AUSTRAC: The Australian ATCS

KEITH LUGSDEN AND RON DAVISON

AUSTRAC is the Australian implementation of the North American Train Control Systems (ATCS) series of signaling specifications. AUSTRAC is being installed on Australian National's Trans-Australian and Central Australian lines. AUSTRAC differs from ATCS in several respects. The development of AUSTRAC pinpointed some problems found with the ATCS specifications and also led to the incorporation of unique features into AUSTRAC.

Australia's present rail network is operated by individual state governments, the exception being the federal government-controlled Australian National (AN) infrastructure across what was the old South Australian country network. Not only are there five independent systems involved in cross-country and interstate operations, the problems and efficiencies are further frustrated by a lack of common gauge. Queensland and Westrail have narrow and standard gauge, New South Wales and AN have standard guage, and Victoria has broad and standard gauge. All of the systems have independent operating rules, different communications and signaling systems, and a variety of management information systems (MIS). With this mismatch of infrastructure and duplication of management and organization overhead, rail transport finds it very difficult to compete with its road and marine competitors. Railways have to maintain their own right-of-way, whereas the competition operates through publicly funded roads and ports allowing them the benefit of moving in and out of transportation corridors at will without exposure to loss of substantial capital investment.

In late 1989, the National Freight Initiative (NFI) was established with the participation and support of the individual railroad systems, major rail users, and the federal government to determine the feasibility of a national rail freight organization to perform the interstate rail transport task in Australia. This organization will be an incorporated company integrated across state borders and operating at cost levels significantly below those now prevalent in the rail system.

In 1989, AN was looking to introduce some form of control and communications infrastructure on the Trans-Australian and Central Australian railways (TAR and CAR respectively). Fortunately, AN's managing director, Russel King, had the forethought to consider the future integrated network. From this coast-to-coast integrated freight network requirement the concepts of AUSTRAC were formulated. Consequently, AUSTRAC has been designed to meet AN requirements for an efficient signaling system on the TAR and CAR. The design is based on the principles of Advanced Train Control Systems (ATCS) specifications. The TAR and CAR cover about 2 000 km of single track east from Port Augusta to Kalgoorlie and north from Tarcoola to Alice Springs, respectively. AUSTRAC is being installed at 41 of the crossing loops, mostly on TAR. It is the first system installed in the world to incorporate the facilities described as ATCS Level 30.

International Railroad Systems Pty, Ltd., 209-217 Wakefield Street, Adelaide, South Australia, 5000.

OVERVIEW OF ATCS

ATCS will not be described in detail here because this topic has been covered elsewhere (*1*). However, there are some important differences between ATCS and AUSTRAC, and some of these will be highlighted in this paper. In this section, a brief overview of ATCS is presented.

ATCS specifications were produced by ARINC Research Corporation under the control of a steering committee formed by the American Association of Railroads (AAR) and Railway Association of Canada (RAC). The specifications have been designed "to facilitate compatibility and standardisation without limiting the individual design approaches of individual suppliers" (*2*). As a practical consequence of this, the specifications as they stand to date are overly constraining in some areas and too loose to achieve interoperability in others. In addition, the specifications are generally in a form that, although readily understandable by signaling engineers, are not very amenable to implementation in software. Therefore, the design of AUSTRAC has highlighted the need to clearly define many concepts that are not covered adequately in the ATCS specifications.

Features

ATCS can be broadly characterized by the following features:

- Management of moving-block track occupancies by a centrally located dispatch center;
- Automatic tracking of the location of trains using a data communications network;
- Issuance of movement authorities over the data network;
- Enforcement of speed and authority limits;
- Automatic control of a diverse range of wayside devices such as motor-operated points and highway crossing devices;
- Reporting of train, switch points, and ATCS component health; and
- Three different modes of operation already defined (known as ATCS Levels 10, 20, and 30) and a fourth envisaged (ATCS Level 40).

ATCS Specification 100 (*2*) defines the three operating modes as representing different levels of sophistication:

- Level 10—Centralized route and block interlocking logic in a computer-aided dispatch system;
- Level 20—Automated transmission of movement authorities and other instructions via a data communications system;
- Level 30—Automatic location reports and full train tracking within the dispatch system; and
- Level 40—Full field locking.

Control Flows

One of the major obstacles to be overcome when attempting to implement the ATCS specifications is caused by its functional description by control flows (*2*). These were still in early draft form in 1988 when the AUSTRAC project commenced. Once a detailed analysis was performed on the control flows, several shortcomings were uncovered: First, there are numerous errors, inconsistencies, omissions, and ambiguities present in the control flows. These include "dangling control" (where a control flow has a path with no defined end point), "hanging control" (where a control flow may be suspended pending some event that may never occur), and conflict with other ATCS specifications (such as messages that do not have the required information, or messages that, according to the control flows, are never sent). Second, the lack of a coherent structure (e.g., hierarchical) makes many of the control flows impossible to comprehend. For example, a control flow may invoke another control flow that may eventually invoke the first one. Third, there are no textual descriptions of any of the control flow functions. This means that the implementor must comprehend the functionality of ATCS just from three or four words written in control flow boxes and by correlation with message definitions in another ATCS specification. Finally, there is no recognition in the control flows that they are to be implemented in software on distributed processing systems (central office, waysides, and locomotives) as defined by ATCS itself. For example one control flow may require action by three physically different devices and hence the control flow cannot be attributed to any one device.

ARINC and AAR have acknowledged that there are problems with the control flows and are currently trying to produce a more coherent set that should facilitate easier implementation in software and hardware. In fact, ATCS specifications have been under constant development since the first drafts appeared a few years ago. This has meant that the specification of AUSTRAC has had numerous changes to its original baselines and has required keeping ATCS specifications under constant review.

OVERVIEW OF AUSTRAC

AUSTRAC has nearly all of the features of ATCS described in the preceding (see Figure 1), but with some important differences that generally relate to AN's implementation requirements. In particular, traffic density was considered sufficiently low on TAR and CAR to allow the removal of some of ATCS' more complex (and hence more costly) features. Consequently, AUSTRAC now has the following characteristics:

- Fixed block only (i.e., an entire section of track is marked as occupied until the entire train has vacated it);
- The communications backbone is based upon an optical-fiber cable that connects a central communications controller (known as the FEP/CC) on a point-to-point basis with a series of radio base stations located near to the track;
- All wayside installations and equipped locomotives are connected to the network by data radio;
- Fail-safe hardware is employed in all safety-critical areas—on-board computers (OBCs), wayside interface units (WIUs), and office interlocking computers (OICs);
- Formal specification and analysis of all safety-critical software;
- Vital interlocking of safety-critical commands from the central office using a pair of safety computers;
- Vital relays inserted between WIUs and points machines;
- Motor and hand-operated points are the only wayside devices currently within the scope of AUSTRAC;
- Software emulation of track circuits, using automatic train location technology, in such a way that real track circuits can be added at a later stage without altering hardware or software;
- Normal operation at Level 30, with partial failure resulting in a degradation to Level 20 or Level 10 as appropriate; and
- The addition of an end-of-train subsystem to determine accurately when the train clears critical points.

CENTRAL OFFICE

AUSTRAC's central office will be located next to AN's headquarters at Mile End in suburban Adelaide. It consists of a dispatch system, safety interlocking system, and a data communications controller.

Dispatch System

The dispatch system is hosted on six operational, networked Sun Sparcstation (Sparc is a trademark of Sun Microsystems, Inc.) work stations and two spare Sparcstations (see Figure 2). Two of the operational Sparcstations are called train control work stations (TCWs) and will be actually located in Port Augusta where AN operationally controls TAR and CAR lines. The TCWs enable the train controllers to enter various authorities, block track sections, receive alarms or other information from the network, and perform other train management functions (see Figure 3). Two other work stations are designated as control computers (CCs). One CC is operational while the other is on standby. The CC controls the release of authorities and other commands from the central office to the field and permits history logging. Another Sparcstation is used as the system manager's work station (SMW). The SMW permits AN's AUSTRAC system management personnel to interrogate the network for fault diagnosis or other information. The SMW can also be used to remove AUSTRAC equipment from service or put it back into service.

AN's traffic information management system (TIMS) is accessed via the TIMS interface work station (TIW), which is the sixth operational Sparcstation. The TIW allows train in-

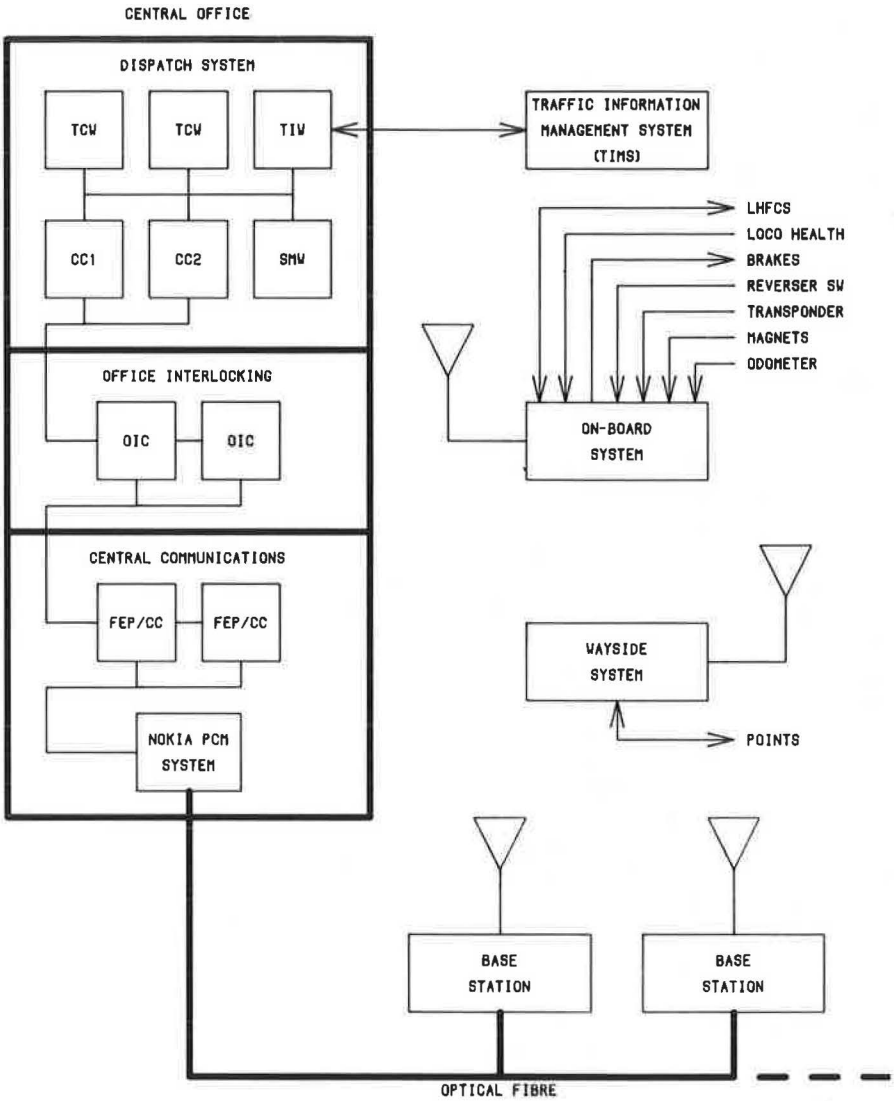

FIGURE 1 AUSTRAC architecture.

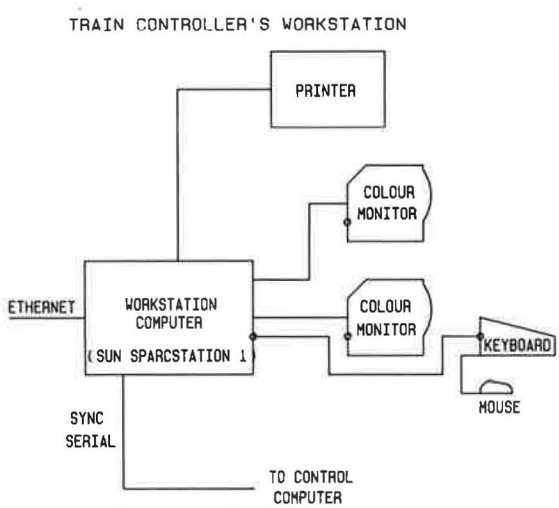

FIGURE 2 Central office.

formation, such as consist, to be downloaded to AUSTRAC. The TIW also provides train running data, such as train location updates, to be returned to TIMS.

Office Interlocking System

The office interlocking system is based on a pair of safety computers known as office interlocking computers (OICs). One OIC is active while the other is on standby. Each OIC has a communications processor associated with it called a quad-serial input/output (QSIO). The QSIO connects the OIC to the dispatch and communications systems. Each QSIO is controlled by an Intel 80C186 microprocessor. The role of the OICs is to ensure that no commands sent to the field could lead to a hazardous situation. To facilitate this, the OICs maintain data bases of train locations, points status, authority information, and other necessary data. The OICs also respond to emergency conditions, such as the overrun of authority

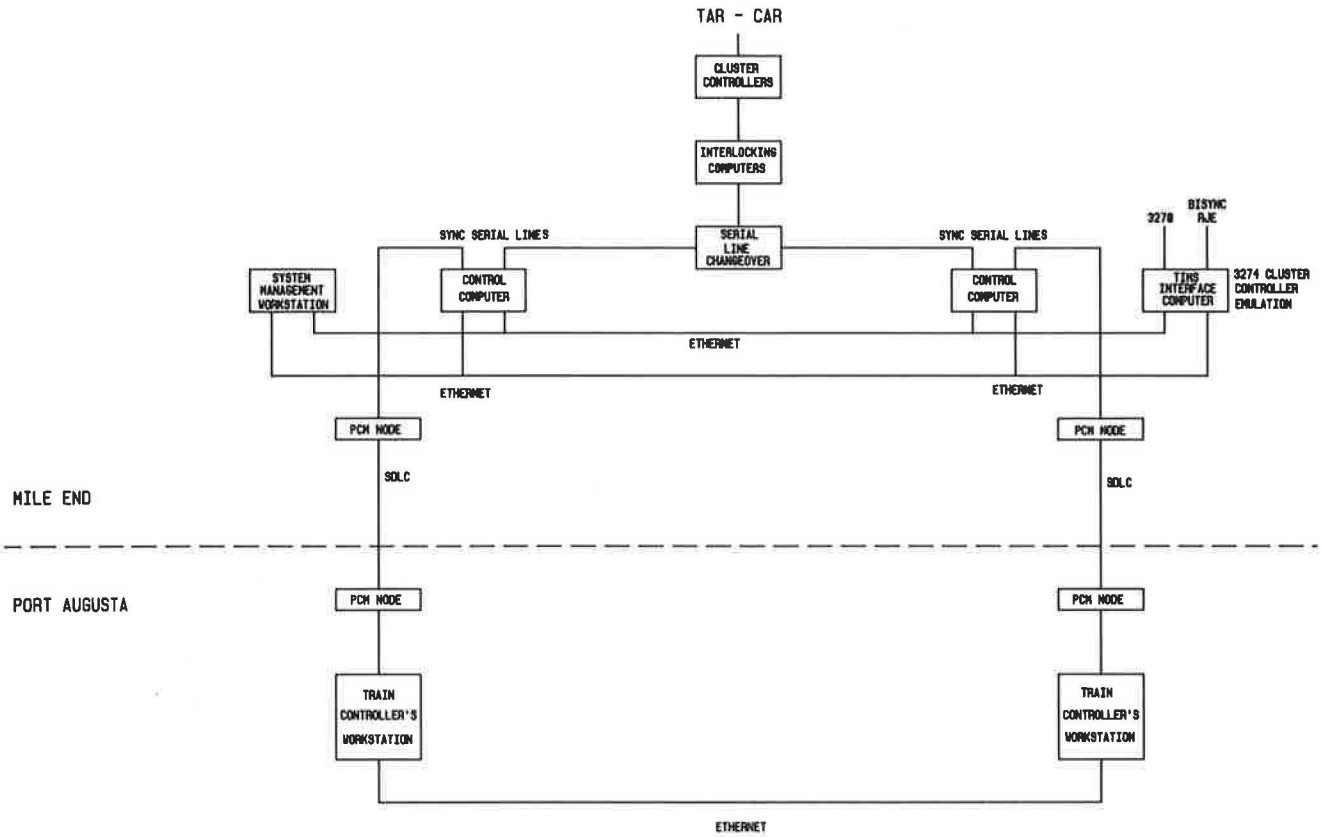

FIGURE 3 Train controller's work station.

limits, by issuing appropriate commands such as restricting the authority limits of opposing trains.

The OICs, as are all AUSTRAC safety computers (i.e., OICs, WIUs, and OBCs), are each based on a pair of VIPER microprocessors. The VIPER chip has undergone a high degree of formal specifications and analysis in order to prove that it can move between its defined states only in a predictable manner.

To enhance safety, the VIPER has no interrupts, no stack, a limited range of addressing modes, and a reduced instruction set. Each VIPER operates in a closely coupled pair. If any discrepancy is detected, such as illegal bus transactions, out-of-range addresses, or parity errors, the VIPER hardware will halt. Note that all VIPER memory contains 8 parity bits for each 32-bit word.

Each safety computer includes watchdog, fault detection, and fault injection circuitry on all vital hardware. This ensures that not only can they detect faults, but they can also determine whether the fault detection circuitry is itself faulty. In addition, software is able to detect other fault conditions such as incorrect I/O module addressing and I/O connectors that are plugged into the wrong I/O module. Any detected failures cause an automatic disconnection of the computer from its vital functions.

Central Communications System

The central communications node is a combined front-end processor and cluster controller (FEP/CC). The FEP/CC interfaces with the optical-fibre–based communications backbone to access the ATCS base stations. Refer to (*2*) for a description of the AUSTRAC communications backbone.

All AUSTRAC data communications conform with the applicable ATCS specifications (200 series). These in turn generally follow the Open Systems Interconnect (OSI) seven-layer model (e.g., ISO-3309, ISO-4335, and ISO-7809). This includes the X.25 error-controlled link-layer protocol (*3*) and a transport layer that features a 31-bit vital cyclic redundancy check (CRC) code. Only the safety computers know the algorithm to encode and decode the vital CRC. This ensures that only vital software can initiate vital actions. The FEP/CC is duplicated for reliability reasons. The FEP/CC can control up to 64 base stations. Provision has been made for an expansion FEP/CC to be added that would enable connection of a maximum of 128 base stations. The initial AUSTRAC configuration has 48 base stations. The FEP/CC comprise's one QSIO module for the FEP and one QSIO module for each CC. Each CC controls four base stations and up to 16 CCs can be installed in a single FEP/CC.

WAYSIDE SYSTEM

AUSTRAC's wayside system consists of a wayside interface unit (WIU), solar power supply, wayside communications package (WCP), and a set of vital interlocking relays.

Wayside Interface Unit

The WIU is comprised of a safety computer (similar to the OICs), a QSIO communications processor, an environmental

input module, and between one and three points control (PC) modules. The QSIO provides the communications interface with the WCP. The WIU's environmental input module permits the WIU to read the wayside identity and to detect conditions such as hut light on and hut door open. Each PC module can control one points machine (or detect one set of hand-operated points) and interface to two track circuits. The WIU ensures that the points are kept in the state previously set by the OIC while a train is in the vicinity of the wayside. The WIU continually monitors the health of all wayside subsystems. It will shut itself down safely if it detects that it no longer has control of its vital functions.

Solar Power Supply

The wayside system is powered by a solar power supply that delivers 24 Vdc to the points machine and 12 Vdc to everything else. The batteries have sufficient capacity to sustain operation of the wayside system for up to a week without sunlight, assuming normal usage rates are maintained. The power supply provides outputs to the WIU to indicate low battery voltage so that the WIU can shutdown the wayside installation at an appropriate time (e.g., not while a train is moving over the points).

Wayside Communications Package

The WCP consists of an ATCS-compatible modem supplied by Harris Corporation, a data radio supplied by UniLab, and an antenna. As the modem and radio are not fully compatible with each other, the WIU's QSIO must translate commands and responses between the two devices. The radio system has been designed to be fully ATCS-compatible, but operates in the 400 MHz band as required by the Department of Transport and Communications. It features forward error correction (FEC) and a channel access procedure that employs busy-bit insertion. The WCP communicates by radio with the FEP/CC via its nearest functional base station.

Vital Interlocking Relays

Unlike ATCS, AUSTRAC specifies the use of vital interlocking relays between the electronic circuitry and the points machines. Their usage makes it virtually impossible for the points to be moved unintentionally even in the highly unlikely event that an undetected software or hardware fault occurs. For each PC connected to a points machine, three vital relays are provided. These are the switch locking relay (SLR), normal control relay (NCR), and reverse control relay (RCR). The points can only be moved if the software operates the relays in the correct sequence. The WIU checks the state of the vital outputs every 50 ms to determine whether any fault conditions are about to attempt an unwanted relay operation. As each relay takes more than 50 ms to operate, AUSTRAC ensures that only intended actions can cause movement of the points.

ON-BOARD SYSTEM

For fully equipped trains (i.e., Level 30), AUSTRAC's on-board system comprises an on-board computer (OBC), mobile communications package (MCP), driver's display and control unit (DCU), train location subsystem, end-of-train (EoT) subsystem, enforcement subsystem and interfaces to the locomotive health system (LHS), and proposed long-haul fuel conservation system (LHFCS). A voice radio system is also supplied so that drivers can keep in contact with train controllers throughout AUSTRAC territory. Note that unequipped and partially equipped trains can also safely traverse AUSTRAC territory, although a higher level of driver and train controller interaction is required.

On-Board Computer

The OBC has a safety computer similar to that of the WIU, except that instead of PC modules it has interfaces to the EoT equipment, odometer, reverser switch, and enforcement subsystem. It also has an extra QSIO to interface it with the DCU, train location system, LHS and LHFCS. The role of the OBC is the safe operation of all locomotive functions. In particular, its role is to accept and validate authorities issued to it by the central office, to keep track of the train's location, communicate with the driver through the DCU, and apply enforcement where safety is threatened.

Mobile Communications Package

The MCP is very similar to the WCP. The main difference is that the EoT receiver (see below) is also incorporated within the data radio enclosure, which is then known as a lococom radio.

Display and Control Unit

The DCU permits text and graphics to be displayed to the driver. It has a touch-sensitive screen so that the driver can acknowledge various actions and provide certain information to AUSTRAC. In normal (Level 30) operation, the driver needs only to provide minimal information, such as the EoT serial number. However if, for example, the location subsystem should fail, the train reverts to Level 20 operation and the driver must enter the train location information manually. Because a touch-sensitive display is used, no valuable cab area is required for a bulky keyboard. The DCU has a 640 × 200 pixel display arrangement on a 190 mm-wide × 95 mm-high monochrome screen. Bit-image graphics permit animation (such as the approach to crossing loops) and the display of any international language (Danish, Thai, and Mandarin versions have already been demonstrated).

Train Location Subsystem

The train location system comprises track-mounted transponders, locomotive-mounted transponder interrogators, and in-

terfaces to the locomotive's own odometer and reverser switch. Together, these devices permit the OBC to determine its location to within the limits of the odometer, which is calibrated every time that a transponder is passed over. The odometer is calibrated by comparing its pulse rate with a known distance (i.e., the distance between two calibration transponders). Transponders are located at strategic locations, such as crossing loops, so that the odometer is not required to be especially accurate (AUSTRAC allows for up to 3 percent error caused by slippage and wheel wear without any danger of a train overruning its authority limits). The transponder equipment is sourced from a third party and interfaces directly to the OBC.

End-of-Train Subsystem

The EoT subsystem consists of track-mounted magnets located at important control points (such as the entry point to a crossing loop), a magnet detector and radio transmitter mounted on the coupling of the last vehicle of the train, and an EoT receiver in the locomotive that passes the magnet detection information to the OBC.

The EoT subsystem is used by the OBC to determine when the train has cleared critical areas, such as the points-fouling area. This is achieved by a data radio transmission from the rear of the train to the OBC whenever a magnet is detected. In the same way, the EoT subsystem also permits the OBC to determine that the train is intact. Because the transponder interrogator is located on the lead locomotive and the magnet detector is mounted on the rear of the last vehicle, the OBC can determine the length of the train by calculating the distance traveled between a transponder and a magnet.

The EoT subsystem is an AUSTRAC addition to ATCS. ATCS specifies the use of track circuits and duplicated odometers. The track circuits are used to determine when a train has completely cleared a critical track section. Duplication of odometers enables the OBC to reliably determine the location of the end of the train.

Enforcement Subsystem

The enforcement subsystem allows the OBC to apply the train's brakes if the authority or speed limits have been violated or are likely to be violated. Failure of the OBC will also cause enforcement to be activated. For AUSTRAC, enforcement would normally be enabled for the entire journey. Enforcement would be disabled while the train is outside AUSTRAC territory and when shunting inside a yard. The OBC continually calculates the train's speed, location, and stopping distance. The stopping distance is based on the track gradient, train speed, and train class. If this distance indicates that a certain limit may be exceeded, the driver is presented with a warning. If the warning is ignored (i.e., the driver fails to reduce the train's speed to within the appropriate limit), the OBC will apply enforcement. The train driver has access to an enforcement override switch. Such action will cause an alarm to be generated on the TCW.

Locomotive Health

The OBC has an interface to the existing locomotive health system (LHS) installed on most of AN's locomotives. The LHS simply permits locomotive running data to be transmitted back to the central office for examination by AN's maintenance staff. Consequently, up-to-date information will be available at all times instead of only when the locomotive returns to the maintenance yard. There are currently no plans for AUSTRAC to process these data itself.

LHFCS Interface

The OBC has an interface to the long-haul fuel conservation system (LHFCS) being developed by International Railroad Systems. This is a bidirectional interface to allow train running data from the OBC to be analyzed by the LHFCS and for driving advice (drive, coast, or brake) to be returned to the OBC for display to the driver on the DCU.

QUALITY ASSURANCE

Because partial or total failure of AUSTRAC has safety implications, a higher than normal level of quality assurance (QA) is being applied to the project. Some of the features of the QA used on the AUSTRAC project are as follows:

- Safety and hazard analysis by a third party;
- A company quality system based on AS3901 (ISO9001 equivalent);
- Application of standards such as software development to DOD-STD-2167A and specification practices generally conforming with MIL-STD-490A;
- A large QA team employed by both the contractor and AN to ensure compliance with all appropriate specifications, procedures, and standards;
- Formal specification of all safety-critical software;
- A team of verification and validation (V&V) experts employed by both the contractor and AN to analyze safety-critical software;
- Use of system specification methodologies and tools, such as Ward-Mellor, Statecharts, Excelerator, and Statemate (Excelerator is a trademark of Index Technology and Statemate is a trademark of i-Logix Inc.);
- Use of MALPAS (MALPAS is a trademark of Rex Thompson & Partners) (Malvern Programme Analysis Suite) static analysis on safety-critical code;
- Careful prototyping of hardware and software; and
- Rigorous formal testing of safety-critical hardware and software.

SAFETY CONSIDERATIONS

Unfortunately, safety can never be guaranteed 100 percent in any railway signaling system. As always, safety depends not only on the signaling system, but also on the associated operating rules and people who use the system. However,

AUSTRAC does have some important safety features, some of which have been previously described:

- Use of vital CRCs to ensure that only empowered software can generate or act on potentially hazardous commands;
- Design of fail-safe hardware that can only fail in predictable safe modes;
- An analysis of the hazards likely to be encountered by the system;
- A rigorous hardware and software development program;
- Use of the latest V&V techniques on safety-critical software;
- Diligent QA and safety teams; and
- A joint safety management group responsible for resolving hazards both during the development phase and over the life of the project.

CONCLUSION

AN's decision to initiate the development of AUSTRAC will put the railroad among the world leaders in railway control and information technology, and leave AN ideally placed to take full advantage of the Australian government's National Freight Initiative.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the assistance provided by colleagues at International Railroad Systems Pty. Ltd. in the preparation and review of this paper.

REFERENCES

1. A. Blakeley-Smith. *ATCS—The Universal Signaling System*. International Railroad Systems Pty, Ltd., Sydney, Australia, July 1989.
2. *System Architecture Overview*. ATCS Specification 100. ARINC Research Inc., Jan. 1989.
3. CCITT Recommendations X.1–X.32. *Data Communication Networks: Services and Facilities, Interfaces*. 9th Plenary Assembly, Melbourne, Australia, November 1988.