WHITE PAPER

Ensure Nonstop IP Surveillance with an Optimized Industrial Ethernet Network

Ray Hsu
Moxa Product Manager

Alvis Chen
Moxa Product Manager

MOXA®

Introduction

What comes to mind when you hear the term "mission-critical infrastructure?" Depending on your experience and background, you might think of oil and gas production fields, railway station monitoring systems, power generation facilities, or highway traffic systems, to name a few. The term "mission-critical" should not be taken lightly since it is used to describe networks that, once they experience instability or transmission problems, could result in serious damage to equipment and facilities, or even injuries or loss of life. In recent years, video surveillance systems have played an increasingly important role in ensuring the reliability and safety of mission-critical infrastructures around the world.

Video Surveillance is Now Standard for Industrial Mission-Critical Infrastructures

Video surveillance systems use "images" to allow security personnel to monitor an entire facility, or even a collection of facilities, from a central location, 24 hours a day, 7 days a week, instead of hiring a large contingent of security guards to man a large number of guard stations. Surveillance systems are certainly not new, but in recent years there has been a big change in how they are implemented. A basic system might simply save all of the images onto a hard drive for future analysis when the need arises. More advanced systems, however, use intelligent cameras that support extremely sophisticated features, including the ability to recognize scene changes in critical areas (e.g., if someone leaves a backpack unattended in an airport), or identify specific types of objects. It goes without saying that a video surveillance system is already a must have standard system for any type of mission-critical facility, both for monitoring events in real time, and for providing a library of images that will be available for future analysis.

Based on a 2014 IHS white paper (Video Surveillance & Storage: Opportunities at the Intersection of IT and Physical Security), the surveillance market will likely see a CAGR (compound annual growth rate) of 14.8% between 2013 and 2018. The forecast for 2018 is that the entire market will generate up to USD 25.6 billion in revenue. Network video surveillance equipment is expected to make up the bulk of the market share compared with traditional analog video surveillance equipment. For example, in 2013, the Gulf region's largest gas production projects spent € 0.8 million for camera surveillance systems alone.

Released on May 25, 2015

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com. You may also contact Moxa by email at info@moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

Challenges of IP-Based Video Surveillance Network Design

Commercial-grade video surveillance systems are used in almost every public facility, including supermarkets, offices, and schools. But when it comes to installing a video surveillance system in a mission-critical industrial application, you need to pay special attention to the following issues:

Data Transmission vs. Video Transmission

Transmitting video streams presents unique challenges that you may not need to consider with basic data transmissions. At the IP packet level, data and video use the same TCP/IP technology to ensure large scale, fast data transmission. But at the application level, video surveillance normally involves establishing and managing network access between multiple devices. For example, an NVR (Network Video Recorder) and a VMS (Video Management System) operating in different control rooms may want to save or show the same video stream at the same time, while a CMS (Central Management System) may want to display images from the same video stream on a large LCD screen. For this kind of scenario, the IP camera would usually need to send the video streams separately. For the particular case shown below, the IP camera would be required to send three video streams over the Internet.

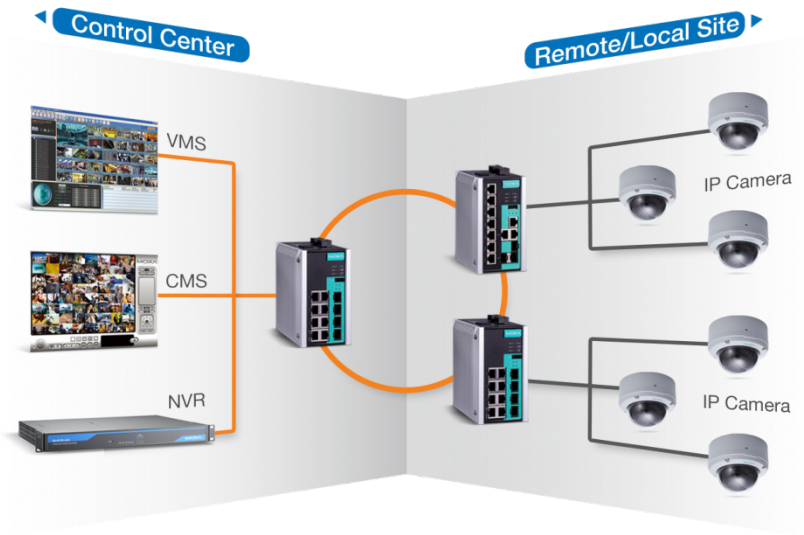


Figure 1: Network video surveillance system

As the number of cameras increases, the need to transmit so many video streams over the same network will occupy a huge amount of the backbone network's bandwidth. In order to reduce the amount of bandwidth used by all of these video streams, we normally configure video streams as "multicast" type. Multicast means that each IP camera only needs to send one video stream at a time, and uses Ethernet switches to reproduce and forward the same video stream to multiple receivers automatically. The following figures illustrate the difference in bandwidth requirements between unicast and multicast configurations. As you can see, using a multicast configuration can save an impressive amount of bandwidth for the entire network.

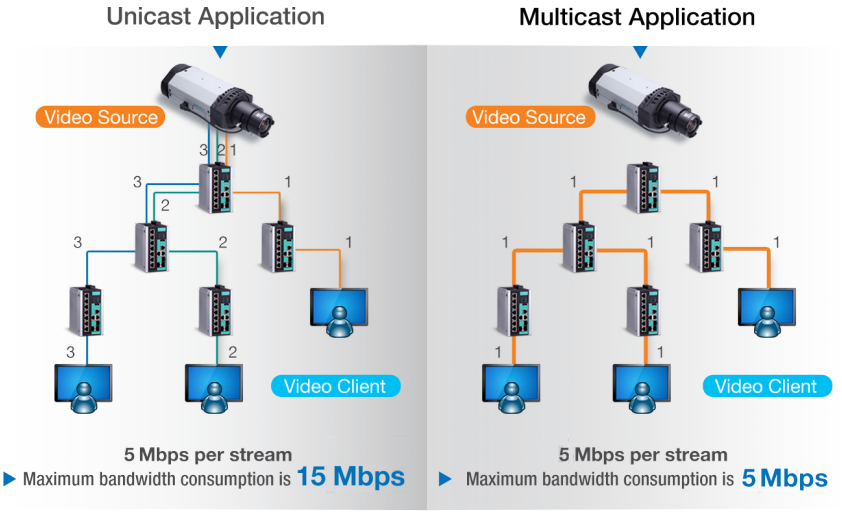


Figure 2: Comparison of unicast and multicast video transmissions

To further illustrate how multicast streaming can save bandwidth, an actual project used 400 HD IP cameras as well as 20 video clients. When configured for unicast based transmission, engineers found that the cameras and video clients could consume up to 46,000 Mbps. However, when configured for multicast streaming, the bandwidth consumption was reduced to only 2,000 Mbps.

Lack of Redundancy for Data Transmission

Most CCTV surveillance networks use a "star" or "daisy-chain" topology to connect and expand the number of IP cameras connected to the network. However, star topologies are not designed to recover from single points of failure. If only one network cable gets disconnected, or one network device crashes, that single point of failure could result in the disruption of a huge number of video streams. Some designers might recommend using "trunking" technology to aggregate multiple Ethernet ports and cables into one transmission path. In this case, if one cable is disconnected, video data will continue to be transmitted through other ports and cables. However, this design cannot prevent interruptions to data transmission due to single node failures, as would be the case if an Ethernet switch stopped working due to a power outage in the field.

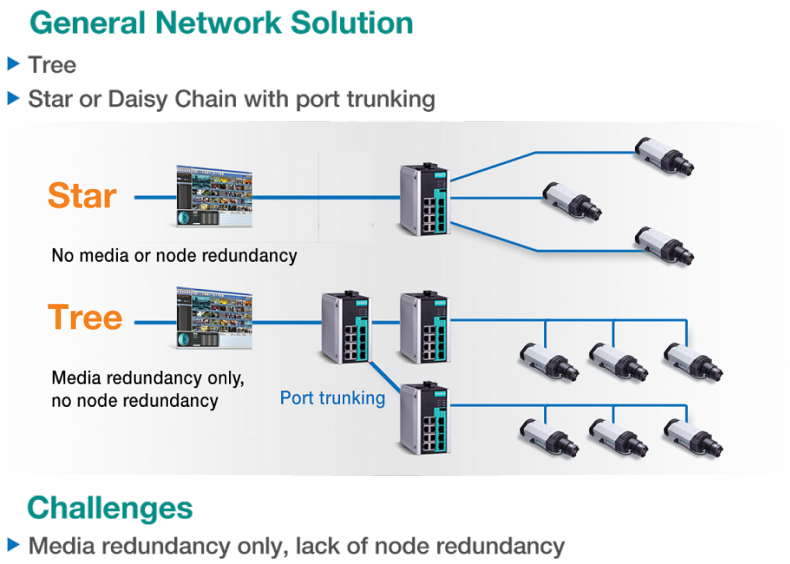


Figure 3: Challenges of tree networks, and star or daisy chain networks with port trunking.

Network Management Efficiency

As your network gets bigger, you will probably want to use network management software to monitor and manage the status of your network and network equipment. Experience has shown that if you have more than 50 Ethernet switches on a single (or extended) network, you should consider using an NMS (Network Management Software), since you can save a lot of time on network management tasks. However, there are three features you should consider when you choose an NMS for a video surveillance network:

Real-time monitoring: How fast can the NMS receive and then display alarms from large numbers of network devices? Many enterprise NMSs use traditional "polling" methods to check the status of each network device. However, with polling, the amount of time between when an alarm is triggered and the NMS notifies security personnel will increase as you add more and more devices to your network. A good industrial-grade NMS will use a "push" or "active" method to ensure that security personnel can receive alarms as soon as they're triggered. In this case, instead of requiring the NMS to continually poll devices in the field, switches installed at remote parts of the network will be smart enough to sense when an alarm is generated by a device connected to the switch, and then immediately send the alarm to the central NMS.

Visualization: When network alerts appear on your screen, how quickly can you locate the root cause? For example, when an alert is triggered, can your NMS determine if the problem is most likely due to a problem with an IP camera, a network device, or a cable? And if the problem is with a cable, how easily can you determine which port on which device it's connected to? A well designed industrial-grade NMS will make the field operator's or maintenance engineer's daily routine easier and more precise.

Integration: Intelligent systems rely on close system integration and message exchange to ensure that your NMS can determine if end devices (IP cameras, for example) are alive or not, and provide meaningful information to higher level central management systems in the control room. However, traditional network management systems focus on the network devices themselves (Ethernet switches and routers, for example); generally speaking, they don't have the capability to support message exchanges or monitoring of third party devices.

Leveraging Industrial Network Technology

For mission-critical network applications, you can consider using industrial grade network technology to overcome the challenges outlined above. Compared with an enterprise network solution, an industrial-grade solution focuses more on hardware reliability, network redundancy, and easy field management. For example, the hardware would be designed to work reliably in harsh environments, where "harsh" could refer to both cold and hot temperatures, as well as environments subject to high EMC (electromagnetic compatibility) radiated emission levels. In addition to hardware reliability, three industrial-grade network technologies that can help you optimize your mission-critical CCTV surveillance network are worth mentioning:

Fast Ring Network Recovery

As we mentioned above, "star" and "tree" topologies are prone to single point of failure events, which occur when only one cable or network device fails. For industrial networks, "rings" and "redundancy protocols" are commonly used. The illustrations below show a typical industrial ring network for a CCTV surveillance application. The Ethernet switches are configured to use RSTP (Rapid Spanning Tree Protocol). RSTP identifies a certain number of network connections as redundant, and then blocks network transmissions through those connections to avoid looping. If one of the active network cables or switches fails, RSTP activates one of the blocked connections to ensure that all of the devices connected to the network can continue to transmit data to the required locations. However, the typical recovery time for RSTP is 2 to 5 seconds. What this means is that you could lose 60 to 150 frames (assuming 30 frames per seconds) of CCTV surveillance images. However, some industrial network device manufacturers have developed proprietary ring recovery protocols that support recovery times between 20 and 50 ms, which is a much more acceptable recovery time for mission-critical CCT surveillance networks.

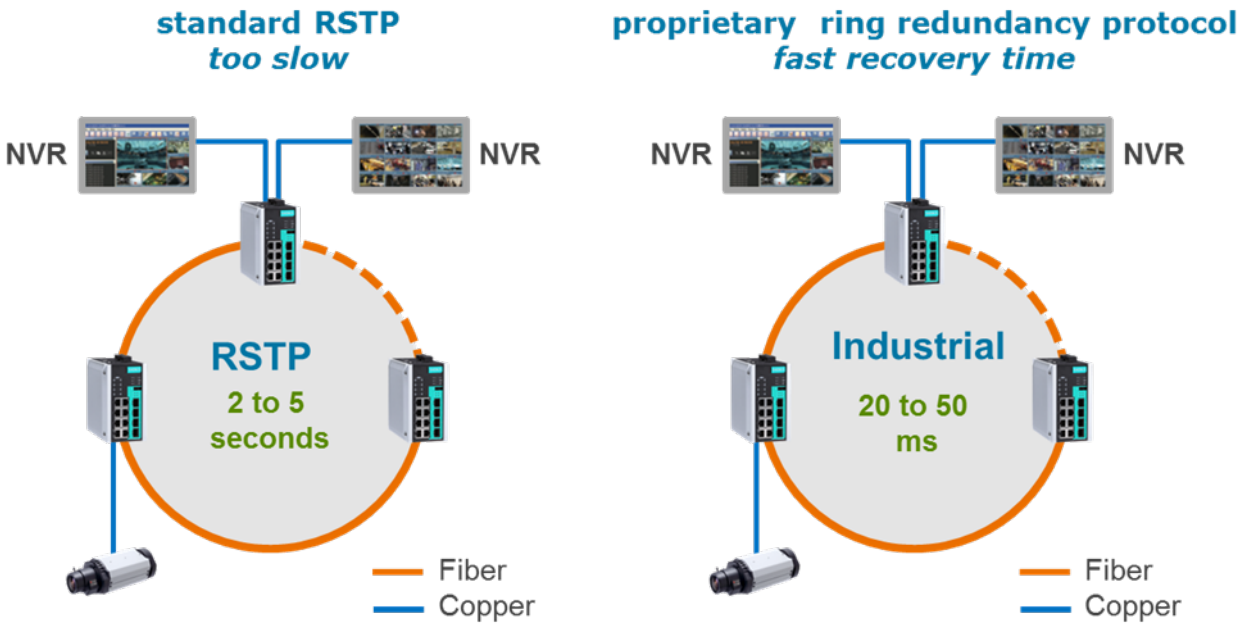


Figure 4: Mission-critical CCTV applications require an extremely fast recover time.

Optimizing Your Network for Video Stream Transmission

If your CCTV system uses multicast transmission over a redundant ring, then even if your ring redundancy protocol is able to activate backup paths in a fraction of a second when a disconnection occurs, it could still take more than 2 minutes for your multicast video streams to recover. This is because a number of different protocols—including IGMP (Internet Group Management Protocol) and PIM-DM (Protocol Independent Multicast - Dense Mode)—are implemented to transmit your video packets around the network, and these standard protocols are not designed for mission-critical applications. For example, since the IGMP protocol updates multicast group tables every 125 seconds, if a network cable gets disconnected or an Ethernet switch loses power, your multicast video streams will not be redirected to the backup path immediately. "Optimizing your network for video stream transmission" means implementing an appropriate non-standard proprietary protocol that makes up for IGMP's sluggishness. The following figures illustrate how without optimization, your multicast video

stream could be disrupted for an unacceptably long period of time, until the next multicast paths are negotiated between the network's Ethernet switches.

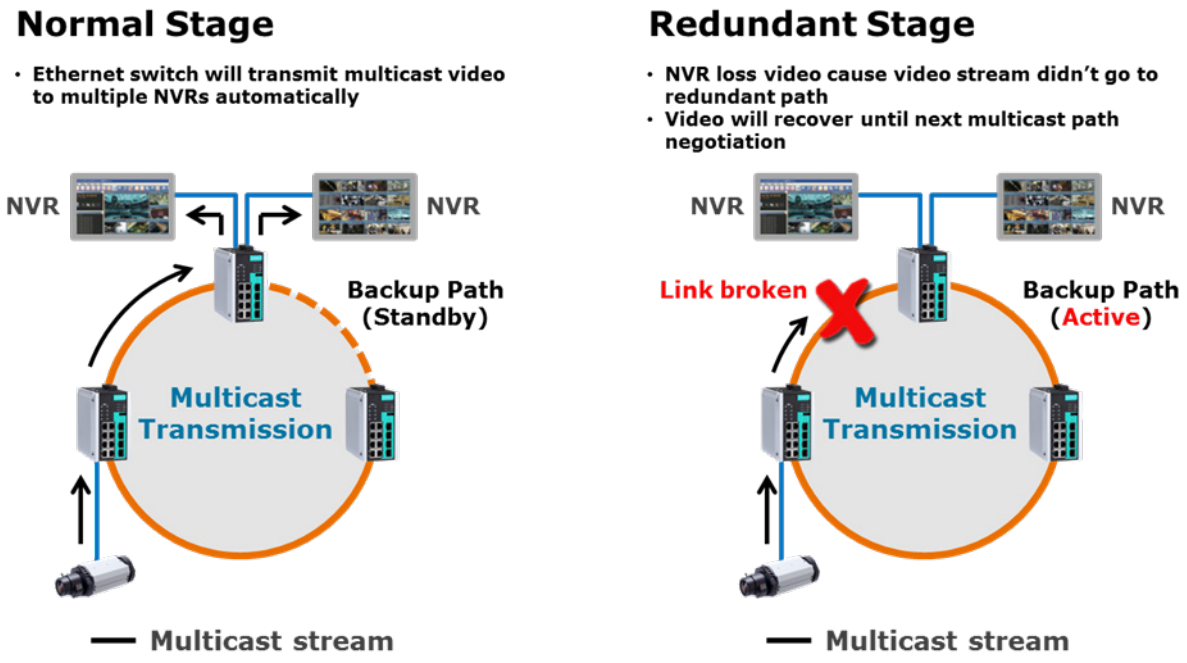


Figure 5: How multicast video streams are disrupted when using RSTP.

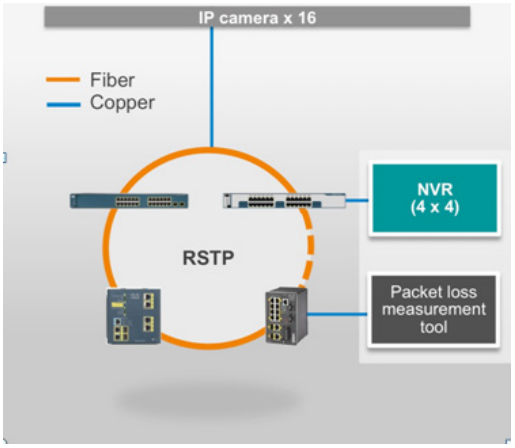
Moxa's V-ON Technology Keeps Your Video Streams Streaming

Let's take a look at some actual test data to see just how important it is to optimize your network for video streaming. The data compares recovery times between the standard RSTP redundancy protocol, and Moxa's V-ON (Video-Always-On) redundancy protocol, which is optimized for video stream transmissions.

The two surveillance networks used for the test were set up in the following way:

- 16 HD IP cameras were connected to each network
- Multicast transmission was used to transmit video streams to two NVRs
- Redundancy Protocol:
  Network 1: Traditional Ring network with RSTP redundancy protocol
  Network 2: Network with redundancy protocol optimized for video streams
- SPIRENT SPT-9000A Ethernet package measuring equipment was used to measure video stream recovery times
- Two scenarios were simulated:
  Scenario A: Media failure due to a disconnected cable
  Scenario B: Node failure due to loss of power to one Ethernet switch

Traditional Ring Network with RSTP Protocol



Moxa V-ON Enabled Ring Network

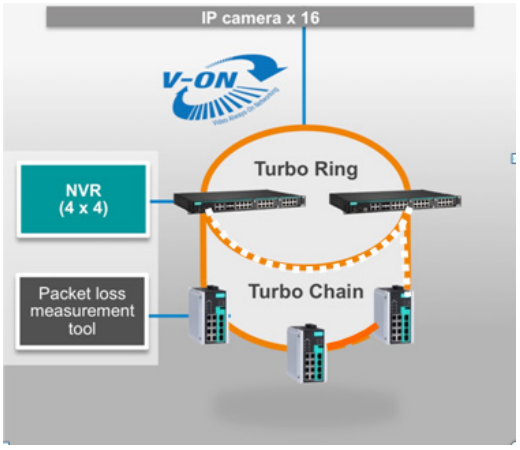


Figure 6: How Moxa's V-ON technology keeps your video streams streaming.

Video stream recovery times after media failure and node failure, with and without optimization:

		Recovery Times	
Failure Mode		**Not Optimized** (Traditional Ring Network with RSTP Protocol)	**Optimized** (Redundancy Protocol Optimized for Video Streams)
Media Failure	Min.	1,280 ms	1.8 ms
	Max.	**11,040 ms**	**37.6 ms**
	Avg.	3,620 ms	6.7 ms
Node Failure	Min.	390 ms	2.5 ms
	Max.	**63,300 ms**	**41.5 ms**
	Avg.	7,320 ms	7.9 ms

From the above data, it should be obvious that RSTP is ***not*** designed for multicast video stream redundancy. In fact, in at least one case it took more than 1 minute for the video streams to recover. Compared with the traditional RSTP protocol, when using the optimized protocol, recovery took less than 50 ms for all of the cases tested, which shows that Moxa's V-ON technology can optimize your network for video streams, therefore making your network suitable for mission-critical IP surveillance applications.

Using Network Management Software

As your network becomes bigger and you need to manage more and more network devices, finding the right network management software is essential to ensure that you can keep your network running smoothly. Here are three tips for choosing a suitable network management software solution:

- **Visualization:** Being able to clearly see the network's topology, pictures of devices connected to the network, and port numbers makes it much easier for engineers to configure, deploy, and troubleshoot network problems that arise at remote locations. Some network management software can also monitor third-party devices that support SNMP and PING. This is important, since it gives your NMS the ability to receive status updates—in real time—sent by the remote devices, eliminating the need for the NMS to wait for what could be several crucial minutes to receive important updates from the remote devices.

- **Real-time Notification:** Traditional network management software polls each device at a preconfigured frequency to determine the device's status and readings. However, as the number of devices increases, the amount of time the network management software needs to wait for a response from the devices increases as well. For this reason, your network can become real-time by using switches that can forward alarm messages to the NMS immediately when the switches receive warning messages from attached devices. The switches you use should also be able to send emails or SMS (Short Message Service) messages, and the NMS you use should be able to receive SNMP trap messages, so that it can receive messages from any switch that can send messages to the NMS.

- **Easy Integration:** SCADA systems are commonly used to remotely monitor and control all of the equipment connected to mission-critical automation system networks. In fact, as a SCADA system is required to handle more and more IP-based Ethernet connections, the network equipment itself becomes just as important as the automation equipment. Industrial network software can help out by giving the administrator the ability to integrate the SCADA system with the equipment. For example, a good NMS will support OPC server to provide network status to the SCADA system, or the SCADA system can send basic comments to control the network status. This type of deep integration is great for network administrators since it allows them to use a single system to monitor or control their entire network system, instead of needing to rely on different tools to handle different parts of the network.

Summary

With video surveillance now standard for industrial mission-critical infrastructures, it is important to choose the best technology for your network. Two of the most important aspects of this problem are the standard protocol and industrial network management.

- **Standard Protocol:** Although RSTP and IGMP are often used, both of these protocols are not optimized for mission-critical surveillance networks. In fact, your video stream transmission could hang for up to two minutes as the standard protocol responds to single point of failure events. A better choice is a new proprietary protocol designed to optimize your network for video stream transmission. Moxa's new V-ON technology is an ideal choice, since it takes up where standard protocols leave off, ensuring that your data stream transmission can recover in under 50 ms for layer 2 networks and in under 300 ms for layer 3 networks.

- **NMS:** The network management software you use can make a big difference in the success or failure of your mission-critical network. An NMS that relies on traditional "polling" technology to check the status of network devices can delay the reception of important warning messages by several minutes for networks comprised of hundreds or thousands of devices. You can save a lot of time and effort by choosing an NMS that supports visualization (allowing you to see the devices and structure of your network onscreen), real-time notification, and easy integration with SCADA systems.