Automated Metro – Ensuring Safety and Reliability with Minimum Human Intervention

Yap Kwee Seng, Ng Hon Wai,
Dr Samuel Chan, Leong Kwok Weng
Systems Assurance & Integration Division
Engineering Group
Land Transport Authority, Singapore
Kwee_Seng_Yap@lta.gov.sg; Hon_Wai_Ng@lta.gov.sg;
Samuel_Chan@lta.gov.sg, Kwok_Weng_LEONG@lta.gov.sg

Abstract. Modern transit systems are very complex and have high level of automation. The introduction of fully automated metro system has greatly reduced the dependency on human to drive the train and offered greater flexibility in the system operation. Prior to the implementation of each new automated metro system, extensive study has to be undertaken to ensure that the safety and reliability of the automated system will not be compromised.

The paper describes Land Transport Authority (LTA)'s systems engineering process on safety and reliability for the design and construction of automated metro system projects in Singapore. The approach adopted has been proven to be successful through its implementation on several recent projects in achieving a high level of safety and reliability of automated metro systems.

Introduction

Land Transport Authority (LTA) of Singapore started the development of North East Line (NEL), a driverless Mass Rapid Transit (MRT) system, back in mid 1990s. Prior to that, LTA introduced the first driverless Light Rail Transit (LRT) in Bukit Panjang estate in 1999 followed by SengKang and Punggol LRT in 2003 and 2005 respectively. The current ongoing projects are the Circle Line (CCL) and Downtown Line (DTL) and will also be fully automated driverless systems.

Drive for Automated Metro

The LTA's drive for fully automated metro started back in the mid 90s, where a few overseas study trips were made to United States (Miami, Vancouver), United Kingdom (Docklands), France (Lyon) and a couple of Japanese light rails. From the trips and other extensive researches, LTA was confident that the technology was available and proven to develop a driverless metro system.

The existing North-South-East-West line trains are provided with Automatic Train Operation (ATO) functions together with the time-tabling facility in the Automatic Train Supervisory System (ATSS) runs the system under normal conditions without much human intervention. This results in the Passenger Train Operator's (PTOs) job being quite monotonous for most of the time and has led occasionally to incorrect actions through inattention. Furthermore, the Operator has had difficulty in recruiting PTOs for the new trains that commenced service on the Woodlands Line back in 1992.

Having a fully automatic metro system provides the Operator with the flexibility in the daily operation to introduce or withdraw trains in response to the passengers' demand. Trains can be introduced into the network easily without the need to rely on the availability of the PTOs.

Drive for a Safe and Reliable Metro

The LTA's mission is "To provide an Efficient and Cost Effective Land Transport System for Different Needs". In the context of metro systems, an efficient system must be highly reliable and must provide a Quality of Service that is acceptable to the passengers. Effective application of Reliability, Availability, Maintainability and Safety (RAMS) management and engineering over the system lifecycle is a key success factor for meeting this objective and especially so for fully automated metro system.

An "Operations-Centric" RAMS policy has been adopted for metro system. The basis and rationale for determining RAMS requirements focus on their influence on operational safety and performance of the metro system. This provides the directions for determining the breadth and depth of RAMS requirements at an appropriate level, and for tailoring a RAMS programme that would be cost effective towards meeting the objectives.

The four prong approach adopted throughout project life cycle for achieving a reliable automated systems are described below:

a) Overall system design/architecture for fully automated system
b) RAM management Process
c) Safety Management Process
d) Testing and Commissioning Process

Main Technical Features for an Automated Metro

In a conventional metro system, the driver is required to handle faults such as resetting of trainborne equipment to allow train operation to continue. In today's technology, the effect of equipment failure affecting operation is minimised by having the system designed with a high levels of Reliability and Availability through the use of redundancy and hot standby configuration.

The operation of a fully automated metro requires a high level of system reliability. In addition, provisions have to be made that if a failure does occur, procedures and systems are in place to ensure that the degraded system can continue to operate safely.

In the event that a fully automated train is stalled in between two stations due to ATO system failure, the Operation Control Centre (OCC) is able to remotely move the train to the nearest station in a safe manner. At the same time, OCC is able to view the situation in the train using the closed circuit television and if required, make public address broadcast to the train to allay passenger anxiety.

In general, fully automated metro are required to be designed with high reliability and redundant system arrangement. This has resulted in several new developments using latest technologies at the time. Examples of new requirements include the following core systems:

- Signalling system – Fully redundant trainborne Automatic Train Control (ATC) system using hot standby design; reliable point machine and track circuit; High availability of the ATC trackside system using 2 out of 3 redundancy architecture and Computer Based Interlock (CBI) using hot standby architecture.

- Communication – Communication Backbone Network (CBN) is fault tolerant and provided with seamless self-healing facilities; Two way communication between passengers and the OCC available via the Passenger Emergency Communication (PEC); In-car CCTV monitoring.
- Rolling Stock/Train – independent traction voltage circuit and propulsion systems on each half of the train; All major equipment/control systems, including the Train Integrated Monitoring System (TIMS), are with redundant design to ensure that a single equipment/system failure will not immobilise a train; Critical train control functions such as emergency brake, traction voltage control circuit, propulsion control and interfacing with the ATP system, employed hardwired interfacing circuits to ensure high reliability and predictable failure modes.
- Integrated Supervisory and Control System (ISCS) – High availability of the ISCS hardware design with fault tolerant, hot standby computers and self-healing networks; Fully integrated control system with generic workstations

Implementation of safety management

Safety Management for the driverless metro has been implemented as part of LTA Project Safety Review (PSR) process, which defines how safety implementation is to be achieved for all transit transportation projects within Singapore. The PSR process is shown in Figure 3 below.

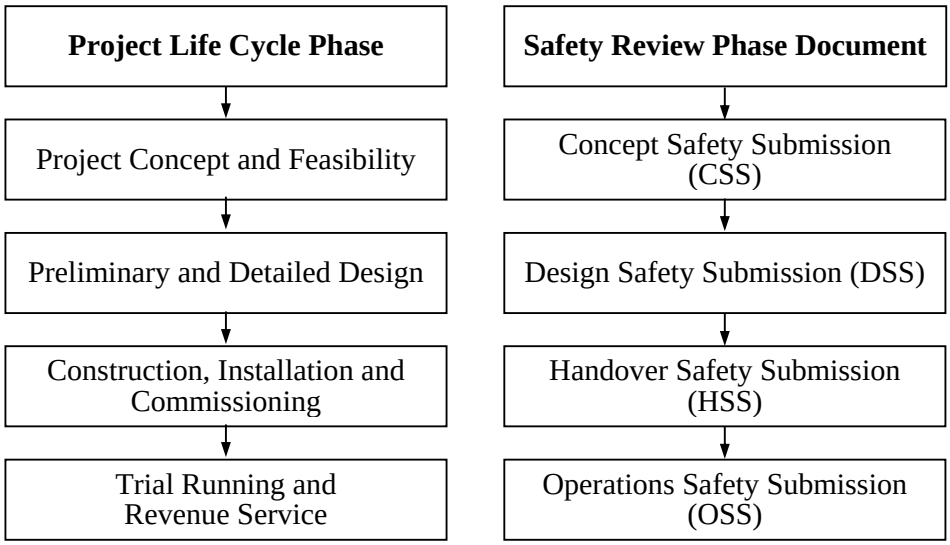

Figure 3: LTA RTS Safety Management Process

All RTS projects developed by LTA have to achieve the Safety Certification prior to opening. This process consists of two key areas of activities – Safety Submission and Safety Audit. There are four Safety Submissions to be prepared namely Concept Safety Submission (CSS); Design Safety Submission (DSS); Handover Safety Submission (HSS) and Operation Safety Submission (OSS). Safety audits are conducted on all the Safety Submission.

CSS is to demonstrate that the system concept is developed to an acceptable level and safety requirements are apportioned to contracts.

DSS is to demonstrate that the system safety is verified and validated during design phase and that all safety requirements from Concept stage are met.

HSS is to demonstrate that the system safety concept and design is validated during testing and commissioning phase, and provide safety evidence for the commencement of trail running.

OSS is to demonstrate that the RTS Operator has established the necessary organisational structure and processes to operate and maintain the RTS system to an acceptable level of safety.

Safety Management Activities. A more comprehensive Safety process has been instituted for the driverless metro system. Some of the safety tasks carried out for driverless metro consists of the following:

a. System level HAZOPs

System-wide HAZOPs studies have been conducted to identify all foreseeable risks associated with operational and maintenance tasks of the driverless system. These cover normal, degraded and emergency modes of operation. All potential worst-case credible scenarios have been considered in the HAZOP study, for example tunnel/train fires during peak periods of operation.

b. Safety Integrity Level (SIL) Determination

LTA carried out the SIL allocation by adopting the process stated in some of the international standards with some customisation to fit our local safety framework. The purpose of determining SIL is to allocate the required integrity level for each safety functions with respect to the required risk reduction so that the risk associated with the individual hazard can be reduced to a tolerable level. The safety functions are identified from the preliminary hazard analysis. Throughout the hazard analysis, all possible mitigation measures will be identified, and the relevant safety functions will be selected and further assessed. The hazard analysis was also used to reduce the risk to the tolerable level via determining the Tolerable Accident Rate (TAR) and Tolerable Hazard Rate (THR). Finally the required SIL are assigned and apportioned to subsystem functions.

c. Software Safety Assessment

The Software Safety is managed under the Software Development and Safety management. All software developments, no matter is safety or non-safety related have to fulfill the requirement of ISO Software Quality Assurance or equivalent. The requirement of Software SIL is assigned to all software safety-related functions based on the IEC 62279 requirements. Software Assessor is independent to the system development team and has been engaged to conduct software assessment to ensure that all relevant requirements required in IEC 62279 are met.

d. Hazard management

The Hazard Management is considered as a key process to control all identified hazards by mitigation, elimination and transfer via the Hazard Log. The ultimate target is to mitigate all hazards and associated residual risks down to a tolerable level and meet the objective of Risk Acceptability and Tolerability. Hazard Log is a live document over the whole project lifecycle. It will be recorded all identified hazards with associated risk level and action items until the hazards are closed out.

e. Probabilistic Safety Assessment

The Probabilistic Safety Assessment has been performed using Fault Tree and Event Tree analyses to ensure that the defined passenger and staff risk targets can be met. Risk models have been developed by the system contractors to assess high level railway accidents, such derailment, collision, fire, etc. In addition, all hazards with Intolerable and Undesirable accident severity were also assessed to evaluate their residual risk after all proposed mitigation measures are applied.

f. Deterministic Safety Assessment

The Deterministic Safety Assessment is a qualitative approach to assess system safety design against recognised international railway safety principles, statutory requirements, standards and Code of Practice that are applied in metro system. Design safety principles used have been based on Part 1 of the Railway Safety Principles and Guidance from the Office of Rail Regulation (ORR, UK). The assessments included fire sizing, ventilation principles, ergonomic, electromagnetic compatibility (EMC), train crash worthiness and evacuation strategy.

Evidences are gathered to verify and validate design safety principles. Any non-compliance, partial compliance and wavier items would be subjected to approval by the project safety committee according to the Project Safety Review process.

g. Integrated Testing and Commissioning

Each integrated testing and commissioning plan has been analysed by LTA to determine whether the equipment can be safely brought into serviceable order in line with the design intent and contractual obligations. The adequacy of the commissioning process adopted has also been scrutinised and on-site witnessing of critical commissioning activities has been undertaken to confirm that the safety objectives have been adequately addressed. A series of degraded mode tests, intended to determine the response of the integrated driverless metro system to faults and abnormal conditions, have been undertaken during Test Running and Trial Running.

Implementation of Reliability, Availability and Maintainability (RAM) Management

A review has been carried out on all the Electrical & Mechanical (E&M) systems to identify the RAM requirements for the fully automated metro system. The criteria of the RAM review are based on the following considerations:

a. Impact to Train service operation

The fully automated metro is required to achieve similar service level as in all existing metro. Therefore, without the driver intervention to reset and/or restore the system when faults occurred, the scope of RAM requirements would be more comprehensive for the fully automated system. For other systems which do not have any direct impact to the metro operations, RAM requirements were reduced accordingly.

b. Operational Performance Standard (OPS)

LTA transit regulator has imposed a minimum level of operation performance on the metro operator. For these E&M systems, RAM requirements have been set so as to ensure

that the contractor delivers a minimum level of systems performance to meet the OPS requirements.

c. Safety Requirements

Reliability/Availability targets have also been set for E&M systems that require to achieve a minimum safety requirement in order to reduce the risk of fatal accidents.

RAM Management Activities. A comprehensive RAM process has been instituted for the fully automated metro system. Some of the RAM tasks carried out for driverless metro are described as follows:

a. Setting of RAM Targets

E&M systems in which failures/malfunctions have direct impact to train service disruptions were specified a minimum level of Reliability so as to achieve an acceptable level of train service Availability. An overall top level train service Availability target has been established, and apportioned to the various E&M systems within the metro system. These targets have been included in the contract specifications such as:

- Electric Train
- Signalling System
- Platform Screen Doors
- Traction Power
- Communication System
- Integrated Supervisory Control System
- Permanent Way

The top level train service availability target has been established based on the Operation Performance Standard (OPS) set by the LTA Transit Regulator. Under the operator's Licence and Operating Agreement (LOA), they are required to comply with a set of quantitative operation performance targets specified in the OPS.

For example, a typical driverless metro Train Service Availability target (TSA) can be set at 99%. This target is based on the Train Service Availability target of 98%, specified in the OPS. It is assumed that 1% of the total system failures are attributed by other contributing factors which are not within the contractors' control. Figure 2 provides flow chart on how the TSA is being apportioned to these E&M Systems.

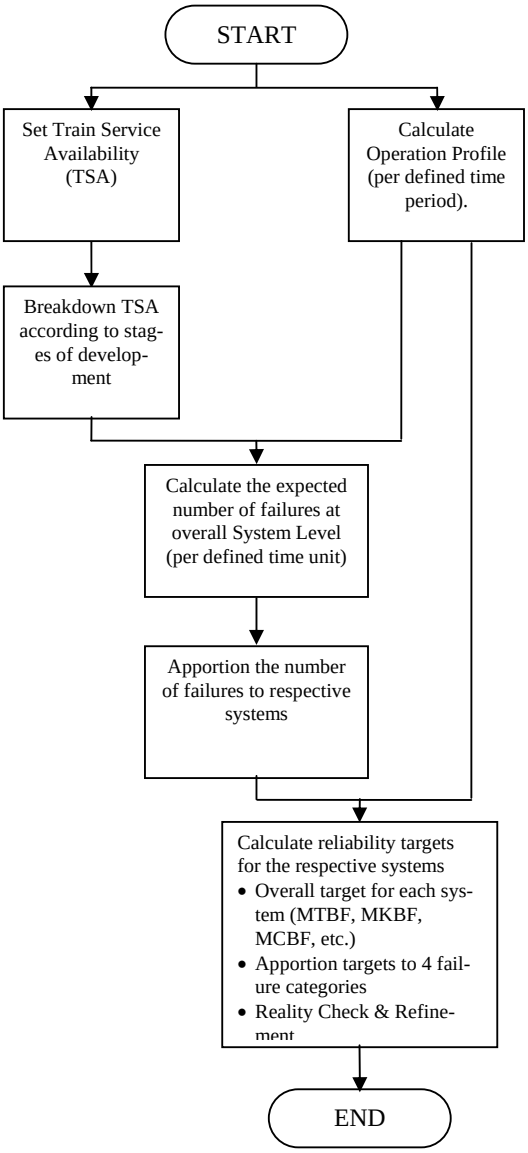

Figure 2: Reliability Apportionment

Availability targets have also been specified at system level as well as sub-systems/equipment level of the E&M systems. Specifying Availability targets at the sub-systems level ensure that the contractors procure reliability equipment and provide suffi-cient redundancy in their design.

Maintainability requirements have been set to ensure prompt restoration of train and station operations when the E&M systems/equipment fails during revenue service. The maintainability target was established for corrective maintenance tasks that must be com-pleted on site (along the mainline or in stations) and tasks which must be completed before train services resume the next day. These targets are set in the form of Mean Time To Re-pair (MTTR) and Maximum Mean Time To Repair at 95^{th} Percentile ($M_{Max95}TTR$).

b. RAM Analysis and Prediction

Contractors performed RAM analyses and predictions to demonstrate that the proposed system design meets the RAM targets. RAM analysis were also used to identify the sub-systems, equipment/ components which have a major effect on overall system Reliability, and warrant particular attentions during specification, design, manufacture and testing.

c. RAM Review & Assurance

The contractors are responsible for implementing and incorporating the RAM requirements within the design requirements. The contractor's RAM team developed the RAM management plan to ensure all the RAM activities are in accordance to the RAM specification.

The contractor's RAM team are also responsible for making the final assessment on RAM performance and provided advice to the design team until all RAM requirements are achieved. LTA ensured that RAM deliverables submitted by the contractors throughout the entire phase of the contract fulfils the contract requirements.

d. RAM Demonstration

The purpose of RAM demonstration is to demonstrate, via statistical testing using defined acceptance/rejection criteria or agreed frequency of testing for systems that operates on demand, that the system meets the contractual RAM requirements.

For Reliability Demonstration Test (RDT), Fixed Duration (Time/Distance) method is applied for most systems in accordance with IEC 61124 standard. The Fixed Duration method requires the systems under demonstration to accumulate a pre-determined total operating hour or mileage, and that the number of failures encountered over this period are within a specified accept/reject criteria. RDT was initiated after the system has been "burn-in" to ensure the system is stable and early failures are rectified.

There are two different types of Availability Demonstration Test (ADT) conducted for the systems. The first type of ADT is to measure the System Service Availability. Service Availability demonstrations are conducted for systems that operate continuously during the revenue services for the transit operation. The second type of ADT is for systems which operate on demand i.e. Availability on Demand (AOD) demonstration. Smoke Purging System and Tunnel Ventilation Systems availability were demonstrated using this method.

The purpose of Maintainability Demonstration Test (MDT) is to demonstrate that the specified MTTR and M_{Max95}TTR of the systems were met. MDT has been carried out in accordance with US Military Handbook 470A.

Testing and Commissioning Process

During the system validation and integrated testing stage, it is necessary to demonstrate that the overall system functioning is in accordance with specification and all interfaces are operating correctly as intended. The typical sequence of testing is illustrated in figure 3. The approach taken to conduct system integration testing has been through specific testing by various contractors followed by the final overall system testing.

As part of LTA's methodology, prior to the commencement of site-testing, different forms of pre-delivery system Integrated Testing will be carried out as part of risk mitigation measures. The main part of pre-delivery system integrated testing relate to testing at

Contractor's Test Track involving trains, signalling systems, communications and a mini control centre. This aims to eliminate major system interfacing problems which could only be identified or would only be surfaced at the Test Running stage and hence minimise the probability of late identification of major problems and consequential delays.

Off-site integrated testing also provides the means to demonstrate the operating principles and to validate the overall system design in terms of performance and safety in advance of site testing.

A number of off-site test platforms have been created to cater to the various interface test needs. Examples include the Signalling integrated testing, the Rolling Stock integrated testing, the Integrated Factory Acceptance Test (IFAT) and the core systems integrated testing. All off-site integrated tests have to be carefully planned and executed to meet the prerequisites for the subsequent higher level integrated tests for progressive bottom-up integration.

Careful planning and review have been conducted to ensure that the contractors have not taken restrictive interpretation of integrated testing biased to their contract in particular on the completeness of all degraded mode related testing. In the final stage, an overall system validation and availability testing will be conducted to ascertain overall system stability.

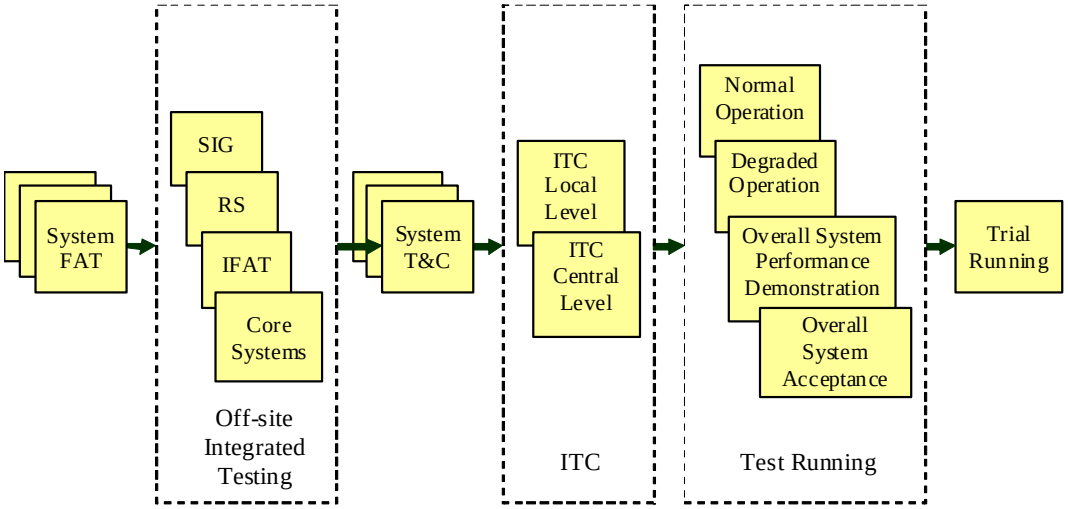

Figure 3. Typical Integration Related Testing Sequence

CONCLUSIONS

The design of a fully automated driverless system should be carried out at the outset of the system definition so that sufficient and adequate provisions can be incorporated in the design phase.

With the implementation of a comprehensive RAM and Safety management processes as well as the testing and commissioning process, we have achieved a robust and reliable driverless metro which can be demonstrated through the very high performance level of availability attained by NEL since opening for revenue service in June 2003. Improved

processes have also been implemented to new driverless projects such as Circle Line and Downtown Line.