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 Complex
1 Legislative Council Road
Central
Hong Kong
(Fax: 2840 0716)

9 June 2020

Dear Ms LAU,

Panel on Transport
Subcommittee on Matters Relating to Railways (RSC)

Letter from Hon Jeremy TAM Man-ho on the collision incident of MTR trains during the testing of new signaling system on Tsuen Wan Line

Thank you for your letter dated 3 June 2019, which forwards the requests from Hon Jeremy TAM Man-ho and 27 May 2019 on the captioned.

2. The Government and the MTR Corporation Limited (MTRCL) are very concerned about the train collision incident near the Central Station on 18 March 2019. Upon the completion of the respective investigations by the Electrical and Mechanical Services Department (EMSD) and the Investigation Panel of the MTRCL, the investigation findings were released and reported to the Legislative Council (LegCo) on 5 July 2019[1]. While these reports and our paper to the LegCo in July 2019, as well as our letter (in Chinese) dated 21 April 2020

[1] The relevant papers can be found on the following links:
https://www.mtr.com.hk/archive/corporate/en/press_release/PR-19-044-E.pdf
https://www.emsd.gov.hk/filemanager/en/content_1377/TWL_New_Signalling_System_Testing_Incident_Report_(Eng).pdf

to your other letter on the same incident ("the April reply") (attached for easy reference) should have, by and large, addressed the questions in Hon Tam's May 2019 letter enclosed in your letter in June 2019, we apologise that we have overlooked and failed to provide a response to you in a more timely manner. In consultation with the MTRCL, we set out our response to each of the questions in Hon Tam's May 2019 letter as below. The MTRCL is happy to arrange a meeting with individual Member(s) should it be considered necessary, to explain in further details the technical aspect of the incident.

Question 1. Qualifications of experts involved, and standards applied, in the investigations

3. The MTRCL set up an Investigation Panel right after the incident to investigate and identify the cause of the incident, and make recommendations to prevent the recurrence of similar incident. The Investigation Panel was chaired jointly by Adi Lau, the then Operations Director and Peter Ewen, Engineering Director of the MTRCL, who are not only senior executives but also personally engineering experts with extensive experience in the field. Members of the Panel included seven senior MTR personnel in various divisions in the MTRCL spanning across Operations, Engineering as well as Strategy, Innovation and Technology. The Panel also included four local and overseas external experts, namely, Gab Parris, Peter Sheppard and Joseph Wong of WSP, a global and renowned engineering consulting firm, and also Prof. S.L. Ho, Associate Vice President (Academic Support) of the Hong Kong Polytechnic University, who has assisted MTRCL in investigating into a number of railway incidents.

4. EMSD also conducted an independent, in-depth and comprehensive investigation into the causes of the incident. Independent railway experts from the trade and academia were appointed to provide professional support in the investigation. They include the TPD System Asia Limited, a 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. The experts assisted EMSD in identifying the causes of the incident with detailed study of the gaps in the system development processes required under the relevant European standards (EN standards)[2]. In addition, the adequacy of factory tests and

[2] The EN standards include EN50126 - Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), EN50128 - Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems and EN50129 - Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling.

simulation tests was assessed with reference to the relevant international signalling system standard[3].

Question 2. Inclusion of a back-up system

5. As mentioned in our reply to your other letter on the same incident *(paragraph 4-5 of the April reply)*, the inclusion of a warm-standby computer (i.e. back-up system/ Computer C) is indeed novel in signalling system application worldwide. That said, in the course of tendering and detailed system design, the software development contractor did not indicate technical difficulty arising from this arrangement. The new signalling system comprises three signalling Zone Controller computers which are of the same hardware and loaded with a common software. These computers are configured to perform functions through a hardware identity plug which allows the common software to process dynamic data among the three computers correspondingly. In order to avoid common mode failure, Computer C should only receive selected dynamic data from Computers A and B. This configuration aims to improve system availability and service recovery through higher resilience.

6. 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 development or change in software development by the Contractor (i.e. the development of the whole signalling system comprising Computers A, B and C) must comply with the international standard of Safety Integrity Level (SIL) 4. SIL is a European railway safety standard depicting the relative level of performance of signalling facilities during when put into operation, whereas SIL4 is of the highest safety level *(paragraph 6 of the April reply)*. After the incident, the Investigation Panel concluded that the contractor's software development process with respect to software quality assurance, risk assessment and the extent of simulation on the software change reflected inadequacies, and therefore a series of improvement actions were recommended accordingly.

Questions 3 – 6. Data synchronisation and Simulation of scenario and testing

7. These four questions are related. We shall first explain Question 5 concerning the process of data synchronisation, and then the remaining questions concerning simulation and testing.

---

[3] The signalling system standard being referred to is IEEE 1474.4 - Recommended Practice for Functional Testing of a Communications-Based Train Control (CBTC) System

Question 5

8. Regarding data synchronisation among Computers A, B and C in the system, based on the Contractor proprietary design, only one Zone Controller Computer should be active to control the trains under all circumstances. The active Zone Controller Computer (either Computer A or Computer B under normal conditions) will receive information of operating trains and tracks at all times.

9. As a contractual requirement, the design of the warm-standby Computer C software should avoid "common mode failure". Hence, the system designed by the Contractor should only transfer some but not all data from Computers A and B to the warm-standby Computer C. In case both Computers A and B are faulty, the warm-standby Computer C will take over and act as the active Zone Controller Computer. Before taking over the function to control the train operations, Computer C should re-create those data which are not transmitted, including "Conflict Zone Data" which are essential to prevent two trains from running on conflict routes at the same time. As a contractual requirement, the Contractor should verify the relevant re-created route-related data to ensure that the data is correct and the most current. *(paragraph 3.5-3.8 of EMSD's report)*.

Questions 3, 4 and 6

10. On the arrangement of simulation tests, it was the Contractor's responsibility 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. The extent of simulations required should have been defined in the software development document before the commencement of on-site testing. The international standard, IEEE1474.4 (Recommended Practice for Functional Testing of a Communication-Based Train Control System), is applicable to these simulation tests, which states that simulation tests "to the maximum extent possible" should be conducted during the stage of factory acceptance tests. On-site functional tests should also include functions of the whole signalling system. (*paragraph 5.2.5 of EMSD's report*)

11. In the process of maturing the software, computer simulation tests had been done by the Contractor to verify whether the system functions were fit for on-site testing. Simulation tests including the switchover sequence among Computers A, B and C were conducted in the Contractor's premises and witnessed by the MTR Operation Project Team in Toronto, Canada using the same hardware and software logics as installed on-site. The simulation results have been verified and validated by the Contractor's independent safety team. After

the Contractor's independent safety team was satisfied with the simulation results, safety documentation had been issued to the MTR Operation Project Team to carry out the on-site drills.

12. The Investigation Panel revealed that the Contractor failed to cover the data transfer and re-create process in the software development document. As a result, the Contractor had not derived specific testing on whether conflict zone protection existed in its subsequent simulations, on-site testing, risk assessment and safety analysis, including the simulation tests mentioned in paragraph 11 above. *(paragraph 5.3 of the Investigation Panel Report)*

Question 7. Independent Safety Accessor and Reviewer

13. To ensure the safety of the new signalling system before it is put into passenger service, the MTRCL has appointed an Independent Safety Assessor (ISA), Arthur D Little Limited, in addition to the Contractor's own safety assurance team. The ISA 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. Furthermore, the MTRCL has appointed an external Independent Reviewer (IR), Kusieog Limited, to provide advice on project implementation risk associated with the operating railway. Both the ISA and IR were reputable in their respective fields. They were appointed taking into account their professional background, reputation and past experience of the MTRCL. The ISA and IR were involved in project activities within their own scope of works, but neither of their mandates covered the assessment of drills. *(paragraph 3.3.3 of the Investigation Panel Report)*

14. Generally speaking, the MTRCL closely works with the ISA and IR during various stages of the project through arrangements including review, assessments, workshops, and site inspections. The ISA provides findings and recommendations to the MTRCL on the compliance of the Contractor with international standards, the development process weakness and its associated risks identified etc., which will then be relayed to the Contractor for review and improvement and re-assessment.

15. As stated in our April reply *(paragraph 11-12)*, the Panel had reviewed the findings and recommendations that the ISA provided before the incident (in October 2018 to March 2019) in relation to their concerns on the Contractor's development process and their product, and noted that the MTR Operations Project Team and the ISA had taken additional measures in the form of extra assessments involving factory visits and extra simulation tests, with extra time given to the contractor in addressing the ISA's concerns. EMSD's report also noted that the MTRCL, ISA and the Contractor has had a few tri-partite

workshops during 19-25 February 2019 to discuss the ISA's concerns and the system's development process. *(paragraph 5.2.7 of EMSD's report)*. The Investigation Panel concluded that there were no specific unsafe issues identified by, nor recommendations from, the ISA to suggest discontinuing on-site testing or drills *(paragraph 6.7 of the Investigation Panel Report)*.

Way forward

16. Having regard to the incident, the MTRCL has already strengthened the monitoring of the Contractor, and the Contractor immediately replaced the design and development team of the software that triggered the incident. The new team is developing the software from a fresh perspective and mindset. Over the past year, under the monitoring of the MTRCL, the Contractor has completed the new development process and work instructions for the software, and has also verified a small part of the software under the new process and work instructions. The ISA appointed by the MTRCL (with its scope of works enlarged to cover the early stage of software development) and a separate independent assessor newly-appointed by the Contractor were both satisfied with the results. The MTRCL will continuously implement other improvement measures recommended by the Panel with a view to completing the signalling system upgrade works as soon as possible, but with the utmost safety standard.

Yours sincerely,

(TSE Yuen-ting)
for Secretary for Transport and Housing

c.c.:
The MTR Corporation Limited (Attn: Mr CHAN Yu-cheong)
The Electrical and Mechanical Services Department (Attn: Mr TSE Lok-him)

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

本局檔號 ：THB(T) L2/1/44
來函檔號 ：CB4/PS/1/16

電話號碼 ： 3509 8159
傳真號碼 ： 2537 5246

香港中區
立法會道 1 號
立法會綜合大樓
立法會交通事務委員會
鐵路事宜小組委員會秘書
劉素儀女士
(傳真號碼：2840 0716)

劉女士：

跟進港鐵列車相撞事故調查結果

你於2019年7月19日轉介譚文豪議員及陳淑莊議員就題述事宜的信件收悉，抱歉我們需時就信中各個問題向港鐵公司查考相關資料。現附上政府當局及港鐵公司的綜合回應，供委員參閱。

由於譚議員及陳議員提出的問題牽涉較多技術資料，如個別議員認為有需要，港鐵公司樂意直接聯絡相關議員，再作詳細解釋。

運輸及房屋局局長

(謝韻婷 代行)

2020 年 4 月 21 日

副本抄送：香港鐵路有限公司

有關回覆譚文豪議員及陳淑莊議員就2019年3月18日港鐵荃灣綫新信號系統測試事故的提問

就2019年3月18日港鐵荃灣綫新信號系統測試事故，政府及港鐵公司已於去年7月5日向立法會鐵路事宜小組委員會提交文件（立法會CB(4)1097/18-19(01)號文件），包括港鐵公司調查委員會及機電署分別就事故進行的詳細調查報告，闡述事發經過、事故成因及相關跟進工作等。

2. 經詳細調查後，港鐵公司調查委員會（委員會）的調查結果顯示，新信號系統承辦商Alstom-Thales DUAT Joint Venture公司（承辦商）在修改軟件時出現軟件編程上的執行錯誤，導致事故發生。委員會向港鐵公司及其承辦商建議了一系列改善措施。在事故後，港鐵公司及其承辦商已即時更換導致有關軟件問題的軟件設計及開發團隊，並根據調查報告內的建議，落實有關措施，以重建公眾對新信號系統的信心。機電署亦審視了委員會調查報告。機電署的調查報告與委員會的調查報告結果並無分歧，亦認同委員會向港鐵公司及其承辦商提出的建議針對修正有關問題及加強新信號系統的開發過程及測試。

3. 港鐵公司承諾採取調查報告內的建議，並會繼續監督承辦商落實各項改善措施，機電署亦正密切監察港鐵公司落實改善措施的進度及其成效。就信件中提問的各部分，現答覆如下。

<u>題(一)及(二) 有關互相衝突數據</u>

4. 一般大型鐵路信號系統都會配備主及副電腦系統[1]。為進一步提升信號系統的可用性及修復時間表現，港鐵公司於新信號系統更新工程的合約中要求除了主、副電腦系統外，多配置一套備用電腦系統[2]。備用電腦系統（即來信中提及的「C系統」）的安排確實是在國際間信號系統應用中屬於嶄新的做法。不

[1] 副電腦系統處於熱備用狀態(hot standby)，與主電腦系統時刻保持同步。當主電腦系統運作不暢順時，便會自動切換至副電腦系統負責控制整體運作。

[2] 備用電腦系統處於暖備用狀態(warm standby)。當作為主控電腦的主電腦系統運作時，備用電腦系統維持於暖備用狀態，並從主電腦系統讀取部分數據。因此，作為主控電腦的主電腦系統與暖備用電腦系統的數據並不同步。當主及副電腦系統均不能暢順運作時，便會自動切換至備用電腦系統負責控制整體運作。

過，在當年投標及詳細設計過程中，承辦商對此安排並沒有表示任何技術困難。

5. 根據承辦商的安排，三套電腦系統的硬件相同，並載入共同軟件。每套電腦系統透過其特定硬件識別插頭（即主、副、備用電腦系統識別插頭），相應地處理三套電腦系統之間的「相互衝突區域數據」*（委員會調查報告附件三及機電署調查報告第3.7段）*。為了避免出現與主、副電腦系統的共同模式故障，承辦商在設計備用電腦系統及相關軟件時，要求備用電腦系統內將由主、副電腦系統收到的「相互衝突區域數據」剔除，而被剔除的「相互衝突區域數據」隨後在備用電腦系統內重新產生。承辦商按其產品技術專有知識，在設計備用電腦系統時，決定甚麼種類的數據應被剔除（即屬於「相互衝突區域數據」）或保留，亦須按此編寫軟件，確保被剔除的數據會按系統設計重新產生，以達至數據準確無誤及系統安全。委員會的調查結果顯示，此軟件程式的編寫出現錯誤，導致被剔除的數據沒有按設計重新產生，在編寫過程中亦未能確保錯誤被發現，軟件程式的核實及驗證過程均有不足*（委員會調查報告第5.3至5.5段及第6.1段，以及機電署調查報告第5.2.1段）*。

<u>題(三)至(四) 有關「C系統」的整體安全性</u>

6. 來信提及安全完整性等級（SIL）。SIL是依照歐盟鐵路安全標準，SIL等級越高，顯示信號設備在營運時正確執行安全機能的機率越高，當中SIL4為最高等級。根據合約條款及設計要求，承辦商開發或修改安全軟件（包括來信中提及的「C系統」），須符合SIL4等級的安全標準。

7. 儘管系統尚未投入服務，但已進入測試的較後階段，出現問題並導致事故，確實顯示出軟件的開發過程中出現不能接受的問題，必須徹查並即時糾正。

8. 經詳細調查後，委員會發現軟件編程的執行錯誤反映承辦商在軟件程式開發過程中，就軟件修改所做的信號系統軟件品質保證、風險評估及模擬範圍方面，均有不足之處*（委員會調查報告第6.2段）*。委員會因此建議港鐵公司要求承辦商作出下列改善措施：*（委員會調查報告第8.2(a)至(d)段）*

(i) 更換軟件設計及開發團隊；
(ii) 糾正有關軟件問題，確保並提供具體證明軟件開發在品質上並無構成進一步影響；
(iii) 加強軟件編碼和測試方法，避免將來再出現程式編寫錯誤，並引入有效及可追溯的措施以偵測任何程式編寫錯誤；
(iv) 聘任外間「獨立軟件評估顧問」，加強區間控制電腦系統的軟件開發過程，以及審視、重新檢查及證明其軟件開發方式恪守安全防護原則，並具備可追溯的證據等。

9. 另外，委員會亦建議港鐵公司採取下列措施，以協助承辦商落實上述建議：*（委員會調查報告第8.3(a)至(d)段）*

(i) 將現時「獨立安全評估顧問」的工作範圍，由載客服務的安全保證，擴展至涵蓋列車實地測試相關的安全認證；
(ii) 提升在本港用作培訓用途的信號系統模擬平台，在切實可行的情況下為更多不同情境進行模擬測試；以及
(iii) 港鐵與承辦商共同成立一個「測試及驗收安全委員會」，同時納入「獨立安全評估顧問」的意見以管理實地測試；以及
(iv) 與「測試及驗收安全委員會」專家一同探究分階段發展備用電腦系統是否有好處，或其他由承辦商所建議在技術上合適的方案。

<u>題(五) 應否保留「C系統」</u>

10. 正如上文所述，港鐵公司正與「測試及驗收安全委員會」專家一同探究分階段發展備用電腦系統（即來信中提及的「C系統」），並探究將來其他由承辦商建議在技術上合適的方案。港鐵公司與專家已展開相關探究工作，並以安全為首要考慮，繼續探討備用電腦系統的發展*（委員會調查報告第8.3(d)段）*。

題(六)及(七) 有關軟件審核工作未能如期完成及獨立顧問的警告

11. 委員會詳細審視了「獨立安全評估顧問」於事故前（即2018年10月19日、2019年2月6日及2019年3月5日）向港鐵公司所提交的評估結果及建議，包括承辦商—

(i) 是否恪守內部程式開發程序；
(ii) 是否完全恪守國際標準；及
(iii) 其核心產品的開發程序是否有不足情況及有關風險。

12. 委員會注意到港鐵公司和「獨立安全評估顧問」已於事故前（即在2018年10月至2019年2月期間）採取額外措施，包括對承辦商的產品開發進行額外評估、多次造訪廠房和進行額外電腦模擬測試，並給予承辦商由2018年5月起計一年多的額外時間，使系統更趨成熟，以處理「獨立安全評估顧問」關注的問題（*委員會調查報告第6.7段*）。

13. 來信提及有關承辦商原訂計劃於2019年2月但最終未有進行的獨立軟件審核工作（*機電署調查報告第5.2.4段*）方面，據機電署了解，承辦商表示因需要更多時間開發軟件而並沒有按其原訂計劃進行有關審核工作。然而，機電署調查報告（*第5.2.7段*）亦指出，於2019年2月19日至25日期間，港鐵公司、承辦商及「獨立安全評估顧問」進行了多次的三方研討會，以跟進「獨立安全評估顧問」之前提及的關注事項及系統的開發進度。

14. 來信問及港鐵公司當時是否明知系統有問題仍安排進行真人實車測試。委員會仔細審視過相關問題，包括應否等待承辦商2019年5月才會推出的軟件更新版本（即Build8.3.4版本）以及2019年3月18日的演練程序等。結論是當時軟件（即Build8.3.3版本）已具足夠成熟程度，並無任何資料指2019年3月18日的演練需要暫停（*委員會調查報告第6.4及6.6段*）。機電署委聘的專家也認為，當時並無清晰意見引使港鐵公司暫停演練（*機電署調查報告第5.2.7段*）。

15. 儘管如此，委員會於調查報告中表示，日後港鐵公司營運項目團隊在評估「獨立安全評估顧問」提出的關注時應更提高警覺，留意對新系統的演練會否帶來影響，並應考慮擴大「獨立安全評估顧問」的評估範圍，以涵蓋實地測試的評估（*委員*

會調查報告第6.7及8.3(a)段)。機電署認為港鐵公司在過程中，應加強警覺性及避免過度依賴承辦商(*機電署調查報告摘要*)。

16. 港鐵公司承諾採取調查報告內的各項建議。同時，港鐵公司亦已表示會按照合約條款及程序繼續作跟進，並保留向承辦商追究責任的權利。

題(八) 有關更換信號系統進度

17. 信號系統的更新工程一直以審慎及循序漸進的原則進行。新系統需要先經多項安全檢查及測試，包括審核、模擬測試、靜態測試以至循序漸進的動態測試，才可正式投入載客服務。

18. 政府及港鐵公司均十分重視是次事件，亦明白公眾關注信號系統更新工程的進度。港鐵公司以安全為首要考慮，正全速落實委員會建議的改善措施，並會確保相關流程妥善執行，避免再次發生同類事故。在去年7月公布調查報告至今大半年的跟進工作中，港鐵公司及承辦商已完成檢視整個軟件開發流程的工作，並訂定了方案以進一步提高系統測試的安全。港鐵公司及「獨立安全評估顧問」亦已就新流程完成技術評估，現正根據新訂定的方案，重新為軟件作整體檢查。在完成整個軟件檢查及必要修正後，港鐵公司才會考慮恢復循序漸進式的實地行車測試。

19. 機電署會繼續密切監察港鐵公司落實改善措施的進度及成效。在港鐵公司完成改善措施，及機電署經審視認為新系統安全後，政府方會容許港鐵公司恢復荃灣綫新信號系統的行車測試工作。

完