新聞稿
Press Release

PR044/19
5 July 2019

MTR Strengthens Monitoring over Contractor of New Signalling System as Software Implementation Errors were Identified as Causes of Tsuen Wan Line Incident on 18 March 2019

The MTR Corporation has today (5 July 2019) made public the results of its investigation into the Tsuen Wan Line ("TWL") incident which occurred during a drill for the new signalling system at non-traffic hours on 18 March 2019. A detailed investigation concluded that the incident was caused by software implementation errors made by the contractor of the new signalling system, Alstom-Thales DUAT Joint Venture ("the contractor") during the process of performing a software change. A number of improvement measures have been recommended for the contractor. The Corporation will oversee the contractor in implementing the improvement measures, and will exercise extra vigilance and strengthen monitoring on the contractor's deliveries.

During the drill conducted on TWL in non-traffic hours on 18 March 2019, an MTR non-passenger train was entering Central Station through a crossover when it collided with another non-passenger train that was departing from Central Station through the same crossover. The Corporation took the incident very seriously and set up an Investigation Panel ("the Panel"), co-chaired by Mr Adi Lau, MTR Operations Director, and Dr Peter Ewen, MTR Engineering Director, comprising other MTR senior personnel as members. With participation of local and overseas external experts, the Panel looked into the cause of the incident and made recommendations for preventing the recurrence of similar incidents. After a thorough investigation, the Panel's report was submitted to the Government on 17 June, and the relevant departments have now just finished their review of the report.

Cause of the Incident

The new signalling system of TWL developed by the contractor is divided into two control zones. In each zone, it comprises three signalling zone controller computers, namely the Primary ("A"), Hot-standby ("B") and Warm-standby ("C") computers. The Panel agrees that the warm-standby arrangement is novel in the contractor's signalling system application for reducing the recovery time during signalling failure incidents. Following software simulation tests in the contractor's laboratory, on-site train tests during non-traffic hours commenced on TWL in December 2016. The scope of the train tests was progressively extended from one train to multiple trains and to cover the Primary, Hot-standby and Warm-standby computers under an incremental and carefully planned programme. The drill on 18 March 2019 was for Operations staff to familiarise with the operational procedures in a scenario when both Computers A and B fail and there is a need to switch to Computer C to control the signalling system.

-more-

During the development process, the contractor needs to make changes to the software for the new signalling system in order to improve software performance and to meet operational requirements. The Panel found that the contractor made three software implementation errors when performing a software change in 2017 to achieve the design intention of avoiding common mode failure in Computer C, should there be a problem in Computers A and B. To do that, the contractor needs to exclude selected data to be transferred from Computer A/B to Computer C, and the excluded data should be re-created by Computer C, so as to avoid common mode failure. During the process, the contractor made the following three implementation errors:

- Firstly, the internal software development documents of the contractor's software team did not denote clearly the exclusion of "Conflict Zone Data" from being transferred to Computer C. This led to no subsequent specific test, risk assessment or safety analysis, including laboratory verification simulation and on-site testing, being done to verify the "Conflict Zone Data" when Computer C took over the control of the signalling system.
- Secondly, the contractor made a software implementation error which resulted in Computer C not re-creating the "Conflict Zone Data" properly.
- Thirdly, while the "Conflict Zone Protection" was absent in Computer C, the software logic developed by the contractor did not stop the computer from taking over the control of the system. The absence of the conflict zone protection resulted in the incident.

The Panel concluded that these errors reflect the contractor's inadequacies in upholding software quality assurance, risk assessment, and the extent of simulation on this software change.

Safety Assurance

According to the contractual conditions and design requirements, the contractor has the responsibility to ensure the safety of the new signalling system, including providing a safe signalling system for drills. The signalling system developed by the contractor is a proprietary system with the contractor owning the proprietary right and knowledge of all technical information and the software. Notwithstanding that, the Corporation has in place a monitoring mechanism with a dedicated team overseeing the project. The replacement of the signalling system has been conducted in a prudent and progressive manner and the new system has to undergo multiple safety verifications and tests including audits, simulation tests, static tests and progressive dynamic tests before it is put into passenger service. The Corporation has also appointed an Independent Safety Assessor ("ISA") to continuously assess the safety assurance processes adopted by the contractor for putting the new system into passenger service and an Independent Reviewer to advise on project implementation risks.

"For a corporation that always puts safety as our top priority, we take every incident which has an impact on the safety of people inside MTR premises very seriously and would spare no effort in identifying the cause and looking at ways to prevent any recurrence. The 18 March incident is no exception. We will make sure all necessary improvements are made by vigilantly monitoring the contractor to implement necessary follow up work and enhancing our own monitoring system," said Dr Jacob Kam, Chief Executive Officer of MTR Corporation.

Improvement Measures

Following the incident, the contractor has replaced the software design and development team who caused the software implementation errors. To enhance the software development quality and prevent the recurrence of similar incident, the Panel recommended the contractor to adopt the following improvement measures:

- Fix the software issue and confirm with substantiation that there are no wider implications in software development quality;
- Enhance the software coding and testing practices to avoid future programming errors, and introduce effective and traceable measures for detection of any programming errors;
- Employ an external Independent Software Assessor to enhance the software development process for the signalling zone controller computers; and
- Review, re-check and demonstrate robustness on its approach with traceable evidence in applying a fail-safe principle.

To assist the contractor to address the measures above, the Panel also recommended the Corporation to adopt the following measures:

- Expand the scope of the ISA from safety assurance for passenger service to the inclusion of on-site train related testing certification;
- Upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;
- Establish a joint safety Test & Commissioning Panel (the Corporation/contractor together with input from the ISA) to manage on-site testing; and
- Explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby computer, or any other technically appropriate alternatives proposed by the contractor.

The detailed findings of the investigation are set out at annex.

- End -

Annex

Executive Summary

During the non-traffic hours on 18 March 2019, a drill was conducted on the new signalling system provided by the contractor Alstom-Thales DUAT Joint Venture (ATDJV) on the Tsuen Wan Line (TWL). The objective of the drill was to familiarize the operators with the system behaviour and the application of operational procedures in a situation in which both the Primary and Hot-standby computers failed and there was a need to switch to the Warm-standby computer.

At around 02:44 hours, a non-passenger train which was heading to a platform of Central Station (CEN) through a crossover collided with another non-passenger train that was departing from CEN for Admiralty Station (ADM) through the same crossover, causing damage to both trains. Both Train Captains were sent to hospital for medical checks, and they were discharged on the same day.

The Corporation was greatly concerned about the incident and therefore set up an Investigation Panel with membership consisting of MTR senior personnel and external experts to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident.

The investigation concluded that ATDJV had created a software issue which led to the missing of conflict zone protection at the crossover, resulting in the aforementioned two trains being allowed to enter into and collide at the crossover. The software issue was created as a result of software implementation errors made during the process of performing a software change.

The Panel further concluded that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

Recommendations were made by the Panel to ATDJV to:

(a) replace the software design and development team causing the software issue;

(b) fix the software change issue and confirm with substantiation that there are no wider implications in software development quality;

(c) enhance the software coding and testing practices to avoid future programming errors and introduce effective and traceable measures for detection of any programming errors; and

(d) develop a full range of effective measures, including but not limited to (i) employing an external Independent Software Assessor to enhance the software development process for Computers A/B and C from its core product; (ii) reviewing, re-checking and demonstrating robustness on its approach with traceable evidence in applying a fail-safe principle; and (iii) conducting risk assessment in its software implementation with support from the Panel's experts.

To assist ATDJV to address the above, the Panel recommended the MTR Operations Project Team to exercise extra vigilance and strengthen the monitoring on ATDJV's deliveries to rebuild public confidence as below:

(a) expand the scope of the Independent Safety Assessor (ISA) from safety assurance for passenger service to the inclusion of on-site train-related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;

(c) establish a joint safety Test & Commissioning Panel

(MTR/ATDJV together with input from the ISA) to manage on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby computer, or any other technically appropriate alternatives proposed by ATDJV.

Only with consent obtained from the Government, will train testing of the new signaling system during non-traffic hours be allowed to resume.

1. Introduction

1.1 At around 02:44 hours of 18 March 2019, which was during non-traffic hours, a drill was conducted on the new signalling system on the Tsuen Wan Line (TWL). A non-passenger train which was heading to a platform of Central Station (CEN) through a crossover, collided with another non-passenger train that was departing from CEN for Admiralty Station (ADM) through the crossover at the same time, causing damage to both trains.

2. The Investigation Panel

2.1 The Corporation was greatly concerned about the incident and therefore set up an Investigation Panel to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident.

2.2 The Panel was chaired jointly by Adi Lau, Operations Director and Peter Ewen, Engineering Director. Membership consisted of senior MTR personnel in the fields of Operations and Engineering as well as external experts, namely Gab Parris, Peter Sheppard and Joseph Wong of a globally recognized engineering consulting firm WSP, and Prof. S.L. Ho, the Associate Vice President (Academic Support), The Hong Kong Polytechnic University.

3. Background

3.1 Signalling Replacement Project

3.1.1 Signalling systems are essential for safe operation of train services in railway networks. To increase train frequency and capacity as well as to progressively replace the existing assets, in January 2015 MTR awarded a competitively tendered contract for the replacement of the signalling systems on seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line and Airport Express). The contract was awarded to Alstom-Thales DUAT Joint Venture (ATDJV), a joint venture between Alstom Hong Kong Limited (Alstom) and Thales Transport & Security (Hong Kong) (Thales). Both Alstom and Thales are internationally renowned railway infrastructure suppliers having proprietary rights and knowledge over their products and technology.

3.1.2 The TWL signalling system is divided into two control zones. In each control zone, the new signalling system comprises three signalling zone controller computers as required by the contract, namely Computer A as the Primary Computer, Computer B as the Hot-standby computer and Computer C as the Warm-standby computer. Computers A, B and C are of the same hardware and loaded with common software. They are configured to perform functions of Computers A, B and C through a hardware identity plug which allows the common software to process dynamic data among the three computers correspondingly. Computer C only receives selected dynamic data from Computers A/B so as to avoid common mode failure. This configuration aims to improve system availability and service recovery through higher resilience. The Warm-standby arrangement is novel in ATDJV's signalling system application. Furthermore, Computer C is housed at a different station which enhances system security through access control and diverse power supply.

3.2 Testing and Simulation

3.2.1 The MTR Operations Project Team managed the replacement work by applying a method widely adopted in the railway signalling industry. This method, which was implemented by the contractor, included software simulation testing in its laboratory and on-site testing to ensure the new signalling system was developed and matured in a safe and controlled manner. All related testing activities were conducted in a step-by-step and incremental approach along key stages with certification protocols and safety documentation issued by ATDJV. The diagram at Annex 1 shows the overall programme of the simulations and testing.

3.2.2 ATDJV started on-site train testing during non-traffic hours on TWL in December 2016 and the scope of test was progressively extended from one train to multiple trains.

3.2.3 Through stage-by-stage system maturity testing, incremental confidence was built up on the readiness of the new signalling system to start drills on the system operation and operator familiarization of the system behaviour in February 2019. The drills were jointly performed by the MTR Operations Project Team and ATDJV.

3.2.4 Based on the previous simulations, which had been conducted with the common software installed on all computers while not repeating in Computer C for the completed simulations done on the common software, and also testing of its specific transition function from Computer A/B to C, ATDJV issued related safety documentations giving the MTR Operations Project Team the confidence in allowing Computer C to become the Primary Computer for the drill. The objective of the drill was to familiarize the operators with the system behaviour. Through the drill, the operators would have the opportunity to become conversant with the multitude of train service situations expected in future day-to-day operations. The drill would also enable fine-tuning of the operational procedures if required before the new signalling system is eventually put into passenger service.

3.3 Safety Assurance

3.3.1 ATDJV has the responsibility to supply a safe signalling system in accordance with the contractual obligations and design requirements. The MTR Operations Project Team required ATDJV to define the scope and the extent of simulations and tests to ensure that a safe signalling system is delivered in accordance with international standards per their responsibility.

3.3.2 ATDJV had a project safety team for vetting and certifying software safety for the on-site testing and drills. Besides, they also separately deployed an independent safety team to assess and certify the system safety before the new signalling system would be certified for passenger service.

3.3.3 In addition to the ATDJV safety assurance described above and to further ensure the safety of the new signalling system before it is put into passenger service, the MTR Operations Project Team also appointed an Independent Safety Assessor (ISA) which was tasked to assess the system safety assurance processes followed by the contractor, and to provide a safety endorsement document upon satisfactory assessment of such processes. The ISA was for certification of passenger service only, but not on other earlier key project stages such as commencement of drills. Furthermore, the MTR Operations Project Team appointed an external Independent Reviewer (IR) to provide advice on project implementation risks associated with the operating railway. The ISA and IR were involved in project activities within their own scope of works as described above but neither of their mandates covered the assessment of drills.

4. The Incident

4.1 During the non-traffic hours on 18 March 2019, the MTR Operations Project Team jointly with ATDJV engineers performed the pre-planned drill to verify the handling procedures for coping with the failure of both Computer A and Computer B, thereby leading to Computer C taking over as the Primary Computer. The objective of the drill was to familiarize the operators with the system behaviour and application of operational procedures when there are Computer failures.

4.2 At around 02:34 hours, Computers A and B were switched off sequentially to simulate the failure and Computer C took over as the Primary Computer as per the system design. All routes that had been set for trains were cancelled and all trains were stopped as expected in the switchover to the Warm-standby Computer C. The Traffic Controller (TC) in the Operations Control Centre (OCC) then had to give "Depart" commands to depart the trains one after another according to normal operational procedures to allow the resumption of train movement.

4.3 At around 02:41:32 hours, the TC gave a "Depart" command to the train berthing at CEN platform 2 in accordance with the procedure. The route for the train to go to ADM platform 1 was then set by Computer C. At around 02:43:53 hours, for normal traffic regulation, the TC disengaged the platform sequencing selection for CEN to allow the waiting train to berth at CEN platform 1 which was vacant. At around 02:44:01 hours, Computer C erroneously set conflicting routes with signal clear, causing the two trains departing within seconds in Automatic Mode to collide at the crossover outside CEN. For such an instantaneous and unexpected system behaviour, it was very challenging and difficult for the TC to respond and intervene at OCC level through the execution of command steps in calling the emergency brake of the trains in time, as the role of the TC was to manage train regulation activities and as such they would not be expected to be checking for and reacting to such unexpected system behaviour. Similarly, although the Train Captain of the train travelling to CEN platform 1 did activate the emergency brake when he saw the train travelling from CEN platform 2 to ADM platform 1, the train was not able to stop before colliding.

The diagram at Annex 2 illustrates the scenario.

4.4 Apart from one of the two Train Captains who had his right knee mildly abraded, none of the MTR staff or ATDJV staff were injured. Both Train Captains were sent to hospital for medical checks, and they were discharged on the same day.

5. Causes of the Incident

5.1 Computers A, B and C were identical in hardware and loaded with the common software but had different identity hardware plugs to configure them to initially perform as Primary, Hot-standby and Warm-standby, i.e. Computers A, B and C respectively. Before June 2017, the data transferred from Computer A to B or from Computer B to C were all identical which meant that any data corruption causing a failure in Computers A and B would be transferred into C creating a common mode failure.

5.2 To avoid common mode failure according to the contract requirement, ATDJV thus initiated a software change in July 2017. Some dynamic data was selected to be excluded (including "Conflict Zone Data" which prevents conflicting routes from being set) from the data transferal from Computer A/B to Computer C, and those excluded data should subsequently be re-created internally in Computer C. The amount of data excluded and re-created was determined by ATDJV with due consideration to the risk of common mode failure and the swift recovery time so required for Computer C to take up as the Primary Computer in case both Computer A and B fail. However, this software change initiated by ATDJV gave rise to a software issue due to a series of software implementation errors made by its software design and development team during the process of performing this software change.

5.3 Investigation revealed that ATDJV had created the software issue which was caused by the following three software implementation errors made during the process of performing this software change. First, while "Conflict Zone Data" was meant to be excluded, out of expectation it was not specified in ATDJV's internal software development document. Because of this lack of specification, no subsequent specific test, risk assessment and safety analysis, including laboratory verification simulation and on-site testing, was done by ATDJV to verify the "Conflict Zone Data" when Computer C took over as the Primary Computer. This was the first software implementation error.

5.4 Second, ATDJV excluded the transfer of the “Conflict Zone Data” from Computer A/B to Computer C, but its software design and development team made a software implementation error in failing to properly re-create the “Conflict Zone Data” internally in Computer C. This second software implementation error resulted in there being no “Conflict Zone Data” when Computer C took over as the Primary Computer.

5.5 Third, the software logic so built by the software design and development team did not stop Computer C from taking over as the Primary Computer when “Conflict Zone Data” was not available; in other words Conflict Zone protection was not available. This is considered as a software implementation error in not implementing appropriate programming logic to prevent Computer C from taking over as the Primary Computer while having no conflicting route protection.

6. Findings

6.1 The Panel found that until the incident, ATDJV was not aware of the software issue as described in Section 5 throughout its verification and validation process, including simulations done as per their process. As the said software issue was not identified by ATDJV, it was therefore not revealed to the MTR Operations Project Team either. The Panel also noted that ATDJV had issued related safety documentation giving the MTR Operations Project Team the confidence that Computer C would be safe for drills. Indeed, since 15 October 2018, there was no restriction on the number of trains used and no restriction on train separation distance required for on-site testing, in accordance with the safety documentation issued by ATDJV. Furthermore, tests had been undertaken with a procedure that allowed Computer C (as Warm-standby) to become the Primary Computer since mid-October 2018, i.e. with Computer C in full control of the system after switching over continuously. Therefore, for any on-site testing from that point, the software issue could have emerged inadvertently if Computer C had taken over as the Primary Computer, depending on the combination of many permitted and probable situational factors. The Panel opined that the three software implementation errors made during the process of performing this software change before the incident by ATDJV were the causes of the incident.

> ***"WSP's Independent Expert Team considers that ATDJV is responsible for providing assurance to MTR that their product is safe.***
>
> ***With respect to MTR's Drills / Exercises, it is clear that those activities are purely designed to allow MTR to develop and test their operational rule book and familiarize their staff with normal and degraded mode behavior in addition to gaining confidence in the operability and reliability of the 3036 CBTC system."***
>
> ***WSP***
> ***External Expert***

6.2 The Panel also considered that the software implementation errors reflected inadequacies in ATDJV's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

6.3 The Panel considered that it is the responsibility of ATDJV to formulate the extent of simulations in verifying and validating the common software installed to Computers A, B and C for performing their intended functions. ATDJV should develop the software to the required maturity through their verification and validation process. Simulations to the extent required as per their process had been done as defined in the software development document by ATDJV before the commencement of on-site testing. Thereafter, extensive on-site testing was conducted, and iterative simulations and testing, with extra time of more than one year given, had been carried out as appropriate in building up the software maturity. Without knowing the software issue and given the results of the simulations and on-site testing conducted including switchover from Computer A/B to Computer C as witnessed by the MTR Operations Project Team, the project moved to the next stage on the basis that the software should have the maturity to allow safe execution of drills for the operators to safely familiarize themselves with the system behaviour in whatsoever operational circumstances, which was allowed as confirmed by the safety documentation provided by ATDJV. Nevertheless, the Panel opined that given the nature of the software change as revealed after the incident, a wider extent of simulation should have been formulated by ATDJV to cover possible impacts to the critical system performance even if changes were not specified clearly in the software development document.

6.4 The MTR Operations Project Team was aware that there would be a further software version to come after the drills. However, the Panel opined that there was nothing to suggest that the drills on 18 March 2019 should be withheld as the maturity of the software already in use should have been sufficient for the purpose as described in paragraph 6.3.

> ***"It would be unreasonable for MTR to make a unilateral decision, based on no solid grounds, to suspend any drills on Build 8.3.3 and wait for the release of Build 8.3.4."***
>
> ***Professor S.L. Ho***
> ***External Expert***

> ***"According to Thales' documentation provided (i.e. Safety Cert and SOR), it was safe to run the drill on 18th March 2019."***
>
> ***WSP***
> ***External Expert***

6.5 In the process of maturing the software, laboratory simulations had been done by ATDJV to verify the system functions were fit for on-site testing. In relation to the drills, their purpose was for the operator to have site familiarization on the system behaviour and to respond to a multitude of possible in-situ scenarios that can be experienced in real-life operations. With the understanding that the required scenario as defined by the software development document, including switching over from Computer A/B to C had been carried out before arranging the drill, the Panel opined that additional situational case scenarios could still be further included in the simulations to enhance the level of assurance.

6.6 The Panel noted that according to the original resource plan, the procedure for the drill on 18 March 2019 was planned with 4 trains. Yet, there was no longer any limitation on the number of trains according to the safety documentation issued by ATDJV at the time of the drill. In order to represent the morning peak scenario, the MTR Operations Project Team instead informed ATDJV on a number of occasions through the Commissioning Plan that they were to run 34 trains instead of 4 trains on 18 March 2019. The drill was subsequently jointly performed with 34 trains by the MTR Operations Project Team and ATDJV. Since there was no restriction in train separation distance under the procedure, and given the non-existence of conflicting route protection, the incident could have occurred with 2 trains or more as verified during the investigation. The Panel was therefore of the opinion that while the running of 34 trains resulted in raising the likelihood of revealing the unknown software issue, it was definitely not the cause of the incident. The Panel also noted that the operators participating in the drill acted properly in accordance with the normal operational procedures for handling the scenario that would be encountered in future day-to-day operations.

6.7 The Panel has reviewed the findings and recommendations that the ISA provided previously in relation to their concerns on i) compliance with Thales' internal development processes, ii) full compliance with international standards, and iii) development process weakness and its associated risks in their core product. The Panel noted that the MTR Operations Project Team and the ISA had taken additional measures in the form of extra assessments involving a series of factory visits and extra simulation tests, with extra time of more than one year given to ATDJV, in building up the software maturity and addressing the above ISA's concerns. While noting that the ISA's findings and recommendations were for passenger service and not for drills and testing as per its remit, ATDJV did make progress in closing some findings but not yet all before the incident . The Panel has confirmed with the ISA that, based on their findings thus far, they had not identified any specific issues for cessation of the on-site tests or drills. The Panel hence concluded with due consideration on the ISA's findings and recommendations that there were no specific unsafe issues identified by, nor recommendations from, the ISA to suggest discontinuing on-site testing or drills. Nevertheless, the Panel opined that the MTR Operations Project Team should exercise extra vigilance in addressing the ISA's comments in monitoring ATDJV's deliveries in future.

6.8 The Panel opined that there was no reason to discontinue the on-site testing, including drills based upon the required safety documentation supplied by ATDJV, at the time when the incident happened. Nevertheless, the Panel opined that the MTR Operations Project Team should in future be more vigilant in assessing implications of the ISA's concerns on drills and consider expanding the ISA's scope to cover assessment of on-site testing.

> ***"WSP Independent Expert team (in MTR's place) would have also allowed the Drills to go ahead on the basis that the required safety assurance documentation had been produced by Thales specifically for the Drills and Tests (Specific Application Safety Case with restrictions (SOR) further amended by a Safety Memo), which was underpinned by the incremental assurance and confidence gained from all previous activities and documentation produced."***
>
> ***WSP***
> ***External Expert***

> ***"MTR had been taking a prudent and incremental approach to gain confidence in the organization of the Tests and Drill & Exercises. Additional steps had also been taken upon receipt of the advices from the Independent Safety Assessor. Hence it was reasonable for MTR to believe the Drill on 18 March should be a routine familiarization exercise."***
>
> ***Professor S.L. Ho***
> ***External Expert***

7. Conclusions

7.1 The Panel has reviewed the facts and factors relevant to the causes of the incident, and concluded that ATDJV had created the software issue as a result of the following three software implementation errors made during the process of performing this software change.

(a) software development document did not specify the exclusion of the “Conflict Zone Data” which led to no ensuing specific test and safety analysis to identify the unknown software issue;

(b) a software implementation error led to no re-creation of proper “Conflict Zone Data” internally in Computer C when Computer C took over as the Primary Computer; and

(c) while Conflict Zone protection was not available, subsequently Computer C still continued its process to become the Primary Computer because the software logic was so built that it did not stop Computer C from taking over as the Primary Computer, resulting in missing the conflicting route protection.

7.2 The Panel also concluded that the software implementation errors reflected inadequacies in ATDJV’s software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change.

7.3 With ATDJV’s weakness as set forth in paragraph 7.2, the Panel also concluded that the MTR Operations Project Team should exercise extra vigilance and additional monitoring measures on ATDJV’s deliveries in future.

8. Recommendations

8.1 The Panel has made recommendations based upon the causes and the lessons learnt from the incident.

8.2 To prevent recurrence of similar incident due to the same causes, the Panel recommended ATDJV to:

(a) replace the software design and development team causing the software issue;

(b) fix the software change issue and confirm with substantiation that there are no wider implications in software development quality;

(c) enhance the software coding and testing practices to avoid future programming errors and introduce effective and traceable measures for detection of any programming errors; and

(d) develop a full range of effective measures, including but not limited to (i) employing an external Independent Software Assessor to enhance the software development process for Computers A/B and C from its core product; (ii) reviewing, re-checking and demonstrating robustness on its approach with traceable evidence in applying a fail-safe principle; and (iii) conducting risk assessment in its software implementation with support from the Panel's experts.

8.3 To assist ATDJV to address the above, the Panel recommended the MTR Operations Project Team to exercise extra vigilance and strengthen the monitoring on ATDJV's deliveries to rebuild public confidence as below:

(a) expand the scope of ISA from safety assurance for passenger service to the inclusion of on-site train related testing certification;

(b) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;

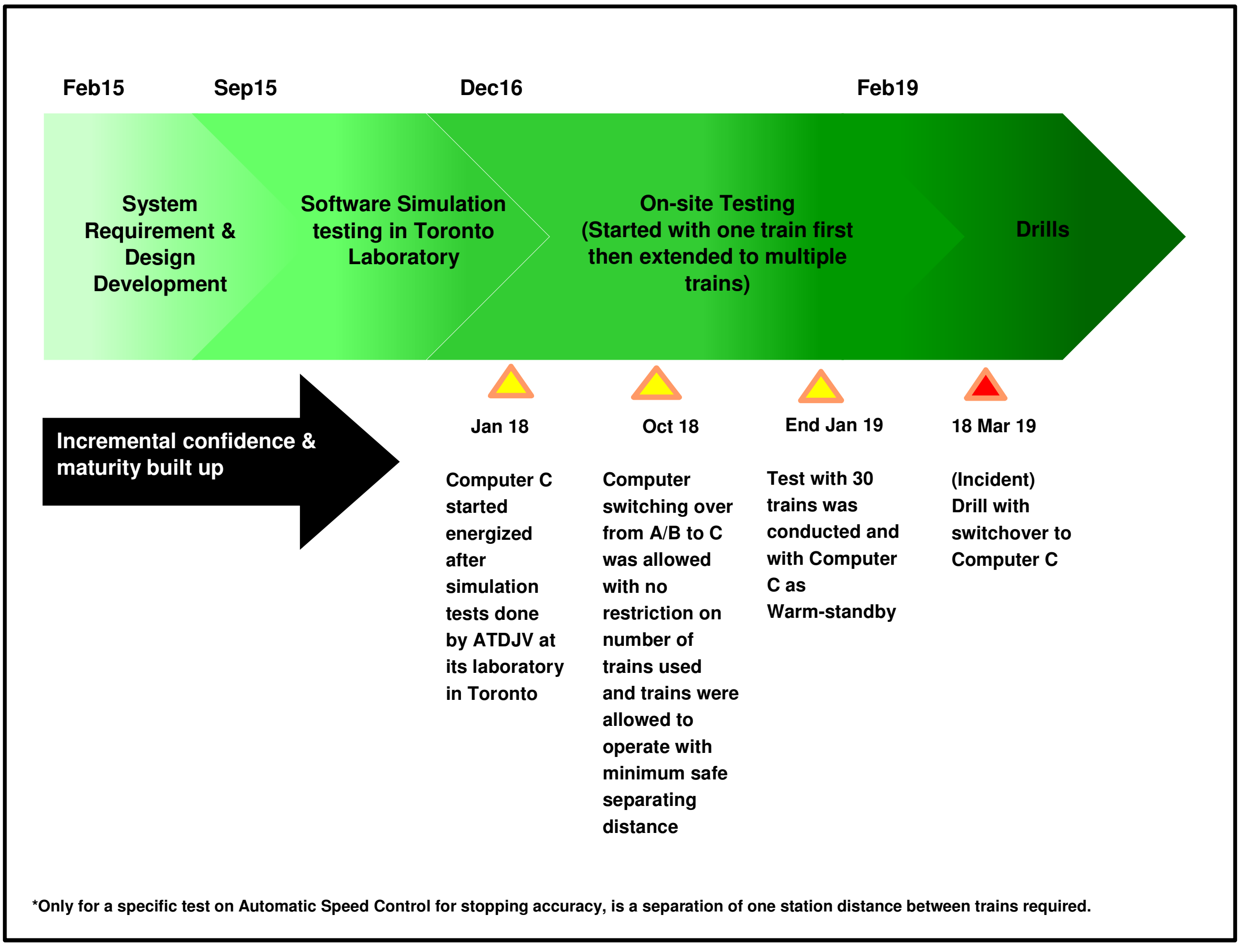
(c) establish a joint safety Test & Commissioning Panel (MTR/ATDJV together with input from the ISA) to manage the on-site testing; and

(d) explore together with the Panel's experts on the merits, if any, for staging the development of the Warm-standby Computer C, or any other technically appropriate alternatives proposed by ATDJV.

8.4 Only with the consent obtained from the Government, will train testing of the new signalling system during non-traffic hours be allowed to resume.

Annex 1

Overall Programme of Simulations and Testing



Feb15
Sep15
Dec16
Feb19
System Requirement & Design Development
Software Simulation testing in Toronto Laboratory
On-site Testing (Started with one train first then extended to multiple trains)
Drills
Incremental confidence & maturity built up
Jan 18
Oct 18
End Jan 19
18 Mar 19

Jan 18: Computer C started energized after simulation tests done by ATDJV at its laboratory in Toronto

Oct 18: Computer switching over from A/B to C was allowed with no restriction on number of trains used and trains were allowed to operate with minimum safe separating distance

End Jan 19: Test with 30 trains was conducted and with Computer C as Warm-standby

18 Mar 19: (Incident) Drill with switchover to Computer C

*Only for a specific test on Automatic Speed Control for stopping accuracy, is a separation of one station distance between trains required.

Notable activities

1. ATDJV started on-site train testing during non-traffic hours on TWL in December 2016 and the scope of test was progressively extended from one train to multiple trains.

2. In January 2018, Computer C started to be energized as Warm-standby after simulation tests done by ATDJV at its laboratory in Toronto.

3. From 15 October 2018 onwards, in accordance with the safety documentation issued by ATDJV, computer switching over from A/B to C was allowed with no restriction on the number of trains used

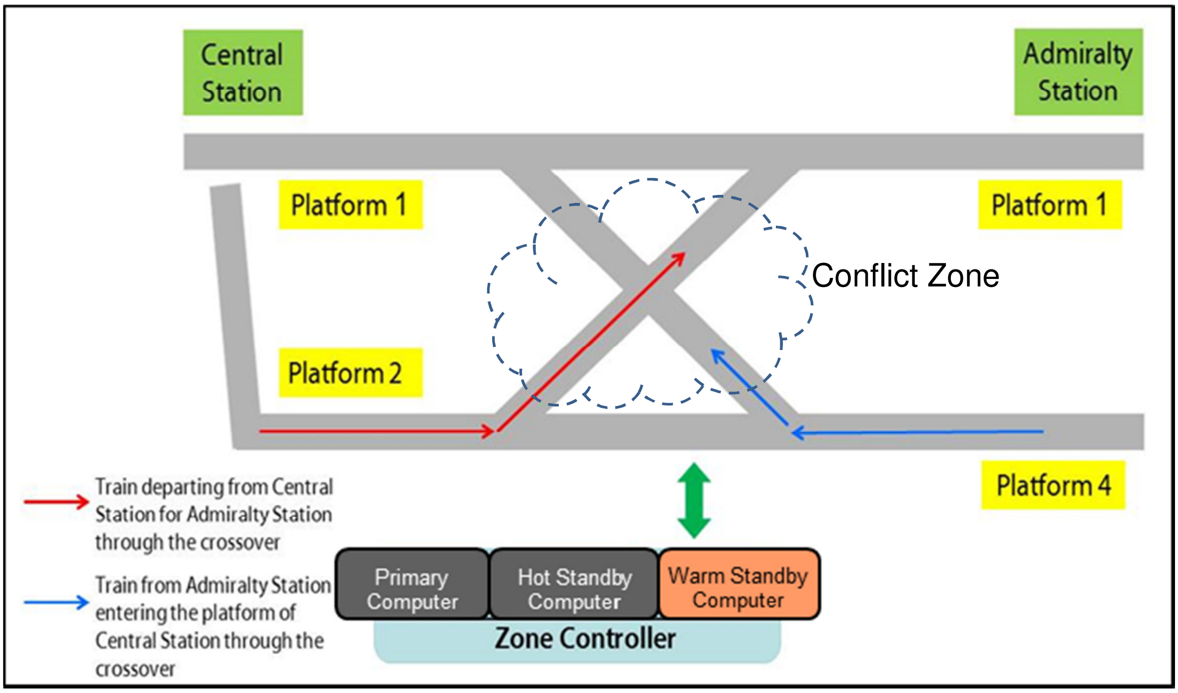
and trains were allowed to operate with minimum safe separating distance. Only for a specific test on Automatic Speed Control for stopping accuracy, was a separation of one station distance between trains required.

4. In January 2019, while there was no restriction on the number of trains, full line testing with 30 trains and with Computer C as Warm-standby was conducted. In other words, Computer C could have taken the overall operational control in case both Computers A and B had failed.

Annex 2

Incident of the New Signalling System Drill on Tsuen Wan Line on 18 March 2019

Illustration of the Scenario

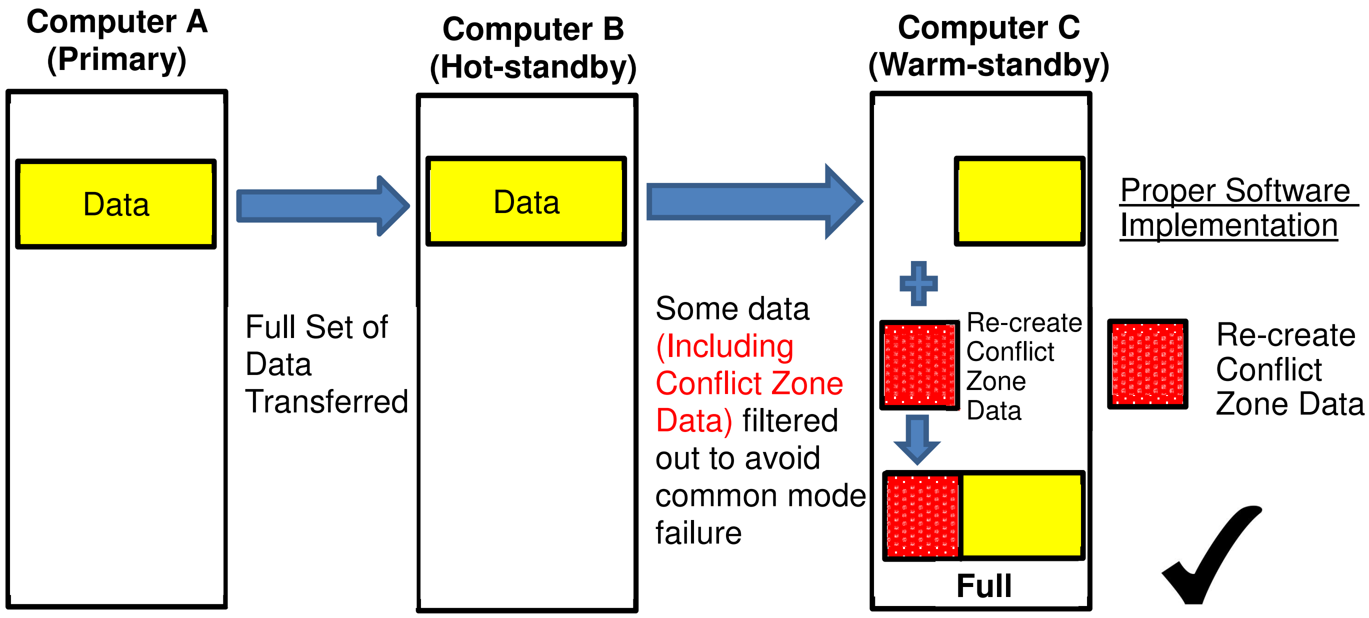

Central Station
Admiralty Station
Platform 1
Platform 1
Conflict Zone
Platform 2
Platform 4
Train departing from Central Station for Admiralty Station through the crossover
Train from Admiralty Station entering the platform of Central Station through the crossover
Primary Computer
Hot Standby Computer
Warm Standby Computer
Zone Controller

Annex 3

Data Transfer among the Three Computers A, B and C

On 18 March, Computer A as "Primary" was switched off and made Computer B become "Primary", thereafter, Computer B was subsequently switched off and made Computer C become "Primary".

Design Intention developed by ATDJV



Computer A (Primary)

Data

Full Set of Data Transferred

Computer B (Hot-standby)

Data

Some data (Including Conflict Zone Data) filtered out to avoid common mode failure

Computer C (Warm-standby)

Re-create Conflict Zone Data

Full

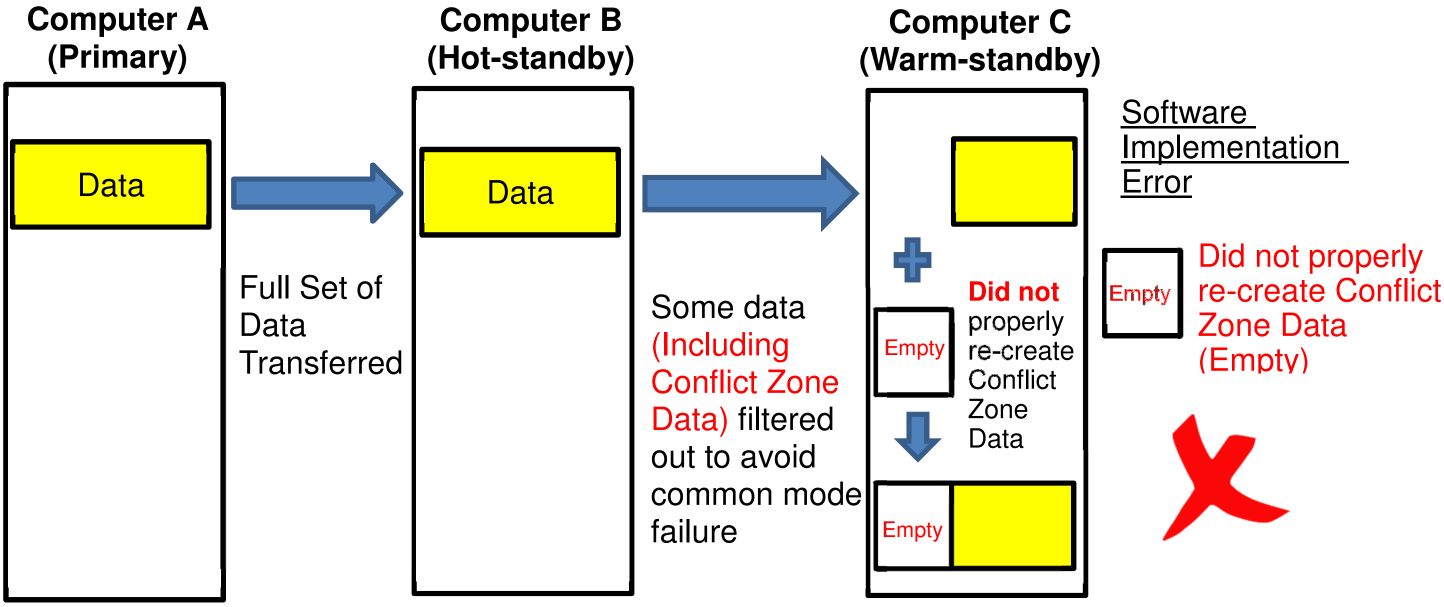
Proper Software Implementation

Re-create Conflict Zone Data

✓

What Happened :

Software Implementation Errors resulted into an unknown software issue



Computer A (Primary)

Data

Full Set of Data Transferred

Computer B (Hot-standby)

Data

Some data (Including Conflict Zone Data) filtered out to avoid common mode failure

Computer C (Warm-standby)

Empty

Did not properly re-create Conflict Zone Data

Empty

Software Implementation Error

Empty

Did not properly re-create Conflict Zone Data (Empty)

✗