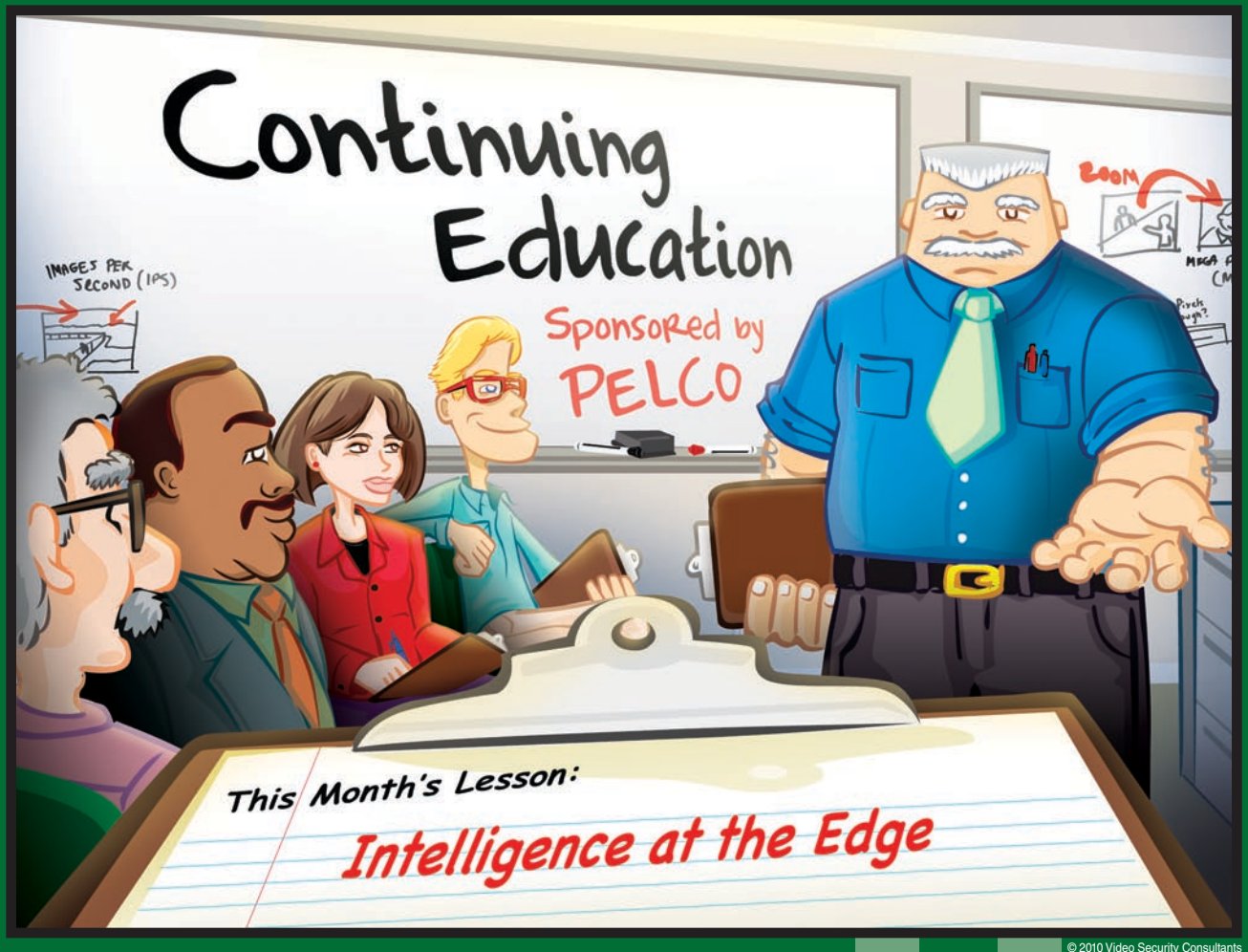
Advanced Video for D.U.M.I.E.S.

Dealers ▪ Users ▪ Managers ▪ Installers ▪ Engineers ▪ Salespeople



Part 3 of 4

Brought to You by PELCO by Schneider Electric

Presented by SECURITY SALES & INTEGRATION

Pushing Video to the Cutting Edge

Placing more intelligence within so-called edge devices is allowing video surveillance systems to place fewer demands on network resources. Better understand and deploy solutions based on this new approach to recording, storage and analytics.

Illustration by Jerry King

BY DAVID JUNIO

Welcome to Part 3 of the 2010 run of *SECURITY SALES & INTEGRATION*'s acclaimed "D.U.M.I.E.S." series: "Advanced Video for D.U.M.I.E.S." Brought to you by Pelco, this four-part course has been designed to educate readers about recent advances in technology and systems that are likely to shape this decade's progression of the video surveillance industry. "D.U.M.I.E.S." stands for dealers, users, managers, installers, engineers and salespeople.

Part 1 of this year's series (see "Redefining High Definition" in the March issue) covered alternate methods of achieving high quality HD video surveillance, including HDcctv and its ability to do so without the need for IP and/or megapixel networked cameras. The article looked at the technology, the organization championing it, how it compares to megapixel, its pros and cons, and its potential in the marketplace.

Part 2 then explored the brains that tie together and facilitate control of today's sophisticated networked video surveillance systems — video management systems/software (VMS). The piece discussed how VMS platforms relate to scalability, hybrid solutions, analytics, remote capabilities, integration, troubleshooting, return on investment (ROI) and total cost of ownership (TCO) metrics.

Now with the third installment, we explore the advent of so-called "edge" devices, in which more processing power, storage and other capabilities are located within surveillance cameras themselves. We'll investigate the pros and cons of this type of topology, and how it affects system design, selection and deployment.

©iStockphoto.com/Nicholas Moore

Studies have shown humans can effectively watch nine to 12 cameras for only 15 minutes. Thus relying on a computer for continuous video surveillance monitoring may be the best method, and video analytics is the software enabling that computer to perform this task.

ANALYTICS LESSEN OPERATOR BURDEN

First we need to define *intelligent video* because it is at the root of pushing higher levels of technology to the edge. The fact is it isn't so much intelligence in the pure sense of the word because it is really only software. *Analytics* is the more accurate term because that is what the software actually does: it analyzes the video.

Video analytics is the practice of using computers to automatically identify things of interest without an operator having to view the video. The software extracts objects and events from surveillance video in real-time and alerts the operator about certain occurrences according to a predefined set of rules or patterns. The system does this by establishing a background or fixed pattern and then goes about identifying any changes. Using sophisticated algorithms, video analytics can perform a number of different tasks by monitoring a digitized security video feed. The software examines the image presented by the video feed, down to the littlest pixel. The analytics can then detect even minor changes in the image.

From a basic vantage point, there are primarily two types of installed video surveillance systems: manned and unmanned.

The unmanned system simply relies on after-the-fact functionality. This means that after an incident, whether it is a robbery, vandalism, mugging or whatever, the operator will review the video in order to try to solve the issue. This type of system operation does not provide the ability to respond in real-time.

One of the most compelling concepts to a customer is the notion that the technology they invest in might actually be able to catch a criminal and potentially stop a crime from occurring. However, in an unmanned deployment, the system only records the event for later review. We know it is very satisfying to a security provider when the thief actually gets apprehended. But the only chance a provider has to help catch a perpetrator is to install *proactive* rather than *reactive* solutions.

So how do you make a solution proactive? Somebody or something needs to watch the video and alert an operator or security guard in real-time as the crime is underway.

In a manned system scenario, the operator is relied upon to provide the real-time response. This means one operator could be watching as many as 16 to 32 cameras, and critical incidents will invariably be missed. Studies have shown that humans can effectively watch nine to 12 cameras for only 15 minutes.

The fiscal outlay associated with continuous monitoring requires a major investment in resources, and the result is neither scalable nor profitable given current labor costs. On the other hand, a computer never blinks, sleeps, takes a break or becomes distracted. It is always active and has the speed to notify someone in time to react accordingly.

But computers are not perfect and still need to be verified by humans to make a definitive assessment. Still, many would agree that using a computer for continuous video surveillance monitoring is the best method, and video analytics software is what enables the computer to perform this task.

CASE FOR INTELLIGENCE AT THE EDGE

Now that we have decided to go with analytics, where should the application reside? There are some compelling arguments for having the analytics centralized in the DVR or NVR.

For example, if we look at the alternative of placing the analytics on the edge with *smart cameras* capable

of storing and analyzing video, you will generally have to throw away existing cameras or purchase encoders with built-in analytics. The majority of cameras deployed in the field today are analog and none of them support analytics. Furthermore, most IP cameras do not have the capability to be upgraded with analytics. As such, even if you deployed new IP cameras six months ago, those too would have to be replaced.

Another advantage of consolidating video analytics at the DVR/NVR is that it can be done more inexpensively. Smart cameras are usually a few hundred dollars more than traditional IP cameras. Smart DVRs/NVRs systems that consolidate both analytics and video recording are usually about $1,000 more than a basic DVR. Replacing existing cameras with smart cameras can easily add up to an expenditure of $5,000 to $15,000 or more.

A final argument in favor of centralized analytics would be maintenance and upgrade costs. Because everything is central to one point, when the software needs upgrading it can be done once, thereby saving time and money.

Despite those issues, there are numerous reasons to move the analytics to the edge — plus, it's the main focus of this article! The most scalable, cost-effective (once TCO and ROI is fleshed out) and flexible architecture is based on processing as much of the video as possible inside the smart network cameras or video encoders. This architecture would be a good match for any size surveillance system running from one to thousands of cameras.

A major justification for an edge approach is minimized bandwidth usage. Cameras or encoders can be programmed to only transmit video when an alarm is dectected such as motion, area entered, line crossed or many other incidents defined in the analytics. This dramatically reduces network bandwidth usage. Less video being streamed to the system also means less storage costs. This would have a major impact on those companies that require 12 months of video archiving.

When using analytics it is necessary to draw trip lines, enclosed areas, direction flow and other types of trip points or virtual lines for the alarms. Proper camera placement is key.

Another argument for edge-based system design is lower server costs. As mentioned earlier, when analytics is added to the server it requires either more processing power or fewer video streams due to the horsepower necessary to get all that work done. When cameras do the processing, servers can handle more video streams.

Improved analysis of the video is another upside when deploying analytics on the edge. When the network cameras process raw video data before it is compressed, the quality of analysis is greatly enhanced. The server processing power is no longer consumed by decompressing or decoding the video packets prior to processing, which would otherwise dramatically increase the number of servers required to process transmissions.

To sum up, by moving the analytics to the edge we have seen that it can reduce bandwidth, storage and server size. These reductions are reflected in the costs of the system. With less bandwidth it is possible to use less expensive network equipment. Also, the servers would need less power and fewer hard drives to do all the work and storage. These factors, in turn, lessen environmental demands since the system's head-end requires less space and its cooling needs are not as great.

ALGORITHMS TRIGGER ALERTS

Now that we have decided to move the analytics to the edge, what other considerations are there? When using analytics it is necessary to draw trip lines, enclosed areas, direction flow and other types of trip points or virtual lines for the alarms. Because these points are key to the analytics, camera placement can be a big factor.

Camera positioning requirements can have a significant impact on the cost and design of video analytic systems. This is true whether you are analyzing license plates, people, faces or intruders.

As an example, an individual monitoring a room entryway would want the camera to offer a low angle on the door from about 10 to 20 feet away. In video analytics applications designed to identify tailgating situations, where an authorized person is granted access but is followed through the entry or exit by an unauthorized person, the camera should be mounted directly overhead. However, while this would provide the optimum angle for certain video analytics, it would be useless to the human operator.

Video analytics rely on patterns or specific scenes or layouts. To accomplish this, first the software needs to calibrate the scene. This is done through the process of detecting changes and extracting those that are relevant. Pixels that do not change are called *background pixels*. Pixels that have changed are referred to as *foreground pixels* (using technology called *background subtraction*). Those changes are detected within an established detection zone according to the set parameters.

Another step in the analytics process is classification, which starts to determine things like the size of a given object and what shape it has. This is where some the camera's perspective or field of view can create some challenges due to varying sizes and orientations of objects.

The difficulty arises because objects closer to the camera appear bigger than those farther away. In cases such as the example of the anti-tailgating placement, with a camera mounted directly above and looking down at the subject, the perspective problem is averted.

REAL-WORLD APPLICATION EXAMPLES

So far we have talked about the two main approaches to deploying analytics, centralized vs. edge, but have not been too specific about the different types that are available. There are about 20 vendors providing analytics solutions to the security industry. Many of them have tailored or optimized their analytics to meet the needs of targeted market applications.

There are a few types of analytics that have been implemented very effectively and achieved a low incidence of false alarms. License plate recognition (LPR) is a prime example. What helps the technology excel in this application is that the subject — license plates — tend to have very consistent sizes and shapes. Also, with the exceptions of large trucks, they are located at a specific height and are required to be lit up at all times. So LPR is one type of installation with minimal variables and mostly impervious to lighting conditions that could trigger false readings.

Similar to the anti-tailgating application, people counting can be done fairly accurately if the camera is placed directly overhead pointing down. This eliminates having to take into account angles and perspectives that can be difficult to set up. There can still be some errors due to the size and shape of people varying from very thin to very heavy.

Another feature that has been shown to be effective and reduce manpower is the "wrong way" or airport analytic. This is an application where, so long as everyone is moving toward the camera or "exiting," things work out just fine. As soon as the analytics detect someone going the opposite direction or back toward the airport, an incident is generated.

Some analytics have also been successfully used for purposes both related to and separate and apart from security functions, such as discouraging loitering activity. In this usage, if an individual is hanging around and perhaps looking for an illicit or harmful opportunity, the system can alert the operator.

The retail industry has taken a different approach with loitering — it wants people hanging out in its stores. Some retailers are using this feature to see how long people spend at a specific display or with a particular promotional item. Observing and measuring how long the average person stays engaged in this manner helps the store determine the effectiveness of its display or marketing technique.

One more interesting application worth mentioning is detecting camera sabotage or tampering. In this situation, an incident is generated when the fixed scene has changed for a specific amount of time. Not only will covering or painting the lens create an alert but so too will turning the camera or any other unexpected change.

We have addressed some practical and effective analytics applications working in the real world field today. However, because there are many dif-

Centralized Vs. Edge System Architecture Comparison

ARCHITECTURE	PROS	CONS
Analytics on Server / Storage on Server	Reuse existing cameras	High bandwidth
	Easy analytics upgrade	Server outage multiple cameras lost
	Easy storage increase	Increased server power needed
	Flexibility reassigning analytics	Video is compressed
	More vendor options	Increased cooling costs
	Access stored/recorded	Video supports fewer cameras
Analytics on Edge / Storage on Server	Cost included with camera	Server outage multiple cameras lost
	Lower bandwidth	More difficult upgrades
	Higher accuracy on raw video	Increased cooling costs
	Less processing power	Not scalable or flexible
	More flexible architecture	
Analytics on Edge / Storage on Edge	Lower bandwidth	Upgrade costs higher
	Higher accuracy on raw video	More complex installation
	Less processing power	Network losses, lose access
	Lower Storage costs	Limited vendors
	Lower total costs	Limited access to recorded video

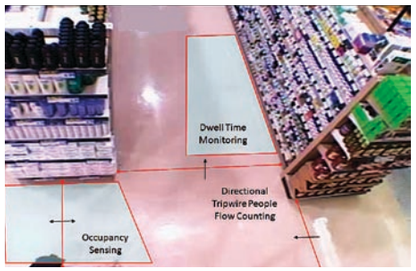
There are numerous advantages to moving analytics to the edge. For example, having the processing work be done on the edge allows for a much more flexible system. Another justification is lower overall cost due to reducing the total system hardware.

ferent types of analytics, we cannot go over each one specifically.

NEGOTIATING THE ENVIRONMENT

When it comes to configuring an analytics system, there are two categories to consider: indoor and outdoor.

Indoor configurations tend to be the easiest and encounter the least false alarm issues. In most cases there is more flexibility where the cameras are positioned. They can be directly overhead or even located at average height. And of course, indoor applications are not subject to weather concerns such as snow, rain or fog. Another problematic false alarm factor, lighting, can also be easily controlled within an indoor environment. An important reality, however, regarding indoor detection is if the incident is missed the subject is already inside the facility where they could possibly do more damage.



Retailers are using video analytics to observe and measure the effectiveness of their display or marketing techniques.

Once we move outside, things become much more difficult. The first issue to consider is weather. Obviously, this is a dynamic that cannot be controlled but by understanding the camera and the analytics' shortcomings, any adverse effects can hopefully be minimized.

As seasons change over a period of weeks or months, a video analytic system's false alerts can start rising considerably due to changes in the environment and the position of the sun. This can suddenly and surprisingly cause major problems. Some industry experts estimate the false alarm rate as one per hour per camera. Even with only a 16-camera system this could become expensive and annoying.

The problem of increased false alerts is compounded by the consequence of users potentially losing confidence and trust in the technology itself. If your perimeter surveillance one day stops functioning properly, you now have a serious flaw in your overall security system.

SETTING REALISTIC EXPECTATIONS

Implementing analytics will continue to become simpler. But for now there are tricks to optimization, and users should be prepared to work with a system for several weeks.

As alluded to in the previous section, the challenges presented by changes in the environment (especially outdoors) such as rolling clouds, trees swaying, shadows and reflections off puddles, have precluded analytics vendors from nailing down any type of performance standards. At best, installers can work to optimize analytics performance for a given installation, and be wary of any vendor that claims its analytics software has self-learning capability.

Setting expectations is everything. It's important not to believe all the ridiculous hype and nonsense about what analytics can deliver. When integrators are selling or promoting video analytics there are a few tips that will make the process much easier.

First, have clearly defined goals for what the system can and will do. Next, have a manufacturer's representative go over the requirements with you that will allow the video analytics system to perform as promised. Also make sure the installer is fully trained in programming the system. Another thing you can do is use the manufacturer's demo system to show the client how the technology works, and what it can and cannot do.

Make sure to have at least one person at the customer site who knows how to maintain and calibrate the system. If the integrator needs to be constantly called out to recalibrate it due to changes in the environment — or for whatever reason — the customer could get frustrated with the system. Finally, demonstrate to the client the fully functioning system with their own operators testing and using it.

COSTS, CAPABILITIES ARE IMPROVING

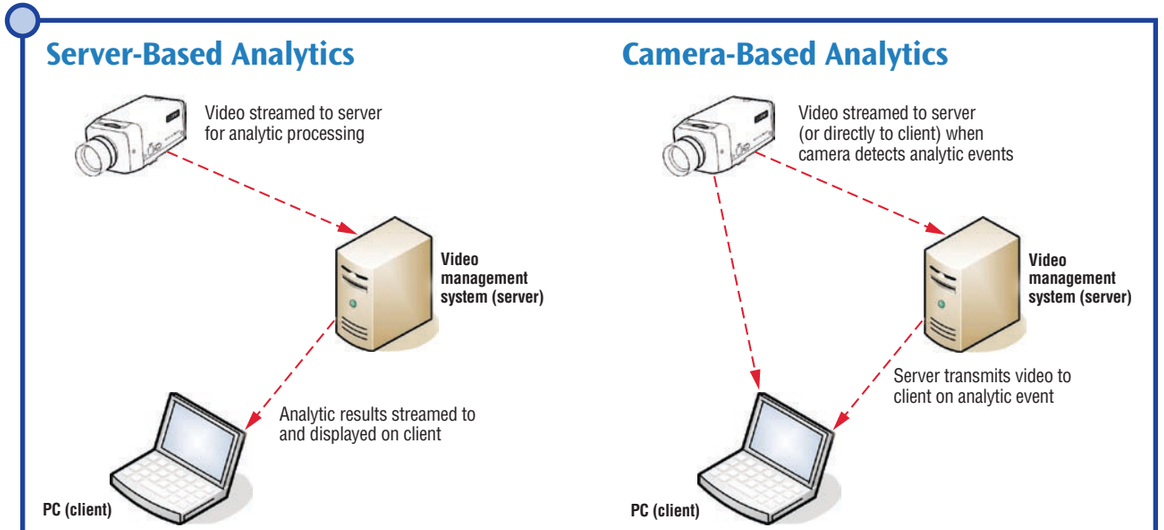
What is the future of video analytics? Most in the security business believe the technology will mature during the next few years. As it does so it should easily and quickly be usable on at least one-third of cameras as the benefits are clear. A few key developments can be identified that will impact architectures in the future and continue the push video intelligence to the edge.

Processing power in edge devices is growing rapidly. In some cases, manufacturers of cameras intended to support analytics are now building them with coprocessors or second processor chips in order to handle the extra horsepower requirements. This results in a favorable dollar/per mega-image/per second ratio for edge device processors that, when compared to processors on the server, will influence pushing analytics to the edge.

To ensure the system meets both immediate and long-term needs, the installation should be scalable and based on open standards. The architecture should be one that minimizes the risk of system failure and downtime. It should scale effortlessly from a few to many cameras and intelligently distribute processing to different system components.

If camera resolutions continue to increase, with the advent of high definition cameras, and existing encoding technologies are retained, then the bandwidth requirements to transmit video streams to the server will likewise increase. Storage on the camera or edge device is one way to reduce those bandwidth issues. Capacity of flash memory on edge devices is steadily increasing. The dollar-per-byte ratio for standalone storage devices is significantly cheaper when compared to storage at the server.

Visit the Special Reports section at www.securitysales.com to access more than five years' of "D.U.M.I.E.S." archives.



Compelling arguments for having video analytics centralized in a DVR/NVR (*left*) include not having to purchase expensive *smart* cameras or encoders with built-in analytics to replace existing cameras. However, justifications for an edge approach (*right*) include minimized bandwidth usage, lower server costs and superior analysis capabilities.

One snag that must be mentioned is that, at this time, support for access to recorded video on edge devices via video management software (VMS) is poor. But more and more VMS vendors are beginning to support this capability.

TRENDS SUPPORT EDGE APPROACH

As we have discussed, functional and economic benefits are hastening the trend of placing more recording capability and intelligence on the edge of networked video surveillance systems. In addition, analytics will continue to grow and become a more viable and reliable tool for standard security, security-related and business-based uses.

Finding ways to reduce bandwidth requirements, such as transmitting video streams only when an incident occurs, are becoming more and more a necessity. This, in turn, dramatically cuts down on the amount of video needed to be monitored and reviewed. In the case of license plate identification, for instance, only the snapshot needs to be transmitted instead of the entire video stream. Also when cameras do the processing, servers can handle more video streams.

Another feature at the edge is that the analytics can process raw or uncompressed video. Being able to do this greatly raises the quality of analysis and thereby minimizes false alarm incidents and customer frustration. All of these benefits enhance the TCO and ROI propositions for the customer.

While these key trends may point to a gradual shift toward edge-based analytics and storage, it's the security objectives that will drive end users to an appropriate architecture. Security directors will have to consult closely with their systems integrator partners to analyze the tradeoffs involved and choose the solution that best meets their requirements.

As customers see the benefits in these analytic tools improve, the business opportunity will expand. As it stands now, those with specialized needs will lead the market in their use of video analytics for targeted applications. As time goes on and the technology improves, it will become apparent to the majority of commercial, retail, industrial and government clients that intelligent video technology can help increase the efficiency and effectiveness of their security staffs. ■

Dave Junio (davejunio@gmail.com) has more than 16 years' experience in video security systems performing installation, system design, curriculum development and training. He has a BSEE and was a design engineer for 15 years.

Next Up for 'D.U.M.I.E.S.': IR Lighting and Thermal Imaging

Be sure to check out the October issue of *SSI* for Part 4 of 2010's "Advanced Video for D.U.M.I.E.S." series. The fourth installment will explore the impact infrared (IR) lighting as well as thermal imaging is having on the video surveillance marketplace. In addition to the application opportunities these technologies offer, end users' interest is being piqued by how IR and thermal imaging reduces light pollution.

Enterprise Video Performance for All

Easy Installation. Even Easier to Use.

You shouldn't have to be a huge enterprise to enjoy the benefits of enterprise IP video performance – robust recording, full HD support, redundancy and reliability. That's why Pelco is introducing the EnduraXpress network appliance. As a network appliance, EnduraXpress removes the complexity of deploying and configuring an IP video solution. The EE500 Series combines the performance, reliability, and robustness of an enterprise-class, mission-critical storage management system into a single appliance. By integrating the recording server, recording software, and storage array into one highly optimized chassis EnduraXpress easily supports standard resolution and megapixel camera recording workloads.

www.pelco.com
1-800-289-9100

PELCO
by Schneider Electric

www.securitysales.com/freeinfo/18167