The comprehensive development and installation of computer based signalling for a fully automatic mass transit system operating in Germany

G. Mutone & S. Lehmann
AEG Transportation Systems, Inc., Pittsburgh, Pennsylvania, USA

Abstract

The development and installation of an Automatic Train Control System (ATCS) for the automatic Passenger Transfer System (PTS) at the Frankfurt airport is described. The paper focuses on measures that were taken in the selection and segregation of functions and the selection of a development process that permitted an effective utilization of various computer technologies so as to achieve a cost effective and fast design, compliant with well defined and demanding regulatory requirements in Germany. Details are provided on the segregation of safety functions from all the other functions, on measures taken to facilitate the safety/reliability assessment by an independent organization, and on features incorporated to enhance the resistance to obsolescence and to facilitate the introduction of changes after installation. The featured German project shows that, if the right approach is followed, real-time computers can be utilized quickly and in a cost effective manner to meet the very demanding safety and reliability requirements associated with the rail signalling applications.

1 Introduction

In the design of an Automatic Train Control System (ATCS), the key questions are:

- What are the relevant Automatic Train Control (ATC) functions?

- How can the ATC functions be best segregated to optimize the relative design process?
- What criteria should be used in implementing the key ATC functions, especially in the safety area?

- How can the advances in microcomputer technology be exploited to optimize the ATC implementation, and broaden its scope?

- How can the right design of the ATC computers, especially those that perform safety critical functions, be sufficiently checked out?

- How can the development of ATC computers take full advantage of the constantly increasing capability of microcomputers?

This paper proposes answers to these questions that come from the long experience that AEG has had in the design of ATCS for a variety of automatic mass transit systems. This experience culminated in the ATCS built for the Passenger Transfer System (PTS), featured here, which AEG designed for, and installed at the Frankfurt-on-the-Main airport in Germany. While the PTS, referred to generically as a people mover system, operates only on the short distances peculiar to airports, it has all the elements of any other mass transit system which AEG also makes, and complies with the same German regulations that any public automatic subway or railroad in Germany must comply with.

2 What are the Automatic Train Control (ATC) functions?

Broadly speaking, the ATC functions are the same functions that are performed by people in a manually controlled train system, on board and on the wayside. They are:

Speed control: the propulsion and breaking systems of a train are controlled to maintain a pre-determined schedule, including stops at stations, while maintaining a suitable level of comfort to the passengers and avoiding collisions.

Door control: the doors are opened and closed so as to allow safe access and egress from a train.

Switch control: the guideway or track switches are controlled to allow the implementation of the various routes in a safe manner, without causing collisions.

Passenger interaction: passengers, on board and at the station, must be informed on the itinerary of the train, and given the means for reporting problems.
In many modern train systems some of these functions are already handled by computers, which are used in a role that aids and supports human operators. However, a train system is not considered automatic unless all the train control functions are handled by computers. Thus, in a fully automatic train system the human intervention is strictly supervisory. This means that there is nothing new in the ATC functions, since they are the same as the "manual" train control functions. The only difference is in the fact that the ATC functions are carried out by computers. There are other functions handled by computers in a train system, like propulsion control, passenger service, heating and air conditioning. But these functions have nothing to do with the operation of the train and are commonly handled, up to now, by dedicated computers that are delivered as integral parts the devices they control.

As in all transitions from manual to automatic computerized operations, the switch from manual train control to ATC begs the important question: should the organization of the functions that are going to be automated be changed so as to be best suited for computer handling? This question is not always asked ahead of time, which leads to microcomputer control systems that, being based on a set of functions that were developed and configured for human implementation, are often more expensive and more unreliable then they need to be. This is not the case for ATC functions, for which an affective segregation has emerged of the past two decades of ATCS experience. This segregation of functions is receiving wide acceptance because it takes into account both the needs of the developer to shorten the design cycle and those of the customers to maximize flexibility and minimize costs. This applies to both new installations as well as the expansions of the train systems already in operation.

3 What is the optimum way to segregate the ATC functions?

The first and foremost goal to reach in the segmentation of the ATC functions is to isolate the safety sensitive functions, referred henceforth in this paper as the Automatic Train Protection (ATP) vital functions. The implementation of the vital functions, which preserve the ultimate safe operation of the train system, is the most critical and rigorous when compared with the implementation of all the other functions. Therefore, by isolating the ATP functions from the others, which are non-vital, it is assured that the design scope of the needed "safety" computer that implements them is not larger than it should be. If this were not the case, and vital ATC functions were mixed with the non-vital functions so that they could not be distinguished from each other, the entire ATC set of functions would have to be implemented as if they were all vital. This would be the only way to guarantee the required level of rigor in the realization of the vital functions. The approach, however, would be wasteful at best. The isolation of these vital functions brings other dividends, relevant both to the developer and the user of the train system. One dividend comes from the fact that the basic ATP functions are simple and universal, that is, they do not
Railway Operations

generally change as the train technologies advance. Therefore, the design of the ATP computer has the best chance to effectively withstand obsolescence.

The ATP functions of the PTS in Frankfurt are listed below as an illustration. They are common to any fully automatic train system.

Issuance and enforcement of speed limits: Appropriate speed limits are calculated on the wayside for each block of track and transmitted to the trains, based on the relative presence of stations, switches and other vehicles. These speed limits assure that in the worst conditions, any train has a long enough stopping distance ahead. The ATP computer must independently apply the emergency brakes anytime the speed limits are exceeded by the respective vehicle. It is to be noted that the ATP computer is not to control speed, but rather just monitor it and turn on the brakes if the speed goes over the limit. This is a simple, well defined and clear function.

Door interlocking: The ATP must keep doors locked at all times. The doors can be unlocked (which does not necessarily mean that they will also be opened) if the train has a vitally detected zero speed, its brakes are applied and the train is located at the appropriate points along the track, like stations. To be noted here, again, is the fact that the ATP is not to control door operation. Rather, the ATP must assure that door are not opened if it is not safe to do so, which is a very simple and clear function.

Switch interlocking: As for the doors, the ATP must keep the track switches locked at all times. The switches can be unlocked only if, based on the location of trains around it, the resulting routes through the switches do not result in train collision with the switches themselves or with another train. This function is also straightforward, independent of any particular routing in effect.

The implementation of these three simple functions assures the safety the PTS, thus making the implementation of all the other functions independent of any safety issue.

The ATP functions make up only a small subset of the ATC functions, which are mostly non-vital. The implementation of the non-vital functions, with safety concerns out of the way, is straightforward. For reasons that are strictly related to computer implementation, these non-vital function are divided into two categories, one comprising the Automatic Train Operation (ATO) functions and the other the Automatic Train Supervision (ATS) functions.

The ATO functions include all the actions that are associated with the operation of the train. The functions implemented at the Frankfurt airport PTS application, listed below, are typical for any automatic train system:
Speed control: The ATO computers must be able to control the speed in the various sections of the track in a way that not only assures passenger comfort, but also complies with the maximum speed limits established by the ATP computers. With the vital aspect of speed out of the way, handled within the separate ATP functions, the non-vital aspects associated with comfort, schedule and other requirements can be handled in the most effective way within the ATO functions. For example, the relatively complex program stop function in which the train comes to a smooth stop within a station and the train doors open in synchronism with the corresponding station doors, can be handled in a non-vital manner.

Door control: The ATO computer must issue the necessary door commands to open and close doors, as required in connection with station stops. As for the speed control, this is a non-vital function, because the ATP computer will actually not allow a door to open unless it is safe to do so.

Passenger information: A significant portion of the ATO functions deal with the customary audio and visual means used to inform the passengers on the operation of the trains. These are typical train operation functions that even today, in the manually controlled systems, are handled in large part by computers.

The only general requirement on the design of the ATO computers is in the special environment in which they must be designed to operate. This is a rugged environment, especially for the on-board equipment, subject to extreme temperature excursions and shock.

The ATS functions are associated with the general operation and supervision of the train system. The ATS system installed at the Frankfurt airport is designed to perform the following functions:

Route and headway control: The ATS must, based on a specific mode of operation selected by a central operator, command speed levels and switch motions as required to achieve the appropriate train route and schedule.

Performance monitoring: The central operator must be able to monitor any aspect of the train system, from the overview of the entire system to the real-time behavior of every single control signal. A diagnostic utility must also be included to aid the operator in the quick resolution of any problem that might arise. AEG normally specifies a backup computer that is immediately activated as the first step in most trouble recovery procedures.

Alarm handling: All the alarms generated throughout the PTS must be received by the ATS and appropriately annunciated.
Report generation: The ATS must record the operating history, including all operator interactions. The data are then searched when a request is made for a report. The reports cover any aspect of the PTS performance, during any specified time span.

Since all of the ATS functions are carried from a central location, there are no hard requirements on the respective computers, beyond the performance requirements. The emphasis is on the use of commercially available workstations, with advanced display and communication capabilities. The ATS for the Frankfurt PTS, for example, utilizes color monitors, touch screens and input/output devices that can be used to perform the supervisory functions from remote terminals located anywhere in the world, using common telephone lines. Such capability is normally utilized only for customer support and trouble shooting of an installed system from the AEG factory in Pittsburgh.

4 What are the design criteria to follow in the implementation of the ATC functions?

In establishing the design criteria on which to base the design of the ATP, ATO and ATP computers, one is faced with two key questions:

A. When is the design of the vital ATP computer safe enough?

B. What will maximize the ability to expand the ATC functions?

Most of the difficulties associated with the design of the ATP computer come from the fact that the design work normally starts and ends without first providing a full answer to question A. As a result, for most implementations, the level of safety ends up being whatever happens to be worked out among the supplier, the customer and its consultants. However, this is not the case in Germany, where standards are in place with clear design criteria for the various rail applications. These criteria were applied in the design of the ATP for the PTS at Frankfurt airport, as described in the paper by Mutone & Rothfelder [1]. According to this paper, the two fundamental regulations applicable in Frankfurt are BOStrab [2] and DIN VDE 0831 [3]. DIN VDE 0831 stipulates that the ATP functions are to be "signal-safe", which defines precise testing criteria to ascertain compliance. There are instances, however, in which neither one of the above two regulations is directly applicable, as in the design of the software. For these cases the regulations ask for the application of other German and international standards that represent the state of the art. This meant that, for the PTS, the additional German standards DIN V 19250 [4], DIN V 0801 [5] and MÜ 8004 [6] were applicable. There is an increasing interest in the rest of the world to follow the same process in the design and certification of vital ATP
computers, since the German process is mature, well defined, sound and achievable.

As for the second question, there happens to be one criterion that will provide the best chance for future expansion, and that is in the implementation of all the ATC functions exclusively in the computer software. This will allow the design of the computer hardware to be completely independent of the functions that are performed. The hardware can thus be generic, consistent with commonly used open architecture and, as such, easily upgraded in the future. The software, on the other hand, should also be modular and written in high level languages that are commonly used, compatible with open and commercially available operating systems.

5 How can modern microcomputers be exploited in the implementation of the ATP functions?

The development and certification of vital ATP computers have been in the past extremely expensive and time consuming. It turns out, however, that these high costs and long development times can be drastically reduced if a recourse is made to the Knowledge-Base/Inference-Engine techniques devised lately in the computer application industry dealing with Expert Systems. Using these well known techniques it is possible to develop a single generic computer certified to execute vital ATP functions for any configuration of the train system. This is done by developing and certifying a computer software package that performs the function of the ATP expert designer, rather than certifying the specific ATP functions themselves, which vary from application to application. The result is an ATP computer that is certified a priori for any configuration of the train system. The difference among the different systems is handled through definition files that the unchanged ATP software reads during initialization. The technique was used in the development of the ATP computer for the Frankfurt PTS, as described in the paper by Mutone and Daubner [7].

6 How can the design of the ATC computers be efficiently verified to perform the relative functions properly

The best way to demonstrate that all the ATC functions are implemented properly, especially the vital ATP functions, is to engage since the early stages of the design process an independent expert organization that continuously checks not only the result of the design work, but also the underlying design process itself. The expert organization involved in the development of the ATP for Frankfurt is TÜV Rheinland. TÜV Rheinland used the so called Project Accompanying Safety Certification (PASC) strategy, which it developed to significantly shorten the time required to both design and validate the ATP computer. The paper by Jansen and Haspel [8] describes the details. Thanks to
this technique, the ATCS for the Frankfurt PTS is being specified, designed, built and formally checked out according to all the applicable German regulations in less than three years.

7 What is the next step in ATC development?

The next step in the utilization of microcomputers for the realization of the ATC functions is to take advantage of the considerable computational power that modern microcomputers have by integrating all the non-vital train functions in a single computer. Such functions would include propulsion control, passenger service, and the control of auxiliary equipment. Eventually, there will be only two computer systems, on board or on the wayside. A vital computer will implement the ATP functions and a non-vital one will carry out all the other functions. The non-vital computer will take the place of as many as five to seven computers that often are found in the cars and locomotives of today. While the integration of all the functions will not be easy because of the liabilities associated with the control of the subsystems normally supplied by different suppliers, the complete integration will occur because of the tremendous simplification of operation and maintenance that would result. The availability of commonly used software operating systems will make such integration feasible, without affecting significantly the supplier's liabilities involved.

8 References

3. DIN VDE 0831/08.90 Elektrische Bahn-Signalanlagen
4. DIN V 19250/01.89 Messen-Steuern-Regeln: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen
5. D5N V VDE 0801/01.90 Grundzätze für Rechner in Systemen mit Sicherheitsaufgaben
6. Grundsätze zur technischen Zulassung in der Signal-und Nachrichtentechnik (Mü 8004), Deutsche Bundesbahn, Bundesbahn-Zentralant München, 01.02.1993