Investigation Report on

Incident of the New Signalling System Testing on

MTR Tsuen Wan Line

港鐵荃灣綫

新信號系統測試事故

調查報告

Date of Incident: 18 March 2019

事故日期：2019 年 3 月 18 日

English Version

英文版

機電工程署 EMSD

Date of Issue: 5 July 2019

出版日期：**2019** 年 **7** 月 **5** 日

CONTENTS

Executive Summary

On 18 March 2019, a two-train collision incident happened during a drill and exercise on the new signalling system of the Tsuen Wan Line. This report presents the results of the Electrical and Mechanical Services Department's (EMSD) independent investigation into the causes of the incident.

The signalling system contractor Alstom-Thales DUAT Joint Venture (ATDJV), which is a joint venture of the Alstom Hong Kong Limited (Alstom) and the Thales Transport & Security (Hong Kong) (Thales), had been carrying out tests of the new signalling system in non-traffic hours at different sections of the Tsuen Wan Line by phases since late 2016. The tests carried out by the ATDJV for the entire section were completed in February 2019. On 16 February 2019, the MTR Corporation Limited (MTRCL) commenced the drills and exercises.

The incident occurred in non-traffic hours at 2:44 a.m. on 18 March 2019, when the MTRCL was conducting drills and exercises on the new signalling system of the Tsuen Wan Line. At the time of the incident, train T131, which was travelling from Admiralty Station to platform no. 1 of Central Station, collided with train T112, which was leaving Central Station for Admiralty Station, resulting in damage to the second to fourth cars of train T112 and derailment of two bogies of the first car of train T131. The train captains of both trains were taken to hospital for medical check and discharged on the same day.

According to our investigation findings, the cause of the incident was a programming error introduced during software rectification of the new signalling system at the design and development stage. This programming error caused a failure to re-create the data of the crossover track at Central Station after switch-over from the primary zone controller (ZC) to the warm-standby tertiary ZC. Hence, the Automatic Train Protection (ATP) system could not function as required to prevent two trains from entering the crossover track at Central Station at the same time, and led to the train collision.

The investigation also identified the following causes of the incident:

(a) the programming error, which was introduced in July 2017 during software rectification of the new signalling system, was not identified by the system contractor during various system testing / software upgrades as a result of poorly specified design requirements and inadequate design, verification and validation processes of the software;

(b) the potential risk arising from the introduction of the warm-standby tertiary ZC was not comprehensively included in the risk assessment by the system contractor for the new signalling system; and

(c) simulation tests were not conducted to the maximum extent by the system contractor prior to the site tests, taking into account the specific requirement for a warm-standby tertiary ZC, which is a unique implementation by the supplier among the supplier's standard signalling system products.

Subsequent to the collision incident, the MTRCL had suspended all testing of the new signalling system on the Tsuen Wan Line, Island Line and Kwun Tong Line immediately. The MTRCL had also announced that all train tests for the new signalling system during non-traffic hours was suspended. The Government will allow the MTRCL to resume testing of the new signalling system of the Tsuen Wan Line only after the EMSD has ascertained the causes of the incident and remedial work has been completed satisfactorily.

The EMSD had also examined the MTRCL's Investigation Panel Report submitted on 17 June 2019 and the EMSD's views are listed at Appendix III.

Investigation Report on
Incident of the New Signalling System Testing on MTR Tsuen Wan Line
on 18 March 2019

1. Objectives

1.1 The purpose of this investigation is to identify the causes of a train collision during the new signalling system testing on the Tsuen Wan Line on 18 March 2019. This report presents the results of the EMSD independent investigation into the causes of the incident.

2. Background of the Incident

2.1 The signalling system contractor Alstom-Thales DUAT Joint Venture (ATDJV), which is a joint venture of the Alstom Hong Kong Limited (Alstom) and the Thales Transport & Security (Hong Kong) (Thales), had been carrying out tests of the new signalling system during non-traffic hours at different sections of the Tsuen Wan Line by phases since late 2016. The ATDJV commenced the full-line train tests in early 2018 and had substantially completed the tests on site, which lasted for more than two years, in February 2019. On 16 February 2019, the MTRCL commenced a series of drills and exercises (**Appendix I**) before putting the new signalling system into revenue service. From 16 February to 18 March 2019, the MTRCL conducted nine drills and exercises simulating various specific scenarios, including train fault, point failure as well as failure of both the primary and secondary zone controllers (ZC).

2.2 The incident occurred during non-traffic hours at 2:44 a.m. on 18 March 2019 (**Appendix II**), when the MTRCL was conducting the 9th drill and exercise on the new signalling system of the Tsuen Wan Line. Participating parties included the MTRCL's project staff, staff from its Operations Control Centre (OCC), station staff, train captains, and the ATDJV's engineering staff. The scenario of that particular drill and exercise was to simulate a failure of both the primary and secondary ZCs controlling the zone between Central Station and Sham Shui Po Station. The MTRCL arranged 34 trains to simulate train operation in a situation where the warm-standby tertiary ZC[1]. would take over control from the faulty primary and secondary ZCs during peak hours, with a view to training up the MTRCL staff's response so as to maintain train operation in such situation.

2.3 According to the train logs, train T131, which was travelling from Admiralty Station to platform no. 1 of Central Station, collided with train T112 at a speed of 19 kph at the Central Station crossover track (Figure 1) at the time of the incident. At that moment, train T112 was travelling from Central Station to Admiralty Station at a speed of 31 kph when passing through the crossover track. The collision resulted in damages to the second to fourth cars of train T112 (Figure 2) and derailment of two bogies of the first car of train T131. The two train captains were taken to hospital for medical check and discharged on the same day.

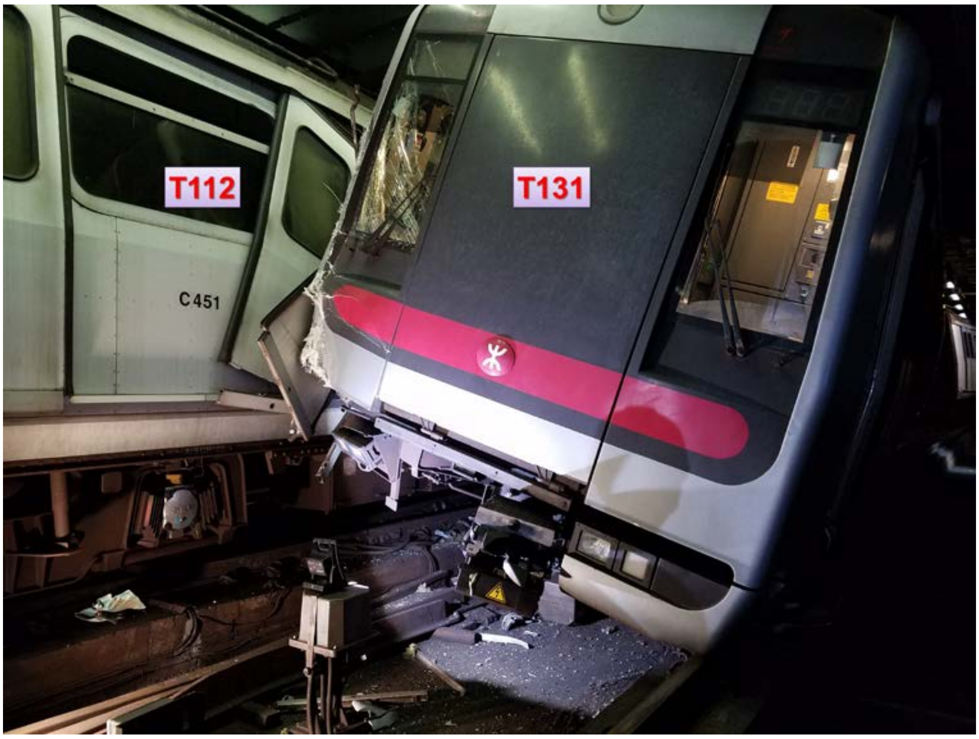


Figure 1: Condition of the trains after collision

[1] Warm-standby is a redundancy system design. When the active primary ZC is in operation, the tertiary ZC remains in the warm-standby mode and obtains partial data from the primary ZC. Therefore, the data of the active primary ZC and the warm-standby tertiary ZC are not synchronised.

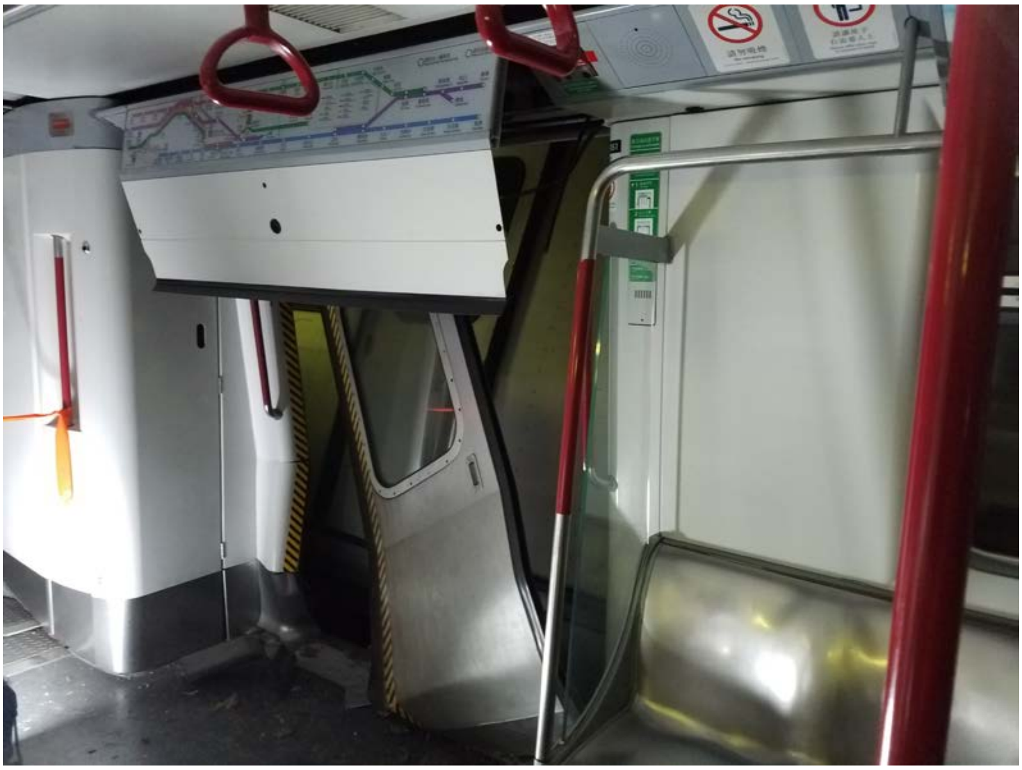
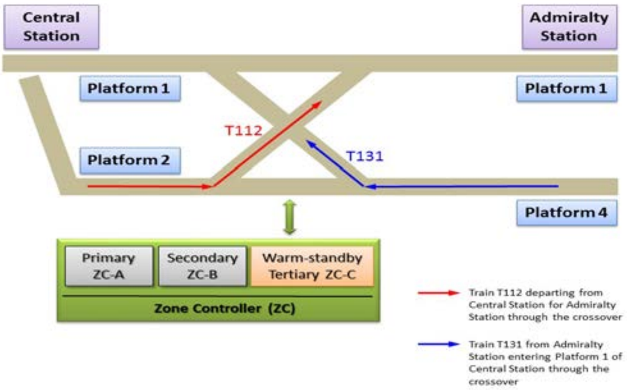


Figure 2: Damage to the saloon of train T112

2.4 According to the train logs and the train captains' interview records, the train captain of train T131 had pressed the emergency brake button before the collision to try to stop the train, but train T131 could not be stopped timely and collided with train T112. Moreover, according to the train logs, the ATP system could not function at that moment to restrict these two trains from entering into the crossover track at the same time. Figure 3 illustrates the train movements during the incident.



Central Station
Admiralty Station
Platform 1
Platform 1
T112
T131
Platform 2
Platform 4
Primary ZC-A
Secondary ZC-B
Warm-standby Tertiary ZC-C
Zone Controller (ZC)
Train T112 departing from Central Station for Admiralty Station through the crossover
Train T131 from Admiralty Station entering Platform 1 of Central Station through the crossover

Figure 3: Train movements during the incident

2.5 The EMSD received notification of the incident at 3:03 a.m. and immediately dispatched staff to the scene for investigation.

2.6 During the drill and exercise on 18 March 2019, the existing signalling system was isolated. All trackside equipment and train-borne signalling equipment were under the control of the new signalling system. Unlike the existing signalling system and other signalling systems of the MTRCL's railway lines, this new signalling system was equipped with a unique tertiary ZC in warm-standby mode. Hence, this incident was not related to the existing signalling systems and similar incidents should not happen on existing railway lines.

3. Technical Information of the Incident Signalling System

3.1 In 2015, the MTRCL awarded a contract for upgrading the signalling systems of seven railway lines (Tsuen Wan Line, Island Line, Kwun Tong Line, Tseung Kwan O Line, Disneyland Resort Line, Tung Chung Line and Airport Express Line) to a joint venture company formed by two signalling system contractors, i.e. Alstom and Thales (known as the ATDJV). The target completion date is 2026.

3.2 A signalling system controls the safe operation of train services in railway network. Railway lines are divided into blocks and only one train is allowed in one block at any one time in order to ensure that trains are kept at a safe distance from each other. The present signalling system of the above-mentioned seven existing railway lines adopts a fixed block design[2], while the new signalling system adopts the "Communications Based Train Control" (CBTC) technology[3] using a moving block design to ensure that a safe distance between trains is still maintained even with increased train frequency and line capacity.

3.3 On 18 March 2019, the MTRCL conducted a drill and exercise on the new signalling system of the Tsuen Wan Line. Through wireless communication, trains sent information such as locations and speeds, etc. to the primary ZC, which

[2] With the fixed block concept, if a train is in a certain fixed block, the signalling system will send commands to the next train requesting it not to enter that block.

[3] The new signalling system uses wireless communication to transmit signals from trains (such as location and speed of trains) to the control computer. The computer then works out the safe distance required between trains.

calculated the safe distances between trains and sent limits of movement authority to the trains in order to achieve higher efficiency in train service management.

3.4 To further enhance the availability of the signalling system, the new signalling system of the Tsuen Wan Line has adopted a three-ZC configuration for train control, namely primary ZC A (ZC-A), secondary ZC B (ZC-B) and tertiary ZC C (ZC-C). This is a unique and non-standard design among its standard signalling system products of the supplier. The respective functions of the different ZCs are as follows (Figure 4):

(a) Primary ZC-A is the active ZC of the system for train control in the designated track section;

(b) Secondary ZC-B is the hot-standby ZC, which synchronises with ZC-A at all times and takes over ZC-A for train control as primary ZC when ZC-A fails;

(c) Tertiary ZC-C is the warm-standby ZC and takes over ZC-A and ZC-B as the active ZC when both ZC-A and ZC-B fail at the same time. To avoid common mode failure[4], part of ZC-C's data is not synchronised with ZC-A and ZC-B, which would be re-created in ZC-C upon taking over as the active ZC.

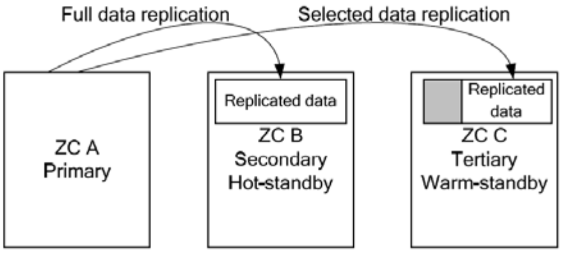


Figure 4: Design functions of the three ZCs

The addition of ZC-C in the new signalling system as warm-standby is a new design and its switch-over mode is more sophisticated than that of conventional design which adopts only two ZCs as active and hot-standby configurations.

[4] Common mode failure means that the same fault occurs at the tertiary warm-standby ZC when it takes over control as the active ZC from the primary ZC and the secondary hot-standby ZC.

3.5 Under all circumstances, only one ZC should be active in the signalling system to control the trains. The active ZC will receive information of operating trains and tracks at all times, including positions, speed, travelling direction and speed limit restriction of the trains at particular sections, points, and crossover positions. Not only does the active ZC calculate and maintain a safe distance between trains, it also restricts the simultaneous entry of more than one train into a point or crossover track to ensure safe railway operation.

3.6 Under normal conditions the active ZC will be either ZC-A or ZC-B. The active ZC regularly sends dynamic data to the warm-standby ZC-C every 100 milli-seconds. In order to minimise common mode failure, based on information extracted from the incident investigation report submitted by the supplier, the following six route-related data items would not be replicated from the active ZC (i.e. either ZC-A or ZC-B) to the warm-standby ZC (ZC-C) (Figure. 5) :

- Conflict zone
- Crawlback
- Crossline
- Border reservation
- Switch control
- Signal control

3.7 In the event when both ZC-A and ZC-B are faulty, the warm-standby ZC-C will act as the active ZC. In handling the route-related conflict zone data, the warm-standby ZC-C will first initialise its internal data space, then call a software subroutine to combine dynamic data collected from the corresponding trackside and signalling equipment with the corresponding static data (which is stored in the ZC-C database) for ZC-C to execute the signalling functions. These dynamic data include :

- Number of conflict zone objects
- Whether the conflict zone has overlapped with non-communicating objects
- Whether the conflict zone has overlapped with non-communicating objects during the previous cycle
- Number of users inside the conflict zone
- Train identification of the user
- Route identification of the user

The above dynamic data of the conflict zone, once collected from the trackside and signalling equipment, will be combined with the following two static data of the conflict zone in ZC-C:

- Conflict zone identification
- Number of paths set in the conflict zone

A complete and correct set of conflict zone data will be re-created based on the above dynamic data and static data for ZC-C to execute the signalling functions, including ATP to prevent train collision in the conflict zone.

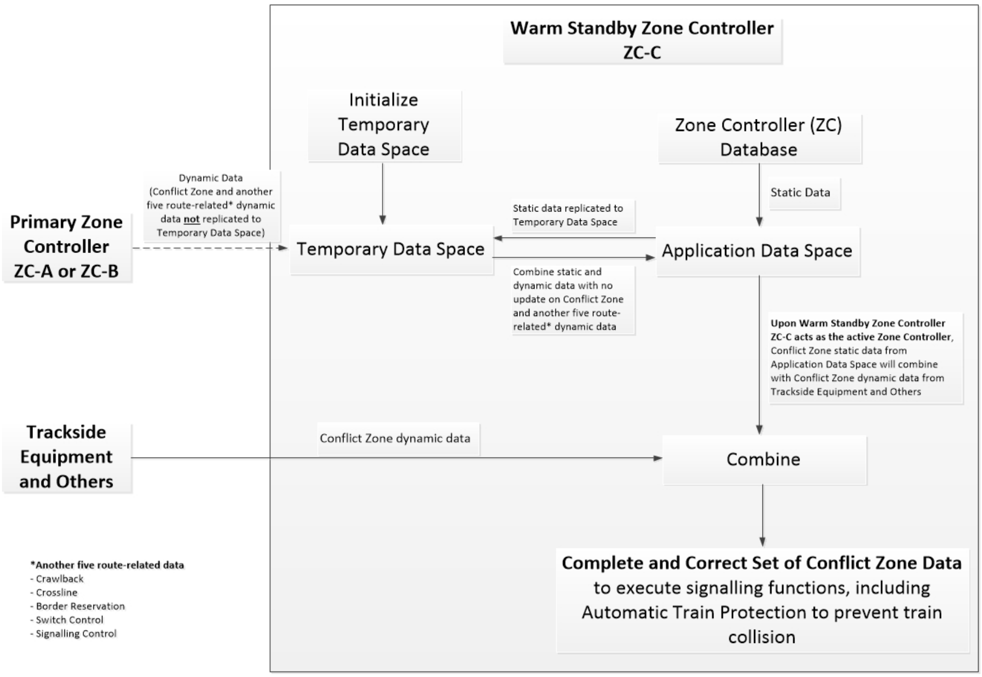

Warm Standby Zone Controller ZC-C
Initialize Temporary Data Space
Zone Controller (ZC) Database
Dynamic Data (Conflict Zone and another five route-related* dynamic data not replicated to Temporary Data Space)
Static Data
Static data replicated to Temporary Data Space
Primary Zone Controller ZC-A or ZC-B
Temporary Data Space
Application Data Space
Combine static and dynamic data with no update on Conflict Zone and another five route-related* dynamic data
Upon Warm Standby Zone Controller ZC-C acts as the active Zone Controller, Conflict Zone static data from Application Data Space will combine with Conflict Zone dynamic data from Trackside Equipment and Others
Trackside Equipment and Others
Conflict Zone dynamic data
Combine
*Another five route-related data
- Crawlback
- Crossline
- Border Reservation
- Switch Control
- Signalling Control
Complete and Correct Set of Conflict Zone Data to execute signalling functions, including Automatic Train Protection to prevent train collision

Figure 5: Integration of conflict zone data from primary/secondary ZCs, warm-standby tertiary ZC and trackside equipment

3.8 However, during the collision incident, due to programming error, the software subroutine mentioned above for conflict zone was not executed in the warm-standby ZC-C when it took up the active ZC role, and therefore the conflict zone data in ZC-C could not be re-created correctly. This error allowed two trains to enter the incident conflict zone and caused the collision.

4. Approach of Investigation

4.1 The EMSD conducted an independent, in-depth and comprehensive investigation into the causes of this incident. The EMSD also appointed three independent parties to provide expert advice, namely TPD System Asia Limited (TPDSA), an railway safety consultant with overseas experts in incident investigation, safety management and risk assessment of systems and processes; Professor Roderick Smith of the Imperial College, an expert in railway safety; and Professor Felix Schmid of the University of Birmingham, an expert in railway signalling systems. In carrying out the investigation, the EMSD has:

(a) conducted more than 65 meetings and reviewed over 250 documents and records, which cover 16 different document categories including project contract documents, design documents, testing and commissioning plans, testing and commissioning reports, testing certificates, procedures for drill and exercise, safety certificates, software programming codes, notes of meetings, recommendations from the Independent Safety Assessor (ISA) and the Independent Reviewer (IR) engaged by the MTRCL, traffic notices, safety briefing records, briefing records for drills and exercises, train logs and investigation reports;

(b) reviewed the traffic notices of the OCC, safety briefing records, briefing records for drill and exercise, incident train logs, trainborne signalling logs of the incident trains and ZC alarm logs on the day of the incident;

(c) reviewed the CCTV footage of the platform and concourse areas before and after the incident;

(d) reviewed the software programming versions of the incident ZCs and trainborne signalling equipment as well as conducted simulation tests on the three incident ZCs;

(e) reviewed the corresponding software programming codes;

(f) reviewed the investigation reports of the MTRCL and the ATDJV;

(g) interviewed 106 MTRCL staff, viz. 53 project team staff, 4 OCC staff, 11 station staff and 38 train captains;

(h) interviewed 27 project team staff from the ATDJV;

(i) interviewed 2 representatives from the ISA (Arthur D Little Limited); and

(j) interviewed 2 representatives from the IR (Kusieog Limited).

5. The EMSD Investigation Findings

5.1 Cause of Incident

According to the EMSD's investigation, the new signalling system performed differently from its intended operation as described in paragraph 3.7. On the day of the incident, the MTRCL performed a drill and exercise on site to simulate a failure in the primary and secondary ZCs, which controlled the stations between Central and Sham Shui Po during peak hours. The purpose of the drill and exercise was to train personnel from the MTRCL to cope with this failure. The scenario of the drill and exercise was that the primary ZC (ZC-A) and the secondary ZC (ZC-B) on hot-standby mode failed simultaneously, and that the signalling system had to be switched over to the tertiary ZC (ZC-C) on warm-standby mode to maintain train operation.

The investigation revealed, when ZC-C took up the active ZC role, the computer programme for handling conflict zone data did not execute the relevant subroutine to combine the dynamic data with the static data and did not re-create the conflict zone information correctly (Figure 6). Because the correct information on the conflict zone was not available, the conflict zone at the crossover track at Central Station did not exist in ZC-C. In the end, the ATP system could not function properly to prevent two trains from entering the crossover track simultaneously and resulted in the train collision.

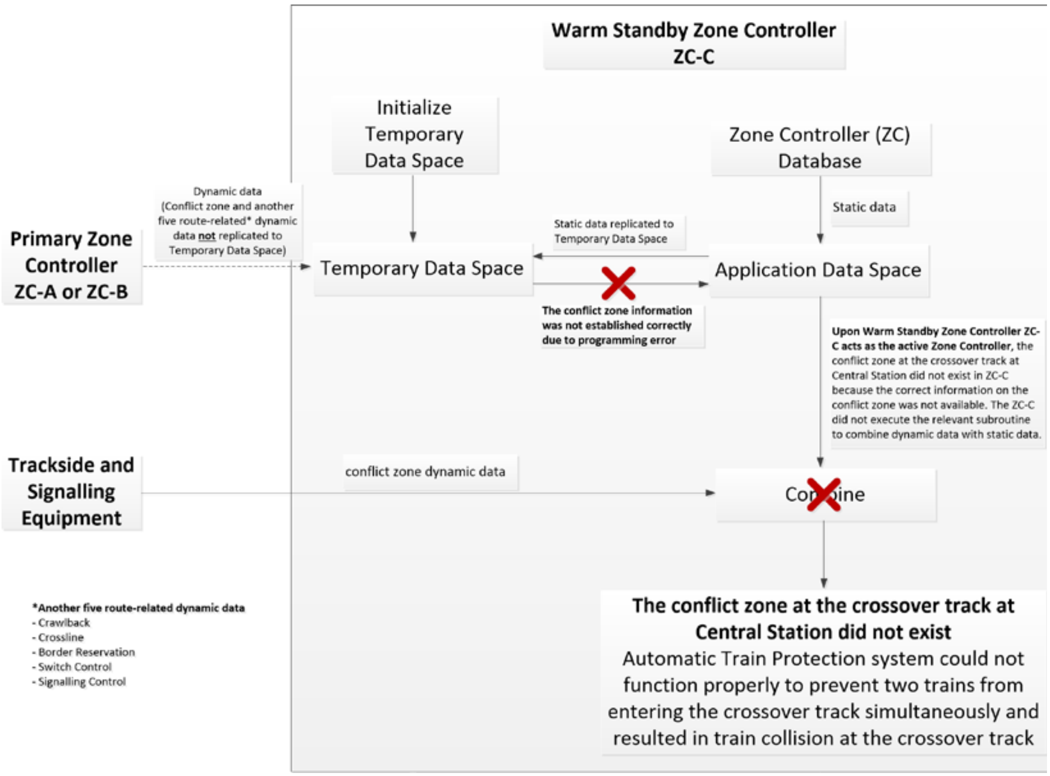

Warm Standby Zone Controller ZC-C
Initialize Temporary Data Space
Zone Controller (ZC) Database
Dynamic data (Conflict zone and another five route-related* dynamic data not replicated to Temporary Data Space)
Static data
Static data replicated to Temporary Data Space
Primary Zone Controller ZC-A or ZC-B
Temporary Data Space
Application Data Space
The conflict zone information was not established correctly due to programming error
Upon Warm Standby Zone Controller ZC-C acts as the active Zone Controller, the conflict zone at the crossover track at Central Station did not exist in ZC-C because the correct information on the conflict zone was not available. The ZC-C did not execute the relevant subroutine to combine dynamic data with static data.
Trackside and Signalling Equipment
conflict zone dynamic data
Combine
*Another five route-related dynamic data
- Crawlback
- Crossline
- Border Reservation
- Switch Control
- Signalling Control
The conflict zone at the crossover track at Central Station did not exist
Automatic Train Protection system could not function properly to prevent two trains from entering the crossover track simultaneously and resulted in train collision at the crossover track

Figure 6: The tertiary ZC did not execute the relevant subroutine to combine the dynamic data with static data

5.1.1 Test items

After the incident, the EMSD and its appointed railway consultant performed multiple tests at the Kowloon Bay Depot, the Ho Man Tin Station[5], the ATDJV Office in Hong Kong and the ATDJV Software Development Centre in Toronto, Canada. The tests were as follows:

(a) Brake tests for the incident trains

A series of brake tests were performed on the incident train T131 at the Kowloon Bay Depot to test the operation of the brake system, with a view to ascertaining whether the incident was related to the brake system of the train. According to the test results, the brake system operated properly and hence was not related to the incident.

(b) Computer simulation tests for the signalling system

Computer simulation tests (Figures 7 and 8) were conducted at the Ho Man Tin Station, the ATDJV Office in Hong Kong and the ATDJV

[5] Ho Man Tin Station is equipped with a new signalling system simulator for training purpose.

Software Development Centre in Toronto by using the same software version as that of the trains in the incident, with the same location and conditions of the incident to ensure that the scenarios were identical. The test results of the simulations revealed that the same collision would happen by using the same software version in the simulators.

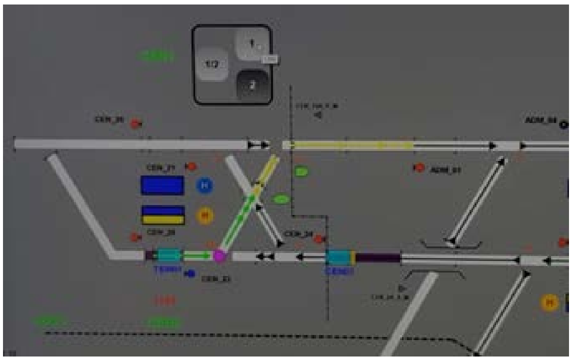


Figure 7: Simulator in ATDJV Hong Kong Office showed the route setting for trains T112 and T131 entering the conflict zone at Central Station at the same time.

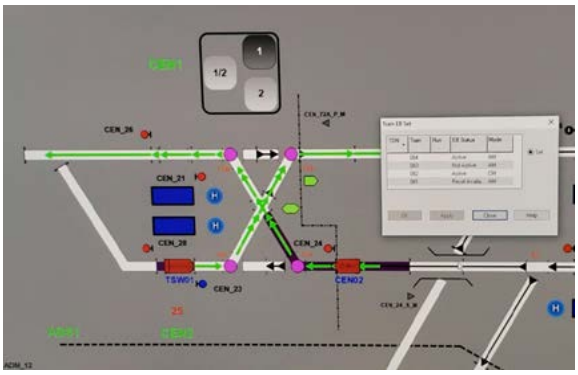


Figure 8: Simulator in ATDJV Hong Kong Office showed the trains entering the conflict zone at the same time at Central Station, as the route setting had allowed them to do so.

(c) Simulation tests for incident ZCs and vehicle on-board controllers (VOBCs)

Simulation tests (Figures 9 and 10) were conducted at Ho Man Tin Station by using the ZCs and VOBCs of the incident trains with the same location and conditions of the incident, with a view to ascertaining whether the incident was caused by the incident ZCs and VOBCs. According to the results of the simulations, the same incident would happen by using the incident ZCs and VOBCs in the simulator.

Figure 9: Simulator in Ho Man Tin Station

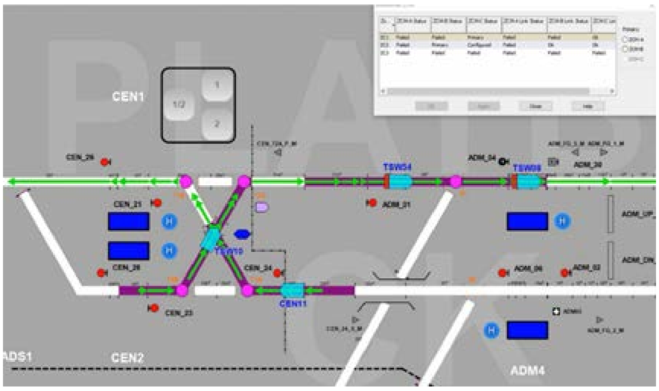


Figure 10: Simulation results showed the ZCs and VOBCs of the incident trains allowing the trains to enter the conflict zone at Central Station at the same time

5.2 Development, Verification and Testing of Signalling System and Drill and Exercise

5.2.1 Programming error in ZC

Investigation showed that there was a programming error in the signalling system software for ZCs after a modification of software coding in July 2017. Due to this programming error, when ZC-C was switched over to become the active ZC, the computer programme for handling conflict zone data did not execute the relevant subroutine to combine the dynamic data with static data, hence the conflict zone at Central Station could not be properly re-created in ZC-C. The ATP system could not function as required to prevent two trains from entering the crossover track at the Central Station at the same time and led to the train collision.

5.2.2 Development process of software programme

It is specified in BS EN 50128 (Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems) that the specification, functional requirements and programming logic of the software should be properly recorded during the development process to allow software developers to formulate relevant tests and reviews in the subsequent verification and validation process. The investigation revealed that the software coding of tertiary controller

ZC-C made in July 2017 regarding the conflict zone data had not been properly recorded in the software design, and therefore the related software coding error was not detected in the subsequent verification and validation process.

This means that the software design and the corresponding change request did not specify how to properly handle the re-creation of conflict zone data in ZC-C. The design and change control documents only mentioned that data related to existing route request, route authorisation and Limit of Movement Authority (LMA) would not be replicated to ZC-C, without mentioning that conflict zone data also would not be replicated to ZC-C. If the software developer had properly recorded all the specifications, functional requirements, programming logic and modifications made in the software, the error codes might have been identified and rectified in the subsequent verification and validation process.

5.2.3 Risk assessment for signalling system

A typical signalling system usually deploys two ZCs (i.e., primary ZC-A and secondary ZC-B) for switch-over between active and hot-standby modes. The provision of tertiary ZC in warm-standby mode in the new Tsuen Wan Line signalling system is a unique implementation by the supplier among the supplier's standard signalling system products. The investigation revealed that risk assessment had not been comprehensively conducted to address the potential hazards due to the unique design of ZC-C during system development. For the design of ZC-C in combining dynamic and static data of conflict zone, if the following activities, including detailed risk assessment, safety requirement identification, verification of safety documents in design documentation, implementation of safety requirements in design, review of design, implementation of the requirements in code, review of the code, and corresponding comprehensive simulation tests or on-site tests had been all properly conducted, the software coding errors might have been identified.

5.2.4 Verification and validation process

In view of the concerns and comments raised by the ISA engaged by the MTRCL, additional verification and validation checking on the software were conducted from October 2018 to February 2019. Most of the additional verification and validation checking were completed on

2019, but the above-mentioned software coding errors were not identified. The independent software assessment scheduled for February 2019 was not completed as scheduled. If such assessment had been completed in February 2019 as required, the software coding errors might have been identified. However, the EMSD's appointed consultant was of the view that the programming error might still not be identified in the above independent software assessment.

5.2.5 Testing of signalling system

The international standard, IEEE1474.4 (Recommended Practice for Functional Testing of a Communications-Based Train Control (CBTC) System), states that simulation tests to the maximum extent possible should be conducted during the stage of factory acceptance tests. Also that on-site functional tests should include functions of the whole signalling system (i.e. including ZC-C), so as to verify that the CBTC functional requirements are satisfied. According to records, comprehensive simulation tests of conflict route were not conducted for the incident scenario (i.e. both ZC-A and ZC-B failed, with ZC-C switched over to be the active ZC) during the factory functional testing stage and on-site functional testing stage. Had comprehensive simulation tests and on-site functional tests been conducted to the maximum extent possible, the programming error and the issue of the ZC-C being unable to re-create conflict zone data might have been identified.

5.2.6 Simulation of signalling system

The provision of tertiary ZC in warm-standby mode in the Tsuen Wan Line signalling system is a unique implementation by the supplier among the supplier's standard signalling system products. The specific requirements of tertiary ZC in warm-standby mode in signalling system were stipulated in the Particular Specification of the contract document. The design requirement was detailed in system design, which only stated the route request, route authorisation and LMA would not be replicated to ZC-C. If the design documents had covered details on the handling of conflict zone data upon ZC-C taking over as the active ZC, and more comprehensive simulation tests had been conducted for the non-standard design prior to the site tests, the corruption of the conflict zone data at the incident crossover track might have been discovered earlier and rectified and the incident on 18 March 2019 might not have happened.

5.2.7 Arrangement of on-site drills

The MTRCL engaged an ISA to certify the safety of the new signalling system before it is deployed to service. On the basis that the new signalling system was to be commissioned in mid-2019 as earlier planned. The ISA reported to the MTRCL on 19 October 2018 that the weaknesses of the signalling safety assurance system might result in an unsafe incident and improvements were required. The ISA raised the following comments on 6 February 2019 and reiterated the subject on 5 March 2019 that:

(a) they did not believe the signalling system fully complies with recognized international standards;

(b) they had significant concerns on compliance with the system developer's software development processes; and

(c) they did not believe that the development processes employed by the supplier are commensurate with the complexity of the signalling system. Many latent safety anomalies were identified on the system core software (Convergence 3.2) since the issue of the safety certification. These revealed the fundamental process weaknesses. The likelihood that such weaknesses might result in an unsafe incident was unacceptably high.

In response to the ISA's comments, the concerned parties carried out tri-partite workshops on 19-25 February 2019 to discuss the ISA's concerns and the system's development progress. After the meeting, the MTRCL postponed the planned service of the new signalling system by six months to Q4 of 2019 to allow time for the ATDJV to respond to the ISA's concerns and improve the new signalling system. The ATDJV indicated that a new version of the signalling system would be released on 24 May 2019. The new version is Build 8.3.4, whilst the version used in the incident was Build 8.3.3. According to records, both the ATDJV and the MTRCL, who participated in the drills and exercises, were aware of the scheduled release of the new software version in May 2019 and the content of the changes. While the said programming error that led to the incident were identified only after the incident, and was not included in the ATDJV's planned update items of the software in Build 8.3.4, we consider it there might still be a very remote chance that the ATDJV might have identified the programming error in the new build, or during software assessment or review to be conducted by an independent software team of the ATDJV. Our appointed railway experts were of the view that there was no clear advice at the time that would have triggered the MTRCL to suspend the drills and exercises in the wait for the new software release, and that there was no evidence either the programming error would have been identified and rectified in the new version in any case.

5.2.8 Procedures of on-site drills

Drills and exercises commenced on 16 February 2019. The incident occurred during the 9th drill, in which 34 trains were deployed for on-site drills without making reference to any relevant drill procedures.

6. Investigation Findings of Railway Experts Engaged by the EMSD

6.1 Investigation Findings of Railway Consultant (TPDSA)

6.1.1 The EMSD has already established that the immediate cause of the collision was a software error in the tertiary Zone Controller (ZC-C) used to control the movement of trains prior to the engagement of TPDSA. TPDSA concurs that this is the immediate cause and has investigated the software defect in detail. TPDSA has also performed further investigations to establish why the error occurred and has identified the underlying causal factors as follows:

(a) A relatively brief examination of the software development processes showed significant deficiencies such that an undetected software error remained.

(b) The need of, or benefit from ZC-C has not been demonstrated and diluted the benefits of the proven core-software.

(c) There was no mapping of software requirements or independent review of the requirement interpretation at sub-system level.

(d) Until a late stage, the ISA had voiced out that the software development and safety engineering processes were inadequate and would affect the integrity of the finished product.

(e) The ISA scope was too limited. It did not cover “readiness for testing” either for one, or several trains, even though a Safety Case and Safety Certificate were produced by the supplier.

(f) The management of testing on the railway was poor with informal communication leading to assumptions and confusion as to the limits of testing and therefore insufficient controls applied.

(g) There was a lack of openness within the system contractor organisation and in its communication with the client. Communication broke down such that a PowerPoint presentation was wrongly interpreted as authority to proceed with any drills and exercises, even though the Safety Case and Safety Certificate had limitations.

(h) The Safety Case and Safety Certificate relating to the drills and exercises lacked clarity and traceability and there were gaps in the safety analysis arising from the introduction of the ZC-C such that compliance with EN50129 (Railway applications -Communication, signalling and processing systems - Safety related electronic systems for signalling) was not achieved.

(i) Programme and commercial pressures to start testing overtook the need for robust process to achieve correct software, the importance of which might not have been fully understood by the parties involved.

(j) The significance of latent safety defects identified in the core software and safety restrictions imposed on it were not understood as a precursor to poor process and therefore poor software. Decisions were made based on assumptions about the dependability of the core software that were shown to be unfounded.

(k) The operational staff (Traffic Controllers and Train Captains) could not reasonably have been expected to have done any more to prevent or mitigate the incident.

(l) The independent software assessment team is considered not sufficiently independent although they are from another unit of the supplier.

(m) The EMSD was kept at a distance in their regulatory role despite regular meetings. The difficult issues, such as the emerging ISA findings were not shared with the EMSD.

6.1.2 In summary, the requirement management, engineering safety management and software development processes were not in accordance with international standards EN50128 and EN50129, which were specified in the contract and are proven internationally for signalling systems. This led to an undetected error in their software.

6.1.3 A contributory cause was that warnings from the ISA that the software could not be relied on, were not fully resolved before the incident. In addition, the ISA remit did not cover "readiness for testing" even though a Safety Case and Safety Certificate were produced. The ISA's limited remit led to a situation where un-validated software without adequate safety controls was used for the drills and exercises for testing.

6.2 Investigation Findings of Professor Roderick Smith

6.2.1 The incident was caused by a weakness in the controlling software which failed to perform the necessary handshake of information when a test was performed to simulate the failure of the first two controllers. It is considered as a sound conclusion agreed by all related parties. This major conclusion is supported without reservation.

6.2.2 Doubts had been expressed by the ISA as early as October 2018 which were repeated in 6 February and 5 March 2019. These doubts contained comments such as lack of belief that the system fully complied with international standards and "latent anomalies" contained in the software might result in an unacceptably high risk of an unsafe incident. There followed tri-partite workshops between 19-25 February 2019 after which the introduction of the new system into revenue service was postponed to Q4 of 2019. This was the fourth of a series of push-backs from the original target of May 2018. This is very clear evidence that all parties were aware of difficulties arising from the testing prior to service introduction of this new system. A new version of the software was promised for May 2019. Between 16 February and the incident on 18 March eight further testing drills were conducted without any problems arising. At the time of the incident on 18 March, 34 trains were involved. There was no clear advice issued by any party to the project proponent outlining the circumstances in further tests which would lead to unacceptable risk, nor any instruction to suspend testing until the new software became available.

6.2.3 Software has become increasingly complex and is being used in a huge variety of situations. It is difficult, perhaps impossible, to test complex software off-line for all eventualities. The authorship of such software is generally a team effort over a considerable period of time and many versions. Ensuring continuity is extremely difficult. The modelling of testing scenarios is only as good as the imaginations of the authors of the risk assessments prior to service introductions. There must be an element of reduction of probabilities in the testing and acceptance of software: a reduction of risk as far as reasonably practical is the goal and this will never be 100%. In this case new ground was being broken by the new signalling system.

6.3 Investigation Findings of Professor Felix Schmid

6.3.1 The significance of implementing a warm-standby rather than a hot- standby configuration in order to reduce the risk of a "data-driven" common-mode failure of all three ZCs, was not clearly understood by the stakeholders. In fact, the warm-standby system with three Zone Controllers A, B and C is a unique and non-standard design among its standard signalling system products of the supplier, which was requested specifically by the MTRCL to satisfy their exacting availability targets.

6.3.2 Individually, both the implementation of a CBTC system on an existing operating railway, and the introduction of a tertiary ZC-C would be deemed major changes. The criticality of combining the two changes was not recognized by the stakeholders.

6.3.3 The non-replication of conflict zone data to tertiary ZC-C should have been detailed in the system design document and in the subsequent formulation of simulation and field testing.

6.3.4 The non-replication of conflict zone data to tertiary ZC-C is not detailed in the system design document. Hence in addition to the programming (logic) omission, the poor system design documentation, the inadequate formulation of simulation and field testing were contributing factors.

7. Conclusions

Based on the investigation findings of the causes of the incident, the EMSD concludes that the train collision incident at the crossover track at the Central Station on Tsuen Wan Line during the drill and exercise in non-traffic hours on 18 March 2019 was due to the following reasons:

(a) there was a programming error in the software of the warm-standby tertiary ZC involved in the incident, resulting in a failure to re-create conflict zone data of the crossover track at the Central Station after switch-over from the primary ZC to the warm-standby tertiary ZC. Hence, the ATP system could not function as required to prevent two trains from entering the crossover track at the Central Station at the same time and led to the train collision;

(b) the programming error, which was introduced in July 2017 during software rectification of the new signalling system, was not identified by the system contractor during various system testing / software upgrades as a result of poorly specified design requirements and inadequate verification and validation processes of the software;

(c) the potential risk arising from the introduction of the warm-standby tertiary ZC was not comprehensively included in the risk assessment by the system contractor for the new signalling system; and

(d) simulation tests were not conducted to the maximum extent by the system contractor prior to the site tests, taking into account the specific requirement for a warm-standby tertiary ZC, which is a unique implementation by the supplier among the supplier's standard signalling system products.

8. Measures Taken after the Incident

8.1 Subsequent to the collision incident, the MTRCL has suspended all testing of the new signalling system on the Tsuen Wan Line, Island Line and Kwun Tong Line immediately. The MTRCL has also announced that all train tests for the new signalling system during non-traffic hours would continue to be suspended until the root cause of the incident has been identified.

8.2 The EMSD notes that the MTRCL Investigation Panel has made a number of recommendations to the system contractor and the MTRCL, and agrees that such recommendations aim to rectify the programming error and enhance the development and testing process of the new signalling system, with a view to preventing recurrence of similar incident. The EMSD will monitor the MTRCL's full implementation of the measures and assess the effectiveness of such. The Government will only allow the MTRCL to resume train testing of the new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.

- End of Report -

Appendix I – Drills and Exercises from 16 February to 18 March 2019

Date	Drills and Exercises
16 Feb 2019	Drills and Exercises No. 1 Simulate points machine failure and train fault
21 Feb 2019	Drills and Exercises No. 2 Simulate OCC blackout, OCC evacuation and other operational exercise
23 Feb 2019	Drills and Exercises No. 3 Simulate Smart I/O failure and assisting train
28 Feb 2019	Drills and Exercises No. 4 Simulate power supply failure and docking failure
9 Mar 2019	Drills and Exercises No. 5 Simulate power supply failure and docking failure
12 Mar 2019	Drills and Exercises No. 6 Simulate Smart I/O failure
15 Mar 2019	Drills and Exercises No. 7 Simulate OCC blackout, OCC evacuation and other operational exercise
17 Mar 2019	Drills and Exercises No. 8 Simulate assisting train
18 Mar 2019 (Date of incident)	Drills and Exercises No. 9 Simulate ZC failure

Appendix II – Sequence of Events

Time	Description
18 March	
0:15 a.m.	The ATDJV conducted briefing to the MTRCL staff, followed by briefing to the MTRCL staff by the MTRCL's drills and exercises in-charge.
2:44 a.m.	Two trains collided at Central Station.
2:54 a.m.	The Fire Services Department and Hong Kong Police Force were notified of the incident. The two train captains were sent to the hospital for medical check, and were discharged on the same day.
2:56 a.m.	The Transport Department (TD) was informed of the incident.
3:03 a.m.	The EMSD was informed of the incident.
3:17 a.m.	The TD was informed regarding the service disruption of Tsuen Wan Line.
4:00 a.m.	"Red alert" issued by the MTRCL. Passengers were informed of the Tsuen Wan Line service disruption through Traffic News and the media. Train service between Admiralty Station and Central Station of Tsuen Wan Line was temporarily suspended.
19 March	
Full Day	Recovery works in progress.
11:00 p.m.	Two bogies of one of the trains were re-railed.
20 March	
0:00 a.m. to 1:15 a.m.	Recovery works in progress.
1:15 a.m.	The trains were moved to the sidings of Admiralty Station and safety inspection was conducted after completion of the recovery works.

Appendix III – EMSD's views on the MTRCL Investigation Panel Report

There is no conflict on the investigation findings between the EMSD Investigation Report and the MTRCL Investigation Panel Report. Nevertheless, the EMSD considers the other facts and factors below are relevant to the incident:

(a) The provision of tertiary ZC in warm-standby mode is a unique and non-standard design among its standard signalling system products of the supplier, as such comprehensive risk assessments should be taken by the supplier and should not be limited by the software development document; and

(b) The simulation tests for the tertiary ZC during the stage of the factory acceptance tests could have been conducted comprehensively by the supplier because of its unique and non-standard design. The scope of simulation tests for tertiary ZC should make reference to IEEE1474.4 be of maximum extent and should not be limited by the software development document.

Besides, the MTRCL's Investigation Panel Report mainly focused on the deficiencies of the supplier in software development and system implementation processes. The Report did not mention the roles of the MTRCL Operations Project Team in overseeing the project implementation. The EMSD considers that, having regard to the significance of this project and the fact that the system design being a non-standard one, the MTRCL should avoid over-reliance on the contractor but ought to be extra vigilant at all times.

The EMSD also notes in the MTRCL's Investigation Panel Report that the Panel has recommended the ATDJV and the MTR Operations Project Team to implement a number of improvement measures to rectify the programming error and enhance the development process of the new signalling system (including the testing), with a view to preventing recurrence of similar incident. Specifically, the MTRCL has undertaken to –

(a) expand the scope of the 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 (MTRCL/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 the ATDJV.

The EMSD will monitor the MTRCL's full implementation of the measures and assess the effectiveness of such. The Government will only allow the MTRCL to resume train testing of the new signalling system after the MTRCL has fully completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.