

## Next generation CCTV surveillance

Tan Boon Chin, Senior Vice President, Systems Integration Group, NEC Solutions Asia Pacific, discusses the current and future capabilities of integrated video surveillance solutions.

Interview: James Smith.

**T**he prompt investigative response to the 7th July bombings in London last year, and the highly visible role that CCTV was seen to play in piecing together the chain of events preceding the attack, have powerfully demonstrated both the need and value of visual surveillance technology as part of a society's defence against terrorist attack. The fact that the technology has a 'dual use' to monitor traditional crime, only serves to underline the flexibility of visual surveillance as a tool to enhance a community's security.

"The London bombings really served to show what the current generation of CCTV technology is capable of, but the fact remains that they were chasing the people after the event and not before it happened. Obviously from a security point of view it is better late than never, but you want to be in a position to preempt the attacks. Security agencies are now looking to see how they can get better leverage out of their surveillance infrastructure. You are always looking to know before the event, to prevent harm," says Tan Boon Chin, Senior Vice President, Systems Integration Group, NEC Solutions Asia Pacific.

Although interest in the current and future functionality of CCTV technologies has surged, NEC has been a longterm innovator in the field of visual surveillance solutions, most recently providing state-of-the-art deployments in Britain's Houses of Parliament, as well as at Helsinki airport.

"Our involvement in CCTV builds on the historical



Tan Boon Chin, Senior Vice President, Systems Integration Group, NEC Solutions Asia Pacific

background that we are very strong in image processing, very strong, and as a result so we are able to research very deeply into CCTV and video processing," Tan continues. "Whilst we didn't anticipate that CCTV would be in such hot demand, we have turned out to be ideally placed to meet that demand because of our strength in the underlying technology of image processing."

"I suppose our approach was to understand the dynamics behind why there is such a need and based on that and this product was researched for a number of years before it was brought to market," he adds. "Following the 7th July attacks in London last year, the need for a new generation of CCTV solutions has escalated, so it has been a question of NEC finding itself in the right place at the right time in order to help government agencies respond to the heightened threats."

NEC's innovation was to uncover a series of algorithms,

out of its Californian research laboratory, that could identify a series of behaviours, that when taken together provide a degree of insight into the likely intentions of those being monitored through an existing CCTV network.

Because the visual analytics is software-driven, the solution can be integrated into an existing CCTV infrastructure without requiring a wholesale redeployment of cameras: "CCTV already exists; it's not a new invention. So our solution has been engineered to work on all existing CCTV platforms. We plug into your existing solution, and we do not specify how many frames a second you have to run. We are very focused on trying to reduce the capital investment of the end user," says Tan.

"Situational awareness and analysis is what we aspire to. The feedback from the various end-users we interact with around the globe, everyone faces the same problem," Tan explains. "They tell us that they

You want to be in a position to preempt the attacks. Security agencies are now looking to see how they can get better leverage out of their surveillance infrastructure

want to know, to predict, to prevent, rather than just respond in the aftermath. Ultimately it is a question of the more they know upfront, the more they can do to make sure that the worst case scenario doesn't happen."

Currently NEC's Vidient SmartCatch solution has reached what Tan refers to as a 'second stage', where users are able to generate alerts based on behaviour. This enables security agencies in the region to enhance the functionality and improve the user feel of visual surveillance solutions, transforming CCTV from being a visual record to a real-time threat management tool.

"From our experience at NEC, when you are working on such important and sensitive projects it is important to be a partner for the end-user. You need to walk together with an implementing organisation, and mature together. It is not a single step, because over time the technology improves, and the terrorists also get smarter. This is why we focus on being a longterm partner with the law enforcer, rather than the traditional vendor/buyer relationship, which is more limiting."

### Meta-CCTV

"By building stakeholder relationships with our end-users we are able to better align our own research and development activities with the current and future requirements of government organisations," reveals Tan. "For example, some of the requests we have had from police agencies ask us to go beyond the distribution of video alerts - they want the

software to be more sophisticated, and to trigger a series of escalating actions. For example a parking violation would lead to a zoom-in on the licence plate number, a zoom-in on the driver, and then subsequent cross-referencing of the facial biometric with the car licensing records."

"They want all this to be automated, and obviously this would require a huge array of cameras," he continues. "But the attitude of security agencies is that they want to be able to set their requirements, and then have their partners on the technology side will come back to them with solutions to these requirements."

"At the end of the day security agencies want intelligence; they want more than alerts, they want CCTV information to be distributed along additional, relevant data that has been pulled in from across government. They want to build up a sense of context as quickly as possible," notes Tan. "There is only so much value to be derived from knowing that someone is lingering. You want to be in a position to assess what happens next. This is really about finding patterns, and that requires a level of insight goes beyond alerts, and which is based on experience and case studies and solid research."

You want to be in  
a position to assess  
what happens next

Tan accepts that no single technology can address all the requirements of today's security agencies, but he also believes that by gathering the requirements of security agencies in the region NEC can channel this feedback to their researchers, and then develop a roadmap to progressively address these needs.

"We currently provide alerts based on certain behavioural triggers. Although this is not yet linked to biometric identification, the technology has really developed very dramatically since the 9/11 attacks in the United States, and I see no slackening in the pace of development in the current high-risk environment."

Tan refers to last year's WTO meetings in Hong Kong, where it was clear that a high proportion of the trouble was caused by a small hardcore of protesters who were known to the global security community.

"I think the parameters of future developments of the technology are becoming more obvious," he argues. "If it is quite clear that the same set of people is involved, then you can build a database so that you know who to look out for. In the case of the WTO meetings it seems to be quite repetitive, with them following the venue of the meetings. This is where I think the technology is headed, with much tighter integration to existing government databases."

### Policy decisions

According to Tan the future roll-out of CCTV will also require a greater degree of coordination amongst end-

users themselves, and potentially the development of policies to enable security agencies to leverage the infrastructure of other operators, such as transport operators, in real time.

"I believe that because traditionally the police are the main user of CCTV they are probably best-placed to formulate policy, and involve other government departments as necessary," he suggests. "I think security agencies in the region have learned from the experiences of 9/11, Madrid, London and Bali. Singapore never had a single body to manage homeland security, but after 9/11 they were quick to see the need for such a taskforce. I believe that around the region this will also extend to ensuring adequate oversight of CCTV policy."

"Ultimately it comes down to the value of what it is you are protecting. If you don't believe in the value of security then even the smallest camera is expensive, but if you are a firm believer in security then I don't think that money is an issue," Tan concludes. "There is no escaping the fact that security can cost a lot of money, create a lot of inconvenience and require a lot of different parties to work together. If you are responsible for preserving the security of a city, then the impact of a terrorist attack getting through might be measured in the billions of dollars. It's not about whether CCTV is cheap or expensive - it's really a question of whether you need it."

**Know More:**  
**NEC Solutions Asia Pacific:**  
[www.nec.com.sg/ap](http://www.nec.com.sg/ap)