INTEGRATING CAMERAS WITH TUNNEL CONTROL SYSTEMS

Tor Tybring Aralt: Norwegian Public Road Authority
Thomas Lyngtun Hansen: Norphonic AS

ABSTRACT

With many tunnels to supervise, and an increased demand from various sources for CCTV surveillance in the tunnels, we were in the need of an open system for camera control. We decided early to go for MPEG4, believing it was enough to say MPEG4 to get an open system. Unfortunately this was wrong. To get an open system we had to demand MPEG4 by RTSP (Real Time Streaming Protocol)

We also decided to develop our own video proxy, and our own video wall merged into the tunnel system.

After negotiations with several development companies, we signed a contract with Trafsys AS, who has developed the tunnel system. Both systems are the propriety of Norwegian Public road Authority, Which mean no further cost for licences.

It is no limits in the numbers of cameras that can be connected. Limits are on numbers of monitors. But how many monitors, is it possible for one or two operators look at?

Keywords: camera, tunnel automation, simplified response, monitoring tunnels.

1. INTRODUCTION

New regulations and many new tunnels have increased our need for an integrated system, taking care of both tunnel control and CCTVs. Having one system for the CCTVs and one for tunnel control makes the situation for the operator unacceptable when you have many tunnels. The operators needed to easily find the proper tunnel and the proper camera without having to remember which camera is where, and to be able to issue commands directly from the same system that controls the cameras. A complete integration of the systems was necessary.

The tunnel control system that is used in the two largest tunnel regions in Norway is a system that was developed and is owned by the Norwegian Public Road Authority. In the western region alone, it controls close to 180 tunnels. This system is based on the OPC standard as well as well-described standards for data transfer between the tunnels and the central system.

As a result of this, 16 different companies have been able to deliver the local control systems for the tunnels. A very strong development criterion was that we should be able to buy cameras through open tenders, which in turn means that only open standards have been used.

2. SPECIFICATIONS

The only open standard we could find that satisfied our needs was streaming MPEG4 delivered over RTSP (Real Time Streaming Protocol).

We discovered that just specifying MPEG4 does not ensure an open standard. The RTSP streaming protocol is an important part of the open standard. Unfortunately, the demand for an open streaming protocol prevented the use of pan/zoom/tilt functions in the cameras. This means that pan/zoom/tilt functions must be performed by the PLC systems. Keeping the system open has a larger effect on price than anything else. Also, remember that automatic
incident detection systems demand stationary cameras, and today, most of the systems demand analogue video input. This will probably change in the future, due to the fact that a high resolution digital camera contains more information than an analogue picture. It is often cheaper to by one or two extra cameras than to have a large camera house with zoom/pan/tilt functionality.

The proxy would have to be able to deliver the video stream to the specified monitors, or to a section of a monitor (on a 4-way split screen). We have prepared 4 large flat-screen televisions (42”) as a “video wall”. This is cheap to implement using one PC with four monitor outputs. Using millions of euros on a video wall today is buying yesterday’s technology for tomorrow’s use.

When a camera sends an alarm, its video output should pop up on the computer screen. From this point, the operator must be able to select a monitor or a screen section of a 4-way split monitor from the tunnel control system. It must be possible to select cameras from the tunnel control system by clicking on a camera symbol, and then to give commands by clicking on arrows for the previous or next camera. When no one is viewing the image from a camera, the video stream must be stopped.

3. CONTRACT

We signed a contract with Trafsys AS for the development of the system. This was done after long discussions with several potential suppliers. The selection was made based on the solution offered, the supplier’s know-how, and the expected price. This was not a fixed-price contract. Trafsys AS developed the current system for tunnel management and control.

4. SOLUTIONS

All the implemented solutions are in accordance with the original demands. The solutions have either been published as open source or are owned by us. When we increase the number of cameras, there are no extra licensing costs, and the implementation is easy. The largest cost of implementation is testing as this is always time consuming.

5. TECHNOLOGIES BEHIND THE SOLUTIONS

At the start of the project, MPEG4 over RTSP was beginning to emerge as a standard, but was only supported in very few commercial products. However, as the project has progressed, the number of available products supporting MPEG4 over RTSP has increased steadily. This indicates that our choice of open standards is a good one.

On the server side, there are two main applications: The streaming proxy and the video wall. All clients that are authorised to view a camera will contact the streaming proxy for access to the video stream. If no other clients are currently watching the camera, the streaming proxy will open a new connection to the camera and start receiving the video stream. The video stream will be forwarded unaltered to the client. Any clients that subsequently request the same video stream will receive an identical copy from the proxy, and no new connections will be made to the camera itself. This means that although the camera may be located at the far end of a low-bandwidth connection, it can still be viewed by multiple clients through the streaming proxy. Since the streaming proxy does not alter the video stream in any way, the main limitation on the number of concurrent connections will be imposed by the available network bandwidth.
When the last client viewing a video stream exits, the streaming proxy will disconnect from the camera in order to save bandwidth.

The video wall server runs on a PC with a quad-head video card (4 monitors at the same time). The server is controlled by a client application available to the system operators, and requests video streams from the streaming proxy in the same way a standalone client does.

The video wall is able to support up to 16 concurrent video streams, showing 4 streams on each monitor. This can be supported by current high-end desktop computer hardware. Due to the processing power required to decode the MPEG4 streams for viewing, the video wall server had a lower limit on the number of concurrent video streams than the streaming proxy, which does no encoding or decoding.

The system is based on an open-source camera proxy server, where access control has been implemented on a higher level. The proxy will also disconnect any cameras that are not being displayed on any monitor. This was necessary due to the number of cameras and to protect the network.

6. SAFETY BENEFITS OF INTEGRATING THE SYSTEMS

The system saves time by merging the video image with commands such as “FIRE HERE” – you see the fire and press a button, unless the system has already automatically done this.

**Automatic Response to Fire Alarms**

A fire extinguisher removed from its holder is regarded as a confirmed fire alarm, and proper procedures are started automatically. Operators can point at fire extinguisher alarms, press “GO TO,” and open the nearest camera to confirm the fire, or can re-open the tunnel. In the mean time the tunnel will be closed and the fire-ventilation system be running.

**Operator Response to Fire Alarms**

We realize that only a minor part of the incidents in a tunnel will be reported in a manner in which an operator can easily identify where the incident is occurring in the tunnel. If a tunnel is equipped with automatic incident detection using cameras, a camera alarm will be reported to the operator if a vehicle stops.

By selecting the alarm, the actual picture will pop up on the computer screen. The operator then has several possibilities. He can:
1) select the video wall control and view the video stream from the relevant camera on the video wall,
2) choose a neighboring camera to the left or right,
3) select the command “FIRE HERE,” or
4) turn the camera off.

Everything is Web-based and is done from the same system. Due to this, the operator can access the system from more than one computer if necessary. This is the operator’s decision. Normally, operators will be watching the system on two computers, one for the main system and one connected to the redundant system located 120 km away.

In a complex highway tunnel, there might be several different fire-ventilation and tunnel-closing scenarios/procedures. It is then important for the operator to know where a fire is
located in the tunnel. By selecting the camera nearest to the fire and the pressing the button "FIRE HERE," the appropriate ventilation and closing procedures will be activated.

The fire-plan control is then transferred down to the local automated system. The PLC system in the tunnel will then activate a predefined scenario. During a fire, we do not regard the operators as qualified to define levels of ventilation or to determine closing procedures. This must be predefined.

7.  NETWORK

This kind of system integration puts high demands on network resources and network planning. It is essential that we have redundant networks, where every kind of information/data can be transferred using all available pathways.

Previously, we would have built on telephone-style star network configurations, with one for the PLCs and one for the cameras. One error would then normally knock out one of the systems completely. By using modern routing technology and Ethernet, you build one large redundant network for everything.

In this situation, no single point of failure exists. You may still have some errors that are more critical than others, depending on how the network is built. Monitoring the network is now just as important as monitoring all the other systems in the tunnel. If you don’t discover that the redundant path is being used, then you are essentially ignoring the advantage of having a redundant path. Errors must of course be repaired quickly, but not necessarily the same night.

We feel that OSPF routers, in combination with smaller spanning three-ring networks, provide satisfactory security for the network, even when all the routers are critical for the networks below them. This could only knock out parts of the tunnel. This is equipment that rarely fails (has a high MTBF). We are now only using open and commonly-used standards. This reduces maintenance costs and is less dependent on a given producer. Producer dependency is always expensive in the long term. Producer-specific solutions would give shorter reconnect times during errors, but it does not matter if it takes 20 seconds or 1 microsecond to reconnect the network.

If you have one alarm a day or even one alarm an hour, then it the incidents are unambiguous. But what happens when you have several alarms in succession from different tunnels? What happens then? Will an alarm message with a possibility for “GO TO” provide the necessary reaction time? When one or two operators are monitoring 180 tunnels, there will be many alarms and the operator must realize which ones are significant. Many false or unimportant alarms are the operator’s biggest problem, although they do ensure that he knows his way around the system.