政府總部
運輸及房屋局
運輸科
香港添馬添美道 2 號
政府總部東翼

Transport and Housing Bureau
Government Secretariat
Transport Branch
East Wing, Central Government Offices,
2 Tim Mei Avenue,
Tamar, Hong Kong

Our ref. : THB(T) L2/1/44
Your ref. : CB4/PS/1/16

Tel no. : 3509 8159
Fax no. : 2537 5246

Ms Sophie LAU
Clerk to Subcommittee on Matters Relating to Railways
Legislative Council Panel on Transport
Legislative Council Complex
1 Legislative Council Road
Central, Hong Kong
(Fax no.: 2840 0716)

21 April 2020

Dear Ms LAU,

Follow-up on the investigation results of the MTR train collision incident

Thank you for your letter dated 19 July 2019, conveying the letter from Hon TAM Man-ho, Jeremy and Hon CHAN Tanya regarding the captioned issue. We offer our apologies as we need time to verify the relevant information concerning the questions raised in the letter with the MTR Corporation Limited ("MTRCL"). The consolidated reply of the Government and the MTRCL is enclosed for Members' reference.

Since the questions raised by Hon TAM and Hon CHAN involve relatively more technical information, if deemed necessary by individual Members, the MTRCL is pleased to approach the Members concerned directly for detail explanations.

Yours sincerely,

(Veronica TSE)
for Secretary for Transport and Housing

c.c.: MTR Corporation Limited

Reply to the questions raised by Hon TAM Man-ho, Jeremy and Hon CHAN Tanya regarding the incident of the new signalling system testing on MTR Tsuen Wan Line on 18 March 2019

Regarding the incident of the new signalling system testing on MTR Tsuen Wan Line on 18 March 2019, the Government and the MTRCL submitted a paper (LC Paper No. CB(4)1097/18-19(01)) to the Legislative Council Subcommittee on Matters Relating to Railways on 5 July last year, including the detailed investigation reports completed by the MTRCL Investigation Panel and the Electrical and Mechanical Services Department ("EMSD") respectively, which outline the course of the incident as well as its cause, and the relevant follow-up actions, etc.

2. After detailed investigation, the investigation results of the MTRCL Investigation Panel ("Panel") revealed that the incident was caused by software implementation errors made by the contractor of the new signalling system, Alstom-Thales DUAT Joint Venture ("contractor"), during the process of performing a software change. The Panel recommended a series of improvement measures to the MTRCL and its contractor. After the incident, the MTRCL and its contractor immediately replaced the software design and development team responsible for the software issue, and implemented the relevant measures according to the recommendations made in the investigation report so as to rebuild public confidence in the new signalling system. The EMSD has also examined the Panel's investigation report. There is no conflict on the investigation results between the EMSD's investigation report and the Panel's investigation report. The EMSD also agrees that the recommendations made by the Panel to the MTRCL and its contractor aim to rectify the relevant errors and enhance the development and testing process of the new signalling system.

3. The MTRCL has undertaken to implement the recommendations made in the investigation report and will continue to supervise the contractor in the implementation of various improvement measures. The EMSD is also closely monitoring the progress of the MTRCL's implementation of the improvement measures and their effectiveness. Regarding the different parts of the questions raised in the letter, our reply is as follows:

<u>Questions (1) and (2): the conflict data</u>

4. Large-scale railway signalling systems are generally operated on the Primary and Hot-standby Computer Systems[1]. With a view to further enhancing

[1] The Hot-standby Computer System is in hot-standby mode. It is fully sychronised with the Primary Computer System at all times. If the Primary Computer System is not running smoothly, it will automatically be switched to the Hot-standby Computer System to control the overall train operations.

the availability and expediting the recovery time of the signalling system, the MTRCL has specified in the contract for the New Signalling Replacement Project that a Warm-standby Computer System should be provided in addition to the Primary and Hot-standby Computer Systems[2]. The arrangement for the Warm-standby Computer System (i.e. the "System C" mentioned in the letter) is indeed novel in the international signalling system application. However, the contractor did not indicate any technical difficulties regarding this arrangement in the then tendering and detailed design processes.

5. According to the contractor's arrangement, the three computer systems are of the same hardware and loaded with common software. Each computer system is configured to process the "Conflict Zone Data" among the three computer systems correspondingly through a specific hardware identity plug (i.e. the identity plugs of the Primary, Hot-standby and Warm-standby Computer Systems) (*Annex 3 of the Panel's investigation report and Paragraph 3.7 of the EMSD's investigation report*). To avoid common mode failure of the Primary and Hot-standby Computer Systems, when designing the Warm-standby Computer System and the relevant software, the contractor requested that the "Conflict Zone Data" received by the Primary and Hot-standby Computer Systems should be excluded from the Warm-standby Computer System and the excluded "Conflict Zone Data" should be subsequently re-created in the Warm-standby Computer System. When designing the Warm-standby Computer System, the contractor decided the types of data to be excluded (i.e. the "Conflict Zone Data") or retained according to its expertise in products and technologies and conducted the software programming accordingly to ensure that the excluded data would be re-created based on the system design with a view to achieving data accuracy and system safety. The investigation results of the Panel revealed that the excluded data could not be re-created as designed due to the programming errors and the programming process could not ensure that such errors could be identified. The verification and validation processes of the software programming were inadequate (*Paragraphs 5.3 to 5.5 and Paragraph 6.1 of the Panel's investigation report and Paragraph 5.2.1 of the EMSD's investigation report*).

<u>Questions (3) to (4): the overall safety of the "System C"</u>

6. The Safety Integrity Level ("SIL") is mentioned in the letter, which is set in accordance with the railway safety standards of the European Union. The higher the SIL, the higher the possibility of an accurate execution of the signalling

[2] The Warm-standby Computer System is in warm-standby mode. When the active primary computer system is in operation, this computer system remains in the warm-standby mode and obtains partial data from the Primary Computer System. Therefore, the data of the active Primary Computer System and the Warm-standby Computer System are not synchronised. When the Primary and Hot-standby Computer systems do not run smoothly, it will automatically be switched over to the Warm-standby Computer System to control the overall train operations.

equipment's safety function in the operation. Among the SILs, the highest one is SIL4. According to the contract terms and design requirements, the contractor shall comply with the SIL4 safety standard in the development and rectification of the safety software (including the "System C" mentioned in the letter).

7. Although the system has not yet been put into service, it is in the later stage of testing. The occurrence of the problem and the resulting incident indeed indicated that unacceptable issue was identified in the software development process which must be investigated thoroughly and rectified immediately.

8. After detailed investigation, the Panel found that the software implementation errors reflected inadequacies in the contractor's software development process with respect to software quality assurance, risk assessment and the extent of simulation on this software change *(Paragraph 6.2 of the Panel's investigation report)*. Therefore, the Panel recommended that the MTRCL should request the contractor to put in place the following improvement measures *(Paragraphs 8.2(a) to (d) of the Panel's investigation report)*:

(i) replace the software design and development team;
(ii) fix the software issue and confirm with substantiation that there are no wider implications in software development quality;
(iii) 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
(iv) 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, etc.

9. In addition, to assist the contractor in implementing the above recommendations, the Panel recommended the MTRCL to take the following measures *(Paragraphs 8.3(a) to (d) of the Panel's investigation report)*:

(i) 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;
(ii) upgrade the Training Simulator in Hong Kong to act as a testing simulation tool to perform more scenario simulation tests as far as practicable;
(iii) establish a joint safety Test & Commissioning Panel by the MTRCL and the contractor, and incorporate the input from the ISA to manage on-site testing; and

(iv) explore together with the safety Test & Commissioning Panel's experts on the merits, if any, for staging the development of the Warm-standby Computer System, or any other technically appropriate alternatives proposed by the contractor.

Question (5): whether the "System C" should be retained

10. As mentioned above, the MTRCL, in collaboration with the safety Test & Commissioning Panel's experts, is exploring the merits for staging the development of the Warm-standby Computer System (i.e. the "System C" mentioned in the letter) and will explore any other technically appropriate alternatives proposed by the contractor in the future. The MTRCL and the experts have commenced the relevant exploring work and will, with safety as the prime consideration, continue to explore the development of the Warm-standby Computer System *(Paragraph 8.3(d) of the Panel's investigation report)*.

Questions (6) and (7): the software assessment was not completed as scheduled and the warnings of the ISA

11. The Panel has reviewed in detail the assessment findings and recommendations that the ISA provided to the MTRCL before the incident (i.e. on 19 October 2018, 6 February 2019 and 5 March 2019) in relation to their concerns on:

(i) compliance with the contractor's internal development processes;
(ii) full compliance with the international standards; and
(iii) development process weakness and its associated risks in their core product.

12. The Panel noted that the MTRCL and the ISA had taken additional measures before the incident (i.e. between October 2018 and February 2019), including extra assessments on the contractor's product development, a series of factory visits and extra computer simulation tests, with extra time of more than one year starting from May 2018 given to the contractor, in building up the software maturity and addressing the ISA's concerns *(Paragraph 6.7 of the Panel's investigation report)*.

13. Regarding the independent software assessment, which was originally scheduled in February 2019 by the contractor but was eventually not carried out, mentioned in the letter *(Paragraph 5.2.4 of the EMSD's investigation report*), according to the understanding of the EMSD, the contractor indicated that it needed more time to develop the software and did not carry out the assessment as scheduled. However, it is pointed out in the EMSD's investigation report *(Paragraph 5.2.7)* that the MTRCL, the contractor and the ISA carried out tripartite workshops between 19 and 25 February 2019 to follow-up on the

concerns previously raised by the ISA and the progress of the system development.

14. It was asked in the letter that whether the MTRCL did know that there was a problem with the system at that time and still conducted the testing with real trains and captains. The Panel examined the relevant issues in detail, including whether the MTRCL should have awaited the release of the updated software version (i.e. version Build 8.3.4) by the contractor in May 2019 and the drill procedures on 18 March 2019, etc.. The conclusion was that there was nothing to suggest that the drills on 18 March 2019 should be withheld as the maturity of the then software (i.e. version Build 8.3.3) should have been sufficient *(Paragraphs 6.4 and 6.6 of the Panel's investigation report)*. The EMSD's appointed railway experts were also of the view that there was no clear advice at the time that would have triggered the MTRCL to suspend the drills and exercises *(Paragraph 5.2.7 of the EMSD's investigation report)*.

15. Nevertheless, the Panel indicated in the investigation report that the MTR Operations Project Team should in future be more vigilant in assessing implications of the ISA's concerns on new system drills and consider expanding the ISA's scope to cover assessment of on-site testing *(Paragraphs 6.7 and 8.3(a) of the Panel's investigation report)*. The EMSD opined that the MTRCL should avoid over-reliance on the contractor but ought to be extra vigilant at all times *(the Executive Summary of the EMSD's investigation report)*.

16. The MTRCL has undertaken to accept various recommendations made in the investigation report. Meanwhile, the MTRCL has also indicated that it will continue to take follow-up actions according to the contract terms and procedures and reserve the rights to pursue the responsibilities of the contractor.

<u>Question (8): the progress of replacing the signalling system</u>

17. The Signalling Replacement Project has all along been conducted according to a prudent and gradual principal. Before commissioning for passenger operation, the new system has to undergo various safety checks and tests, including assessments, simulation tests, static tests as well as gradual dynamic tests.

18. The Government and the MTRCL attach great importance to this incident and are aware of the public's concern about the progress of the Signalling Replacement Project. With safety as the prime consideration, the MTRCL is implementing the improvement measures recommended by the Panel at full steam and will ensure that the relevant workflow will be carried out properly with a view to preventing recurrence of similar incident. Having taken follow-up actions for nearly half a year since the release of the investigation report in July

last year, the MTRCL and the contractor have completed the review of the whole software development workflow and formulated a plan to further enhance the safety of system tests. The MTRCL and the ISA have also completed the technical assessment of the new workflow and are conducting an overall checking of the software again in accordance with the newly formulated plan. The MTRCL will consider resuming on-site train testing in a gradual and orderly manner only after completing the whole software checking and the necessary rectifications.

19. The EMSD will continue to monitor the progress of the MTRCL's implementation of the improvement measures and the effectiveness of the measures. The Government will allow the MTRCL to resume train testing of the new signalling system on Tsuen Wan Line only after the MTRCL has completed the remedial work and the EMSD has confirmed the safety of the new signalling system upon inspection.

End