



# WiseEye™ System

## Installation Requirements Guide

Rev 1.009

17 March 2009

Revision	Date	By	Comments
1.002	Sep, 15, 2007	YG	
1.07	Jan 15, 2008	YG	
1.08	March 17, 2009	YG	
1.09	July 20, 2009	MP	



This document has been prepared by **Emza Visual Sense Ltd (the “Company”)**. The purpose of this document is to introduce the Emza’s **WiseEye™** products to its business partners and customers. so that they might better understand the products and the company. All rights, including copyright, in this document are owned by the **“Company”**.

Except where expressly stated otherwise, you are not permitted to copy, broadcast, download, store (in any medium), transmit, show or play in public, adapt or change in any way the content of this document for any other purpose whatsoever without the prior written permission of the **“Company”**. Any unauthorized copying of material from this document will constitute an infringement of copyright.

PRELIMINARY



### 1. Overview

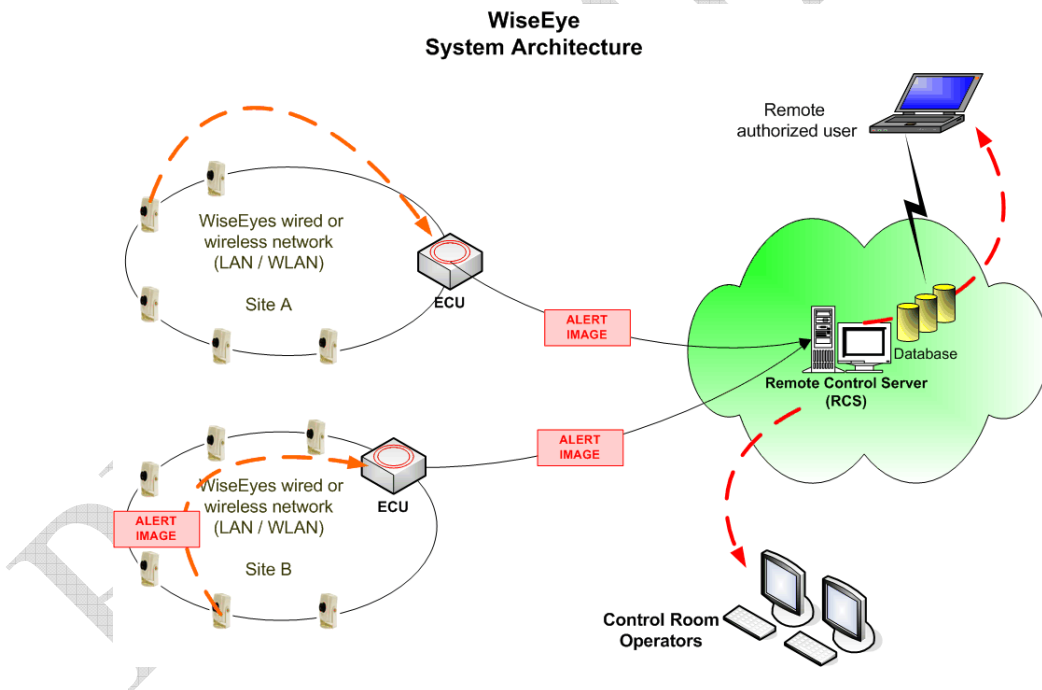
**WiseEye™** is a purpose-built outdoor intrusion detection camera designed to protect outdoor perimeters and assets such as utility and chemical stations, oil and gas production areas, communication towers, etc.

**WiseEye™** features on-board adaptive analytics algorithms which automatically discount environmental changes such as clouds, rain, wind, tree movements, shifting shadows.

Upon an alert situation (detection of intruder, car stopped, new object appears in the area of interest, someone is moving in direction that is not allowed, etc.) the WiseEye sends out sequence of JPEG alert image to a local or remote recording and control unit called the **ECU** (EMZA Control Unit). The **ECU** is capable of receiving such alerts from many WiseEye sensors installed in the local site.

The **ECU** is often connected to a remote (off-site) control room server that collects the alert events from multiple sites. The remote server is usually located in a central control room where alerts are inspected by security operators.

See typical the network architecture below:





## 2 Infrastructure Preparation

Prior to installation, it is recommended to conduct a Site Survey. Based on a site survey, the site should be prepared before the system is physically installed in the field. The site preparation includes the physical setup of all infrastructure requirements including:

- **Sensor Mounting** - Prepare the physical mounting location for each WiseEye (brackets, polls, fences, walls etc.) at each physical location defined in the site survey.
- **Power Supply** - Installing the power supply infrastructure (12 VDC) including wiring to each WiseEye location. Power requirements for wired WiseEye are about 2 Watt for wired unit and about 4 Watt for wireless unit.
- **UPS** - For power stability we recommend to use UPS to regulate the AC power and filter unnecessary spikes. The UPS should be connected to ECU and all network equipment and the sensors, and power supply to minimize electric grid interference
- **Network** - Installing the network infrastructure including:
  - Ethernet wiring to each WiseEye location in case of wired network
  - Wiring of the switches and routers as defined in the site survey
  - Locate the wireless router and the wireless access points as needed to cover the required air range
  - Installing and configuring the router that is used as a gateway for remote access over WAN or cellular channel
  - Establishing the communication link from the site router to the remote server
  - If a firewall is used, IT coordination is required to “open” the right channel and ports for port forwarding.
- **CAT5 wires** - Check the wire continuity by network tester
- **Network Test** - Check the installed wires and the network configuration by connecting laptop in the end of the cable (WiseEye location) and verify that the laptop can access to the various network devices. This test will ensure proper installation of the wires and will save time during the WiseEye installation.
- **Night Illumination** - Verify existing of night illumination in the sensors area. For good detection at night you should measure minimum of 2 LUX illumination level, depending on the FOV background (light gray ground, dark green etc.), darker background, higher LUX.

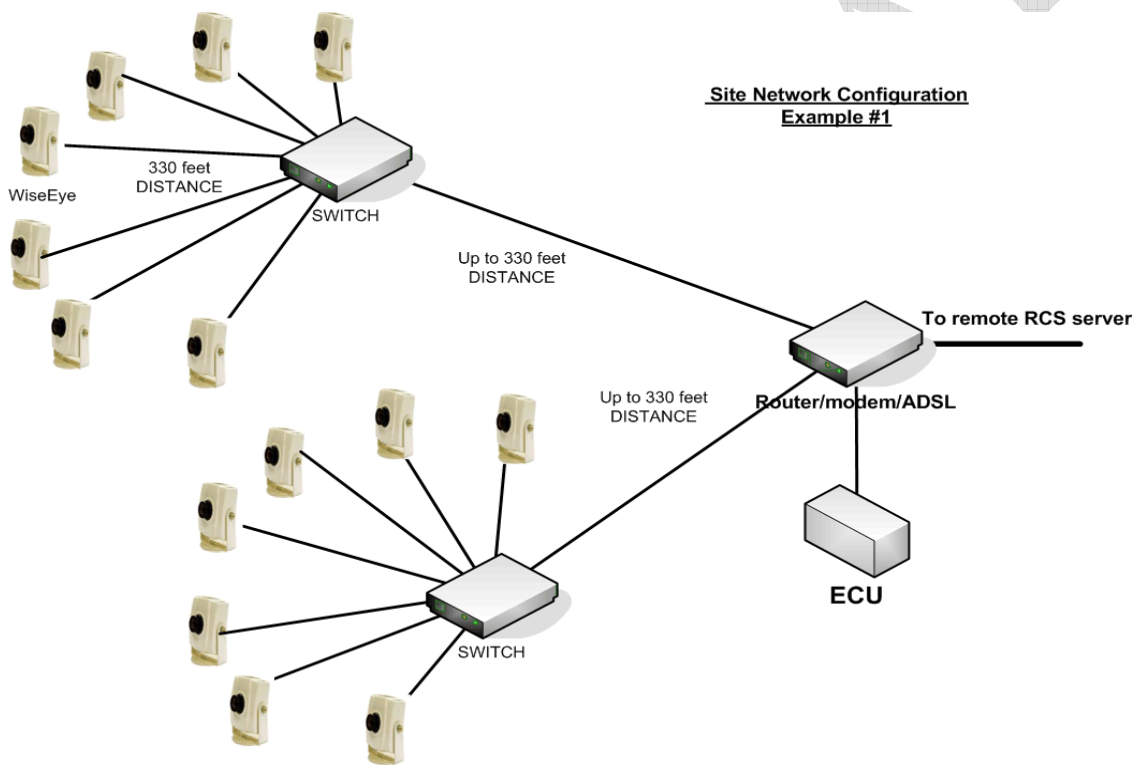


### 2.1 Network Architecture

The network architecture depends on the physical structure, size, security requirements, and local network configuration for each site, and should follow Ethernet electrical specifications and limitations (e.g., wire length)

See Appendix A for general wiring rules.

The following example #1 chart displays a network configuration for a typical site where two levels of switches are needed to implement the network wiring between the farthest WiseEye units and the ECU. In this example the maximum distance between the farthest WiseEye units and the ECU is about 660 feet (wire distance), assuming the ECU and the router are located in the same room.



A more complex architecture is shown in the following chart. In this example the use of fiber converters extends the distance between the farthest WiseEye's location and the ECU to thousands of feet. In this configuration we see also that it is required to use two ECU units to manage tens of WiseEye units in the same site.

#### 2.1.1 Wireless Network Architecture

In case of a wireless network (WiFi) at the site (at least one of the WiseEye sensors is wireless unit), a wireless router or access point should be installed. If all the WiseEye sensors are wireless units, install a wireless router with at least 2-4 RJ45 wired ports.



One of the wired ports is required to communicate with the ECU unit; additional ports may be used during installation for optional alert viewing by a laptop that is located in the site.

### 2.1.2 Wireless SSID

For test installations, the wireless router does not use encryption and the WiseEye sensors communicate with it in a regular WiFi channel.

#### **ATTENTION:**

When configuring the access point, ensure the SSID is:

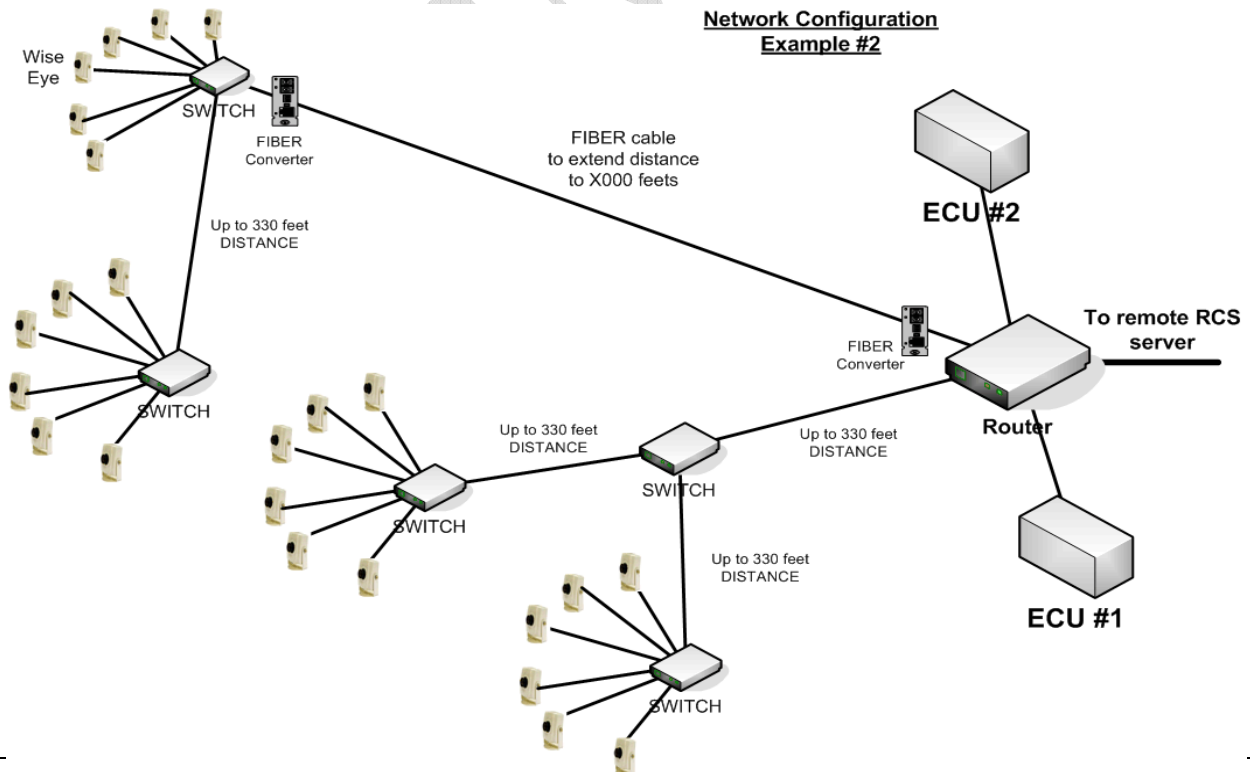
SSID = "emzaecu"

Note the name "emzaecu" is ***all lower case***.

The WiseEye sensors automatically search for an access point with that name; otherwise they will not establish communication. In fact, the WiseEye sensors ignore any wireless device in the area except "emzaecu." The router should be configured to enable the DHCP server.

WiseEye sensors may come pre-configured with a static IP address in the segment 192.168.112.XXX. The ECU is always configured with the address 192.168.112.100

More details on wireless network configuration in Appendix B.





### Appendix A – General Wiring Rules

Wiring runs should always follow the wiring rules listed here. It's much easier to do the job right the first time than having to go back and figure out why the connectivity is poor--after the wire has been run. The total length of wire segments between two network devices should not exceed 100 meters (330 feet or about the length of a football field) for CAT5 runs.

- a. Use quality components and tools to construct cables. As the saying goes, "Buy Quality, Only Cry Once."
- b. Under no circumstances should cable bends be less than four times the diameter of the cable. The Cat 5E standard is no bend radius less than 5 inches.
- c. When bundling groups of cables together with cable ties (zip ties), keep the ties snug but not excessively so. Do not over-cinch them. Keep them snug but don't tighten them so much that any of the cables deform.
- d. Keep cables away from devices that can introduce EMI noise. Among others, these include: copy machines, computer monitors, power supplies, UPS units, electric heaters, speakers, printers, TV sets, fluorescent lights, AC power cables, RF antennas or transmission lines, copiers, welding machines, radio transmitters, X-Ray Machines, un-shielded transformers, refrigerator compressor motors, dishwashing machine motors, microwave ovens, telephones, fans, electric garage door openers, elevator motors, electric ovens, dryers, washing machines, and shop equipment.
- e. Power cables and Ethernet twisted pair cables don't co-exist well. Do not run Ethernet cables parallel to AC power cables. Yes, we know that this is a repeat of number (d) but it is worth repeating... **DO NOT RUN ETHERNET CABLES PARALLEL TO AC POWER CABLES!**
- f. Do not stretch UTP cables when pulling cable. The maximum force on a cable should be 25 LBS or less.
- g. Do not use metal staples or insulated metal U shaped cable clips to secure UTP cables. Use telephone wire hangers, preferably ones with plastic hangers for the wire.
- h. Never, never run UTP cable outside a building. It presents a very attractive lightning rod and will prove dangerous to you and your network's health!



## Appendix B – Guidelines for setting wireless network

### A. For optimal network performance, use the following guidelines:

1. First and foremost, don't settle prematurely on a location for the wireless AP.
2. Experiment; try placing the AP in several different promising locations. While trial-and-error may not be the most scientific way to find a good spot for the sensor, it is often the only practical way to assure the best possible Wi-Fi performance.
3. Strive to install the wireless access point or router in a central location. Find a good compromise position. Sensors too far away from the base station will manage only 10% - 50% the bandwidth of sensors nearby to it. You might need to sacrifice the network performance of one sensor for the good of the others.
4. Next, avoid physical obstructions whenever possible. Any barriers along the "line of sight" between the WiseEye sensor and base station will degrade a Wi-Fi radio signal. Plaster or brick walls tend to have the most negative impact, but really any obstruction including cabinets or furniture will weaken the signal to some degree. Obstructions tend to reside closer to floor level; therefore, some folks prefer to install their wireless access point / router on or near the ceiling or the roof.
5. Avoid reflective surfaces whenever possible. Some Wi-Fi signals literally bounce off of windows, mirrors, metal file cabinets and stainless steel countertops, lessening both network range and performance.
6. Install the unit away from electrical equipment that also generates interference. Avoid electric fans, other motors, and fluorescent lighting.
7. Likewise install the wireless access point or router at least 1 m (3 feet) away from other home appliances that send wireless signals in the same frequency range. Such appliances include some microwave ovens, cordless telephones, baby monitors, and home automation equipment like X-10 devices. Any appliance that transmits in the same general range as 802.11b or 802.11g (2.4 GHz) can generate interference.
8. If the best location you find is only marginally acceptable, consider adjusting the base station antennas to improve performance. Antennas on wireless access points and routers can usually be rotated or otherwise re-pointed to "fine tune" Wi-Fi signaling. Follow the specific manufacturer's recommendations for best results (see below)

\* \* \*