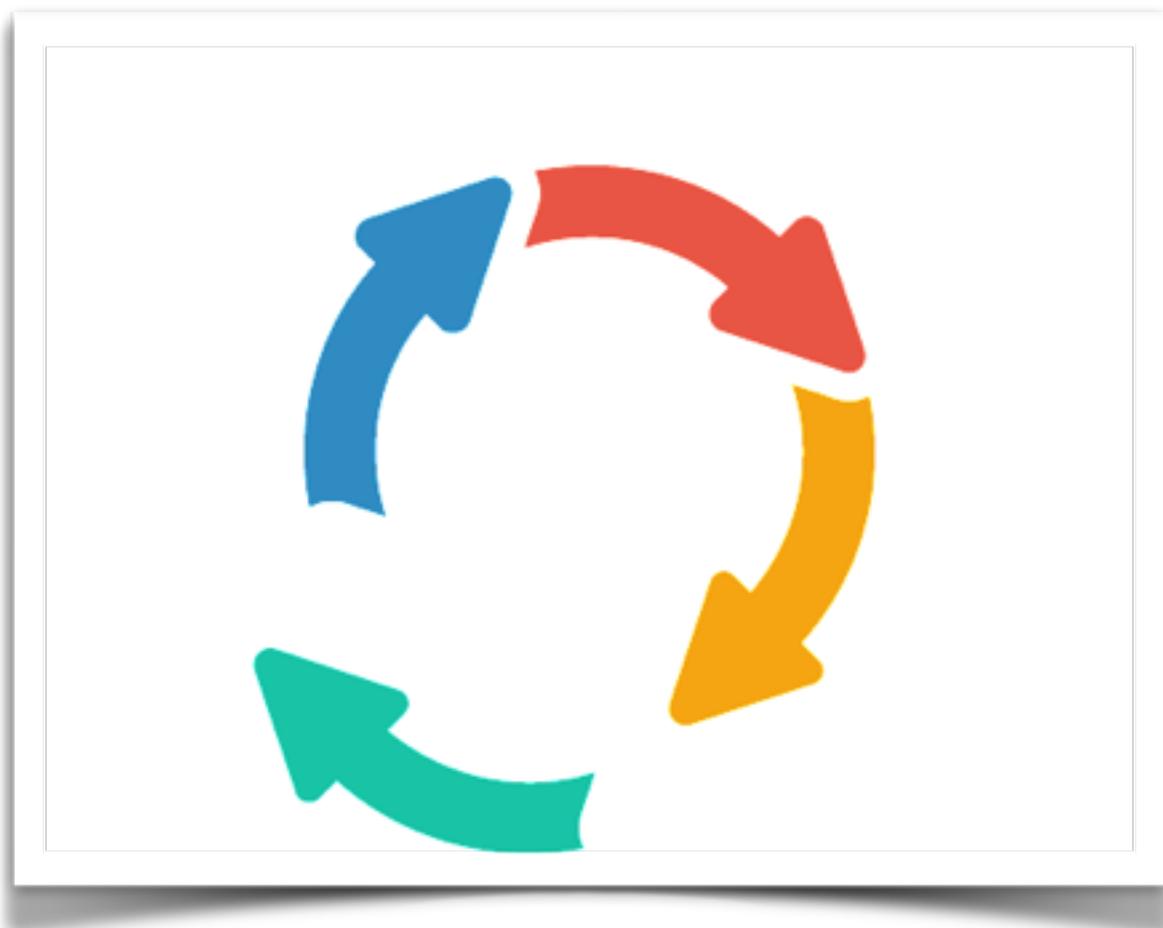


Open, End-to-End?

What's The Right Path For Your IP Video Security?



IndigoVision

Introduction

Before choosing a video security system the most important thing to weigh-up is not so much the technical issues behind a system, but what the system can deliver to you. How easy is it going to be to operate? Will the various elements work together? Is it likely to be simple and cost effective to maintain? Are you going to be able to call up relevant video footage in a timely way when the worst happens?

When demystifying the world of IP video security systems, there are two main options on how these requirements would be delivered - an 'open' IP video security system or an 'end-to-end' IP video security system. Is there is a right and wrong choice when it comes to IP video security? Let's investigate further.

Open Or End-to-End?

An 'open' IP video security system would be one where you could pick and choose any camera, any recorder or any video management software - from any manufacturer. There are benefits from an 'open' video security system, like freedom of choice and not being tied to a single manufacturer. But with that freedom comes greater risk, leading to reduced reliability and less functionality.

With an 'end-to-end' IP video system, each individual component is provided by a single manufacturer and they are rigorously tested to ensure they work together. These systems typically give a guarantee of backwards compatibility, protecting any investment you make now. This is achieved by future versions of the video management software supporting legacy hardware, as the manufacturer can easily include them as part of their testing program. 'End-to-end' systems often give more features than 'open' systems, such as faster access to live or recorded video.

Not Just Security

Outside of the security arena, Apple have demonstrated the powerful benefits that can be realised from developing an operating system that is intrinsically part of the hardware. You might be one of the 300 million people that have had one in your hand today - the iPhone. This 'end-to-end' approach ultimately gives more control over the end result, which Apple say delivers more reliability and a better user experience. Likewise, newer versions of the operating system can still support legacy hardware, meaning the iPhone you buy today will receive new software features in the coming years.



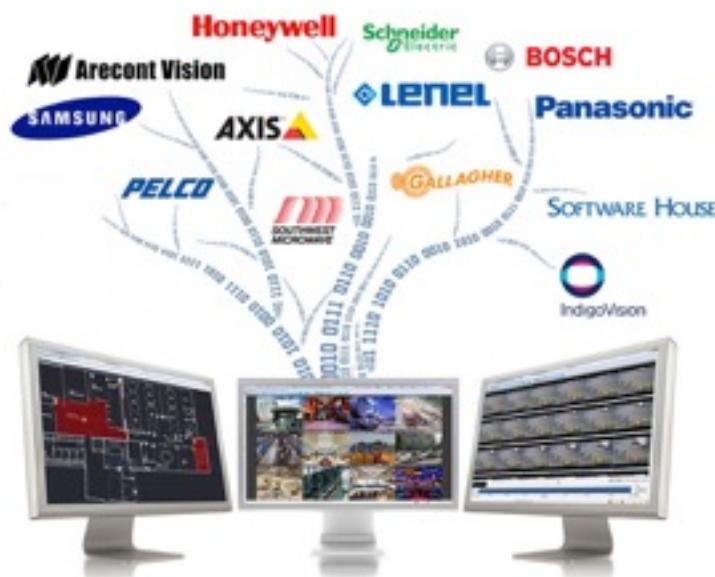
This is no different to an 'end-to-end' approach with IP video security, the hardware and software are all tested and optimised to work with each other. New management software is released, giving legacy hardware a new lease of life.



Open And End-to-End?

When looking at 'open' and 'end-to-end', are the two approaches mutually exclusive or can you still go for 'end-to-end' and bring in some of the best aspects of 'open' as well?

Although people may have viewed 'end-to-end' as being synonymous with proprietary - completely tying you in to hardware from one manufacturer – things have moved on in video security. Looking at the wider physical security perspective, it's possible to integrate with systems outside of video surveillance such as: access control, perimeter detection, alarm systems.



It's also possible to integrate third party cameras into 'end-to-end' systems through the open ONVIF standard and even proprietary camera communication protocols. Although the truth is that the more third party cameras you bring in, the more likely you are to dilute the benefits associated with true 'end-to-end' functionality.

Keep in mind that even when open standards like ONVIF come into play, there are sometimes compatibility issues. For instance a camera can be claimed to be ONVIF Profile S - and has been certified according to the ONVIF standards - but it might not work in a way that might be expected.

Ask The Questions. Choose The Right Path.

When deciding what path to take for IP video security, look at what's right for you and examine in detail what is being proposed. Is the video security system 'open' or 'end-to-end'? Both have their advantages, 'open' gives complete freedom and 'end-to-end' gives better reliability, future-proofing and often more features. Likewise, both have their potential downsides, an 'open' video security system comes with more risk and with 'end-to-end' you are potentially tied into that manufacturer's long term roadmap.

There is a third option, an 'open, end-to-end' IP video security system. One that removes the risks by giving access to third party cameras and wider security applications, while delivering the outstanding benefits that come with an 'end-to-end' system.

So ask yourself the question. Who develops and manufacturers the components of the video security system - are they from multiple manufacturers ('open')? Or from a single manufacturer ('end-to-end')?

If it's a single manufacturer, does the system support third party cameras? Does the system integrate into additional security systems, like access control, from multiple manufacturers? If the answer is yes to the last two questions, then you are looking at a true 'open, end-to-end' IP video security system, bringing the best of both worlds.