

# Opening Up IP Security Solutions

*With the ONVIF Open Standard gaining traction in the marketplace, Alex Swanson, IndigoVision's Head of Engineering, discusses the current situation with the standard and looks at what being 'Open' really means.*

The debate about so called 'open' and 'closed' IP Video surveillance solutions has been ongoing for some time. Each side suggests that their approach is better for the end-user, with a reasonable amount of disinformation being added for good measure. To a large extent this debate is being extinguished with the release of the ONVIF Standard. However, even with this standard, defining exactly what is meant by an 'open' system is still up for debate.

## The ONVIF Standard

The global security and surveillance market is at a landmark stage as, finally, a 'standard' for IP Video is really gaining traction in the market. Open Network Video Interface Forum (ONVIF) can boast nearly 800 conformant products as of Spring 2011 and it has clearly left the other competing standard, PSIA, far behind. This was most apparent at an interoperability demonstration at ISC West in April 2011. The ONVIF event was buzzing, with 200+ visitors, while the PSIA event attracted only a small number of people.



It is clear that ONVIF is on the way to being the de-facto standard for IP based surveillance products and open standards in the IP security market are here to stay. ONVIF is also being incorporated into the IEC (International Electro-technical Commission) standard for Video Surveillance Systems and, once ratified, will mean that ONVIF is a true international standard.

ONVIF provides the common language that enables IP security products from a diverse range of manufacturers to work together. Rather than defining just a media data format like H.264, ONVIF encompasses system control; for example, it defines how the Video Management System (VMS) asks a camera to start and stop a video stream or move to a particular position.

Although initially focussed on Video, including cameras, analytics and Network Video Recorders (NVRs), ONVIF is being extended to include Access Control. If this is also adopted by the market, it will be a substantial achievement, as the Access Control market is even more proprietary and fragmented than video was.

As the market moves towards the adoption of an open standard like ONVIF, the end-user can expect to see a number of benefits:

- Increased flexibility and greater freedom of choice - ONVIF enables end-users to select interoperable products from a variety of different brands to suit their needs

- More sophisticated and differentiated features in VMS as vendors are freed up to be more innovative rather than writing endless proprietary drivers
- Confidence that their investment is secure as it is possible to replace or upgrade parts of the system as required
- Less integration costs - end-users can choose the most suitable combination of IP-based physical security products, regardless of vendor

Because of these benefits, many tenders and RFPs are specifying that solutions must be ONVIF-conformant. However, at this stage in the game, it must come with a health warning. 'Plug & play' interoperability of ONVIF products will take time to achieve, as the standard settles down, and in the meantime there will be some 'teething' issues.

## End-to-End Solutions

Prior to the emergence of ONVIF, multi-vendor solutions were based on proprietary protocols, with a new driver needing to be written for each manufacturer's cameras - costly and time consuming.

In contrast, end-to-end solutions from a single vendor provide a tightly integrated system, with components designed to work together. The benefits are: smoother project roll outs, optimum performance and reliability, lower support and maintenance costs and a single point of accountability. End-to-end solutions can also incorporate special features such as advanced real-time analytics in the camera and bandwidth-saving capability that are not supported within the ONVIF Standard. Consequently, end-to-end solutions can often out-perform multi-vendor ONVIF systems.

End-to-end may have strong benefits, however in the past this came with a drawback that you were locked in to a proprietary system. Some providers of end-to-end solutions are now opening up their software to third party cameras through ONVIF. They are probably more likely to provide robust ONVIF solutions earlier as they will need to test and certify a range of cameras to demonstrate their openness, unlike the management software providers who use the proprietary drivers. One suspects VMS-only vendors might also prefer end-users to continue using the proprietary protocols, since their sales pitch is to support any manufacturer and ONVIF enables everyone to make that pitch. The main 'raison d'être' of the independent VMS providers just disappeared.

The end-user can therefore get the best of both worlds by choosing an end-to-end solution that is also ONVIF-conformant. End-users will be able to mix third party ONVIF cameras with cameras that have been designed to work in the end-to-end system. This offers the benefits of a complete integrated solution with the ability to choose cameras from other manufacturers to suit specialised needs.

## Open Architecture means much more than just ONVIF

Being 'open' is about giving people freedom to choose. True open systems give users choice in every aspect, i.e. not just cameras but also storage, access control, analytics, workstations, etc.

'Open' also means giving access to the inner workings of the system through a Software Development Kit (SDK). This allows third parties to integrate with wider systems such as process control, oil & gas monitoring, EPOS, manufacturing, etc. An example of this is with the integration of ANPR/LPR systems with IP Video. Specialist licence plate recognition cameras can be interfaced to the network through video encoders and thereby benefit from the distributed architecture and 'virtual matrix' switching inherent in the best IP Video systems. ANPR/LPR processing engines can also analyse video streamed across the network from any camera in the system.

Integration between security systems is becoming an increasingly important part of efficient security management and incident response. With operators in large surveillance systems having to monitor hundreds of cameras, the use of alarms from other systems to highlight incidents and events is invaluable. The best 'open' IP Video systems allow tight integration with third party systems, of which the most commonly used is Access Control. Until access control adopts open standards, such as ONVIF, this involves the IP Video manufacturer writing interfaces for each Access Control system, in the same way as the original pre-ONVIF 'open' VMS systems did for IP cameras.

Integration interfaces can also be written for non-security systems such as BMS and Electronic Point of Sale (EPOS). Integrating EPOS, access control and video surveillance together becomes a very powerful solution for applications such as casinos and retail, where cash handling is a major issue. Cashier transactions can be stored automatically with the relevant camera video, enabling powerful post-incident analysis.



*Integrating EPOS, access control and video surveillance becomes a very powerful solution for casinos and retail operations.*

## IP Video Architecture

When comparing IP Video solutions there are many factors to consider. The issue of cameras has now largely been solved through the ONVIF standard. This leaves other components such as VMS and video recording. However, one area that needs very careful consideration is the system architecture.

The architecture has a significant impact on the flexibility, resilience and scalability of the solution. Centralised server-based systems have a single point of failure as all video has to be transmitted through the server. In large systems the amount of video streamed through the central server can place significant demands on the network. This means increased bandwidth, latency, maintenance and costs. In contrast, in a distributed server-less architecture video can be sent from a camera to a local workstation, without the need to go through a central server. NVRs can also be located at the network edge near clusters of cameras, to reduce bandwidth and improve resilience. A failure on any part of the network will not cause the whole system to fail.

## Compression and Video Recording

The ONVIF Standard defines how video streams are managed and controlled but not how they are compressed. The way video is transmitted within the ONVIF framework is defined by video standards such as H.264 and MPEG-4. These ensure that any VMS system or NVR can decode any video stream that meets these video standards. However, the quality of the compression, i.e. the trade-off between video quality and bandwidth, can vary significantly depending on how well the video compression standard has been implemented in the camera encoder. The amount of video, for a given resolution/framerate, that an NVR can store is very dependant on how good the compression is in each vendor's camera. For the same quality picture, one camera can compress video 10 times more than another, even though they both output H.264 compliant data.

Calculating the amount of storage required is an important part of the costing and design of an IP Video system; on large enterprise solutions the storage cost can be a significant part of the overall cost. Vendors of end-to-end solutions typically supply storage calculator tools that considerably ease this process. However, in an ONVIF-conformant system, with cameras from multiple vendors, the storage capacity calculations become potentially much more complicated.

The latest version of the ONVIF Standard (2.0) now enables ONVIF-conformant storage devices such as DVRs and NVRs to be developed. For example, a DVR manufacturer could produce a product that enables the video recorded by that DVR to be played back in any VMS system that supports the ONVIF Standard for storage devices.

There are already storage products on the market which are labelled ONVIF-conformant, but only from the camera to NVR side. They can record video from a range of third party ONVIF cameras, but a proprietary interface is still required to review and playback the video. Fully ONVIF conformant storage devices have not yet emerged, but when they do they will have a profound affect on the market.

In many cases the recording solution, whether it is standalone NVR hardware or a software application, is an intrinsic part of the VMS. ONVIF will enable the decoupling of the storage from the main VMS, providing increased flexibility and a choice of storage, plus potentially lower costs for end-users.

Storage array manufacturers will be able to produce standalone storage products that can be integrated into ONVIF-conformant VMS solutions without the need for additional recording servers. To date this has been achieved by the storage array manufacturers pre-loading the recording application software from the VMS provider onto their appliance, thus requiring them to create customised products and to certify each VMS provider, which is both costly and time-consuming.

As the ONVIF standard does not define how recordings should be stored on disk, just the interface, there is an opportunity for differentiation of products, e.g. optimised storage and data retrieval methods, reliability, and so on, giving end-users the freedom to choose products that meet their requirements and budgets.

However, in addition to the benefits, there will be challenges. For example, setting up redundancy and failover between storage devices from different vendors could be complex and the ONVIF Standard does not currently support this. Today, the ONVIF Standard also does not provide a full configuration interface, so a proprietary interface from the storage vendor is still needed for configuration. Until the standard matures, these limitations could be a barrier to ONVIF storage devices appearing any time soon.



*In many cases the recording solution, whether it is standalone NVR hardware or a software application, is an intrinsic part of the VMS.*

## Summary

With so many of the big names in the IP Video market committed to ONVIF it has unstoppable momentum. It brings wider choice and peace of mind for the end-user. But it is not by itself the definition of an 'open' IP Video system; it is just one of the many facets that make up a truly 'open' solution. ONVIF also strengthens the benefits of end-to-end solutions by offering the best of both worlds: it installs easily yet still gives freedom of choice.

ONVIF will undoubtedly bring significant change to the market, which will in the long-term benefit the end-user. In the short term there will be a period of 'bedding down' as the standard matures.



### About the Author

Alex Swanson has worked in IndigoVision for nine years and was appointed Head of Engineering in 2010. Previously he was Chief Technical Officer at Vebnet, a market-leading global service provider of flexible benefits schemes. Before that he led engineering teams in 3Com, Axon Networks and Spider Systems working in network technology. He holds a BSc (Hons) in Physics and an MSc in A.I. both from Edinburgh University.

Alex Swanson, Head of Engineering  
IndigoVision

E-mail: [enquiries@indigovision.com](mailto:enquiries@indigovision.com) or visit [www.indigovision.com](http://www.indigovision.com)