EXPANDING YOUR VISION
ZISTOS®
PORTABLE VIDEO SYSTEMS

Zistos Corporation
1736 Church Street
Holbrook, NY 11741

November 2013

A Word about Wireless Video and Tactical Applications

A question that keeps recurring during our meetings and discussions with the tactical community relates to the approach that Zistos has adopted with regard to integrating wireless video technology into our products. Historically, Zistos products have always had wireless technology available only as an optional peripheral component and not as a required internal feature necessary for basic operation. This document discusses the reasons that were considered in adopting this design approach.

Worst Case Scenario Design Concerns

Planning for a tactical mission needs to consider worst case scenario possibilities. In a worst case scenario basic wireless technology won't work because of random environmental or premeditated factors. That is why when we initially designed the Zistos tactical surveillance tools we decided that wireless video would not be included as a core function in many of the hand-held and body-worn equipment implementations. We have offered wireless video in Zistos products, but only upon the request of a customer and/or as a peripheral option and never to facilitate basic operation. Our tools are designed for wired operation and this is how our end users train with their use. Many wireless tools that rely on the transmission of video via radio to operate do offer a parallel feature of using a wired option. In most instances, this configuration is an afterthought to the design and many times the wireless tools become far more difficult to deploy and operate when used in a wired configuration.

Potential Risk Factors: Detection & Interception

The potential risks associated with wireless in military and law enforcement applications have been a longstanding issue. Despite this concern, many individuals felt that the potential problems associated with the use of wireless video were worth the extra convenience of having fewer external wires required in a typical tactical surveillance system. As a result of this type of thinking, many tactical surveillance products were designed with this perceived benefit in mind. These products feature wireless video as a core function for their basic operation and the potential liability concerning its use are ignored.

Now, more than ever before, there are even greater risks associated with using this wireless video in tactical surveillance tools. This is due to a new array of consumer accessible technologies that makes it trivial for a third party, (such as criminal/terrorist operatives, or more likely - media), to detect and even intercept, view and record wireless video transmissions. A key component to any tactical surveillance mission is stealth. If an individual is armed with any of these new low-cost devices, wireless technology can now compromise this most important facet of a tactical operation. In many cases, even if a transmission uses encryption it may still be able to be detected by low-cost tools.

Potential Risk Factors: I.E.D.'s

Historically, wireless transmissions and the possibility of spontaneous detonation of explosives has always been a concern in the industry. There has been much debate on this issue and in the past, the probability of this type of event occurring had been viewed as low. Hazards associated with the use of wireless transmitters in proximity to explosives were viewed by many as an unnecessary concern. This

situation has changed. As a result of technology and information that is readily available through the internet and elsewhere – it is now easier than ever for a wireless signal to be used as a trigger event to detonate an IED, not by accident, but by design. This is more likely to occur when an operative has some intelligence on the type of equipment and frequencies of transmission that is being used. Unfortunately, much of this sensitive information is currently available in the public domain.

Know the Risks Before Use

Wireless technology does have a place in tactical missions. It is important that a thorough understanding of wireless video and the risks associated with its use are understood in advance of its application in a tactical mission. Operations where wireless may be an appropriate risk include those where stealth is no longer a requirement are remote robotic cameras and perimeter surveillance platforms.

Summary

Wired technology may be a slightly less convenient, but it does have the following advantages over wireless video transmission:

Advantages of Wired Video Systems

- Will always work in a noisy RF environment, no dropouts or dead zones
- It cannot be easily detected,
- It cannot be intercepted
- It cannot be used to detonate an IED.

Our design approach has factored the above information into the design criteria for our products in order to come up with the most effective and safest tactical surveillance tools to be used in unknown conditions. It is for these reasons that Zistos has adopted a wired approach to our line of tactical surveillance tools.

Rather than providing details on any of the above concerns that could be used as a "How To Guide" to criminal/terrorist elements, we would ask that if you would like further details on these issues to contact Zistos by e-mail and list your contact phone number, agency/dept. name and best time to contact you. We will be happy to answer any of your questions and share our concerns in more detail.