Independent safety assessment of a computer based signalling system - progress report

J. Catmur[a], F. Fabbian[b]
[a]*Arthur D. Little, Science Park, Cambridge CB4 4DW, UK*
[b]*MTRC, Chevalier Commercial Centre,*
8 Wang Hoi Road, Kowloon Bay, Hong Kong

Abstract

The Hong Kong Mass Transit Railway Corporation (MTRC) has undertaken a major project to replace their existing Automatic Train Control (ATC) system with a new system (the first such project in the world). As part of this project they appointed an Independent Safety Assessor (ISA) who would act as an independent auditor of the development of the new signalling system and who would report their findings back to MTRC for action. At two previous Comprail conferences MTRC have reported on aspects of this work. By the time this paper is presented MTRC will have started service with the new system, so this paper presents the overall programme the ISA has followed and gives an overview of the results achieved.

1. Introduction

The Hong Kong Mass Transit Railway Corporation (MTRC) has undertaken a major project to replace their existing Automatic Train Control (ATC) system with a new system. Throughout this project (the Automatic Train Control Replacement Project - ATCR) MTRC have been aware of the need to ensure the safety of the final system and have taken appropriate measures at all stages of the project to ensure that the final system will provide a safe means of transport for the travelling public in Hong Kong.

In order to help ensure the safety of the final system MTRC decided to appoint an independent safety assessor (ISA) who would have a role in auditing the work of both MTRC and the system's supplier. The results (findings) of these audits were then used to help the MTRC manage the safety of the final system.

1.1 Scope and Objectives of the ATCR Project

Since the MTR opened to the public in 1979 the patronage has increased from 400,000 to over 2.4 million passengers per day which represents approximately 25% of the total passenger journeys by public transport in Hong Kong. To meet this continued increasing passenger demand, there is a need to reduce headway and therefore replace the existing ATC system. The main objectives of the new ATC system are to reduce headway, maintain or improve the existing safety level, reduce the costs of maintenance, and to increase both the reliability and availability of the railway.

With the new signalling system, the overall system performance will be improved with respect to existing systems or sub-systems ensuring the same functions. The main improvements are :

- dynamic performance, i.e. reduction of headway,
- regularity, through the increase of headway margin with respect to nominal headway and the possibility of self-regulation on each train,
- overall availability, taking into account the degraded modes through the rational use of re-configuration and fallback mode to maintain service while minimising the amplitude of disturbance following local failures,
- provision of data exchange facilities between train and track, for both safety data and non-safety data,
- reduction of installation and operating cost, and
- improved quality of ride

1.2 Safety of the Final System

The safety of the final system will depend on a number of factors. Clearly the project must ensure that the chance of an unsafe failure of the signalling system leading to an unsafe situation is reduced to a tolerable level. MTRC must also ensure that the need to continue operation after a 'safe' failure of the signalling system does not cause other unsafe situations to arise (for example, while working over failed track circuits). If MTRC are to ensure that the chance of such an unsafe situation is tolerable the project must ensure that the causes of such failures have been managed appropriately at all stages of the project.

The causes of such failures are commonly described as being either due to random failures or systematic errors. Random failures will arise when equipment fails due to age, wear or other reliability problems. Systematic errors will arise if the system is incorrectly specified or if design errors are made while developing or installing the system.

The ISA had a role in auditing all the activities involved in this project, including those associated with estimating the chances of random failures as well as those used to avoid systematic errors.

2. Project Programme

The ATC replacement project involves the replacement of all trackside and trainborne equipment of the existing system with all new cabling, fixed and trainborne equipment for the new system. For the Kwun Tong and Tsuen Wan Lines all the existing track circuits will also be removed with associated equipment such as impedance bonds and Insulated Rail Joints.

To enable the regular service to continue during this changeover it is necessary to first install, test and commission all of the new trackside equipment, whilst leaving in service the existing ATC system. Next the trainborne equipment will be progressively changed over. The existing ATC System cannot be decommissioned until all of the rolling stock has been fitted with the new system. Therefore two ATC systems will be operating simultaneously for a number of years. This is seen as one of the most safety critical aspects of the project and MTRC have, therefore, taken special measures to ensure that it does not present unacceptable safety risks, including the appointment of an ISA.

3. Project Organisation

To manage this project the MTRC has appointed a project team comprising Design and Implementation staff who are to approve and witness the works by the contractor. The MTRC project team comprises existing staff transferred from the Design and Implementation sections of the Engineering Department. At peak resource demand this project team has totalled 50 people.

This project team has been responsible for all control, co-ordination and management of the supplier. To assist in this activity MTRC have chosen to appoint an Independent Safety Assessor (ISA), Arthur D. Little who have been responsible for auditing the activities of both the MTR and supplier project teams and for reporting their findings back to MTRC in order to allow MTRC to take the action they deemed necessary.

The Independent Safety Assessor (ISA) was appointed to audit both the supplier and MTRC project teams against their systems assurance and safety plans and to feed their findings back to MTRC for action.

4. ISA Activities

4.1 Overall Audit Programme

During this project the ISA has been involved in carrying out both pre-tender and post-tender audits of the supplier.

Pre-tender Audits As part of the tender evaluation MTRC commissioned a series of studies (already reported to COMPRAIL) on the new ATC as they wished to ensure as far as possible that:

- the core ATP system they are purchasing is capable of delivering the level of safety required,
- the supplier has methods in place needed to make any required modification to the core system, and
- no special hazards exist which could not be managed within the time scale involved in this application of an existing system.

As a result of these studies MTRC had some confidence in the supplier's ability to deliver a system which could be installed and operated safely.

Post-tender Audits Once the contract had been awarded MTRC recognised the need to ensure that the final system actually achieves the desired safety

levels. MTRC therefore decided to appoint an Independent Safety Assessor (ISA) who would, through audits of the specification, design, development, approval and installation processes, help MTRC ensure that the supplier and MTRC meet the safety requirements.

The ISA Safety Plan details the work that the ISA carried out in order to achieve the aim given above, and an abstract of it is given below.

4.2 Detailed Audit Programme

The new ATC is based on an existing system which required: some modification of the core software and hardware in order to adapt it to MTRC's needs; specific designs for each line; approval of these designs; installing, testing and commissioning; and finally operating. The ISA has five areas of responsibility during the ATCR project:

- **Supplier Development Audits:** Carrying out audits of the supplier's work in modifying the core software and hardware and of their manufacturing processes. These audits aim to ensure that the supplier complies with the Project Safety Plan and continues to maintain the necessary controls that were identified, and considered suitable, during the pre-tender assessments of their system.
- **Supplier and MTRC Installation and Commissioning Audits:** Carrying out audits of the design approval, installation, test and commissioning processes in order to ensure that they meet the standards agreed upon by MTRC and the supplier, and that these standards in turn represent good practise for such a safety critical system. These audits are carried out for system safety while MTRC's Safety Services Department is responsible for industrial hygiene and safety audits. This work therefore includes review, with the aim of confirming compliance with their respective Safety Plans, of the documents, plans, programmes and work carried by both the supplier's and MTRC's ATCR Project Teams.
- **Safety Audit Reports:** Issuing Safety Audit Reports (SAR) for each audit that is carried out. An SAR indicates the work undertaken by the ISA, and any findings that arose.
- **Developing and maintaining an ISA Safety Plan:** In order to ensure that the work carried out by the ISA achieves the requirements of the Project Safety Plan the ISA developed and maintained a plan for the ISA's activities.
- **Liaison and Reporting:** Reporting to MTRC on the progress of the work which has been carried out. This includes reports on each audit carried out, quarterly progress reports, tracking of the resolution of findings, updates of the ISA Safety Plan, attendance of meeting called by MTR, and general liaison with MTR staff on the ATC project.

Summary of Audits

The work outlined above includes a number of audits which are being carried out in France and Hong Kong. The table given below presents a summary of the audits. For each type it indicates the number of audits, duration, status, scope, and timing.

Type	No.	Duration	Status	Scope	Timing
Design and development work at the supplier	4	2 of 1 week 2 of 2 weeks	1 complete, 1 - 50% complete 2 complete	Basic ATP specification, design, development, testing and validation	During first 24 months of the project
Installation and commissioning work by the supplier	3	2 weeks	1 complete	All site work carried out by The supplier	Every 6-9 months during these phases
Design and review activities carried out by MTRC	2	2 weeks	1 complete	All review and design work done by MTRC	
Additional audits	1	2 weeks	2 days	Any of the above	As appropriate

5. Results of the Audits

This section gives a general overview of the findings and an example of how resolution of the findings was tracked.

5.1 Types of Findings

In order to give a better understanding of the type of findings this section gives a brief summary of the main classes into which the findings fell and the typical importance the ISA have given to each class. The ISA can in general classify the findings as being in the following areas:

Management

- Lack of well defined responsibilities for different teams or members of project teams. The ISA felt this to be an area of importance and stressed the need to improve this where found.
- Lack of a clear definition of the activities that were to be carried out. The ISA typically considered these to be of medium importance, unless the activity had a major role in assuring the safety of the system.
- Not following defined processes, and/or not justifying or documenting the changes made to the processes. The ISA considered these to be some of the most important findings made and placed significant emphasis on their resolution.
- Problems with co-ordination and data flow between different team. These were considered to be of major importance as interfaces are often the most critical aspects of a project of this nature.

Documentation

- Inconsistencies between similar documentation or between writers guides and the final document. The ISA generally considered these to be of low to medium importance.

- Problems with understanding the role of the documentation developed, or confusion caused by documents that gave different definitions of very similar activities. These were normally considered to be minor, unless the documentation was of significant importance.
- Lack of key documentation. This was normally considered to be of medium to high importance.

Methodology

- Activities that did not fully address the objectives defined for them or what was required to ensure a pro-active approach to safety management. These ranged from minor to major concerns.
- Areas where the methodology used could better respond to the safety requirements of the project. The ISA normally considered these to be of medium concern.

Progress

- Lack of progress in the project. Where the ISA felt that these could put pressure on the final stages of the project and thus potentially cause safety concerns to be overlooked or not correctly managed the ISA considered them to be major concerns.
- In certain cases critical activities were not being carried out within an appropriate time scale. The ISA considered these to be significant.

Traceability and visibility

- The traceability of changes was not always clear. Minor problems were considered to be of minor importance, but in a few cases the ISA considered the findings to be important.

Safety studies

- Areas where safety studies needed to be amplified or completed before the start of service. These ranged from low to very high importance.

5.2 Resolution of Findings

As an example, the percentage of findings resolved is, as would be expected, higher for the earlier audits and in general has shown a clear commitment by both MTR and the supplier to close findings and to thus improve their processes and respond to our concerns.

- Of 17 findings from the first visit to the supplier 14 (82%) have been resolved and some action has been taken on all of them but one.
- Of 21 findings from the second visit to the supplier 14 (67%) have been resolved and some action has been taken on another five. In one case no action was taken and the remaining one will be finalised in the near future.
- Of 25 findings from the first visit to Hong Kong 22 (88%) have been resolved and some action has been taken on all of the remaining three.
- Of 15 findings from the third visit to the supplier nine (60%) have been resolved and some action has been taken on two other findings.

So overall from the first four visits 75% of findings have been resolved. In the cases where the ISA was particularly concerned over the non-resolution of a finding the ISA have carried it forward into later audits and re-raised it as a new finding, so the ISA can essentially consider these audits to have been closed of all major findings.

For the more recent audits there has been less time for findings to be resolved so the overall percentage is lower (the last audit was completed on the 3 April 1996). The ISA has, however, noticed that both MTR and the supplier have made significant efforts to resolve those findings that the ISA considered to be most critical to the safety of the overall signalling system.

During the last audit carried out before the start of service the ISA conducted a full review of all remaining major findings in order to ensure that none of significant concern have remained open. At the time of writing this paper there were only four findings remaining that give significant concern, and MTRC fully intend to ensure that these are closed out before the start of revenue service.

6. ISA Conclusions

The ISA audited the activities of both the supplier and MTR and found a significant number of findings. These findings were reported to MTR action was taken to resolve them in a timely manner.

The ISA concluded that the activities carried out to analyse and manage the safety of the system would in general be considered to be appropriate and during the audits the ISA did not find any major areas of concern in this work.

7. Conclusion

For MTRC this project was the first that used an ISA to assist in managing the safety of the final system. As this involved the replacement of a system that is critical to the safety of the railway MTRC felt, from the outset, that this could only be beneficial.

Now that the project is nearing completion MTRC can see the benefits of the presence of an ISA on the project. As expected the ISA generated a number of findings and MTRC had mechanisms in place to help the project team take action to ensure that these were resolved. MTRC believe that this approach has helped all parties involved ensure the optimal management of the safety of the system and the presence of an independent assessor, with no contractual responsibilities for completion of the project, has had a very positive impact on the project and has reaffirmed MTRC's confidence in the system's safety.