

The truth, the hole truth...

by Frank L. Roark & Roger L. Shaffer, Advanced Traffic Control, Inc, USA

Tunnels may have been around many, many hundreds of years, but upgrading safety equipment is still a minefield of compatibility, cost and reliability issues. What's more, the safety critical nature of the environment means that there is no room for error

Man has been building tunnels for thousands of years. In Mesopotamia, for example, as early as 2100 BC, the Sumerians, the same civilization that brought us bureaucracy, writing, and abstract mathematics, also managed to build a pedestrian tunnel under the Euphrates river. Where today's tunnel control systems employ a wide range of field equipment (overheight detectors, fire detectors, fans, lights, pumps, plus dynamic signs and signals to name a few) the 'field equipment' in the Sumerian tunnel's 'control system' would most likely have been limited to a burly Sumerian guard. In the tunnel's next significant control system iteration, that legacy Sumerian guard would have been upgraded to Hammurabi's burly Babylonian guard.

Upgrading today's tunnels still requires dealing with legacy field equipment, but it's a bit more complicated.

Upgrade issues

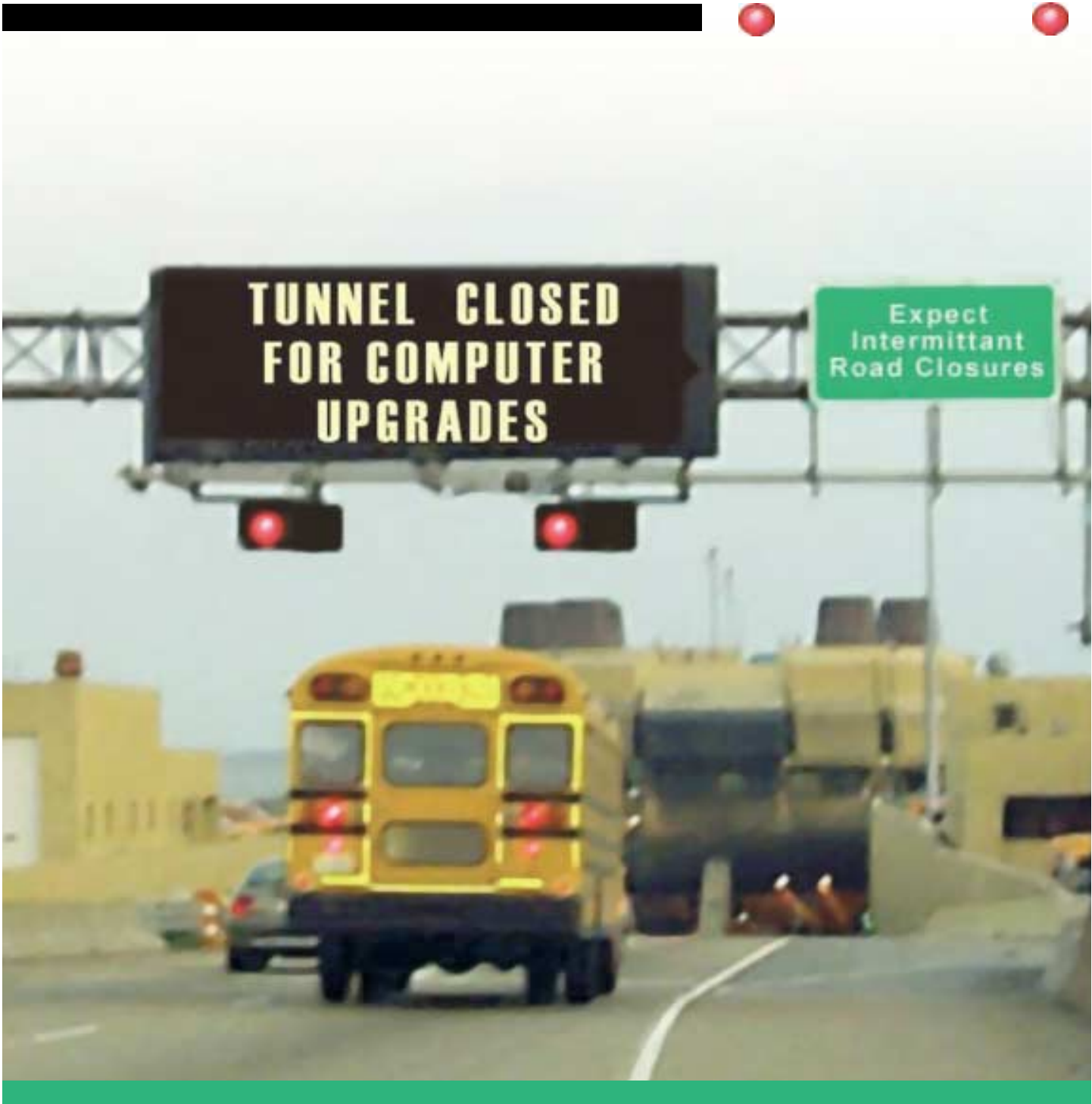
Safety is a critical issue for the tunnel's administrator. Today's controlled tunnels handle large volumes of truck, SUV and automobile traffic moving at expressway speeds. In the narrow confines and restrictive environment of a tunnel even ostensibly minor incidents

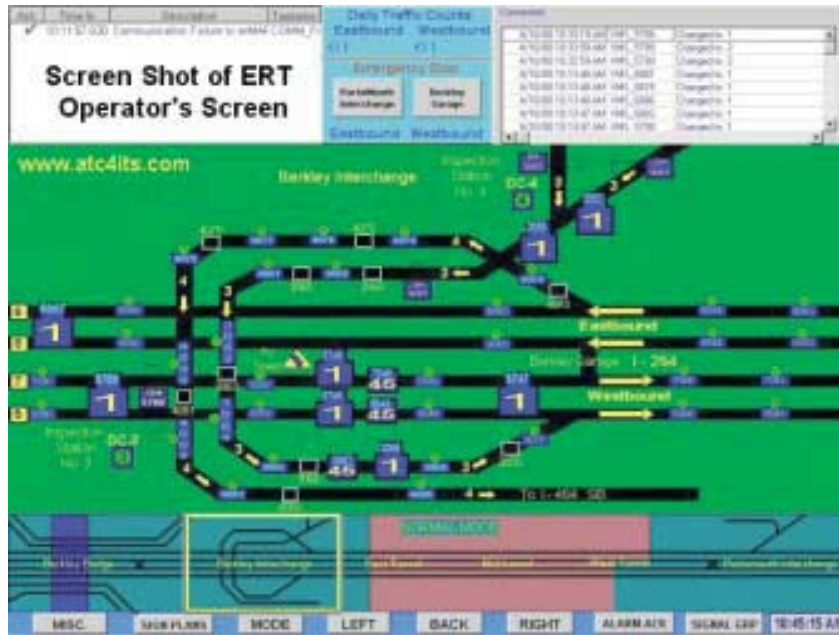
can soon become deadly serious since critical mass for a catastrophic incident may be achieved far more quickly than on surface highways.

Time becomes a significant issue. To effectively minimize incidents through implementation of sign and signal plans and the dispatch of appropriate emergency services, tunnel control operators must have real-time data from their field equipment, and they must have real-time control over their equipment. And, like the highway systems they serve, tunnels are around-the-clock operations. That means the tunnel control system must also have constant availability fault tolerance.

Costs are always a significant concern. Administrators of today's maturing tunnel control systems are hampered by high maintenance costs and missing functionality. A significant portion of the ever-increasing maintenance cost is attributable to aging computer systems and 'orphan software'. Expertise drain is a direct consequence of an aging computer system. Where there are a diminishing number of people capable of maintaining older systems, costs will go up. Moreover, in the past, control systems were often designed using proprietary code developed by a company that has either gone out of business or one that no longer offers support for the product. This leaves administrators







Tunnel systems in Virginia's Tidewater area

saddled with orphan software. Lacking both source code and expertise, they are unable to maintain their system. Administrators are also limited by their inability to enhance or expand the control system with new functionality, desirable as it may be, as it is often not compatible with the limitations of the aging system.

Finally, while there will often be the exchange of a Sumerian field device for a superior cutting edge Babylonian device, the time-honored saying 'if it ain't broke don't fix it' still applies, and much of the performing legacy equipment already in place will be retained in the new system. That means the upgraded tunnel control system must be able to talk to both new, and legacy equipment in real-time.

Advanced Traffic Control, Inc (ATC) has developed cost-effective solutions that resolve these issues.

Intelligent tunnel solutions

Operating under the flexibility of RFPs, as opposed to the constraints of RFQs, in the fall of 1998, ATC began designing and implementing upgraded tunnel control systems for Virginia's Department of Transportation. The ATC designed control systems, designated 'newTON' by VDOT, are based on Microsoft® Windows® operating systems (specified by VDOT as part of their own COTS contribution to cost reduction). The newTON systems replaced the aging MODCOMP®-driven TOMAC control systems then in use at the Hampton Roads Bridge Tunnel,

"When the back-up computer takes control of the system it appears to the network exactly as if it were the primary machine"



A tunnel control center at the Hampton Roads Bridge Tunnel

the Elizabeth River Tunnel and the Monitor-Merrimac Memorial Bridge Tunnel, all located in Virginia's tidewater area.

These innovative newTON systems rely on proven and supported commercial off-the-shelf components (ATC's basic SCADA engine is Intellution's iFIX™ product line, well recognized and in the market with over 100,000 licenses), thereby solving the problem of expertise drain and orphan software inherent in the TOMAC systems they replaced. The newTON control system design was a resounding success ('Virginia DOT uses SCADA for tunnel traffic control'. Better Roads (October 2000); and 'A New Wind Blows at ITS?', *Advanced Transportation Technology News* (April 1999)). The success of the initial Hampton Roads Tunnel upgrade system

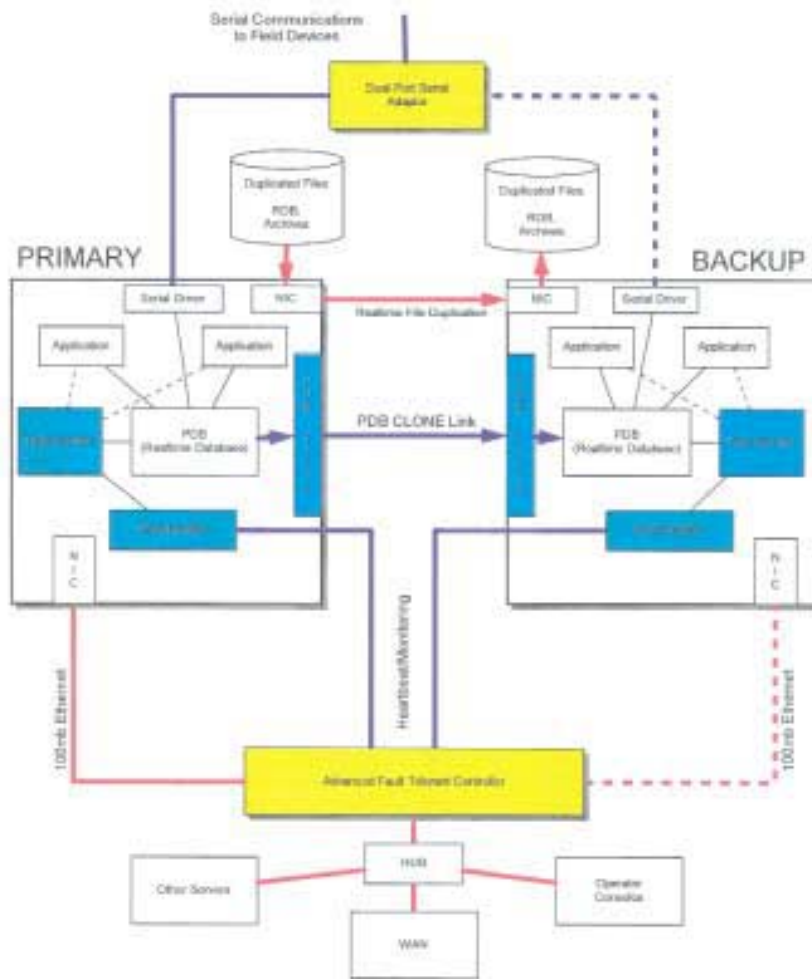
garnered VDOT's Computer Systems Engineers the prestigious Commissioner's Award of Excellence, and ATC went on to author the winning RFPs for both the Elizabeth River and the Monitor-Merrimac newTON upgrades ('Under the river', *Traffic Technology International Annual Review 2002*, pp42-46).

An integral component of the newTON system at Hampton Roads was a COTS data fault tolerance system. But data fault tolerance alone was found to be insufficient. Thus the Elizabeth River iteration called for a COTS hardware and data fault tolerance system, which was also retrofitted to the Hampton Roads tunnel. Ultimately this, too, was found wanting. The culprit was the threat of the occasional crashing of the OS (the so-called blue screen of death), or the OS locking up and requiring a reboot.

Occasional crashes and locking are

familiar to many Windows users. Without a satisfactory fault-tolerant solution, either one is unacceptable in a tunnel environment. However, while it is true that more stable and robust systems are available, Windows operating systems are well supported and offer both variety and convenience in developer tools. Thus, code for some tunnel applications on Windows OS can be written in days, whereas code for the same applications in other systems may take months. That is a significant cost issue for the tunnel administrator. It became clear that what was actually needed was solutions for all three: data, hardware and software fault tolerance.

No satisfactory commercially available off-the-shelf system that met the data, hardware, software and real-time fault-tolerant requirements of the tunnel systems was found. Some availability statements claimed 'no unplanned downtime' but inferred the need for 'planned downtime'. Accordingly, Advanced Traffic Control, Inc designed a continuous availability system that does meet the needs of tunnel control systems. It is this unique Advanced Fault Tolerant Solution (AFTS) that is the key to seamless



ATC's AFTS system diagram

communications with both the new and legacy field equipment. Moreover, with the AFTS system, computer maintenance is accomplished with no impact on tunnel operations. And, AFTS permits future expansion and development of the

newTON system. Consistent with a commitment to avoiding orphan software, ATC (for maintenance only) provides the source code for the firmware and PC side software, parts lists and board layouts for this proprietary feature. These

strategies assure tunnel administrators of a safe, supportable, expandable, yet cost-effective control system ('Tolerating Faults Improves Control', *Advanced Transportation Technology News*, February 2002).

The AFTS system overview

AFTS is a continuous availability system consisting of a combination of hardware and software that permits two independent computers to function as a redundant single computer. One machine is designated primary and runs the newTON system. The other is a hot back-up, ready to take over and run newTON in the event of a hardware or software fault in the primary.

When the back-up computer takes control of the system it appears to the network exactly as if it were the primary machine. This dual configuration effectively provides hardware fault tolerance for the system.

Fault tolerance for the relational database is achieved through off-the-shelf mirroring software. This mirroring software updates files to the back-up machine that have changed from specific directories on the primary, assuring that the back-up RDB is always current. Additionally, the software dealing with the RDB is configured to immediately flush all writes to the database. These features prevent the data loss that could otherwise occur when data is in the cache and a system fails.

Dealing with legacy equipment

Combining legacy field equipment with new field equipment in the same control



ATC rack-mounted controller and intelligent dual-ported serial interface switches



A close up of a smart switch face



system can present challenges as it may require transmitting multiple protocols over the same RS232 line (as it did on the Monitor-Merrimac project). Rather than developing control software compatible with the various legacy devices, this process is made possible through intelligent dual ported serial interfaces designed and built by Advanced Traffic Control.

This dual porting allows for either of the computers to access the field equipment. Processors in the switch allow for hard real-time communications with the field, while allowing soft real-time communications with the Windows computer.

Fault tolerance for this serial I/O is provided by these intelligent dual-ported serial interfaces. These rack-mounted

physically attached to the network at a time. Ethernet switching is accomplished through the AFTS Fault Tolerant Controller. To maintain current output states for all of the devices, the PDB clone, programmed to transfer the data points, runs between the two systems using a dedicated serial link that copies the output tags from the primary PDB to the back-up PDB. This insures that there will not be a change of field devices during any failure, and thus accomplishes fault tolerance for the PDB.

Fault detection

The AFTS's Fault Tolerant Controller is a microprocessor-controlled device that is the core of the AFTS system. Rack-mountable, the FTC provides two basic but critical functions. First, it controls

back-up system will assure continuous availability.

The bright light: continuous system expansion and development

As the reader may have already recognized, in addition to no planned or unplanned downtime for maintenance, the AFTS system also gives the administrator a safe and cost-effective method for continuous expansion and development of the control system.

System changes of every nature, whether Microsoft service pack installations, software revisions, functionality additions or any other changes, can all be added and tested on the back-up system without affecting the configuration or the operations of the primary system.

These changes are easily accomplished by installing the service pack, revision or new function on the back-up machine. After testing, if necessary an offending product can be uninstalled. If the change is a success, the administrator would then switch into the 'improved' machine, (accomplished by hand throwing a switch on the Fault Tolerant Controller) thereby making it the primary, and then making the identical change on the other (now) back-up computer.

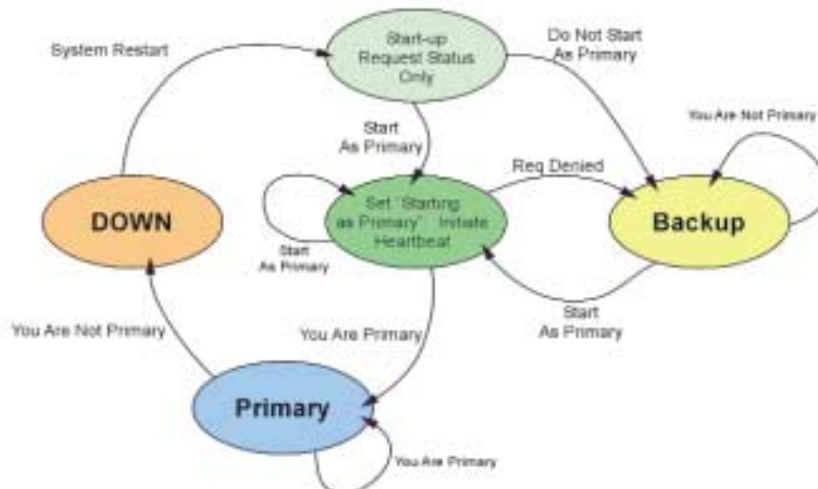
By this simple means, the tunnel administrator can constantly maintain and upgrade his control system with no impact on tunnel operations, and no more revision lock. Every service pack and every software revision, can be installed contemporaneously with its issue. New functionality can be added without disruption of the tunnel operation. The control system can always be 'up to date'. Expertise drain becomes a non-issue and maintenance costs remain manageable.

Hammurabi's legacy

Hammurabi's tunnel upgrade solution was not the only traffic issue he influenced. Archeological excavations show that the King of Babylon also had the city's streets laid out in straight lines that intersected at (approximately) right angles.

That street grid system was surely one of the earliest examples of an intelligent traffic solution. Cost-effective, constant availability intelligent tunnel solutions are another.

There can be a light at the end of the tunnel. Hammurabi would be proud. ■



AFTS system state transition diagram

devices accept two serial ports, one from the serial controller card in the primary and back-up computers, and provide a single surge suppressed serial port to connecting the modems to the field equipment. They can be set to switch from one input channel to the other input channel should there be a loss of communications, or to synchronize to a master port so that all the serial ports switch at the same time. The cards are hot swappable and require no cable disconnection.

The fault-tolerant path to the iFIX process database by iFIX View Clients and other nodes, is accomplished by having both the primary and back-up computers having identical Ethernet cards (including identical MAC addresses), but having only one card

which of the two computers the serial ports and network interface are connected to.

Second, it serves as the heartbeat monitor. This monitoring function and the reporting of system status is done via serial communications to each computer.

Critical custom tasks and workspace applications are monitored by a software heartbeat mechanism within the primary computer by the Task Monitor program. Each critical application must use an iFIX simulation PDB tag as a heartbeat. Each time the application runs it will increment the value of the PDB tag.

The Task Monitor checks that all of these tags have incremented. If an application fails to increment its PDB tag, it will be considered to have failed and the