13/07/04

Forum on IP technology and the CCTV industry

The reason the forum was initiated was in response to a number of conversations with CCTV manufacturers, both during and following IFSEC. These conversations indicated that IP-based product sales were not matching expectations, predominantly in the mainstream CCTV sector. Much of this could be attributed to a reluctance by installers to embrace the technology, combined with misleading messages which promoted the technology more as an IT-based product than as a security one.

The conclusion of the conversations was that interest amongst installers might be stimulated if the technology was promoted more as a CCTV tool, with specific reference to security rather than to the more IT-biased benefits. All manufacturers approached felt that this approach was worthy of further debate, and as such the Forum (held at Rules on 13 July 2004) was organised.

Attendees:
DM - Angela Raynor
Samsung - Simon Shawley
Bosch Security Systems - Adam Breeze
Panasonic - Sean Taylor
Panasonic - Rob Healey
Vicon - Guy Nixon
Baxall – Karl Haw
Sanyo - Bob Groom
Norbain - Huw Edwards
Redcare - Alison Arney
JVC - Geoff Bwye
JVC - Hanish Shah
Remguard – John Ellison
Honeywell - Nick Bowden
Honeywell - Chris Brown
Pro Activ - Mark Quittenton
Pro Activ - Pete Conway
Pro Activ – David Lewis

Apologies from:
Pelco - Kevin Smith
Siemens - Colin McLuckie
Sanyo - David Hammond

Forum background

The topic of debate concerned the fact that in both mainstream CCTV installations and in larger projects, IP-based technology is not enjoying the high profile that was anticipated a few years ago. Whilst the technology is often discussed and debated, sales are not in line with expectations.

Looking at the mainstream market-place first, installers are hesitant to take the first steps toward using the technology. Anecdotal evidence has indicated that the overall feeling is that IP-based security devices and systems are not being presented to installers as CCTV tools. Many companies see the technology as from outside the security industry, and question its need.

Until installers start working with the technology, sales will always be slow, and growth in the market will be stifled. The vast majority of manufacturers will only further develop and launch products when there is sufficient demand, and this means that R&D is bound to slow, as products are not being sold in large enough numbers.

There is confusion over the technology, a fear of working with unproven systems, and a lack of understanding of the real benefits on offer in the installation sector. As CCTV manufacturers have backed off the promotion of IP-enabled products – predominantly because of the low sales figures – the message coming across to installers has been from the companies with an IT-background and purely IP-based product lines. Whilst these companies obviously know networking, their knowledge of security isn't that good!

On the project side, some end users are certainly more familiar with the concepts. However, as the IT-based companies become more involved in this sector, the emphasis could potentially shift toward management benefits, process control and gimmicks rather than focussing on security, and ensuring that nothing compromises that.

These issues were obviously of concern to the CCTV manufacturers, and the purpose of the forum was to discuss whether – and how – the CCTV industry should take control to possibly create guidelines and ensure that security is always the prime concern, in both projects and mainstream installations.

The areas suggested for debate were:
- The use of externally accessible networks, or closed circuits for security.
- Availability concerns on networks for monitoring.
- The use of appropriate terminology for security installers, with a focus on security rather than IT.
- A common configuration approach from all manufacturers.

Specific comments

The use of externally accessible networks, or closed circuits for security It was pointed out that a move toward using closed circuit networks for CCTV – and security in general – was not acceptable as the whole concept of IP was based upon opening up communications. Installers would have to accept the use of existing networks as IT managers would drive things that way, and once they had trust in the security devices were happy to allow them to be used on the network.

Rob Healey (Panasonic) stated that the IT manager was now an essential part of most large CCTV solutions, even where a composite system was installed. Increasingly, as most systems had some element of IT, facilities and risk managers with no knowledge of security were handing the systems over to IT managers.

Angela Raynor (Dedicated Micros), Karl Haw (Baxall), Hanish Shah (JVC) and John Ellison (Remguard) all agreed that the use of networks offered too many benefits for the additional security of a closed circuit system to be credible. However, Alison Arney (Redcare) did point out that the costs of using a general network were only marginally lower than if a closed circuit network were to be used. Chris Brown (Honeywell) also pointed out that the benefits of IP could be realised over dedicated links using DVRs as the base for the system.

In general, the opinions reflected the feeling that opting to keep CCTV and other security-based technologies discrete from business-critical networks was not a realistic option. When smaller sites were discussed, the feeling remained the same. Overall security created by a closed circuit was not seen as being more important than the IT-related benefits that could be sold to end users. The point was also made that with installers losing business to communications companies, the emphasis was moving away from pure security and more into IT-based offerings.

The subject of support of systems arose when Bob Groom (Sanyo) pointed out that on one installation, an installer had used IP-based equipment to create a closed circuit solution. However, once the end user had decided to expand the system to also utilise the existing network, the installer had been unable to support it.

Hanish Shah (JVC) added that as a manufacturer, they were only prepared to support their devices on a network, and not any other elements of the system. Guy Nixon (Vicon) argued that manufacturers cannot walk away from the support of a system where security is concerned. John Ellison (Remguard) pointed out that IP-enabled solutions grow beyond pure security, and being multi-facetted means installers have to take responsibility rather than manufacturers.

Angela Raynor (Dedicated Micros) stated that all manufacturers should follow the lead of Baxall, and offer training in IT to prescribed levels. Rob Healey (Panasonic) added that manufacturers have invested in IP as a technology, and other parts of the security

industry need to move with them or risk losing business to other communications and IT sectors – a situation which was agreed is already occurring.

The overall feeling was that training was necessary for installers, and whilst manufacturers seemed happy to help installers on large projects, it was agreed that those involved in the commodity market (i.e. bulk sales of IP-enabled products) would have to seek training and support elsewhere. No one was sure who should take responsibility for this training.

When asked whether such a level of training excluded the growth from installers who might consider trying out IP-based solutions in a smaller sites initially, Angela Raynor (Dedicated Micros) pointed out that Baxall had advanced some installers with virtually no knowledge to a high level of capability.

The issue of support was underlined by Nick Bowden (Honeywell), who pointed out that where IP-enabled security equipment was used over existing the networks, installers did not want to have support other devices as it was seen as a high risk scenario. For example, they might not have enough knowledge of other devices to know whether problems are being caused by the security equipment of not. Bob Groom (Sanyo) added that installers will have to learn when to pass problems on to other suppliers of additional devices on the network. Chris Brown (Honeywell) raised the point that even getting installers to keep up with changing technologies and devices such as routers might be an issue.

Essentially, the issue of support was further compounded by Alison Arney (Redcare), who pointed out that in security applications, and especially with emphasis on BS8418, continuity of service had to be guaranteed – which could not be achieved with IP-enabled networks. The only responses to this were inconclusive (i.e. people do banking online, ISDN isn't stable, etc.).

Karl Haw (Baxall) stated that growth might be achieved by promoting the level of end user demand for IP-based solutions. It was also considered that promoting the potential revenue from maintenance might be another option, although a lack of overall support might make this difficult.

General summary

Interestingly, conversations which led to the organisation of this forum identified several trends. These were:
- A need to stimulate sales of IP-based equipment
- A better focus on IP-enabled solutions as CCTV tools
- Consideration of the security of systems using IP-based devices
- Terminology and working practices designed for security installers
- Consideration of 'closed circuit' networks to increase security (especially with BS8418)
- Training and support for installers to become a focus

However, the overall feedback showed that manufacturers preferred to concentrate on the IT-related benefits of such systems, and did not see the emphasis on security and closed circuits as a positive step. Rather than promote IP-based CCTV devices and systems as security tools, it was felt the best way forward was to continue much as at present, offering support and training where large projects exist. Installers in the commodity market, seeking to use the devices in hybrid or smaller solutions, should seek some training and learn to support the systems themselves.

The obvious conflict between using networks for user-requested benefits and the security requirements associated with new standards such as BS8418 did not seem to be an issue, which is surprising given that all attendees represented companies within the CCTV security sector. Also, there seemed to be little concern that the overall security of systems will be reduced by end users seeking IT-based solutions rather than a pure security system.

Feedback

Our feeling was that even within companies from the CCTV sector, there are varying views of the way in which IP technology should be used and developed, according to the background of the individual being asked. As such, we would like to clarify a few points, and so have attached a brief questionnaire on the opinions put forward at the forum. We would be grateful if you could spend a few moments responding to this, as we need to ensure that some of the grey areas are clarified. Also, if you have any additional comments, please feel free to contact me.

Commodity-type sales (smaller solutions and hybrid systems)

1: Is the acceptance of IP technology in CCTV systems at a satisfactory level amongst security installers?

2: Is the acceptance of IP technology in CCTV systems at a satisfactory level amongst end users?

3: Do you see greater growth through installers working over existing networks or on closed circuit hybrid solutions?

4: Should there a common approach to IP-enabled device configuration and installation?

5: Should IP-enabled devices be presented to installers as CCTV devices or as IT devices?

6: Who should be responsible for initial training, and at what level should it be set?

7: What level of support is your company willing to offer?

8: What balance should be gained between security and additional functionality of systems?

Project-based systems

1: Is the acceptance of IP technology in CCTV systems at a satisfactory level amongst security installers?

2: Is the acceptance of IP technology in CCTV systems at a satisfactory level amongst end users?

3: Do end users have enough focus on the main purpose of the system; i.e. site security?

4: Is there a danger that systems over networks might be consider less secure than is required for security-based standards (such as 8418)?

5: Where do you IP-enabled products and systems sit, with regard to being security products or building management products?

Many thanks for your help in this. We will circulate the feedback and any further comments received in the very near future.

Regards

Pete Conway