function, when the density of fog is high, the camera will change the brightness and contrast to improve the quality of image.

AntiFalseColor
Set anti false color function, can cancel the Moore profile effect in high frequency part.

AntiTrembling
Click Close to disable or Open to enable the anti trembling function.

Click Save to confirm the settings

1.1.1 Picture Parameter

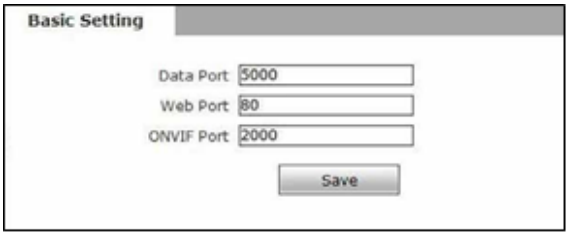


Currently supports only images of JPG format and the Resolution the same as the video stream.

Click Save to confirm the settings

7.2 NETWORK SETTINGS

1.1.1 Basic Setting

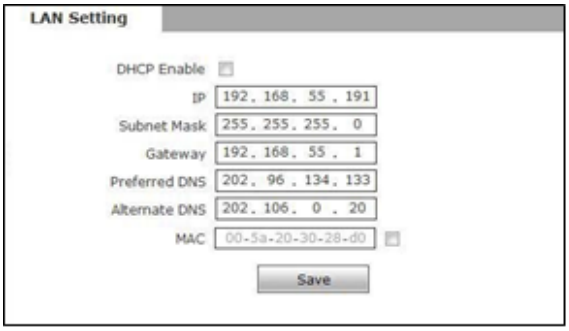


Data port
Default value is 5000 (changing is not recommended).

Web port
Default value is 80 (changing is not recommended).

ONVIF port
Default value is 2000 (changing is not recommended). Click save to confirm the settings (Camera will restart)

1.1.2 LAN Setting



DHCP Enable
If DHCP function of the router is enabled, IP camera will automatically fetch IP address from the router.

IP
Set the camera's IP address.

Subnet mask
Default value is 255.255.255.0.

Gateway
Set the gateway IP of IP camera, for example when the device is connected to public network via a router, the gateway IP is the router IP.

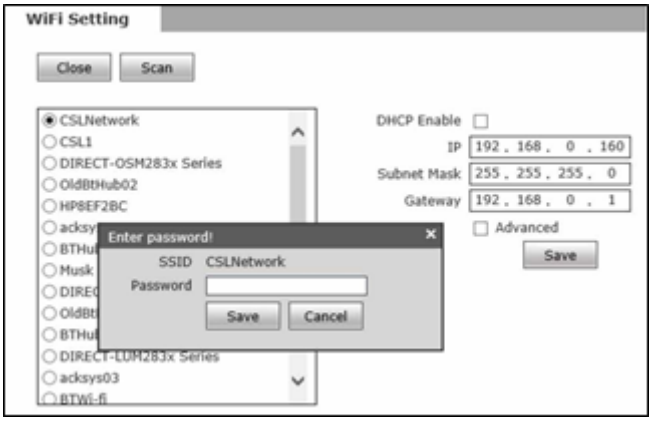
Preferred DNS
: Enter the IP address of the DNS server if this is provided by an ISP.

Alternate DNS
: If your ISP provided you with a secondary DNS address, please enter it here.

MAC
The Physical address of IP camera. (changing is not recommended)

Click save to confirm the settings (Camera will restart)

1.1.1 Wireless Setting



Scan

Scan for nearby WIFI access points.

Select SSID

Select the Wireless network SSID that you want to join and then enter the password of the WIFI access point. Click Save to confirm the settings.

Wireless Network Settings

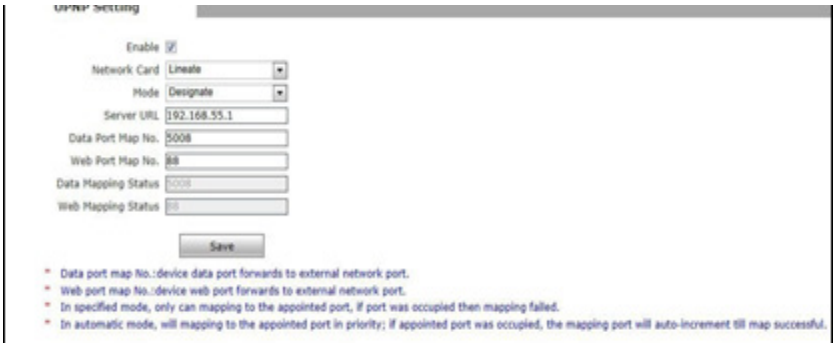
Enter the wireless IP address, Subnet mask and Gateway that you require for the connection. You can select DHCP Enable and let the camera get the IP address from the router.

Advanced

When you click the advanced box more wireless parameters can be setup these include Encryption type, Auxiliary Encryption type and Key Format, normally these will not need altering as they are received from the wireless access point.

Click Save to confirm the settings

1.1.1 UPNP setting



Auto-mapping of port, when IP camera is connected to a router with UPNP function enabled, the router will automatically map the port in UPNP settings to public network, manual port mapping by users is not necessary.

Network Card
Select the type of NIC connecting UPNP router. For WIFI models, when IP camera is connected to router via WIFI network, select "wireless" mode.

Mode
Designate mode and auto mode.
Designate mode means to specify data mapping port and web mapping port to router.
Auto mode means data mapping port and web mapping port are set up by router.

Server URL
IP address of the router with UPNP function.

Data port map No .
Data mapping port of user-specified device on the router
(works only under specified mode).

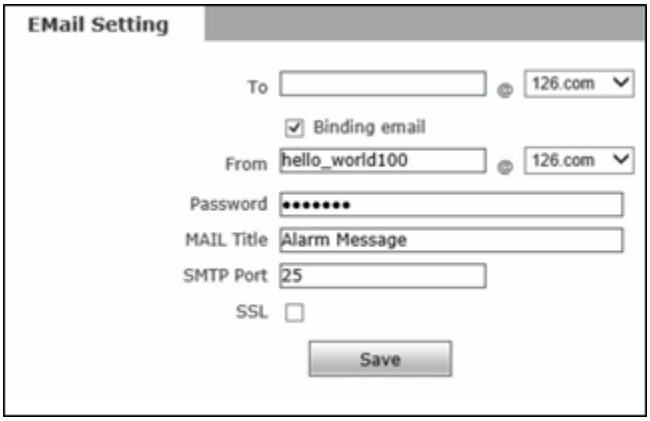
Web port map No .
Web mapping port of user-specified device on the router
(works only under specified mode).

Data mapping status
When UPNP function runs successfully, the status bar will echo the data port mapped to the router by the device.

Web mapping status
When UPNP function runs successfully, the status bar will echo the web port mapped to the router by the device.

Click save to confirm the settings

1.1.1 Email setting



To set the mailbox addresses and parameters of alarm mails and public network IP mails.

SMTP server
The address of servers that send the mails, the address format of mail servers varies from provider to provider, e.g. the SMTP server of 163 mailbox is smtp.163.com.

MAIL From
Mailbox that sends mails.

MAIL To
Mailbox that receives mails.

SMTP username
The login user name of the mailbox that sends mails.

SMTP password
The login password of the mailbox that sends mails.

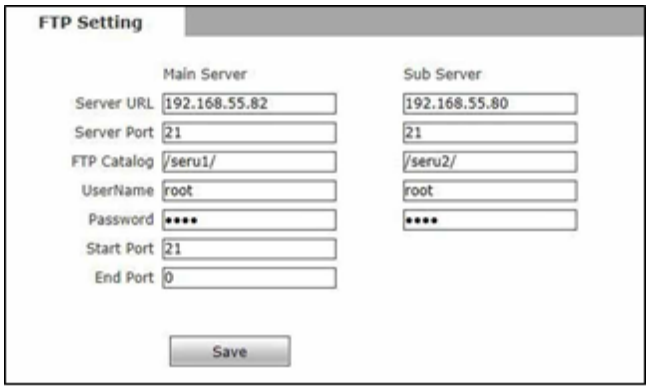
MAIL title
Title of mails.

SMTP Port
Port of SMTP port.

SSL
Enable Secured Socket Layer on the connection.

Click save to confirm the settings

1.1.1 FTP setting



FTP server sends the record files and snapped images generated after alarm is triggered in FTP mode to specified FTP server, supports 2 FTP servers, when the preferred one goes wrong, system will switch to the alternate one.

Server URL
The IP address or HTTP address of FTP server.

Server Port
Port of FTP server, the default port is 21.

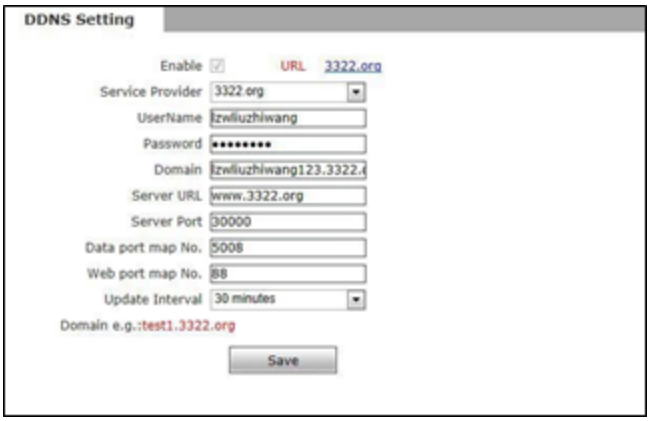
FTP Catalog
Path on remote FTP server, if the path does not exist or has not been filled in, the device will create a file folder under the root directory of FTP server.

User name

Password
User name and password of FTP server.

Click save to confirm the settings

1.1.1 DDNS setting



Bind the device with a fixed domain name by DNNS setting so that visiting to the device can be realized no matter how the public IP changes.

Enable
Enable or disable DDNS function.

Service Provider
The camera supports 3322.org or dyndns.org.

User Name
User name registered in DDNS server.

Password
Password registered in DDNS server.

Domain
The domain name set up e.g.: test1.3322.net.

Server URL
DDNS server address.

Server port
DDNS server's port. Default value is 30000.

Data port map No .
Fill in the external data port mapped by the IP camera on the router.

Web port map No .
Fill in the external web port mapped by the IP camera on the router.

Update Interval
Choose the update interval that the camera will update the WAN IP to the DDNS.

Click save to confirm the settings

1.1.1 VPN setting

Enable
Enable or disable VPN function.

Server URL
IP address or domain of VPN server.

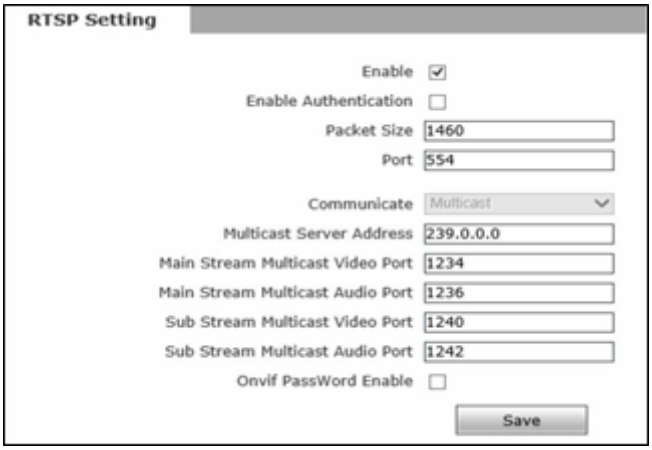
User Name
User registered in VPN server.

Password
User password registered in VPN server.

IP
Display IP after VPN dial-up success.

Status
Display the status of dial-up.

1.1.1 RTSP setting



Enable RTSP
Check RTSP switch to enable RTSP function, RTSP function enabled as default.

Enable Authentication
Enable Authentication, when enabled you need to us the username and password when using connecting to the camera by RTSP

i.e. rtsp://ip/av0_0&user=admin&password=admin

If the authentication mode is changed, the camera reboot.
Authentication by default is disabled

RTSP port
Default port is 554.

Communication
Multicast function is enabled as default.

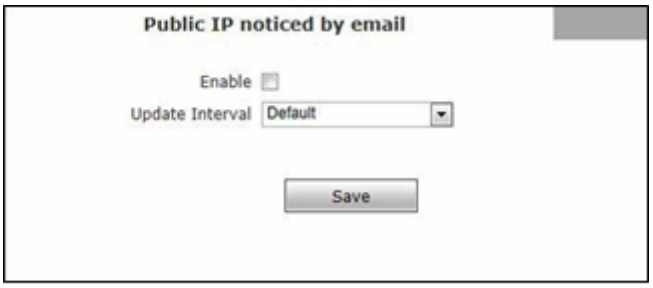
Multicast Server Address

When camera support multicast, camera will be the multicast server, and have the multicast address,239.0.0.0 as default address.

Multicast port
Video of main stream and sub stream using port 1234 and 1240, audio of main stream and sub stream using port 1236 and 1242.

Click save to confirm the settings

1.1.1 Public IP noticed by email



Enable Email
Check this switch to enable public IP mail notification function.

Update Interval
Select the interval of public IP mail notifications.
After enable this function, when the device detects public IP changed, it will send notification mail to the mail address set in the mail setting.

Click save to confirm the settings

1.1.2 Connect setting

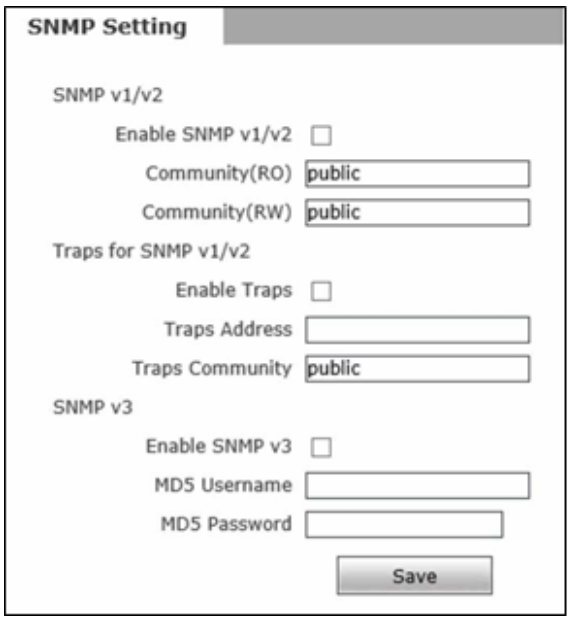
Auto connect
Enable or disable active connection of the device to surveillance center.

Central URL
The address of surveillance center (e.g. 192.168.55.99).

Central port No .
The port of surveillance center (e.g. 6000).

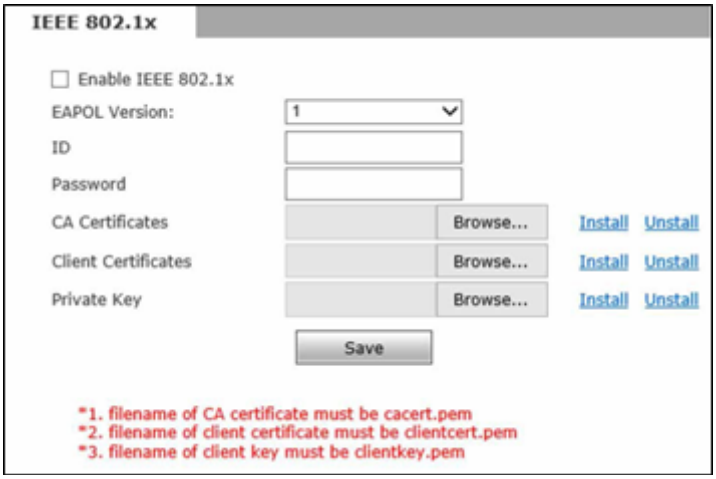
Click save to confirm the settings

1.1.1 SNMP


SNMP Setting
SNMP v1/v2
Enable SNMP v1/v2
Community(RO)
public
Community(RW)
public
Traps for SNMP v1/v2
Enable Traps
Traps Address
Traps Community
public
SNMP v3
Enable SNMP v3
MD5 Username
MD5 Password
Save

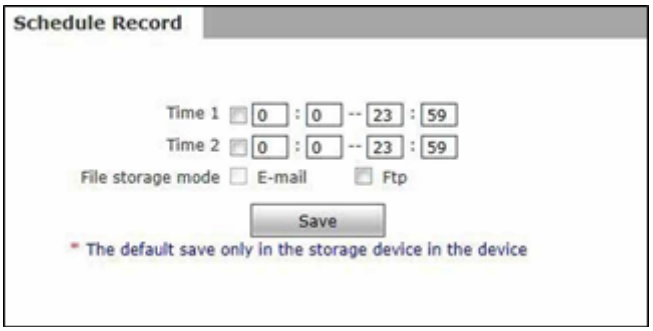
1.1.1 HTTPS

1.1.2 IEEE 802 .1x



7.3 Storage settings

1.1.1 Record Setting

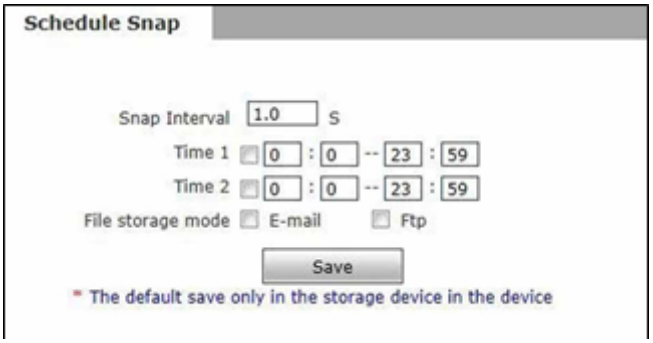


Schedule Record
Set the period of scheduled recording, two periods allowed.

File storage mode
Set the save scheduled recorded files to FTP server via FTP uploading. The FTP server can be set up in the FTP settings.

Click save to confirm the settings

1.1.1 Snap Setting



Snap Interval
Set the interval of IP camera picture snapping, minimum interval is 1 second.

Schedule Snap
Set the period of scheduled snapping, two periods allowed.

File save mode
IP camera snapped pictures can be saved via E-mail sending or FTP uploading.

TheE-Mail server can be set up in Mail Settings.

The FTP server can be set up in FTP Settings.

Click save to confirm the settings

7.4 Alarm Settings

1.1.1 Motion detection

On this page, users can set features like motion detection on/off, sensitivity, detection time, linkage alarm output, alarm output duration, E-mail sending when alarm been triggered, linkage snapping/recording, etc.

Motion Detection Area
Left click and drive the mouse to set the surveillance areas (4 areas at most).

All
Set the whole video as motion detection area.

Clear
Clear all motion detection areas.

Sensitivity
Sensitivity range is 1 5, greater value means higher sensitivity.

Enable
Enable or disable motion detection.

Time
Set the period of time for motion detection, two periods allowed.

Linkage Alarm output
Support Email, IO output, snapshot and record.

E-mail
Send motion detection alarm messages to users via E-mail, details about E-mail setting please refer to the Network Settings.

IO output
Enable or disable alarm output.

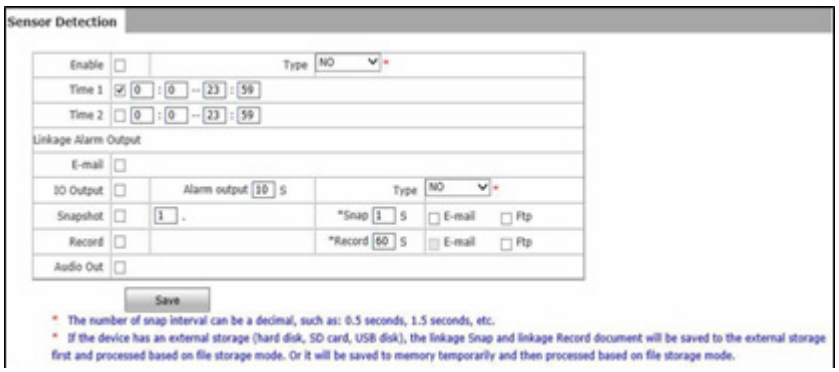
Alarm Output duration
Set the duration after being triggered (in seconds), the range of the duration is 0~86400s.0 means that there is no limit for alarm output.

Snapshot
When an alarm is triggered, the device will start to snap pictures. The pictures can be send via or FTP. For snapping parameters, if the number of pictures snapped at one time is set as 10 and the snapping interval is 1 second that means when there is an alarm, 10 pictures will be snapped and the interval between each picture is 1 second.

Record
When an alarm is triggered, the device will start to record files. The record files can be saved to FTP server.

Click save to confirm the settings

1.1.1 Sensor Detection



Set sensor alarm parameters here: Enable detect, sensor type, detect time, linkage alarm output, linkage output duration, E-mail sending when alarm has been triggered, linkage snapping/ recording, etc.

Enable
Enable or disable sensor alarm detection.

Sensor type
NO and NC mode.

Time
Set the period of time for sensor alarm detection, two periods allowed.

Linkage Alarm output
Support Email, FTP, IO output, snapshot and record.

E-mail
Send sensor alarm message to users via E-mail, details about E-mail setting please refer to [Network Settings].

IO output
Enable or disable linkage alarm output.

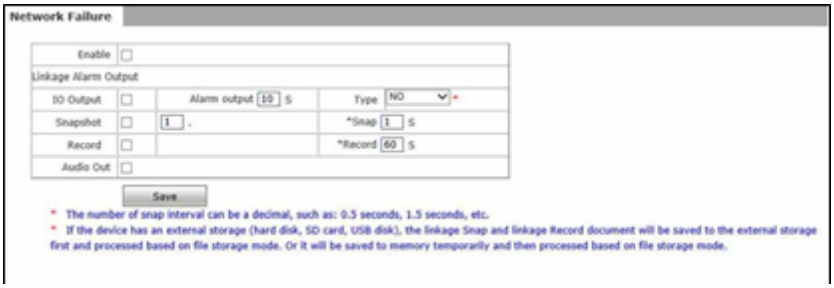
Alarm Output duration
Set the duration after being triggered (in seconds), the range of the duration is 0~86400s.0 means that there is no limit for alarm output.

Snapshot
When an alarm is triggered, the device will start to snap pictures. The pictures can be saved via E-mail sending or FTP uploading. For snapping parameters, if the number of pictures snapped at one time is set as 10, and the snapping interval is 1 second, that means when there is an alarm, 10 pictures will be snapped and the interval between each picture is 1 second.

Record
When an alarm is triggered, the device will start to record files. The record files can be saved to FTP server.

Click save to confirm the settings

1.1.1 Network Detection



Set network failure alarm parameters here: detection on/off, linkage alarm, alarm output duration, E-mail sending when alarm has been triggered, linkage snapping/recording, etc.

Enable
Enable the network failure alarm.

Linkage Alarm output
Support IO output, snapshot and record.

Alarm output
Enable or disable linkage alarm output.

Alarm Output duration
Set the duration of the linkage alarm output after being triggered (in seconds), the range of the duration is 0~86400s.0 means that there is no limit for alarm output.

Snap
When an alarm is triggered, the device will start to snap pictures. The pictures can be saved via E-mail sending or FTP uploading. For snapping parameters, if the number of pictures snapped at one time is set as 10, and the snapping interval is 1 second, that means when there is an alarm, 10 pictures will be snapped and the interval between each picture is 1 second.

Record
When an alarm is triggered, the device will start to record files. The record files can be saved to FTP.

Click save to confirm the setting

7.5 System settings

1.1.1 System Info

Display device name, VO standard, Language device ID, version.

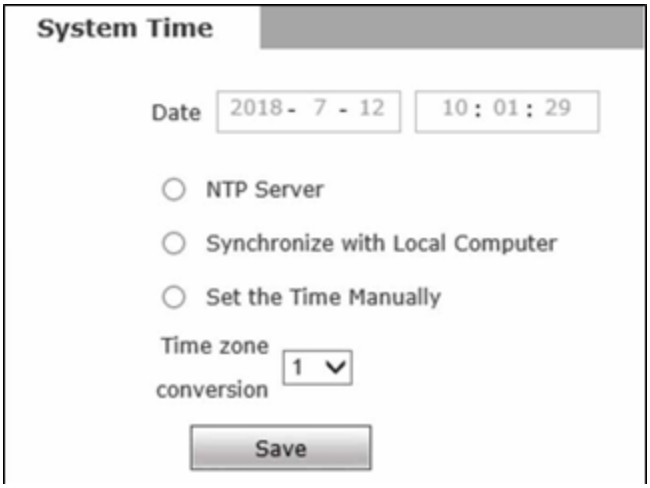
Device Name
You can define the device name.

VO standard

Language
Support Chinese and English, after changing the language. Please reopen the IE browser to login the camera again.

Click save to confirm the settings

1.1.1 System Time



Support three method to upgrade the device's time.

NTP Server

After starting the function, switch on NTP switch and select time zone, and click save, the camera will send the query to NTP server, after get the message from NTP server, the camera will upgrade the system time, the system time will be displayed in live view.

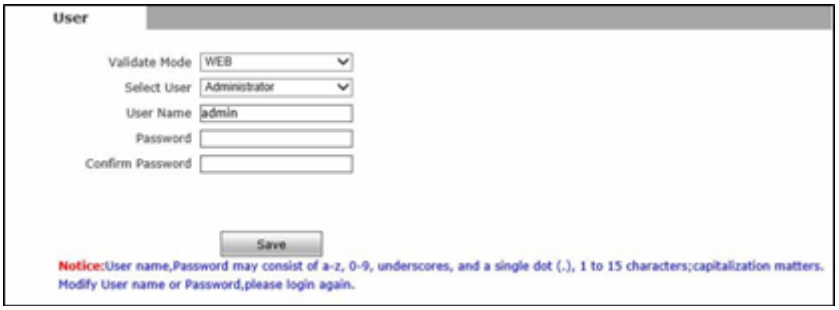
Synchronize with Local Computer

After starting the function, the date and time of IP camera will be synchronized with the local PC.

Set the Time Manually

If you select this option, you can modify the time manually.

1.1.1 User Manage



You can set three users for every camera, one is Administrator, and others are general users.

Administrator

Can operate and set all functions and parameters of IP camera.

General User

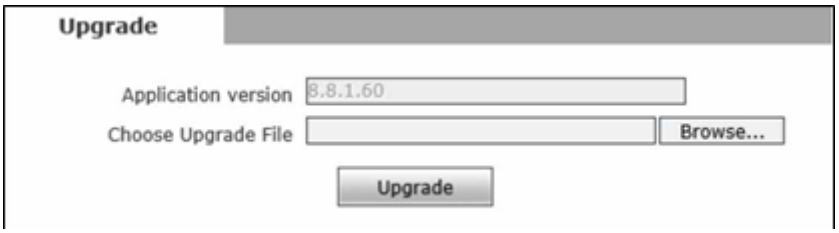
Can perform operations like snapping, recording, playback, talkback, monitoring, alarm clearing, log searching, zooming and full-screen reviewing.

Can perform operations like visit setting, image lightness and color adjustment, PTZ and lens control, etc.

NOTE
The user name and password are case sensitive Default user name of administrator: admin Default password of administrator: admin Default user name of general users:user 1 \ user 2 Default Password of general users: user 1 \ user 2

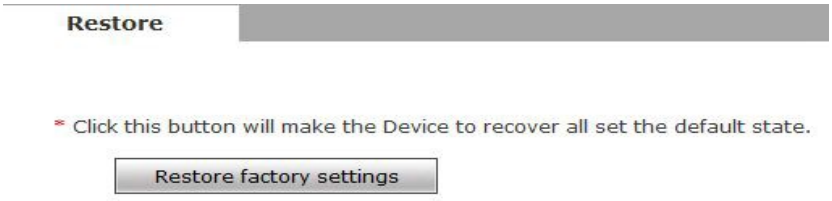
Click Save to confirm the settings

1.1.1 Upgrade



Click Browse button, and select correct file of upgrade (kernel file, suffix.uot), click [upgrade], and then you can upgrade your system; the completion rate will be displayed during this process. After upgrade completes, IP camera will restart automatically. Re-log in device, enter into system settings page, check to see whether the kernel edition is the upgraded edition

1.1.2 Restore

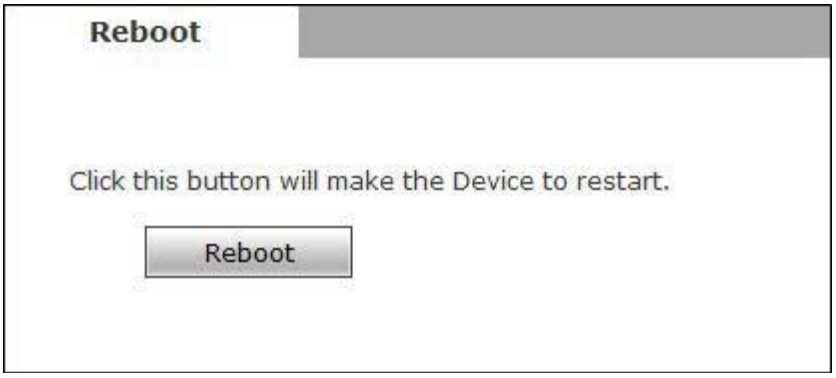


All device parameters (including network parameters) will be reverted to factory setting values.

1.1.1 Parameter Backup

On this page the camera parameters can be saved to a file and restored back from a file.

1.1.2 Reboot



Click Reboot, it will pop up a box, enter the password, and then the IP camera will restart.

1.1.1 System log

This page allows the searching of the operation and alarm logs, There is a maximum capacity of 512 messages

8 MECHANICAL DETAILS

All values are approximate.

Width	Height	Depth	Weight
87mm	92mm (WIFI) 79mm (no WIFI)	165mm	4.5Kg

9 ENVIRONMENTAL

Operating Temperature	-20°C…+60°C
Storage Temperature	-20°C…+60°C
Humidity	0…95% RH, non-condensing
Ingress Protection	IP66

NOTE
The RugiCAM-IP Camera unit is certified for use in an ambient temperature of-40°C to +60°C, the reduced operating range specified in the above table (Environmental) is guaranteed by design; operation over the full certified range should only be undertaken after careful consideration and in agreement with the manufacturer.

10 WASTE REMOVAL INFORMATION

The electronic equipment within must not be treated as general waste. By ensuring that this product is disposed of correctly, you will be helping to prevent potentially negative consequences for the environment and human health, which could otherwise be caused by incorrect waste handling of this product.

11 MAINTENANCE

No routine maintenance is required other than cleaning the glass window.

Any damage that may affect the safe operation of the unit, e.g. – damage to the enclosure, glass window, connectors or cables should be corrected by replacing the unit / part / cable with manufacturer approved spares. There are no user serviceable parts inside and to maintain dust/ water seals the unit should not be disassembled by the end user, other than to reset the camera if required

All screws must be fitted to ensure the integrity of the sealing O-rings.

NOTE
The complete Camera sub-assembly is encapsulated

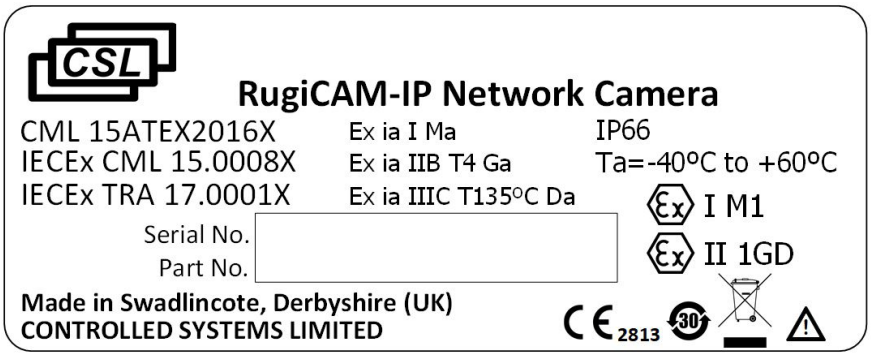
12 CERTIFICATION

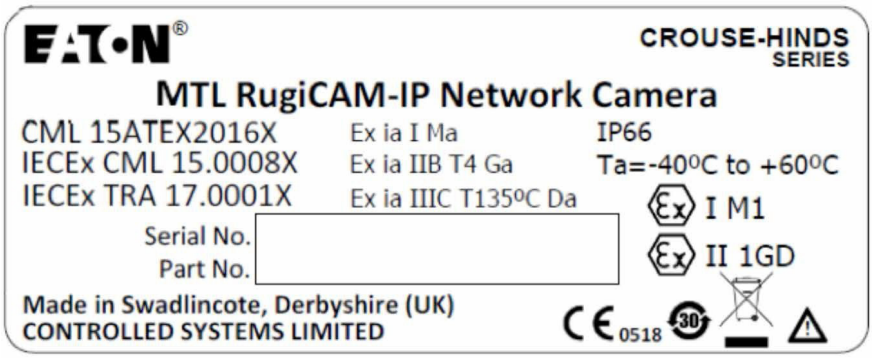
Ex ia I Ma, Category M1, Ex ia IIBT4 Ga
Ex ia IIICT135°C Da

CML 15ATEX2016X, IECEx CML 15.0008X, IECEx TRA 17.0001X

See certificates for further information

Marking Details





(Australia Only)

13 ORDERING INFORMATION

9459-ETplus-CSL*	CSL IS IP-Camera (with WiFi)
9459-ETplus-CSL-XX**	CSL IS IP-Camera (with WiFi)
9459 ETplus-SS	MTL IS IP Camera with WiFi (Australia only)

*Standard version (Stainless Steel 316)
**XX in the above part number relates to the enclosure material
AA = Anodised Aluminium
CS = Coated/Painted steel)

Additional accessories

9409-ET5	Camera Ethernet Cat6a Cable 5m (M12 connector 8-pole RJ45)
9409-PWR5	Camera Power Cable 5m (M12 connector 4-pole Free end)

*Also available in other lengths (subject to MOQ)

14 GLOSSARY OF TERMS

Alarm	An alarm can be in the form of an e-mail or an FTP upload of an image, that occurs when a sensor is triggered, or motion is detected.
AVI	Audio Video Interleaved. A Windows multimedia video format from Microsoft
CBR	Standard Bit Rate Encoding. This aims for a constant or unvarying bandwidth level but the video quality can vary.
CIF	Common Interface Format. A standard video resolution format used in video conferencing. CIF resolution is 352x288 and bit rate is 36.5 Mbps (at 30fps).
DHCP	Dynamic Host Configuration Protocol. A system by which each piece of equipment on a network is allocated an address IP dynamically.
Ethernet	The most widely used local area network (LAN) access method, defined by the IEEE as the 802.3 standard.
FTP	File Transfer Protocol. A standard protocol designed for transferring files over a TCP/IP network
IP	Internet Protocol. The network layer protocol in the TCP/IP communications protocol suite (the "IP" in TCP/IP). IP contains a network address and allows messages to be routed to a different network or subnet.
LED	Light Emitting Diode. A semiconductor device that emits light when a voltage is applied.
Motion detection	Camera function that causes an alert to be triggered when movement is detected in the field of view.
Protocol	Standards governing the transmission and reception of data.
Resolution	Screen resolution is expressed as a matrix of dots. For example, the VGA resolution of 640x480 means 640 dots (pixels) across each of the 480 lines.
RJ-45	Registered Jack 45. RJ-45 type connections are used in Ethernet devices.
SNTP	Simple Network Time Protocol. A protocol that allows devices to update internal clocks using a standard source available on a network.
Static IP address	A static IP address that is assigned manually and never changes.
TCP/IP	Transmission Control Protocol/Internet Protocol. A communications protocol developed under contract from the U.S.
VBR	Variable Bit Rate Encoding. This allows the bit rate to vary but maintains a constant video quality level.
VGA	Video Graphic Array. The video display standard for the PC.

15 APPENDIX A

END-USER LICENSE AGREEMENT

Revised: September 16, 2016

IMPORTANT

READ CAREFULLY .

THIS END USER LICENSE AGREEMENT (THE "AGREEMENT") IS A BINDING CONTRACT BETWEENYOU, THE END-USER (THE "LICENSEE") AND EATON CORPORATION OR ONE OF ITS AFFILIATES ("EATON" OR "LICENSOR").

BY DOWNLOADING, INSTALLING OR USINGTHIS SOFTWARE PRODUCT, YOU, THE LICENSEE, ARE AGREEINGTO BE BOUND BYTHETERMS, CONDITIONS, AND LIMITATIONS OFTHIS AGREEMENT. READTHETERMS AND CONDITIONS OFTHIS AGREEMENT CAREFULLY BEFORE DOWLOADING, INSTALLING OR

USINGTHE SOFTWARE.

IFYOU DO NOT AGREETOTHETERMS OFTHIS AGREEMENT, PROMPTLY RETURN THE UNUSED SOFTWARE PRODUCTTO EATON CORPORATION.

15.1 Definitions

15.2 Documentation

"Documentation" means the user guides and manuals for the installation and use of the Software, whether made available over the internet, provided in CD-ROM, hard copy, or other form.

15.3 Software

"Software" means the computer software programs for which Licensee is granted a license hereunder, the Documentation therefor and, to the extent available, Updates thereto. All computer programs are licensed hereunder in object code (machine-readable) form only except that certain software programs may include limited portions in source code (human-readable) form.

15.4 Update

"Update" means: (a) supplemental programs, if and when developed and distributed by Eaton, that may contain bug fixes or alternate program functions for the Software; and (b) a subsequent release of the Software, if and when developed by Eaton. An Update does not include any release, new version, option, or future product, which Eaton licenses separately.

16 SOFTWARE LICENSE

16.1 Ownership

Ownership. Eaton or its third party licensors retains all title, copyright and other proprietary rights in, and ownership of, the Software regardless of the media upon which the original or any copy may be recorded or fixed.

16.2 License Grant

Eaton grants to Licensee a limited, revocable, non-exclusive, non-assignable license to use the Software in conjunction with the operation of Eaton products to which the Software pertains or other products as described by Eaton in the Documentation. Licensee does not acquire any rights, express or implied, other than those expressly granted in this Agreement.

16.3 Restrictions and Requirements

Licensee will not, nor will it permit others to, modify, adapt, translate, reverse engineer, decompile, or disassemble the Software or any component thereof (including the Documentation), or create derivative works based on the Software (including the Documentation), except to the extent such foregoing restriction

is prohibited by applicable law. Licensee will not use the Software except in conjunction with the operation of Eaton products to which the Software pertains or other products as described by Eaton in the Documentation. Copyright laws and international treaties protect the Software, including the Documentation.

Unauthorized copying of the Software, the Documentation or any part thereof, is expressly prohibited. Subject to these restrictions, Licensee may make one (1) copy of the Software solely for backup or archival purposes, and may make one (1) copy of the Documentation for use by Licensee in connection with its authorized use of the Software. Licensee will number and account for all such copies. All titles, trademarks, and copyright and restricted rights notices included in the Software and Documentation will not be removed and must be reproduced in any copies. For avoidance of doubt, Seller does not grant Buyer a license to any of Seller's brands, logos, designs, trade dress, service marks, trademarks, domain names or trade names, in whole or in part.

Licensee agrees to install all corrections of substantial defects, security patches, minor bug fixes and updates, including any enhancements, for the Software in accordance with the instructions and as directed by Eaton.

16.4 Transfer and Assignment Restrictions

Licensee will not sell, assign, lease, sublicense, encumber, or otherwise transfer its interest in this Agreement or in the Software, or the Documentation in whole or in part, or allow any other person (except Licensee's bona fide employees and contractors) or entity, including any parent or subsidiary of Licensee or other subsidiary of Licensee's parent, to use the Software without the prior written consent of Eaton. Licensee may transfer the Software directly to a third party only in connection with the sale of the Eaton product in which it is installed, and only after the transferee has agreed in writing to be bound by the terms herein. In the event of such a sale, Licensee may not keep any copies of the Software or any portion thereof.

16.5 Verification

At Eaton's written request, not more frequently than annually, Licensee will furnish Eaton with a signed certification verifying that the Software is being used in accordance with the provisions of this Agreement. Eaton may audit Licensee's use of the Software. Any such audit will be conducted during regular business hours at Licensee's facilities and will not unreasonably interfere with Licensee's business activities.

17 TERMINATION

17.1 Termination

This Agreement and the license granted hereunder automatically terminates if Licensee breaches any provision of this Agreement. Eaton may terminate this license at any time with or without cause.

17.2 Effect of Termination

Immediately upon termination of this Agreement or the license granted hereunder, Licensee will cease using the Software, will delete the Software from its computers and will either return to Eaton or destroy the Software, Documentation, packaging and all copies thereof. If Licensee elects to destroy the Software,then Licensee will certify in writing to Eaton the destruction of the Software. Termination of this Agreement and return or destruction of the Software will not limit either party from pursuing other remedies available to it, including injunctive relief. The parties' rights and obligations under the following sections of this Agreement will survive termination of this Agreement: Article 1.0, Section 2.1, Section 2.3, Section 2.4, Section 2.5, Article 3.0, Article 4.0 and Article 5.0.

18 INFRINGEMENT AND WARRANTIES

18.1 Infringement

If Licensee learns of a threat, demand, allegation, or indication that the Software infringes or misappropriates any third party intellectual property rights (including but not limited to any patent, copyright, trademark, trade dress, or trade secret) ("Intellectual Property Claim"), Licensee will notify Eaton promptly of such claim. Eaton may, in its sole discretion, elect to assume sole control of the defense and settlement of said Intellectual Property Claim and Licensee will provide reasonable information and assistance to Eaton for the defense of such claim.

18.2 Disclaimer of Warranties

THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF CONDITION, UNINTERRUPTED USE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET

ENJOYMENT, OR NON-INFRINGEMENT. EATON DOES NOT WARRANT THAT THE SOFTWARE WILL BE UNINTERRUPTED, ERROR-FREE OR SECURE FROM UNAUTHORIZED ACCESS. THE LICENSEE EXPRESSLY ACKNOWLEDGES THAT TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE INSTALLATION AND USE OF THE SOFTWARE IS AT LICENSEE'S SOLE RISK.

19 GENERAL PROVISIONS

19.1 Update Policy

Eaton may from time to time, but has no obligation to, create Updates of the Software or components thereof.

19.2 Limitation on Liability

NOTWITHSTANDING ANY PROVISION OF THIS AGREEMENT TO THE CONTRARY, LICENSEE EXPRESSLY UNDERSTANDS AND AGREES THAT EATON, ITS AFFILIATES, AND OTHER LICENSORS, WILL NOT BE LIABLE FOR: (A) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY LICENSEE OR ANY THIRD PARTY, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY. THIS WILL INCLUDE, BUT NOT BE LIMITED TO, ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED,

COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR OTHER INTANGIBLE LOSS; (B) ANY LOSS OR DAMAGE WHICH MAY BE INCURRED BY LICENSEE OR ANY THIRD PARTY. THESE LIMITATIONS ON EATON'S LIABILITY WILL APPLY WHETHER OR NOT EATON HAS BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

TO THE EXTENT PERMITTED BY LAW, THE TOTAL LIABILITY OF EATON, ITS AFFILIATES, AND OTHER LICENSORS, FOR ANY CLAIMS UNDER THESE TERMS, INCLUDING FOR ANY IMPLIED WARRANTIES, IS LIMITED TO THE AMOUNT PAID FOR THE SOFTWARE.

THIS SECTION 5.2 STATES EATON'S ENTIRE LIABILITY AND LICENSEE'S SOLE AND EXCLUSIVE REMEDY UNDER THIS AGREEMENT, AND IS SUBJECT TO ALL LIMITATIONS STATED IN SECTION 4.2.

19.3 Notices

All notices required to be sent hereunder will be in writing and will be deemed to have been given when mailed by first class mail to the address shown below:

LICENSE NOTICES

EATON LEGAL DEPARTMENT

Eaton Center 1000 Eaton Blvd.

Cleveland, OH 44122-6058

(440) 523-5000

19.4 Severability

If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions of this Agreement will remain in full force.

19.5 Waiver

The waiver by either party of any default or breach of this Agreement will not constitute a waiver of any other or subsequent default or breach. Failure to enforce or delay in enforcing any provision of this Agreement will not constitute a waiver of any rights under any provisions of this Agreement.

19.6 Entire Agreement

This Agreement constitutes the complete agreement between the parties and supersedes all prior or contemporaneous agreements or representations, written or oral, concerning the subject matter of this Agreement. This Agreement may not be modified or amended except in a writing specifically referencing this Agreement and signed by a duly authorized representative of each party. No other act, document, usage or custom will be deemed to amend or modify this Agreement. The Software, or portions thereof, may also be subject to additional paper or electronic license agreements. In such cases, the terms of this Agreement will be supplemental to those in the additional agreements, to the extent not inconsistent with the additional agreements. If a copy of this Agreement in a language other than English is included with the Software or Documentation, it is included for convenience and the English language version of this Agreement will control.

19.7 Heirs, Successors, and Assigns

Each and all of the covenants, terms, provisions and agreements herein contained will be binding upon and inure to the benefit of the parties hereto and, to the extent expressly permitted by this Agreement, their respective heirs, legal representatives, successors and assigns.

19.8 Export Restrictions

Licensee agrees to comply fully with all relevant export laws and regulations of the United States and all other countries in the world (the "Export Laws") to assure that neither the Software nor any direct product thereof are (I) exported, directly or indirectly, in violation of Export Laws; or (ii) are intended to be used for any purposes prohibited by the Export Laws. Without limiting the foregoing, Licensee will not export or re-export the Software: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services (see http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx), or to any national of any such country, wherever located, who intends to transmit or transport the Software back to such country; (ii) to any end user who Licensee knows or has reason to know will utilize the Software in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any end-user who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.

19.9 U .S . Government Restricted Rights

The Software is a "commercial item" as that term is defined at 48 C.F.R. § 2.101, consisting of "commercial computer software" and "commercial computer software documentation", as such terms are used in 48 C.F.R. § 12.212, and is provided to the U.S. Government only as a commercial end item. Consistent with 48 C.F.R. § 12.212 and 48 C.F.R. §§ 227.7202-1 through 227.7202-4, all U.S. Government End Users acquire the Software with only those rights set forth herein. Contractor/manufacturer is Eaton Corporation, 1000 Eaton Boulevard, Cleveland, Ohio 44122.

19.10 Third Party Intellectual Property Rights

The Software may contain components (including open source software components) that are owned by third parties ("Third Party Licensors") and are provided with, incorporated into, or embedded in, the Software pursuant to license arrangements between Eaton and such third parties. Third Party Licensor components in the Software are not licensed or warranted under the terms

of this document, but are instead subject to the Third Party Licensors' license agreements. Licensee will not modify, delete, or obfuscate any copyright or other proprietary rights notices of Third Party Licensors contained in the Software.

19.11 Indemnity

Licensee shall defend, indemnify and hold Eaton and its officers, directors, employees, and agents harmless from and against all losses, damages, liabilities, claims, actions, and associated costs and expenses (including reasonable attorneys' fees and expenses) by reason of injury or death to any person or damage to any tangible or intangible property arising or resulting from the negligence or willful misconduct of the Licensee, its employees, contractors, or agents, in connection with Licensee's use of Software and Documentation.

Licensee shall be responsible for any breach of this Agreement by its officers, directors, employees, contractors, or agents. Licensee shall defend, indemnify, and hold Eaton and its officers, directors, employees, and agents harmless from and against any and all losses, damages, liabilities, claims, actions, and associated costs and expenses (including reasonable attorneys' fees and expenses) arising out of or in connection with any breach of this Agreement.

19.12 Confidentiality

Licensee acknowledges that confidential aspects of the Software (including any proprietary source code) are a trade secret of Eaton, the disclosure of which would cause substantial harm to Eaton that could not be remedied by the payment of damages alone. Accordingly, Eaton will be entitled to preliminary and permanent injunctive and other equitable relief for any breach of this Section 5.12.

19.13 Note on JAVA Support

The Software may contain support for programs written in JAVA. JAVA technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, direct life support machines, or weapons systems, in which the failure of JAVA technology could lead directly to death, personal injury, or severe physical or environmental damage. EATON DISCLAIMS ALL DAMAGES INCLUDING DIRECT, INDIRECT ANDCONSEQUENTIAL DAMAGES RELATINGTOTHE FAILURE OF ANY SOFTWARE INCLUDING JAVA PROGRAMS AND/OR JAVATECHNOLOGY.

19.14 Governing Law

This Agreement will be interpreted and enforced in accordance with the laws of the State of Ohio, U.S.A., without regard to choice of law principles. Licensee consents to the exclusive jurisdiction and venue of the courts of the State of Ohio for any action to enforce or construe the terms of this Agreement.

Eaton Corporation EULA

20 APPENDIX B

PRODUCT TEAM GUIDELINES

13/12/18

RugiCAM-IP MK2 has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.

The following Eaton whitepapers are available for more information on general cybersecurity best practices and guidelines:

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN): http://www.cooperindustries.com/content/dam/public/powersystems/resources/ library/1100_EAS/WP910003EN.pdf

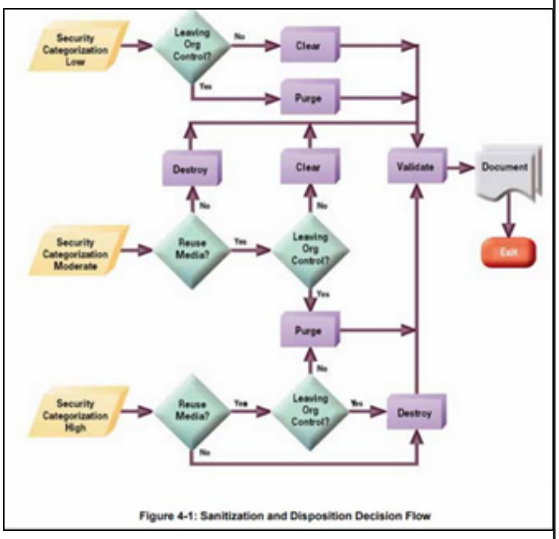
Category	Description
Asset Management	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, **<Product Name>** supports the following identifying information: **<Include for hardware>** - manufacturer, type, seria number, f/w version number, and location. **<Include for software> -** publisher, name, version, and version date.
Risk Assessment	Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system | device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.
Physical Security	An attacker with unauthorized physical access can cause serious disruption to device functionality. Addi- tionally, Industrial Control Protocols don't offer cryp- tographic protections, making ICS and SCADA com- munications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. RugiCAM-IP MK2 is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your device: - Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate. - Restrict physical access to cabinets and/or enclosures containing RugiCAM-IP MK2 and the associated system. Monitor and log the access at all times. - Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications - RugiCAM-IP MK2 supports the following physical access ports. - RJ45 - Wifi Access to these ports should be restricted.

Category	Description
COTS Platform Security	Eaton recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or plat- forms that are used to run Eaton applications / products (e.g., third party hardware, operating systems and hyper- visors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.).
	- Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components. - Vendor-neutral guidance is made available by the Center for Internet Security https://www.cisecurity.org/ Irrespective of the platform, customers should consider the following best practices: - Install all security updates made available by the COTS manufacturer. - Change default credentials upon first login. - Disable or lock unused built-in accounts. - Limit use of privileged generic accounts (e.g., disable interactive login). - Change default SNMP community strings. - Restrict SNMP access using access control lists. - Disable unneeded ports & services.
Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/ functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies: - Ensure default credentials are changed upon first login. RugiCAM-IP MK2 should not be deployed in production environments with default credentials, as default credentials are publicly known. - No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security. - Restrict administrative privileges- Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use.

Category	Description
Account Management (continued)	- Leverage the roles / access privileges to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role). RugiCAM-IP MK2 supports 3 users, administrator, user1 and user2. Administrator has full access users can simply view video and cannot configure anything. - Perform periodic account maintenance (remove unused accounts). - Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization's policies). - Enforce session time-out after a period of inactivity.
Time Synchronization	Many operations in power grids and IT networks heavily depend on precise timing information. - Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588). Please refer to section 9.7.4 of this manual
Network Security	RugiCAM-IP MK2 supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive informa- tion and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be seg- mented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control. Eaton recommends opening only those ports that are re- quired for operations and protect the network communica- tion using network protection systems like firewalls and in- trusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for RugiCAM-IP MK2 to operate smoothly The default ports used on the RugiCAM-IP MK2 are:= 80 Web Port (HTTP) 2000 Onvif Port 5000 Data Port Refer to section 9.3.1 for changing these settings

Category	Description
Remote Access	Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security. The RugiCAM-IP MK2requires additional hardware to allow Remote Access. This hardware will need securing correctly to ensure security
Logging and Event Management	- Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. - Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). - Ensure that logs are retained for a reasonable and appropriate length of time. - Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes.
Vulnerability Scanning	It is possible to install and use third-party software with RugiCAM-IP MK2. Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device | system into production. - Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at https://nvd.nist.gov/. - Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. **Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.**
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Category	Description
Secure Maintenance	**Best Practices** Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly. Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates. Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates. New firmware for the RugiCAM-IP MK2 will be available on the products page on the Eaton website
Business Continuity / Cybersecurity Disater Recovery	**Plan for Business Continuity/Cybersecurity Disaster Recovery** Eaton recommends incorporating RugiCAM-IP MK2 into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including: - Updated firmware for RugiCAM-IP MK2. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. - The current configuration. - Documentation of the current permissions / access controls, if not backed up as part of the configuration. The following section describes the details of failures states and backup functions:
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connec- tivity, log data, personal information) that may be stored by RugiCAM-IP MK2 be adequately protected through the deployment of organizational security practices.

Category	Description
Decommissioning or Zeroisation	It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.  Figure 4-1: Sanitization and Disposition Decision Flow **from NIST SP800-88** - **Embedded Flash Memory on Boards and Devices** Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory. - **Clear:** If supported by the device, reset the state to original factory settings. - **Purge:** If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. - **Destroy:** Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

21 CYBERSECURITY REFERENCES

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):

http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:

https://ics-cert.us-cert.gov/Standards-and-References

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST special Publication 800-41", October 2009:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:

http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

This page is left intentionally blank

This page is left intentionally blank

AUSTRALIA
Eaton Electrical (Australia) Pty Ltd,
10 Kent Road, Mascot, New South Wales, 2020, Australia

Tel: +61 1300 308 374 Fax: +61 1300 308 463
E-mail: mtlsalesanz@eaton.com

BeNeLux
MTL Instruments BV
Ambacht 6, 5301 KW Zaltbommel
The Netherlands

Tel: +31 (0) 418 570290 Fax: +31 (0) 418 541044
E-mail: mtl.benelux@eaton.com

CHINA
Cooper Electric (Shanghai) Co. Ltd
955 Shengli Road, Heqing Industrial Park
Pudong New Area, Shanghai 201201

Tel: +86 21 2899 3817 Fax: +86 21 2899 3992
E-mail: mtl-cn@eaton.com

FRANCE
MTL Instruments sarl,
7 rue des Rosiéristes, 69410 Champagne au Mont d'Or
France

Tel: +33 (0)4 37 46 16 53 Fax: +33 (0)4 37 46 17 20
E-mail: mtlfrance@eaton.com

GERMANY
MTL Instruments GmbH,
Heinrich-Hertz-Str. 12, 50170 Kerpen, Germany

Tel: +49 (0)22 73 98 12- 0 Fax: +49 (0)22 73 98 12- 2 00
E-mail: csckerpen@eaton.com

INDIA
MTL India,
No.36, Nehru Street, Off Old Mahabalipuram Road
Sholinganallur, Chennai- 600 119, India

Tel: +91 (0) 44 24501660 /24501857 Fax: +91 (0) 44 24501463
E-mail: mtlindiasales@eaton.com

ITALY
MTL Italia srl,
Via San Bovio, 3, 20090 Segrate, Milano, Italy

Tel: +39 02 959501 Fax: +39 02 95950759
E-mail: chmninfo@eaton.com

JAPAN
Cooper Industries Japan K.K.
MT Building 3F, 2-7-5 Shiba Diamon, Minato-ku
Tokyo, Japan 102-0012

Tel: +81 (0)3 6430 3128 Fax:+81 (0)3 6430 3129
E-mail: mtl-jp@eaton.com

NORWAY
Norex AS
Fekjan 7c, Postboks 147,
N-1378 Nesbru, Norway

Tel: +47 66 77 43 80 Fax: +47 66 84 55 33
E-mail: info@norex.no

RUSSIA
Cooper Industries Russia LLC
Elektrozavodskaya Str 33
Building 4
Moscow 107076, Russia

Tel: +7 (495) 981 3770 Fax: +7 (495) 981 3771
E-mail: mtlrussia@eaton.com

SINGAPORE
Eaton Electric (Singapore) Pte Ltd
100G Pasir Panjang Road
Interlocal Centre
#07-08 Singapore 118523
#02-09 to #02-12 (Warehouse and Workshop)

Tel: +65 6 645 9888 ext 9864/9865
Fax: 65 6 645 9811
E-mail: sales.mtlsing@eaton.com

SOUTH KOREA
Cooper Crouse-Hinds Korea
7F. Parkland Building 237-11 Nonhyun-dong Gangnam-gu,
Seoul 135-546, South Korea.

Tel: +82 6380 4805 Fax: +82 6380 4839
E-mail: mtl-korea@eaton.com

UNITED ARAB EMIRATES
Cooper Industries/Eaton Corporation
Office 205/206, 2nd Floor SJ Towers, off. Old Airport Road,
Abu Dhabi, United Arab Emirates

Tel: +971 2 44 66 840 Fax: +971 2 44 66 841
E-mail: mtlgulf@eaton.com

UNITED KINGDOM
Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds LU2 8DL

Tel: +44 (0)1582 723633 Fax: +44 (0)1582 422283
E-mail: mtlenquiry@eaton.com

AMERICAS
Cooper Crouse-Hinds MTL Inc.
3413 N. Sam Houston Parkway W.
Suite 200, Houston TX 77086, USA

Tel: +1 800-835-7075 Fax: +1 866-298-2468
E-mail: mtl-us-info@eaton.com

Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

© 2021 Eaton
All Rights Reserved
Publication No. INM MTLRugiCam-IP MK2
Rev 2 180521
May 2021

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.