ABSTRACT

A CAD/AVL system allows for the highly efficient management of transit operations, therefore transit management and operation relies on stable and reliable CAD/AVL systems.

The communications operating system must keep the availability of voice and data radio systems high, even if a radio system component fails. This requires key subsystems and devices to have standby devices to take over during a failure.

So what happens if system components fail? What if the GPS system does not work? What about radio communication failures? These and other questions are critical for transit operations management and will be addressed by this paper.

Strategies and concepts range from 100% availability of mission critical systems (i.e. police, military), to “We will improvise with the tools and resources we have.”

This is an economical decision between the necessary level of availability and the cost. This paper will discuss different backup and fallback concepts that keep the most important features of a CAD/AVL system up and running with minimal additional equipment.

As an example, if data radio system components are failing, the whole system is automatically switched into a fallback level where the vehicles operate in a vehicle autonomous mode. In this mode, automatic vehicle location, destination signs, next stop displays and next stop announcements are still working as well as voice radio and voice radio features like silent alarm, listen in, and selective call.

Topics

- Full integrated voice and data radio systems basics
- Backup and fallback level strategies
- Combined Automatic Vehicle Location (GPS and Dead Reckoning)
- “Security versus Money” How to backup important radio system components
- Graceful degradation fallback level concept
- Vehicle autonomous mode (data radio missing)
- Voice radio only (On-board computer failure)
- Transferring duties and functionality from one dispatch workplace to another during a failure

INTRODUCTION

Before spending time describing some the areas where fault tolerance can be addressed within a CAD/AVL System, we should consider what exactly is Fault Tolerance?

One definition states that it is the ability of a system to respond gracefully to an unexpected hardware or software failure. There are many levels of fault tolerance, the lowest being the ability to continue operation in the event of a power failure. Many fault-tolerant computer systems mirror all operations — that is, every operation is performed on two or more duplicate systems, so if one fails the other can take over.

An example of this type of redundant system approach can be seen on the space shuttle where “the on-board shuttle software runs on two pairs of primary computers, with one pair being in control as long as the simultaneous computations on both agree with each other, with control passing to the other pair in the case of a mismatch. All four primary computers run identical programs. To prevent catastrophic failures in which both pairs fail to perform (for example, if the software were wrong), the shuttle has a fifth computer that is programmed with different code by different programmers from a different company, but using the same specifications and the same compiler (HAL/S). Cutover to the backup computer would have to be done manually by the astronauts.”

Obviously for public transit this level of fault tolerance or pure duplication of hardware and software is not within most budgets, but it is also not entirely necessary. Instead public transit agencies need to take the time to plan accordingly for problem areas in the beginning of a project to assess what types of safety and fallback measures are necessary and affordable.
The basic function of a Computer Aided Dispatch and Automatic Vehicle Location (CAD/AVL) System for public transit is to provide improved passenger service and operational performance through the use of advanced computer and communications technology. This includes the areas of vehicle navigation and fleet monitoring, vehicle operator support and communication, on-board and wayside passenger information, vehicle dispatch and service restoration, fare collection and accounting, and performance data collection and analysis.

As a result CAD/AVL systems are often extremely useful and powerful tools that are complex and need to be safe and reliable. This safety and reliability should be planned for through the use of products and systems that offer inherent fault tolerance and fall back capabilities.

As you can see from Figure 1, a transit system can have several areas of hardware and software including computer control centers, dispatch centers, communication systems, and vehicle equipment. Each of these areas is important and requires some level of fault tolerance.

**THE COMPUTER CONTROL/DISPATCH CENTER**

We will begin by looking at the Computer Control/Dispatch Center portion of the CAD/AVL System. This area is one where the use of pure redundancy is worth considering. With the costs of computer equipment coming down as rapidly as their computing power is going up, it might be worth the initial investment to duplicate systems or employ other fall back methods right from the beginning.

The CAD/AVL server should contain a high performance preemptive multitasking operating system running on a modern computer platform, for example Windows NT or Linux. Additionally, these machines should include a multi-processor Pentium configuration that can provide the required computing capacity for both file and printing services and for computer-intensive applications are recommended. These machines also offer reliable system performance for complex applications and an increased number of users. So for this system it is recommended that two master computers be used to distribute the application software (for example, radio operation and passenger information on one computer and the CAD/AVL database and control programs on the other).

Thankfully with computer equipment there are as many choices when it comes to fault tolerance or back up systems, as there are equipment and software vendors. So we will only point out a few of the more common approaches that can be employed to ensure a secure and reliable computing environment.

The use of Redundant Array of Independent (or Inexpensive) Disks (RAID) drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren’t generally necessary for personal computers. Disk Mirroring, which is a technique in which data is written to two duplicate disks simultaneously. This way if one of the disk drives fails, the system can instantly switch to the other disk without any loss of data or service. Disk mirroring is used commonly in on-line database systems where it’s critical that the data be accessible at all times. Additional things to consider include multiple servers, duplicate workstations, additional monitors, and UPS Systems for power fluctuations.

While the main components within the Computer Control/Dispatch Center are network and database servers and PC workstations, typically there are also radio interface equipment and dispatch consoles. These devices can be more expensive than PC’s and thus it is less likely that a transit authority would have a redundant or replacement unit laying around in inventory. Though some thought might be given to this idea.

**THE COMMUNICATION SYSTEM**

The key to any successful CAD/AVL system is the voice and data radio communications infrastructure.

The Basic Radio system shown in Figure 2 provides simple voice radio and data radio communications between the vehicle fleet and the dispatch center.

In this system data communications can include information about vehicle location, schedule adherence and text messages between vehicles and the central CAD/AVL server, and is conducted by the data radio system. All vehicles are polled continuously via data radio and transmit information back to the control center. Therefore the vehicle is, except for during voice communication, in data radio mode.

In the basic system that data radio system and voice radio system are completely separate. The data radio system including the dispatch workstation is used for the monitoring and control of the daily operations. However, all voice communication is done over a separate voice console at the dispatch center, and this voice console is not interfaced to the data radio system or the CAD/AVL system. So any switching between voice and data systems are done manually by the dispatcher. This radio system configuration is often used in systems with only one dispatch center, a relative small coverage area and a small fleet size where one radio
site equipped with one data channel and 1 to 3 voice channels is sufficient.

Because this Basic System uses a minimal amount of equipment, it has the lowest initial cost for implementation. Since the data radio and voice radio systems are not fully integrated, if there is a problem within the voice system or the data system, you will likely lose use of that part of the system. In the case of a problem it will be the responsibility of the dispatcher or supervisor to take corrective action.

Obviously, the simplest method of providing fault tolerance would be to acquire a complete redundant or duplicate system of radios, consoles, repeaters, links, antennas, CAD/AVL servers etc. However the cost of such an approach makes it impossible for most transit authorities to implement.

An alternative approach would be to analyze the needs of the current system with an eye towards future growth and potential problem areas. From this perspective it might make sense to consider purchasing and installing back up units for select pieces of the system i.e. consoles, repeaters and antennas.

An Extended Radio system provides a full-featured voice radio communication system that is fully integrated with the data radio system and the CAD/AVL server.

Because the operations of the voice radio and data radio are integrated, this system is capable of managing several voice consoles and several voice radio channels at different radio sites. Besides the basic voice communication, this system provides advanced features like random connect of voice consoles to voice channels. To reach a maximum of flexibility, all voice consoles and all voice radio channels are connected to a Voice Radio Interface (VRI). The VRI is based on the latest digital signal processing technology. The VRI manages all voice radio channels (e.g. signaling) and all voice consoles. The VRI communicates with the CAD/AVL server to reach full integration into the CAD/AVL system. This radio system configuration is often used in systems with multiple dispatch workplaces that are all placed in one dispatch center. The coverage area and fleet size demands several radio sites (simulcast, common channel or cellular) equipped with one or more data channels and several voice channels.

The ability to link several voice consoles with the Extended System provides the opportunity to implement fall back strategies and graceful degradation steps that are not available with the Basic Systems single voice console approach. With multiple voice consoles you have ability to transfer responsibility between the consoles should one of them begin to have problems.

The Extended System also offers the user more options for configuration and management of activities. With a fully integrated voice and data radio system the all of dispatch operations can be done using one primary dispatch console and user interface component. There is no need to switch back and forth between different voice radio consoles and the dispatch workstation computers to get all of the required information. Additional features are also available; from the dispatch workstation the dispatcher can easily make a fleet call for every vehicle, or just call vehicles on a certain route. Also, it’s possible for the dispatcher to make voice announcements directly to passengers on a particular bus or all vehicles. It’s true these features can be available with a separate voice radio system, but when integrated within the data radio and CAD/AVL system, these operations are seamless and easier to conduct. The Dispatcher can just mouse click on a particular, vehicle, route etc. on the GIS map display to get all of the information they require or conduct various levels of communications.

Though integrated into a system, both the voice and data radio functions can be carried out independently from each other, should a problem arise.

Voice communications should be the ultimate fall back level.

**VEHICLE SYSTEMS**

When looking at all of the components, systems and subsystems that make up a CAD/AVL system, the best place to implement fault tolerant hardware and software may be on-board of the vehicle.

The Mobile Data Terminal as shown in Figure 5, is the heart, or more appropriately the brain, of the vehicle equipment should be a state-of-art Mobile Data Terminal. This unit should not only be the driver interface or control head, but should contain a powerful computing system that is able to provide full feature functionality for the monitoring and control of all vehicle systems.

The MDT should be capable of monitoring and controlling all of the interfaced components on-board the vehicles. If there is a problem with any of the on-board equipment the MDT should alert the driver so that a corrective action can take place, or the component can be disconnected. Additionally, the MDT may offer the driver the ability to manually override the failing the system. For example if the audio announcements system is failing the driver can simply make the announcements manually.

The situation that has the potential causing the most disruption to normal vehicle operations is a loss of data radio
Figure 1. CAD/AVL System.
Figure 2. Basic System.

Figure 3. Extended System.
communication between the vehicle and the dispatch center. As you can imagine, the ability of the transit vehicle to autonomously perform its regularly planned actions during a time of communications degradation or loss has never been more important.

Vehicle autonomous operation is possible when stored within the MDT is the actual intelligence about the transit system. This intelligence should consist of the operational data and information from the management and control center (central computer). It is important that all on-board functions and components can easily be initiated without radio connection to the central computer and would also function when the control center is unattended or even without existence of a control center for the vehicle autonomous concept.

Figure 4 shows a compact version of the on-board computer utilized on a bus. A similar system would be used for minibuses/vans, articulated buses or light rail vehicles.

Data for Download / Offload

Since the autonomous mode of operation relies on the fact that at the MDT will have all of the operational data required to fulfill daily operations, we should look at how we can add some fault tolerance to the task of getting the data to the MDT.

For the basic data transfer between the control center equipment and the on-board computers, data radio communication is the primary method used for the download of the database into the on-board computers and/or to retrieve data and information from the vehicles. However, if the data radio is inoperable there are several additional methods and media available and can be used for this function.

- Portable memory modules are a high performance contact-less memory card which and memory card drives are integrated into the on-board computers and the loading/reading station(s).
- Laptop PCs can be used for download and offload of the basic data and information.
- WLAN is a radio transmitting technology, but with much more speed than conventional data radio.

Naturally the choice of which approach is best is an individual one and will be based on cost and resources available.

Autonomous Dispatch Functions

Vehicle location is one of the most important pieces of information that a vehicle system can provide. This is accomplished in several ways:

GPS is a worldwide satellite-based tracking system consisting of a network of twenty-four satellites continuously transmitting signals with extremely high clock accuracy. The GPS network allows anyone with a GPS receiver to determine highly accurate geographic positions.

“Differential GPS (DGPS)” is a method of post-processing GPS location data to eliminate some of the errors of the GPS system affecting the accuracy of the location data. Operational experience with the utilization of DGPS has shown that:

- “Normal GPS” is the sufficient means of vehicle tracking when fixed routes in a wide network pattern are involved, e.g. light rail, track-guided bus, bus in rural area. Location synchronization takes place through corresponding software algorithms.
- “Differential GPS” is the favorable means of vehicle tracking in networks with high route density and in applications where a high positioning accuracy is required (e.g., signal switching in light-rail operation, traffic signal priority in complex signal systems).

Logical Location or “Dead Reckoning” is a simpler method of vehicle location that is still used throughout the world and is offered here as a level of fault tolerance for the autonomous operation of the vehicle. Though GPS technology has proven itself to be reliable and accurate, we still must be prepared to operate without it. When utilizing “dead reckoning” the determination of the actual vehicle location takes place through:

- Odometer readings
- Door sensor signals (send messages “door open” or “door closed”)
- On-board software algorithms using the sequence of stops, the stored distances between the stops (or additional points of the network), the pulses received from the pulse counter, and the messages received from the door sensors for location determination and synchronization. The software location algorithm is fail safe against irregular situations such as passing by a stop, operating with door(s) open.

Since pre-selected stops or other pre-defined points on the route can be determined as “calibration points”, stationary vehicle location supports like infra-red beacons, GPS or induction loops are not necessary. The logical location monitoring needs network data stored on the MDT, which contains the distances between the stops. The vehicles have a counter for the number of wheel rotations (odometer reading).
Figure 4. Vehicle Components.
Figure 5. Sequence of Stops.
ADVANCED DISPATCH ACTIONS IN AUTONOMOUS MODE

Since the MDT is capable of determining its logical location, it can utilize the route and schedule information stored on-board to conduct additional operations. To do this we should look at a description of one piece of information available to the MDT to assist it in conducting certain functions.

A vehicle run is a sequence of stops and time-points from the beginning (usually the pull-out) to the end (usually the pull-in) of the shift or run. Contained within the sequence of stops will be information about which stops to serve, the stop numbers and/or names in the operationally relevant sequence, the distances between the stops or other relevant points, and the nominal arrival and/or departure times at/from the stops.

The central scheduling software generates the sequence of stops, together with the other relevant information, for each individual vehicle. From this information Action points or “Trigger points” can be defined along the route as those points where some activity is to take place. For example, an action point may be defined as a point 300 feet or meters from a stop where the audio next stop announcement has to take place. The allocation of the sequence of stops to the corresponding vehicle is performed via the data download/offload medium, e.g., portable memory module or data radio.

- Violation of a pre-determined “Dt” leads to both the display of the schedule deviation in the on-board computer display and the transmission to the central computer.
- Passing a “capture area” without stopping automatically leads to setting all relevant peripherals to the subsequent stop.
- Passing an action point of the type “stop announcement” automatically leads to triggering the visual and/or audio on-board announcement system. Usually, the visual “next stop” display is triggered “x” meters after leaving a stop while the audio annunciator is triggered “y” meters before reaching the upcoming stop.
- Passing an action point of the type “TSP (Traffic Signal Priority)” automatically leads to generating the relevant procedure for autonomous traffic signal priority. Depending on the authority’s requirement, the preemption request is triggered in any case or only when the on-board computer detects a delay when passing the action point (e.g., when the vehicle is behind schedule).

- Passing an action point of the type “connection protection” automatically leads to initiating the relevant procedure for connection protection. Usually, the on-board computers of both the feeder and the distributor vehicle trigger schedule adherence messages to the control center; the dispatcher transmits “wait for feeder” or “release transfer” instruction to the corresponding vehicle(s) upon automatic dispatch action or own decision.

Dispatch activities that can be triggered using the defined “action points” include:

- Schedule adherence monitoring. At terminals or major transfer points, the on-board computer continuously displays to the vehicle operator the time remaining until the scheduled departure (“countdown” in minute or half-minute increments). When the vehicle is due to leave, a distinctive audible and visual alert can be produced. When en route or scheduled to be en route, the on-board computer continuously displays the number and/or name of the next stop, the exact time, and the deviation from schedule, in operationally predetermined time increments, to the vehicle operator.

- Nominal vs. Actual Schedule Comparison/Schedule Adherence Monitoring. In the vehicle autonomous operation mode, schedule comparison is performed autonomously by each individual vehicle by comparing the nominal departure and arrival times from/at stops (derived from the nominal data stored in the on-board memory) with the actual situation (derived from the actual vehicle location) and measuring and reporting the differences.

All transactions or reports generated from the above mentioned activities are sent to the on-board computer and are automatically stored in the on-board memory. This information together with time and location “stamp for end-of-day or end-of-shift off-load and subsequent evaluation.

Safety and Security in Autonomous Mode

For emergency cases and increased safety, a hidden push-button is additionally provided in each vehicle for silent alarm. Upon pressing the button, the voice radio request is transmitted to the central computer together with an indication of “highest priority”. The use of the silent alarm button does not result in acknowledgement or other audible or visible response to the bus operator, but triggers the “listen-in” function, which enables the dispatcher(s) or other security persons to monitor the sounds on-board the vehicle via the vehicle operator’s microphone and/or additional microphones installed on-board.
Fall-Back Communications (Voice Radio)

Whether the vehicle is in autonomous mode or operating with a fully functioning data radio system, the voice radio communication should mainly be provided as a back-up for the digital radio system and for specific operation-related calls (e.g. Emergency calls) or messages (e.g. announcements to either vehicle operator or passengers).

SUMMARY

As you can see a CAD/AVL system offers a transit authority a state-of-the-art means of the highly efficient management of day-to-day operations. But as was discussed, there are potential risks as a transit authority begins to truly rely on a stable and reliable CAD/AVL system.

The communications operating system must keep the availability of voice and data radio systems high, even if a radio system component fails. This requires key subsystems and devices to have standby devices to take over during a failure.

So what happens if system components fail? As you can see it depends on what you have planned for. The main thing to remember is that the fault tolerance can be planned for and built into a system at many levels. So don’t get caught thinking that the only solution for system integrity is buying two of everything. Take the time to learn about what types of fault tolerance are necessary and compare this with the costs, and make an informed decision.

So the motto that has served the Boy Scouts for decades, should be applied to the implementation and operation of a Fault Tolerant CAD/AVL System; Be Prepared!