ATCS at CP Rail—Steady and Measured

R. J. Hipfner and R. A. Shea

At CP Rail, an extension of an installed computer system for a radio block dispatching method provides the features of advanced Train Control Systems (ATCS). The design strategy followed calls for a progressive installation—both in terms of equipment and functions. The base system was installed in 1985 and has been upgraded several times since inception. It now is used on every CP Rail dispatching desk and has been installed on three other railways. This new implementation adds a local area network and connection to ATCS Specification 200 data communications. Extended principles of operation were developed to allow for mixed-mode issuance of train operating clearances and track occupancy permits. The system works better with more equipment installed, rather than requiring a threshold for ATCS operation. Locomotive engineers receive their operating authority on a flat panel monochrome screen by data radio in the same format as if issued by the rail traffic controller (RTC) by voice. When data communication is not available, the crew enters the movement authority into the on-board computer with point-and-select menuing. A check word is calculated and exchanged between the locomotive crew and the RTC to ensure accurate transcription into the on-board computer. This mode allows smooth interaction across areas and subdivisions with and without radio data communications. A phase 1 pilot between Calgary and Edmonton is under way, having been installed in the fourth quarter of 1991. CP Rail is now at work on its future plans for the system.

CP Rail's involvement with the Advanced Train Control Systems (ATCS) dates back to the initial concept stage conducted by Canadian Railways in the early 1980s. At this point, it is possible to summarize CP Rail's internal developments in ATCS to the present time and to outline what developments the railroad is considering in the next several years.

To date, CP Rail has accomplished the following:

- Developed and installed a computer-assisted dispatch system on all territory not under centralized traffic control (CTC);
- Developed and installed its own CTC office system with an eventual goal of a single parameter-driven office system;
- Demonstrated ATCS concepts with "in track" installations; and
- Progressed from the development of an "ATCS-like" system to a pilot production system.

Before expanding on the above it is useful to outline some of CP Rail's policies regarding its approach to ATCS development:

- CP Rail is its own systems integrator.
- CP Rail uses systems and components built to Association of American of Railroads and Railroad Association of Canada specifications wherever possible. Decisions to deviate from these specifications are made only after an analysis of the impact of that deviation. Equipment availability, implementation schedule, or testing ability are some of the considerations permitting deviations.
- CP Rail directs its efforts to systems intended for revenue service. This means that development must address such issues as robustness, serviceability, reliability, and above all, safety.
- CP Rail recognizes that implementation requires many years. Consequently, development and implementation proceed in incremental steps. Development must adapt and work with existing systems that cannot be replaced all at once.

R. J. Hipfner, CP Rail, 40 University Avenue, Suite 1200, Toronto, Ontario, Canada, M5J 1T1. R. A. Shea, CP Rail, P.O. Box 6042, Station A, Montreal, Quebec, Canada, H3C 3E4.

COMPUTER-ASSISTED DISPATCH

In 1985, CP Rail began production installations of a computer-aided manual block system (now called the occupancy control system, or OCS). Each rail traffic controller (RTC) has an OCS work station with the following features:

- Simultaneous entry and issuance of train and maintenance-of-way authorities by the RTCs. Advanced rules checking prevalidates menu choices and presents only valid options for selection. Forced rules items are inserted automatically on authorities during issuance;
- A graphics monitor that shows the subdivision in a train sheet format and individual locations in a station format like CTC;
- Minimal data entry and familiar formats, which means training can usually be accomplished within hours;
- Full backup and recovery of authorities and train supplies is provided. Information is automatically logged to a central computer in real time for long-term storage and second backup, and to feed other applications with train activity and location information;
- Data-driven rules and graphics. Mainframe data bases are updated by local personnel and automatically fed to the individual RTC work stations at shift transfer, which immediately reflect the table changes;
- Rules logic resides in the RTC work station. The RTC may continue dispatching without regard to the status of communication links to other computers;
- Tracking of manually operated switches permitted to be left out of correspondence. Subsequent train authorities over the switch are warned to normal the switch. OCS also tracks the reporting of normalling of switches;
- Compatibility with IBM PC family of computers; and
- Bilingual operation (French/English) where necessary.

CP Rail developed a version tailored to track warrant control rules for the Burlington Northern. Installations began in

1988. OCS or its derivative, computer track warrant control, is now in use on 85 percent of CP Rail track, as well as on Burlington Northern, SOO Line, Algoma Central, BC Rail, and Chicago Central and Pacific.

COMPUTER CTC SYSTEM

In 1987, CP Rail began work on an office system to communicate with and control the CTC field devices. It has the same design goals as OCS: table-driven graphics and rules, quick response, high-quality graphics, interactive rules on forms processing, mainframe logging, IBM-PC compatibility, low failure rate, and low mean time to recover.

Revenue service began in 1989. Five installations are now in use and several more in development. A second-generation CTC system is underway to attain the design goals more completely.

GENERIC DISPATCH SYSTEM

Since 1987, CP Rail has been steering its development efforts to a single integrated train-dispatching system. The goals are as follows:

- Reduce RTC workload by providing for single recording of train operating, status, or delay information;
- Reduce RTC stress by improving hand-off among the varying protection methods and rules;
- Improve system assurance and availability by reducing the variety of hardware components and connections;
- Improve information by capturing more data directly at the source and time of creation;
- Improve traffic control by consolidating all information faster and improving the quality of the decision making;
- Reduce installation and upgrade costs by building a single data-driven system; and
- Improve safety by reducing and streamlining the rules base.

CP Rail has some way to go before the ultimate goal is reached, but in increments and by careful design considerable progress is being made.

ATCS DEMONSTRATION AND PROOF OF CONCEPT

In 1980 and 1987, CP Rail installed and demonstrated remote switch control from a moving locomotive. Two different control systems were installed. Both interrogated switch position and allowed switches to be changed from the locomotive. Radio communication was used between the switch and the locomotive. Because only one locomotive was equipped for a particular switch, this demonstrated the principle but did not address the more complex problem—having multiple locomotives equipped with the ability to throw a particular switch and having only one locomotive at a time in possession of this control and all other locomotives locked out.

Automatic enforcement of authority limits and speeds was clearly demonstrated as being feasible. Apparatus was installed on one locomotive and proved to be effective in both slowing and stopping a train. The demonstration revealed that there was significant variation in braking performance and that considerable technical effort will be required to develop a means of predicting braking distance. Providing a braking algorithm that is selfcorrecting for the many variables that affect braking performance is now under development. Significant simulation and field-testing work has been carried out with additional testing scheduled for 1991.

ATCS PILOT AREA

In late 1987, a CP Rail group was given the mandate to implement an ATCS pilot project. From that time to about 1989, a detailed analysis was carried out to do the following:

- Define the expected outputs from the pilot project;
- Understand and interpret the industry specifications and identify the issues that needed to be addressed, particularly with respect to integration;
- Prepare a design and implementation sequence; and
- Evaluate apparatus being developed by various suppliers.

PRIMARY RADIO TESTS

During the initial stages to develop a design for the pilot project, an early conclusion was reached that communication in the 900 MHz bands could present a problem if CP Rail were to use existing base station sites. Consequently, CP Rail carried out a set of tests, using message success rates as a criteria for coverage and using radios and modems that were as close to ATCS specifications as were available at that time. These tests provided sufficient information to make CP Rail confident that the use of the UHF bands would not require a substantial increase in base station infrastructure.

The remainder of this paper will describe the purpose, approach, and implementation of the pilot project.

PILOT PROJECT

The pilot project can be best discussed under these headings:

- Policy,
- Purpose,
- Phased implementation,
- ATCS office components,
- ATCS on-board components,
- Software quality,
- Safety assurance, and
- Future phases.

For the pilot project, these specific policy decisions were made:

1. The primary use of the pilot project would be for train control. Secondary uses of the communication system could be examined in later phases of the project.
2. The installation would provide for a production system to be used in normal revenue service.

3. The system would provide for the simultaneous operation of trains that were equipped with ATCS apparatus and those that were not.
4. Integration and application programming would be carried out by CP Rail.
5. The ATCS communication 900 MHz frequencies and protocol would be used.
6. The design of the pilot would allow for installation, testing, and production implementation in discrete steps.

These specific policy decisions are consistent with the policy laid down in the earliest stages of CP Rail's development cycle.

PURPOSE

The decision to proceed with a pilot project was predicated on satisfying four major purposes:

1. To prove the ability to run a mix of equipped and unequipped trains (this was seen as the implementation scenario CP Rail would be faced with for some time);
2. To prove the ability to install functions in a progressive manner without interfering with railway operations;
3. To provide a platform for carrying out operational integration of components and subsystems from different suppliers; and
4. To provide a concrete means of establishing the costs and benefits of ATCS functions.

PHASED IMPLEMENTATION

It was determined during the analysis phase of CP Rail's development cycle that pilot project implementation was best thought about in terms of these specific functions:

1. Electronic transfer of train movement authorities from office to train;
2. Electronic transfer of crew acknowledgments or rejections of these authorities to office;
3. Provision for insertion into on-board devices of the train movement authorities that are issued to a crew by voice communication from the RTC; and
4. Reports of train location and speed using tachometer and transponder technology transferred electronically to the RTC work station displays.

Another consequence of the phased implementation policy was the decision to maintain existing operating rules. (Canadian railways all operate under the authority of a single rules set, the Canadian Rail Operating Rules, unlike U.S. railways, which have a proliferation of operating rules and practices.) ATCS specifications require adoption of another set of operating rules, one that is not in use on any existing railway. CP Rail decided that maintaining an operation with two differing rules sets was not an expense or risk that it was prepared to undertake.

Given this decision, CP Rail has maintained its use of OCS logic and rules. This led to the use of OCS data bases, data elements, and data messages that do not conform to ATCS Specification 250. However, where new data elements were needed, for instance transponder serial numbers, CP Rail adopted the specified ATCS format.

With the equipment installed in Phase 1, CP Rail is in a position to add and test additional functions:

- Switch control;
- Automatic track release using train tracking;
- Automatic brake enforcement;
- Issuing track occupancy permits to track maintenance forces.

As a major consequence of CP Rail's requirement and design philosophy of adding functionality in incremental steps, the system also allows for incremental fallback when parts of the system either fail or are unavailable. For example, if electronic data communication fails, an ATCS-equipped train does not inevitably revert to manual, paper-based authorities. If voice communication is operational, the train crew continues to use the on-board computer, entering the authorities into the computer as they are voiced by the RTC. An exchange of computer-generated cyclic redundancy check (CRC) codes between the RTC and the train crew ensures that authorities have been entered correctly on each of the computers. CP Rail has named this "voice/on-board terminal mode." When data communication is restored, the two computers immediately begin to use the data radio (DNET), by preference.

OFFICE COMPONENTS

The base for the new office system is OCS, but several changes and enhancements have been made for the ATCS pilot (see Figure 1):

- Split the existing OCS system onto two machines. The RTC interaction and rules verification modules are isolated on their own computer, separate from the mainframe communications modules on the server.
- Connect the RTC work stations to the server with a local area network. Ensure that a failed RTC work station can be rebuilt from the server, and the server can be rebuilt from the RTC work stations.
- Connect the ATCS radio data network interface to the server. Implement ATCS Specification 200, "wrapping" and "unwrapping" OCS clearances and messages to and from the mobiles.
- Design and build a DNET manager to handle and report on the messages, queues, trains, base stations, and other DNET components, both hardware and software.
- Enhance the RTC work station logic to handle multiple unsolicited updates, in this case from the RTC's keyboard and, through the server, the corporate mainframe computer, other RTC work stations, and the DNET.
- Add a larger, superresolution monitor to the RTC work station with simultaneous OCS- and CTC-style graphics. New icons would show the status of the new data available from DNET, such as a train's head-end and tail-end location.
- Enhance the RTC work station to implement new synchronization logic to ensure that both the train onboard com-

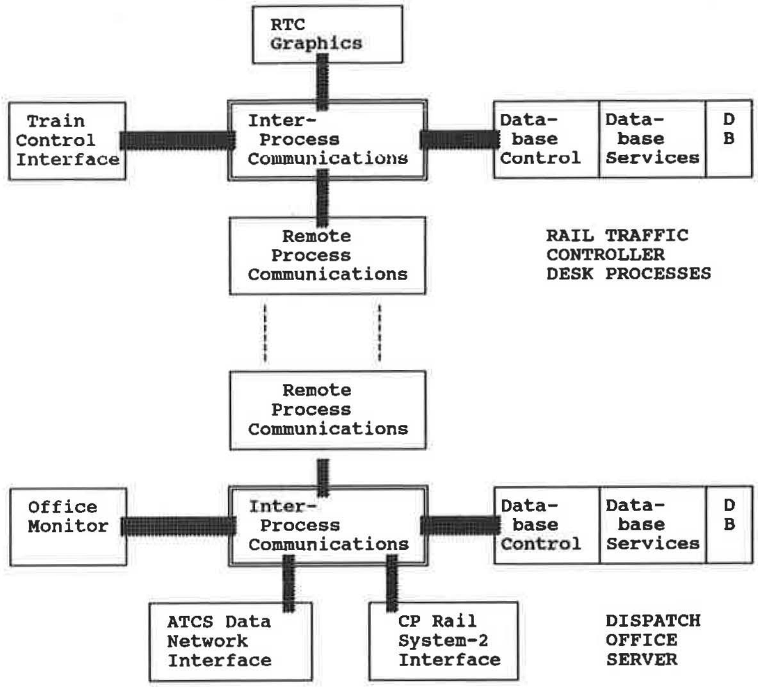

FIGURE 1 The office architecture.

puters and the office have protected their authorities. Calculate and test the check words for voice/on-board terminal mode.

- Add new logic on the RTC work stations and server to ensure that corrupted messages and data bases are detected immediately.

OFFICE COMPONENTS FUNCTIONAL BREAKDOWN

1. Train control interface

RTC functions

Train supply:	create, edit, delete, change lead unit, display
Authority:	issue, track release, cancel, acknowledge, change call time, display
Bulletins:	edit
Report times:	over main track switch
Switch report:	normalized report
Transfer:	same desk, new desk, mainframe, diskette
Sign-on:	recover, receive territory

Service functions

Switch status:	tracks the known position of manually thrown switches
First rules calculator:	calculates the valid options for authorities and supply choice, by display field
Second rules checker:	postvalidates the selected and generated authority items prior to generating a complete time for the RTC
Receive MTP supplies:	automatically introduces new train supplies, and updates to them, as received from CP Rail's master train plan (MTP)
Update graphics:	updates the RTC's graphics monitors when information is received, deleted, or modified
Local backup/recovery:	maintains a data image on local hard disk; rebuild random-access memory (RAM) data image from hard disk after power restored
Router backup/recovery:	maintain a data image on router disk; rebuild RAM data image from router disk after failed RTC work station replaced
RTC printouts:	print authorities, supplies, transfers, status reports on RTC local printer
Activity logging:	maintain an audit trail of RTC activity for problem analysis.

2. Router/server

Host management functions

Security:	validate RTC access, force password changes, control territory ownership
Session management:	maintain communications session with host, including error recovery and automatic application sign-on
Incremental download:	detects updates to MTP supplies and loads them onto the router
Initial download:	detects the out-of-sync condition for a territory's track tables, MTP trains, or complete operating sit-

uation and forces a full refresh of the necessary components

Incremental upload: logs any change in the operating situation (supplies, authorities, etc.) for backup and audit

Office functions

Distribution: queues and switches messages between the connected entities, the DNET, the RTC work stations, CP Rail's host

Backup/recovery: provides a second-level situation backup for the RTC territories, recovers an RTC work station on demand

DNET functions

Locomotive maintenance: establish a communications session between a locomotive and an RTC, ensure that on-board terminal/computer software is of the correct release/version, update the on-board track tables if necessary, terminate a session

Message tracking: transmit field-bound messages, track message status and retransmit as necessary; acknowledge messages arriving in assurance mode; track health of on-board equipment.

ATCS ON-BOARD COMPONENTS

The locomotive on-board configuration consists of two computers: (*a*) An input/output processor, which links the mobile communications package, the transponder interrogator, and the axle generators; and (*b*) an MS-DOS–compatible 80286 computer, which also provides a flat-panel 24 × 80 VGA display and a limited function keypad.

Applications programs for receipt and acknowledgment of clearances, creation of track releases, cancellation of clearances are resident on the second machine (the on-board terminal) and have been written by CP Rail. Internal logic is based on the logic of the office OCS process.

ON-BOARD COMPONENTS FUNCTIONAL BREAKDOWN

1. On-board computer

Initialization: establish the existence and status of the connected devices (transponder interrogator, dual tachometers, locomotive I.D. unit, on-board terminal [OBT], mobile communication package); obtain ground address table and send to OBT; report on-line status to OBT and office; set distance from zero for movement tracking

Message routing: routes ATCS Spec 200 messages to/from the connected devices; processes vital messages addressed to OBT as follows: on input, the on-board computer intercepts the message and does a CRC check before routing it to OBT; on output, the on-board computer intercepts the message and appends the CRC value before passing it to the mobile communication package; the onboard computer implements a 31-bit CRC failure check and sends message to office

Movement tracking: acts on a transponder hit and sends to OBT the serial number of the transponder encountered; each second reports (distance from last transponder encountered, tacho [i.e., wheel] direction, speed

Diagnostics: monitors status of connected devices and reports to OBT and office; on-board computer will not shut down if OBT link, or other device fails

2. OBT

Locomotive engineer functions

Train supply: display, edit train characteristics

Clearance: acknowledge, copy, cancel, change call RTC time, reject, track release, display

Coupling: report train coupled/uncoupled

Transfer: off duty, on duty

Time/date: manual correction

Sign-on: voice-respond to version request, mark track table as valid

Service functions

Power-up/sign-on: establish connection with on-board computer, initialize, respond to version request, check validity of track tables and software

Clearance: maintain synchronization with office—receive or reject clearances from DNET, allow or reject crew actions

Location tracking: report speed and location to office

Diagnostics: tests the state of the on-board computer link, manipulates mobile communications package via the onboard computer link

Message testing: generates a CRC for all application messages, ensures that both electronic and keyboarded messages pass the CRC check

SOFTWARE QUALITY

The largest problem CP Rail has encountered in building control system software has stemmed from the lack of understanding between the developers and the clients. For ATCS, CP Rail has instituted several types of documentation that help the designers clarify their thoughts and provide logical, complete guidance for the developers:

- *Principles of operation*—Describes the root concepts of the control system, including maintaining synchronization, effects of failure, recovery methods, detection of errors, etc. A small set of flow charts illustrates the more complex authority protection mechanisms.
- *OBT software, high- and low-level design*—Documents the functions, screen layouts, edits of each field, data flows, logic flows, and internal data bases.
- *Office architecture, high- and low-level design*—Describes the extensions to the OCS product, including the modified logic, data structures, interprocess communications, data flows, and logic flows.

Changes to the design documents are passed through a change control board, which includes both the developers and the client designers. Software is checked in and rebuilt by a control officer, who is independent of the development team. This officer checks coding standards, checks that the modules conform to standard quality metrics of complexity, ensures that documentation is complete and matches the code, and protects the module by submitting it to version-controlled backup.

The control officer is also responsible for testing, documentation of the tests, tracking of defects, and final resolution. Testing is carried out by experienced independents in a site off the development floor using both white box and black box principles.

Much of the regression testing has been automated with programs and computer files of previously generated tests. Test machines have been set up to generate bad data into the on-board computer, respond incorrectly to good queries from the OBT, and pretend to be a misbehaving data network—to give some examples.

CP Rail decided as well to include the radio system components as part of the test facility. Thus, several levels of stepwise testing and integration have been possible without resorting to field work.

SAFETY ASSURANCE

The OCS office program is the basic protection against the generation of authority overlaps. It presently has two separate and distinct algorithms for checking and rejecting potential overlap conditions, as well as ensuring that all dispatch rules have been complied with in the generation and issuance of an authority. With the development for the pilot project, some fundamental considerations have been established as a result of the design process and the fault analysis contained therein. Examples of this are as follows:

- The crew will remain in the control loop for all processes associated with the granting, altering, or cancelling of movement authorities.
- Basic functions are protected by at least two checks, e.g., OCS has two separate algorithms for overlap checking. Assurance that a clearance as generated by the RTC on the OCS system is replicated exactly on the locomotive is provided by having an independent mathematical check carried out on the complete text of the authority as displayed on the OCS machine and on the locomotive OBT. The mathematical check is carried out by a different algorithm on the OCS machine than that used on the locomotive. Note that this check is over and above the cyclic redundancy checks being carried out on the messages moving between the office and the locomotive.
- The loss of a message never results in the potential for the generation of an unsafe condition.
- Messages arriving in a different sequence than that in which they were generated will not result in an unsafe condition.
- Messages from the office crossing messages from the locomotive cannot result in an unsafe condition.
- Temporary failures, however short, of any component (for example, loss of power to an on-board computer or OBT) will require complete consistency checking between the office and the locomotive.
- Software and data base version checks are inherent in all activities.

Future Phases

The 1991 pilot between Calgary and Edmonton will be incrementally expanded in future phases. Once confidence in location tracking has been established, we will move to automatically release track behind trains operating with proceed clearances. Both portions and entire clearances could be released by the OBT logic, using the identical logic now used in the OCS system.

As OCS currently tracks the reported position of manually operated switches, it is a small step to centrally control the position of powered switches, incorporating the CTC control logic already developed. However, CP Rail is still studying the merits of direct locomotive control of the switches through the on-board computer and the operational considerations before committing to either central, distributed, or dual-switch control.

Considerable effort has been expended on the development of a braking algorithm. CP Rail's approach is to develop a self-correcting algorithm that will converge from an initial, conservative, braking curve for a given consist toward an algorithm tailored for the actual operating characteristics of the train, track, and conditions. Each braking action taken by the locomotive engineer would add to this data base and improve the situational algorithm. Pilot implementation of such a predictive algorithm is a priority item but will require significant additional effort. Testing and development is continuing.

In a recent RTC workload study it was noted that, where train lineups have been abolished, more than 50 percent of the RTC's time is spent dealing with maintenance-of-way forces. CP Rail is looking at automating both the delivery of real-time train location and speed, and the issuing of the authority to occupy the track. These functions are likely to be deployed on several technologies using both fixed and mobile communications.

CONCLUSION

Compared to some other railroads, progress on ATCS at CP Rail may not have been as observable. The deployment of the live pilot this year in the Calgary–Edmonton corridor should go some way toward changing this.

The unique element, an incremental approach to deployment, matches more closely CP Rail's tradition of installing new technology on a steady timetable. This approach allows safety to be maintained and new methods adopted in small, manageable increments where affordable and where benefits are obtainable.