答集體運輸服務工作小組文件2019／第 11號
（於25.9.2019會議討論）

機電工程署 EMSD

香港特別行政區政府 機電工程署
香港九龍啟成街3號
Electrical and Mechanical Services Department
Government of the Hong Kong Special Administrative Region
3 Kai Shing Street, Kowloon, Hong Kong
www.emsd.gov.hk

Our reference 本署檔號：
EMSD/RB-1/8-1/3/1.1

Your reference 來函檔號：
HAD YLDC 13/35/35

Telephone 電話號碼：2808 3741
Facsimile 圖文傳真：3579 2016

(傳真: 2478 7334)

元朗區議會
集體運輸服務工作小組秘書
黃曉慧女士
元朗橋樂坊 2 號元朗政府合署 13 樓

黃秘書：

元朗區議會交通及運輸委員會
集體運輸服務工作小組
2019 年度第二次會議
討論港鐵測試新訊號系統引致列車相撞事故

你於2019年3月20日就題述事宜的來信收悉。本署回覆如下：

本署非常關注今次事故，港鐵公司已停止新信號系統的測試。

本署已就該事故展開詳細、獨立及全面的調查及已要求港鐵公司於事故後三個月內向本署提交調查報告。本署亦會在審視港鐵調查報告後，完成獨立調查。而調查方向包括系統設計、操作、硬件軟件配合，以至實際測試過程，以徹底找出事故原因。政府會適時向立法會、區議會及公眾交代調查結果。

本署將未能派代表出席2019年3月27日的會議。

機電工程署署長
(葉偉良 代行)

2019 年 3 月 25 日

副本送：

運輸署署長	(經辦人：譚樂忻女士)	(傳真: 2381 3799)
運輸署署長	(經辦人：梁加諾先生)	(傳真: 2381 3799)

來函檔號：HAD YLDC 13/35/35　　傳真：2478 7334
本函檔號：CA/EA/DC/YL/1903/051

元朗橋樂坊 2 號
元朗政府合署 13 樓
元朗區議會交通及運輸委員會
集體運輸工作小組主席
姚國威議員
（經辦人：黃曉慧女士）

姚主席：

元朗區議會
交通及運輸委員會-集體運輸工作小組會議
討論「2019 年 3 月 18 日荃灣綫新信號系統測試事故」

就　貴會擬於二零一九年三月廿七日討論之題述事宜，港鐵公司現謹向　貴會提供書面回覆如下：

港鐵公司以安全為首要原則及考慮，並一直以審慎及循序漸進的方式測試新系統。這次兩列列車發生的事故，正值荃灣綫在非行車時間進行新的「通訊為本列車控制技術」列車測試。測試所採用的是新系統，與現時日間鐵路服務所採用的信號系統是兩套完全無關的系統，現有系統的安全防護保障設計一直有效運作。

事故發生後，港鐵公司會成立包括本地及海外專家組成的調查委員會，詳細及深入調查事故原因，預計可於三個月內完成報告。在未查明事故原因之前，我們會全面暫停非行車時間新信號系統的所有列車測試工作，直至確認今次事故原因。

荃灣綫金鐘站至中環站的路段在事故發生後暫停服務兩日，對乘客造成不便，港鐵公司深表歉意，並感謝乘客體諒及配合。我們亦感謝工程人員、承辦商員工

(.../2)

MTR Headquarters Building, Telford Plaza, Kowloon Bay,
Kowloon, Hong Kong. GPO Box 9916, Hong Kong
Tel (852) 2993 2111 Fax (852) 2798 8822

香港九龍灣德福廣場港鐵總部大樓
香港郵政總局信箱9916號
電話 (852) 2993 2111 傳真 (852) 2798 8822

MTR Corporation Limited
香港鐵路有限公司
www.mtr.com.hk

在極具挑戰的環境下完成修復工作，同時十分感謝香港消防處一直提供協助，加快復修進度。事故期間，港鐵公司額外調配約二百五十名人員前往車站協助乘客，並一直與相關政府部門保持緊密溝通，同時透過多個渠道向乘客發放最新車務資訊。

有關事故詳情，可參考附件之時序表。如有進一步資訊，我們會再向　貴會提交補充文件供議員參考。

對外事務高級經理

陳裕昌

二零一九年三月二十六日
附件

MTR Corporation Limited
香港鐵路有限公司
www.mtr.com.hk

附件

事故經過時序表

大約時間	事項
3 月 18 日 凌晨 2 時 45 分	一列荃灣綫列車於非行車時間進行新信號系統列車測試期間，在經渡綫準備進入中環站時，碰撞到另一列從中環站開出正駛經渡綫的列車。一名列車車長右膝受輕傷，送院治理；另一名列車車長沒有受傷，但為審慎起見亦安排送院檢查。
3 月 18、19 日 早上首班車起	荃灣綫來往金鐘站至中環站的列車服務全日暫停，來往金鐘站至荃灣站的列車服務在繁忙時間維持每三分半鐘一班。
3 月 19 日 晚上約 11 時	工程人員完成將有關列車的轉向架放回路軌，並在隨後的翌日凌晨完成中環站附近的復修工作。
3 月 20 日 早上首班車起	荃灣綫來往金鐘站至中環站的路段恢復行車，荃灣綫全綫列車服務回復正常。

MTR Corporation Limited
香港鐵路有限公司
www.mtr.com.hk

來函檔號：HAD YLDC 13/35/35　　傳真：2478 7334
本函檔號：CA/EA/DC/YL/1903/051

元朗橋樂坊 2 號
元朗政府合署 13 樓
元朗區議會交通及運輸委員會
集體運輸工作小組主席
姚國威議員
（經辦人：黃曉慧女士）

姚主席：

元朗區議會
交通及運輸委員會–集體運輸工作小組會議
有關港鐵荃灣綫新信號系統試驗事故

就三月十八日港鐵荃灣綫新信號系統試驗事故，我們現謹提供補充資料如下：

港鐵公司十分重視上述事故。我們已成立包括本地及海外專家組成的調查委員會進行詳細調查，了解事故成因，務求令事情水落石出，確保鐵路安全。我們預計可於三個月內完成調查。為審慎起見，我們已即時暫停所有新信號系統的行車測試，直至確認事故成因及確保新信號系統安全。

我們明白受事故影響的市民眾多，謹在此再次向乘客致歉，並感謝乘客的忍耐及合作。有關事故經過、我們採取的即時措施、初步觀察結果，敬請參閱夾附的立法會鐵路事宜小組委員會會議文件，也可由以下連結下載及檢視文件 https://www.legco.gov.hk/yr18-19/chinese/panels/tp/tp_rdp/papers/tp_rdp20190329cb4-687-3-c.pdf。

對外事務高級經理

陳裕昌

二零一九年四月三日
附件

附件

立法會交通事務委員會
鐵路事宜小組委員會
2019年3月29日

2019年3月18日港鐵荃灣綫新信號系統試驗事故

前言

鐵路安全至關重要。政府及港鐵公司高度重視2019年3月18日凌晨非行車時間內，兩輛列車以新信號系統進行功能試驗期間，在中環站附近發生碰撞的意外。

2. 政府已要求港鐵公司進行深入調查。港鐵公司已成立包括本地及海外專家組成的調查委員會進行詳細調查，了解事故成因，預計可於3個月內完成報告。為審慎起見，港鐵公司已即時暫停所有新信號系統的行車測試，直至確認今次事故成因及確保新信號系統安全。另外，機電工程署（機電署）作為監管鐵路安全的法定部門，會同時作專業及獨立調查，務求令事情水落石出，確保鐵路安全。

3. 本文件向委員解說更換信號系統的流程、事故經過及港鐵公司初步調查所得資料。

提升信號系統流程

4. 港鐵公司在2015年批出合約，投資33億元更新七條港鐵綫（荃灣綫、港島綫、觀塘綫、將軍澳綫、迪士尼綫、東涌綫及機場快綫）的信號系統。

5. 信號系統控制鐵路網絡內列車的安全運作。鐵路綫會被劃分成區間，同一時段內一個區間內只允許一列列車通過，令列車與列車之間保持安全距離。現時以上七條港鐵綫的信號系統採用固定區間[1]模式，而新的信號系

[1] 採用固定區間模式，如某固定區間內有列車，則信號系統會指令後車不得駛進該區間。

統則採用「通訊為本列車控制」(CBTC)技術[2]，以移動區間的原理運作，在確保列車之間有安全距離的情況下加密列車班次，提升載客量。

6. 港鐵公司一直以嚴謹方式進行信號系統更換工程各個環節，當中包括制定功能規格、招標、設計、安裝、模擬測試、實地系統測試、功能試驗等去確保新系統安全及可靠，才投入服務。

7. 在招標階段，港鐵公司按世界貿易組織政府採購協定的要求，以公開和公平的程序進行招標。在招標過程中，公司會詳細審視所有標書，並對投標者的相關經驗、規模、過往表現等各方面因素進行評估，以確保中標公司具有所需能力、技術及經驗按合約訂明的條款完成工程。

8. 港鐵公司與信號系統承辦商的合約中，已列明新信號系統要配備主、副及備用區間電腦及其表現和功能的要求。一般信號系統都會配備主及副電腦。而為進一步提升信號系統的可靠及可用性，港鐵公司於合約中要求多配置一套備用電腦。

9. 根據合約，信號系統承辦商須負責系統設計及其硬件與軟件的開發，並進行模擬測試及實地測試，以確認及核實系統能安全及可靠運作。港鐵公司作為系統的使用者及鐵路服務提供者，會檢視承辦商就新系統進行各項所需測試，再以多年營運鐵路的經驗編制不同營運情景，進行實地演練。

10. 港鐵公司自2015年展開荃灣綫信號系統更換工程，在設計階段、安裝、模擬測試，及至實地測試，一直與承辦商緊密協作，包括舉行定期會議，與承辦商就系統設計要求進行磋商，並定期派員到承辦商在加拿大多倫多的系統模擬實驗室檢視模擬測試的情況。承辦商須按其專有軟件之特性、港鐵公司的要求及香港鐵路網絡的實際情況就不同情景進行模擬測試。當承辦商完成相關

[2] 新的信號系統利用現代無線通信技術以列車所發出的信息，將列車位置及車速等資料傳送至控制電腦，透過電腦運算以維持列車之間的安全距離。

的模擬測試以及通過其內部安全審核，及按所需要求向港鐵公司提交安全相關文件後，承辦商才會於其現場設備安裝有關軟件，及在相關路綫進行實地測試。

11. 新信號系統採用的CBTC技術，當中包括三套區間電腦，分別為前述的主、副和備用電腦。在模擬測試的階段中，承辦商曾就新信號系統的主、副及後備電腦分別進行測試，確認各系統均能獨立安全地運作；亦曾測試以上系統轉換的場景，如將主、副電腦切換至備用電腦運作，及在完成模擬測試後，以多輛列車進行實地測試等。

12. 自2016年年底開始，荃灣綫已開始於非行車時間在不同路段分別進行新信號系統的實地測試。測試一直以審慎及循序漸進的方式分階段進行。港鐵公司會先進行不涉及列車運行的實地測試，然後展開列車運作測試，而測試涉及的列車數目亦有序地逐步增加。而在測試範圍方面，會先由一個較小的範圍例如一至兩個信號設備開始，逐步擴大至一個車站以及在兩個車站之間進行測試，直至2018年初開始進行全綫測試。整項信號系統更換工程以及持續進行的測試工作，均嚴格按照國際標準的要求執行。

13. 為了確保新信號系統能安全及可靠運作才投入服務，港鐵公司委任了獨立安全評估顧問 (Independent Safety Assessor)，持續監察整個新信號系統建設及測試過程，並在新信號系統測試完成後，對信號系統承辦商系統安全保證工作進行評估，並提供安全認可文件。另外， 港鐵公司亦外聘國際獨立顧問，提供意見。

14. 在整個新信號系統的測試過程中，機電署切實執行作為規管者的把關工作，除了要求港鐵公司於每一個重要階段必需擁有由承辦商發出證明系統安全的安全證書才能進行測試外，機電署亦抽樣實地參與及觀察港鐵公司進行的安全測試，以確保符合有關的安全要求。抽樣參與測試項目包括信號系統的安全防護功能、緊急停車、超速保護、列車與月台幕門操作配合等。在港鐵公司完成新信號系統測試後，機電署亦會進行獨立評估（包括要求港鐵公司再作有關的安全實地測試），以確認新信號系統安全良好，才會批准港鐵公司使用新信號系統作日常營運。

事故詳情

15. 3月18日凌晨約2時45分，荃灣綫於非行車時間完全以新信號系統進行試驗。一列由金鐘站經渡線[3]準備進入中環站月台的列車第一卡，碰撞另一列由中環站開出，向金鐘方向駛經渡線的列車，導致該列車第二至第四卡損壞。請參閱附件一。

16. 兩列列車碰撞，導致其中一列列車的一卡有兩個轉向架偏離路軌。按車務工程人員評估，需要較長時間才能把有關列車移離現場。港鐵公司遂於凌晨2時56分向運輸署緊急事故交通協調中心通報有關事故，並於3時17分通知協調中心事故會影響當天荃灣綫的列車服務，並於凌晨4時發出「紅色警報」[4]。

17. 在3月18日至19日期間，港鐵公司派出約120名車務工程人員日以繼夜工作，將偏離路軌的列車移離正線，期間荃灣綫中環站及金鐘站的列車服務暫停，荃灣站至金鐘站之間，繁忙時間服務維持3分半鐘一班。往返金鐘站與中環站的乘客，需轉乘港島綫或改乘其他交通工具。

18. 在事故期間的繁忙時間，港鐵公司已加派約250名人員到受影響車站協助乘客及實施人流管理措施，根據觀察，車站的秩序大致良好。事發後至3月20日凌晨，港鐵車務工程人員一直全力進行復修，包括詳細檢查及維修路軌及附近設施、將涉事列車移離行車主綫。在確保安全及設備完整無損後，港鐵荃灣綫的服務在3月20日恢復正常。

19. 事故經過時序表見附件二。

---

[3] 渡線是連接兩條主鐵路軌之間的路軌。

[4]「紅色警報」是鐵路服務已持續或預計會持續嚴重受阻 20 分鐘或以上，並需要其他公共交通服務營辦商提供緊急交通支援服務的警告。收到警報後，運輸署會協調其他公共交通服務營辦商，立即調動資源，盡快提供適當支援服務。

事故期間的應變安排

事故通報及資訊發放

20. 事故發生後，港鐵公司已適時通報消防處、機電署及運輸署，並發出代表重大事故服務延誤的「紅色警報」。同時港鐵公司亦透過傳媒，向市民發放荃灣綫車務將受影響的信息，讓市民當天出門上班前可以及早準備。

21. 於車務受影響期間，港鐵公司一直透過其手機應用程式“Traffic News”、車站和車廂廣播、車站內和路面的指示，及車站入閘機旁的服務資訊顯示屏，通知乘客最新車務安排，以及提供其他公共交通的資訊。當列車服務回復正常後，港鐵公司亦透過手機應用程式及傳媒通知公眾。事發當天至修復完成期間，港鐵公司代表定時向傳媒匯報事故進展、列車服務安排及後續跟進工作。

22. 接獲港鐵公司通報後，運輸署緊急事故交通協調中心（協調中心）因應事故嚴重性將運作模式提升至最高的第三級別（聯合督導運作模式）[5]，由運輸署首長級人員領導，並增派人手統籌其他公共交通及作出應變。協調中心於事故期間一直與港鐵公司保持緊密聯繫，密切留意港鐵公司向乘客發放訊息及管理車站人潮的情況，並盡早透過傳媒發放新聞稿、網站及手機應用程式通知市民事故的最新發展及交通安排。運輸署亦派員到主要受影響鐵路站（即尖沙咀、金鐘站、中環站、香港站及北角站）及主要巴士站（包括位於海底隧道收費廣場、金鐘道及德輔道中等地點的巴士站）實地監察情況。機電署亦即時派員到場調查事故及監察修復工作。

[5] 在一般情況下，緊急事故交通協調中心每日 24 小時會以第一級別處理日常較輕微的交通運輸事故。如遇上小規模預早策劃的活動、嚴重的道路或隧道事故、公共交通服務嚴重或廣泛受阻等情況，協調中心的運作會提升至第二級別，並增派人手工作。如遇上大型預早策劃的活動或發生重大事故，需要作出跨部門高層次的督導和協調，協調中心的運作會提升至第三級別，即聯合督導運作模式，運輸署會邀請其他部門例如警方、路政署、公共運輸營辦商或活動主辦單位到協調中心處理事故，由副總監(首長級的職員)領導及統籌協調中心的運作。

其他交通服務

23. 在接獲港鐵公司的通報後，運輸署協調中心於3月18及19日一直與專營巴士公司、電車公司及渡輪營辦商保持緊密聯繫，要求加強服務和加派外勤人員協助乘客排隊。在運輸署協調下，39條專營巴士路綫、23班額外電車及6班天星小輪於事故期間加強服務，協助接載受影響乘客。協調中心於事故期間也一直與港鐵公司保持緊密聯繫，並盡早透過傳媒發放新聞稿、手機應用程式通知市民事故的最新發展及交通安排。運輸署亦透過電台呼籲市民預早計劃行程，或根據其所在的位置和目的地改變出行路線或模式、及考慮使用其他交通工具，以盡量減低事故造成的影響。

復修情況

24. 3月18日列車服務暫停後，港鐵公司的車務工程團隊及承辦商員工已爭分奪秒進行修復。但由於涉事位置在隧道內，活動空間有限，工程團隊必須確保修復過程安全，只能逐少移動列車重回路軌。期間，港鐵公司聯繫了消防處要求提供技術支援。基於現場環境限制，復修時間比預期長。直至3月19日晚上11時，工程團隊完成將偏離路軌的列車兩個轉向架移回路軌，並於3月20日凌晨約1時15分完成現場設備的修復工作。其後，港鐵公司把涉事列車移到金鐘站的側綫及進行安全檢測。車務於當天早上回復正常。機電署全程監察整個復修過程，並在中環至金鐘站恢復服務前，與港鐵公司進行一系列安全測試，以確保鐵路安全運作。

確保現有信號系統安全穩妥

25. 新信號系統與現有的信號系統所採用的軟件及硬件不相同，是兩套不同的系統。事發時，荃灣綫正以新信號系統進行試驗，原有的信號系統已被完全隔離。事故時，所有路軌旁信號設備及車載信號系統皆由新信號系統控制。因此，是次事故與現有的信號系統完全無關，同類事故不會在現有鐵路綫發生。

26. 儘管如此，機電署已於事發當日的非行車時段，實地抽驗現有鐵路綫信號系統各電腦控制道岔的聯鎖功能。結果顯示現有系統繼續有效運作，列車及公眾安全受到保障。

初步觀察

27. 新信號系統發生事故的確切原因，仍有待調查委員會的深入調查及分析。在事故發生當天，港鐵公司已即時與信號系統承辦商 Alstom-Thales DUAT JV 公司[6]召開緊急會議，而承辦商亦即時收集事發時系統數據分析，並在加拿大多倫多系統模擬實驗室重組事發經過。

28. 初步觀察而言，正如前文所述，新信號系統採用的CBTC技術包括主、副和備用的三套區間信號電腦。事發時正進行由主及副電腦切換至備用電腦的試驗，模擬在主及副電腦未能如常運作的場景下，系統自動轉至備用電腦所須的應變措施、復修程序，及備用電腦能否繼續暢順運作。

29. 於上述場景試驗期間，當主及副電腦轉換到備用電腦後，一列中環站二號月台列車獲新信號系統授權經渡線向金鐘方向開出行駛，其後另一列由金鐘站向中環方向行駛的列車亦獲系統授權經同一渡線進入中環站一號月台，繼而發生碰撞。事件發生後，承辦商在加拿大多倫多系統模擬實驗室重組事件經過，在模擬相同的場景時亦出現同樣的問題。

30. 正常情況下，信號系統必須時刻掌握運作中所有列車的所在路段，確保列車之間保持安全距離，及不會同時行駛相互衝突路線（即安全聯鎖功能的作用），釀成意外。這是現代化鐵路信號系統體現運作安全的最基本設計。然而，初步調查顯示，當日事故發生時，在主及副電腦被轉換到備用電腦後，備用電腦的安全聯鎖功能在肇事路段未有一如預期根據系統設計要求正常運作。結果，信號系統安排兩列列車駛進相互衝突路線，引致事故。港鐵公司與承辦商正進行全面的調查，包括系統結構、設計、各電腦之間的切換、軟硬

[6] 新信號系統的承辦商是 Alstom Hong Kong Limited (Alstom) 和 Thales Transport & Security (Hong Kong) Limited (Thales)組成的 Alstom-Thales DUAT JV 公司，兩間公司總部位於法國，CBTC 技術由 Thales 加拿大技術部門提供。港鐵公司於 2015 年 1 月將七條港鐵綫的訊號系統提升工程合約，批予這間系統供應商，合約總值 33 億元。

件整合、系統安全保證工作、測試程序等各方面，以確定系統出錯的原因。

跟進工作

31. 港鐵公司一直將乘客及員工安全放在首位。港鐵公司及信號系統承辦商的專家會全力配合調查委員會，深入調查事故原因。機電署亦會同時作專業及獨立調查，包括委任獨立顧問覆檢港鐵公司及其承辦商和專家提交的資料和報告，確保能夠查明事故成因。

32. 港鐵公司已通知機電署並公佈，在未查明事故原因之前會繼續全面暫停非行車時間新信號系統的行車測試工作。港鐵公司亦會根據合約的條款保留按將來的調查結果向信號系統承辦商追究的權利。只有在港鐵公司及機電署確認事故原因查明並作出改正後，政府才會容許港鐵公司恢復非行車時間新信號系統的行車測試工作。

33. 港鐵公司強調，現時進行的信號系統提升，必須通過嚴格及重複的測試，得到機電署及相關政府部門確認確保行車安全後，才會正式投入服務。機電署亦會聯同相關政府部門，就新信號系統進行嚴謹、獨立的審批，在確保有關系統的運作安全及暢順後，才會批准系統正式投入服務。

34. 根據票價調整機制內「服務表現安排」，港鐵發生31分鐘或以上因機件故障或人為因素導致的服務延誤事故，即會撥出款項放入票價優惠帳戶，透過「車費優惠」回饋乘客。由於荃灣綫來往中環站與金鐘站的列車服務暫停了兩天(3月18日及19日)，港鐵公司會撥出相應款項。政府亦會與港鐵公司嚴肅跟進相關問題。

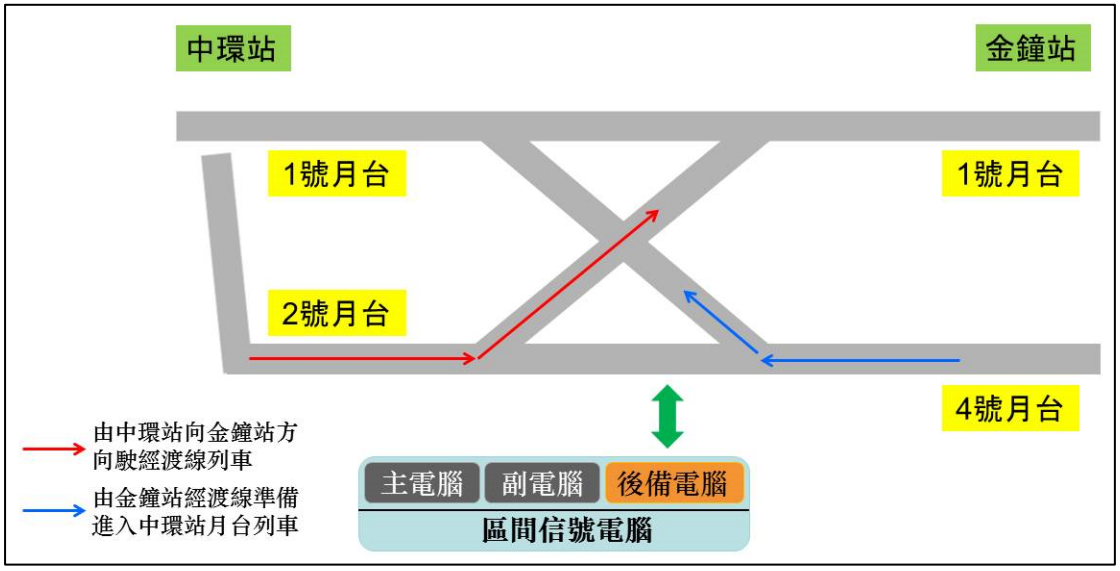
35. 港鐵公司就事故引致市民的關注及不便致歉，亦衷心感謝乘客的體諒及配合。

運輸及房屋局
港鐵公司
2019年3月

附件一

2019年3月18日港鐵荃灣綫新信號系統試驗事故

事發經過示意圖



附件二

2019年3月18日港鐵荃灣綫新信號系統試驗事故

發生時間	事項
3月18日	
凌晨2時45分	兩列車在中環站附近碰撞。
凌晨2時54分	通知消防處及警方，兩名車長隨後被送往醫院治理或檢查，同日早上出院。
凌晨2時56分	通知運輸署有關事故。
凌晨3時	通知機電工程署。
凌晨3時17分	通知運輸署當日早上荃灣綫列車服務會受影響。
凌晨4時	港鐵公司發出「紅色警報」，並透過Traffic News及傳媒，通知市民當日荃灣綫列車服務將受影響，而荃灣綫金鐘至中環站的服務需暫停。
上午6時30分	向傳媒簡報事故及車務的最新情況。
上午11時30分	向傳媒交待事故的最新發展，並宣佈成立調查委員會，徹查事故原因。
下午2時	港鐵與信號系統承辦商進行會議，要求承辦商提交報告及配合跟進調查工作。
下午5時	向傳媒報告與信號系統承辦商開會後的初步觀察。
3月19日	
全日	全力進行復修。
上午6時30分	向傳媒報告復修工作進度，及宣佈荃灣綫金鐘至中環站的服務仍需暫停。
下午6時	向傳媒報告港鐵董事局就事故的跟進及解釋事故。
晚上11時	將偏離路軌的一卡列車兩個轉向架，移回路軌。
3月20日	
凌晨0時至1時15分	全力進行復修。
凌晨1時15分	復修完成及後把涉事列車移到金鐘站的側綫及進行安全檢測。
凌晨4時45分	透過Traffic News及傳媒，通知市民事件中列車已移離主行綫，而復修工作已完成，及宣佈當日早上荃灣綫列車服務回復正常。
上午10時	向傳媒報告恢復服務後的車務運作情況，及交待復修過程的情況及挑戰。

答集體運輸服務工作小組文件2019／第 11號
（於25.9.2019會議討論）

機電工程署 EMSD

香港特別行政區政府 機電工程署
香港九龍啟成街3號
Electrical and Mechanical Services Department
Government of the Hong Kong Special Administrative Region
3 Kai Shing Street, Kowloon, Hong Kong
www.emsd.gov.hk

Our reference 本署檔號：
EMSD/RB-1/8-1/3/1.1

Your reference 來函檔號：
HAD YLDC 13/35/35

Telephone 電話號碼：2808 3741
Facsimile 圖文傳真：3579 2016

(傳真: 2478 7334)

元朗區議會
集體運輸服務工作小組秘書
黃曉慧女士
元朗橋樂坊 2 號元朗政府合署 13 樓

黃秘書：

元朗區議會交通及運輸委員會
集體運輸服務工作小組
2019 年度第三次會議
有關「討論港鐵測試新訊號系統引致列車相撞事故」的跟進工作

閣下於2019年4月30日就題述事宜的來信收悉。本署回覆如下：

本署非常關注今次事故，港鐵公司已停止新信號系統的測試。

本署已就該事故展開詳細、獨立及全面的調查及已要求港鐵公司於事故後三個月內向本署提交調查報告。本署亦會在審視港鐵調查報告後，完成獨立調查。而調查方向包括系統設計、操作、硬件軟件配合，以至實際測試過程，以徹底找出事故原因。政府會適時向立法會、區議會及公眾交代調查結果。

本署將未能派代表出席2019年5月27日的會議。

機電工程署署長

(葉偉良 代行)

2019 年 5 月 2 日

MTR Corporation Limited
香港鐵路有限公司
www.mtr.com.hk

來函檔號：HAD YLDC 13/35/35　　傳真：2478 7334
本函檔號：CA/EA/DC/YL/1903/051

元朗橋樂坊 2 號
元朗政府合署 13 樓
元朗區議會交通及運輸委員會
集體運輸工作小組主席
姚國威議員
（經辦人: 黃曉慧女士）

有關 2019 年 3 月 18 日港鐵荃灣綫新信號系統測試事故

港鐵公司十分重視今年 3 月 18 日荃灣綫新信號系統測試的事故，並成立了調查委員會進行深入調查。港鐵公司已公佈有關調查結果，現附上有關報告，以供參考。

對外事務高級經理

陳裕昌

二零一九年七月十八日
附件

附件

新聞稿
Press Release

編號零四四/一九　　二零一九年七月五日

二零一九年三月十八日荃灣綫事故確定因軟件編程執行錯誤所致
港鐵公司加強監察新信號系統承辦商

港鐵公司今天(二零一九年七月五日)就二零一九年三月十八日非行車時間於荃灣綫新信號系統演練期間發生的事故，向公眾交代調查結果。經詳細調查後，總結事故是新信號系統承辦商 Alstom-Thales DUAT Joint Venture 公司在修改軟件時出現軟件編程上的執行錯誤所致，並向承辦商建議了一系列改善措施。港鐵公司會提高警覺及加強監察，確保承辦商落實改善措施。

二零一九年三月十八日非行車時間荃灣綫進行演練期間，一列港鐵非載客列車在經渡綫準備進入中環站時，與另一列由中環站開出正駛經該渡綫的非載客列車發生碰撞。港鐵公司十分重視事件，成立了調查委員會，由港鐵公司車務總監劉天成先生和技術工程總監顏永文博士共同擔任主席，委員會成員包括其他港鐵高級職員，本地及海外的外間專家亦有參與調查工作。委員會旨在調查事件成因及提出改善建議，防止類似事件再次發生。委員會已完成全面調查，並於六月十七日向政府提交報告，相關部門剛完成審視工作。

<u>事故成因</u>

承辦商建立的荃灣綫新信號系統分爲兩個控制區，每個區由三套區間控制電腦系統所組成，分別為主電腦系統(A 電腦系統)、副電腦系統(B 電腦系統)及備用電腦系統(C 電腦系統)。委員會同意備用電腦系統的安排在承辦商信號系統應用中屬於嶄新的做法，目的是爲了縮短發生信號故障事故時的修復時間。承辦商在實驗室完成軟件的模擬測試後，二零一六年十二月開始在荃灣綫進行列車實地測試。按照循序漸進及小心策劃的計劃，列車測試的規模由一列列車逐步增加至多列列車，並測試 A、B 及 C 電腦系統。二零一九年三月十八日進行的演練，目的是讓車務人員熟習在 A 及 B 電腦系統同時發生故障而須切換至 C 電腦系統時的操作程序。

(轉下頁)

承辦商在開發新信號系統軟件過程中，爲了提升軟件表現及符合營運要求，須對軟件作出適當的修改。委員會發現，承辦商於二零一七年修改軟件時衍生了三個軟件編程的執行錯誤，該次修改是爲了令軟件符合其設計目的，即在 A 及 B 電腦系統出現問題時，避免 C 電腦系統出現共同模式故障。承辦商須在 A/B 電腦系統向 C 電腦系統傳送數據時剔除部分數據，而被剔除的數據應由 C 電腦系統重新產生，從而避免共同模式故障。修改過程中，承辦商發生了下列三個軟件編程的執行錯誤：

- 首先，承辦商的軟件團隊沒有在其內部軟件開發文件中清楚列明傳送數據至 C 電腦系統時剔除「相互衝突區域數據」，以致隨後並無進行特定測試、風險評估及安全分析，包括在實驗室進行的驗證模擬測試及實地測試，以驗證當 C 電腦系統取代成為主電腦系統時的「相互衝突區域數據」；
- 其次，承辦商發生軟件編程的執行錯誤，令 C 電腦系統未能適當地重新產生「相互衝突區域數據」；
- 第三，承辦商建立的軟件邏輯配置，並沒有阻止 C 電腦系統在沒有「相互衝突區域防護」的情況下取代成為主電腦系統，導致發生今次事故。

委員會認為，這些錯誤反映承辦商在是次軟件修改時的軟件品質保證、風險評估及模擬測試範圍方面均有不足之處。

<u>安全保證</u>

根據合約條款及設計要求，承辦商有責任確保新信號系統的安全，包括有責任提供一個安全的信號系統以作演練。由承辦商建立的信號系統乃專屬技術系統，承辦商擁有所有技術資料包括軟件的專利知識。儘管如此，港鐵公司有一套監察機制，包括專責的團隊監察工程，信號系統的更換工程一直以審慎及循序漸進的原則進行，新系統需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。同時，港鐵公司亦委任了「獨立安全評估顧問」及「獨立檢討顧問」，分別持續地評估承辦商為新系統投入載客服務所執行的系統安全保證程序，以及就落實相關工程時所帶來的風險提供意見。

(轉下頁)

港鐵公司行政總裁金澤培博士表示:「安全一直是港鐵公司的首要任務，我們十分重視任何會影響鐵路處所內人士的安全的事件，並會竭盡所能，找出事件成因及防止類似的事情再發生，三月十八日的事故也沒有例外。我們一定會落實改善措施，嚴格監察承辦商跟進，亦會同時加強公司的監察系統。」

<u>改善措施</u>

事故發生後，承辦商已更換導致有關軟件問題的軟件設計及開發團隊。為了提升軟件開發的品質及防止類似事件再發生，委員會向承辦商提出下列改善措施:

- 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;
- 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;
- 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；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。

同時，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:

- 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;
- 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;
- 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；及
- 與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。

有關調查結果詳情，請參閱附件。

(完)

關於港鐵公司

每天，港鐵聯繫市民及社區。作為世界級可持續鐵路運輸服務的營運商，港鐵公司在安全、可靠程度、顧客服務和效益方面都處於領導地位。

由設計、規劃和建設，以至開通、維修和營運，港鐵擁有全方位的鐵路專業知識和四十多年的鐵路項目發展經驗。 除了參與各項鐵路項目及營運，港鐵透過鐵路、商業和物業發展的無縫整合，建設並管理鐵路沿線充滿活力的新社區。

港鐵在香港、英國、瑞典、澳洲和中國內地擁有超過四萬名員工*，每週日的全球客運量超過一千二百萬人次。港鐵更致力發展和連繫社區，創建更美好未來。

如欲進一步了解港鐵公司，請瀏覽 www.mtr.com.hk。

* 包括香港及全球各地的附屬和聯營公司

附件

摘要

2019 年 3 月 18 日非行車時間內, 在荃灣綫就承辦商 Alstom-Thales DUAT Joint Venture (ATDJV) 所提供的新信號系統進行一項演練。此項演練目的是讓車務人員熟習系統的特性，及如何應用操作程序處理主電腦系統和副電腦系統同時發生故障而需要切換至備用電腦系統的情況。

於大約凌晨 2 時 44 分，一列非載客列車經渡綫駛向中環站月台時，與另一列從中環站開出同時駛經該渡綫往金鐘站的非載客列車碰撞，導致兩列列車受損。兩名列車司機被送往醫院接受檢查，並於同日出院。

港鐵公司十分關注是次事件，故此成立調查委員會，成員包括港鐵高級職員及外間專家，調查及找出事故成因，並提出建議以防止同類事件再次發生。

調查總結事件的成因, 是承辦商 ATDJV 的一項軟件問題令有關渡綫失去相互衝突區域防護功能，容許上述兩列列車同時駛進渡綫，造成碰撞。而該項軟件問題是承辦商在進行一項軟件修改過程中所衍生的軟件編程的執行錯誤所造成。

委員會亦進一步認為該軟件編程的執行錯誤反映 ATDJV 在軟件程式開發過程中， 就該次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。

委員會對 ATDJV 作出以下建議：

(a) 更換導致有關軟件問題的軟件設計及開發團隊；

(b) 糾正有關軟件修改問題，確保並提供具體證明軟件開發在品質上並無構成其他影響；

(c) 提升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日後任何可能發生的程式編寫錯誤；及

(d) 制定一系列全面的有效措施，包括但不限於 (i) 聘任外間「獨立軟件評估顧問」，以加強主、副和備用電腦系統的軟件開發過程，(ii) 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；及 (iii) 在委員會專家的協助下，就其軟件編程的執行方面，進行風險評估。

為協助 ATDJV 落實上述建議，委員會建議港鐵營運項目團隊提高警覺及加強監察，確保 ATDJV 落實有關措施，以重建公眾對新信號系統的信心：

(a) 將現時「獨立安全評估顧問」(Independent Safety Assessor, ISA)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；

(b) 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；

(c) 港鐵與 ATDJV 共同成立一個信號系統測試及驗收安全委員會，管理

實地測試（並納入「獨立安全評估顧問」的意見）；及

(d) 與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，並探究將來其他由 ATDJV 所建議在技術上合適的方案。

在取得政府同意後，方會恢復在非行車時間內進行新信號系統的列車測試。

1. 引言

1.1 2019 年 3 月 18 日大約凌晨 2 時 44 分，即非行車時間內，在荃灣綫就新信號系統進行一項演練期間，一列非載客列車經渡綫駛向中環站月台時，與另一列從中環站開出同時駛經該渡綫往金鐘站的非載客列車碰撞，導致兩列列車受損。

2. 調查委員會

2.1 港鐵公司十分關注是次事件，故此成立調查委員會，調查及找出事故成因，並提出建議以防止同類事件再次發生。

2.2 委員會由車務總監劉天成及技術工程總監顏永文擔任聯合主席，成員包括港鐵車務營運及技術工程的高級職員，以及外間專家，包括來自國際知名的工程顧問公司 WSP 的 Gab Parris、Peter Sheppard 和王志威，以及香港理工大學協理副校長（學術支援）何兆鎏教授。

3. 背景

3.1 信號系統更新工程

3.1.1 信號系統對於鐵路網絡中列車服務的安全運作至關重要。為加密列車班次和提升載客量，並逐步更新現有資產，港鐵於 2015 年 1 月透過公開招標，將更新 7 條鐵路綫（包括荃灣綫、港島綫、觀塘綫、將軍澳綫、廸士尼綫、東涌綫及機場快綫）的信號系統合約批出予 Alstom Hong Kong Limited (Alstom) 和 Thales Transport & Security (Hong Kong) (Thales) 所組成的聯營公司 Alstom-Thales DUAT Joint Venture (ATDJV)。Alstom 和 Thales 均為國際知名的鐵路基建供應商，就其產品及技術擁有專有權及專有知識。

3.1.2 荃灣綫信號系統分為兩個控制區。按照合約要求，新信號系統在每個控制區內均由三套區間控制電腦系統組成，分別為主電腦系統(A 電腦系統)、副電腦系統(B 電腦系統)和備用電腦系統(C 電腦系統)。A、B 及 C 電腦系統的硬件相同並載入共同軟件。這三套電腦系統透過其硬件識別插頭(hardware identity plug)，按其配置執行 A、B 及 C 電腦系統的功能，而共同軟件可相應地處理三套電腦系統之間的動態數據。但為免出現共同模式故障(common mode failure)，C 電腦系統只接收來自 A/B 電腦系統的部分指定動態數據。這項三套區間控制電腦系統的配置安排的目的是透過更高的復原能力，以提升系統的可用性和縮短系統發生故障後恢復提供服務的時間。備用電腦系統的安排在 ATDJV 信號系統應用中屬於嶄新的做法。此外，C 電腦系統是設置於另一

個車站，透過地點出入的控制和獨立的電力供應以加強系統保安。

3.2 測試及模擬

3.2.1 港鐵營運項目團隊按照鐵路信號業界廣泛採用的方法管理這項信號系統更新工程，包括檢視由承辦商進行實驗室軟件模擬測試及實地測試，以確保新信號系統在安全及可控情況下開發至成熟階段。所有相關測試活動均按步就班、循序漸進，在每個關鍵階段，均按照認證程序及由 ATDJV 發出的相關安全文件進行。附件 1 的示意圖展示各項模擬及測試的整體計劃。

3.2.2 2016 年 12 月，ATDJV 開始於非行車時間內在荃灣綫進行實地列車測試。測試規模由一列列車逐步增加至多列列車。

3.2.3 通過分階段進行的系統成熟度測試，形成對新信號系統開展演練的準備程度逐步增加信心。因此港鐵營運項目團隊和 ATDJV 由 2019 年 2 月起，共同開展各項演練，包括系統運作及車務人員熟習系統特性等演練。

3.2.4 基於先前對安裝在所有電腦系統的共同軟件已進行了多項模擬測試（因而在 C 電腦系統上沒有重複進行該些在共同軟件已完成了的模擬測試），並完成了由 A/B 電腦系統切換至 C 電腦系統的特定傳輸功能測試後，ATDJV 發出了有關安全文件，給予港鐵營運項目團隊信心讓 C 電腦系統切換為主電腦系統並進行演練。有關演練的目的是讓車務人員熟習系統的特性。透過演練，車務人員有機會熟習將來日常運作中可能出現的眾多不同行車服務狀況。有關

演練亦有助新信號系統在最終投入載客服務前，按需要微調車務操作程序。

3.3 安全保證

3.3.1 ATDJV 必須按照合約訂明的責任和設計要求提供一個安全的信號系統。港鐵營運項目團隊要求 ATDJV 按其責任釐定模擬和測試的範圍和程度，以確保其根據國際標準交付一個安全的信號系統。

3.3.2 ATDJV 擁有其工程項目安全團隊，負責審查和證明軟件安全及可供實地測試和演練。此外，他們亦另外委任了獨立安全小組，負責在新信號系統獲得可投入載客服務認證前，評估和證明系統的安全性。

3.3.3 除了上述 ATDJV 提供的安全保證外，為了在投入載客服務前進一步確保新信號系統的安全，港鐵營運項目團隊亦委任了「獨立安全評估顧問」，負責評估承辦商所執行的系統安全保證程序，並對有關程序評估為滿意後，提供安全認可文件。「獨立安全評估顧問」是基於系統最終投入載客服務時的表現而作出安全評估，並非就其他前期主要工程階段（例如各項演練等）進行安全評估。此外，港鐵營運項目團隊亦委任了外間「獨立檢討顧問」 (Independent Reviewer, IR) ，就相關工程落實時對營運中的鐵路所帶來的風險提供意見。「獨立安全評估顧問」和「獨立檢討顧問」按上述各自的工作範疇參與工程項目活動，惟均不包括對演練工作的評估。

4. 事故

4.1 於 2019 年 3 月 18 日非行車時間內，港鐵營運項目團隊與 ATDJV 的工程師進行預先編排的聯合演練，目的是驗證有關操作程序，以應對 A 和 B 電腦系統同時發生故障而導致 C 電腦系統需取代成為主電腦系統的情況，並讓車務人員熟習系統特性，及應對電腦系統出現故障時的操作程序。

4.2 於大約凌晨 2 時 34 分， A 和 B 電腦系統相繼被關掉以模擬故障發生，C 電腦系統即按系統設計取代成為主電腦系統。當切換至 C 電腦系統時，按預期般，原先為所有列車設定的路綫被註銷，所有列車停下。隨後，在車務控制中心的行車控制主任須根據正常操作程序，向每列列車逐一發出「開出」 (Depart) 指令，以恢復列車運行。

4.3 於大約凌晨 2 時 41 分 32 秒，行車控制主任遵照程序向停泊於中環站 2 號月台的列車發出「開出」指令，然後 C 電腦系統為該列車設定路綫以駛往金鐘站 1 號月台。於大約凌晨 2 時 43 分 53 秒，行車控制主任按當時行車需要，進行正常行車調度，解除中環站的月台排序安排，讓電腦系統按實際情況選擇月台，使等待中的列車可進入無列車的中環站 1 號月台。大約凌晨 2 時 44 分 01 秒，C 電腦系統錯誤地設定了相互衝突的路綫並發出可前進信號，導致兩列列車於頃刻間以「自動模式」開出，並在中環站外的渡綫相撞。對於這瞬間出現及系統突發的情況，行車控制主任極難在車務控制中心的層面作出即時反應和制止，透過指令步驟及時緊急剎車。事實上，行車控制主任的角色是處理列車調度工作，因此，不應由他們查找及應對此種系統特性上的突發問題及情況。同樣地，雖然駛

往中環站1號月台列車的車長在看見另一列列車由中環站2號月台駛往金鐘站1號月台時，已啟動了緊急制動器，但列車仍未能在碰撞前及時剎停。

附件2的示意圖展示有關情況。

4.4 除了兩名列車車長其中一人的右膝輕微擦傷外，並無其他港鐵員工或ATDJV員工受傷。兩名列車車長被送往醫院接受檢查，並於同日出院。

5. 事故成因

5.1 A, B和C電腦系統的硬件相同並載入共同軟件，但各配備不同的識別硬件插頭，用以初步配置為主電腦系統、副電腦系統和備用電腦系統，即是A、B和C電腦系統。在2017年6月前，由A電腦系統傳送至B電腦系統或由B電腦系統傳送至C電腦系統的數據全是相同的，意味著任何導致A和B電腦系統出現故障的數據損毀情況亦會傳送至C電腦系統，因而造成共同模式故障。

5.2 為了符合合約要求，避免出現共同模式故障，ATDJV遂於2017年7月著手進行一項軟件修改，在A/B電腦系統傳送數據至C電腦系統時將部分動態數據剔除，包括防止設定相互衝突路綫的「相互衝突區域數據」(Conflict Zone Data) (以提供安全聯鎖功能)；而被剔除的數據隨後應在C電腦系統內重新產生。被剔除及重新產生的數據量由ATDJV決定，主要考慮共同模式故障的風險，以及當A和B電腦系統同時

出現故障時，C 電腦系統需要迅速取代成為主電腦系統的修復時間。然而，是次由 ATDJV 啟動的軟件修改，卻因為軟件設計及開發人員於進行軟件修改期間出現以下軟件編程的執行錯誤，導致軟件出現問題。

5.3 調查發現由 ATDJV 進行的軟件修改過程中出現以下三項軟件編程的執行錯誤導致軟件出現問題。第一，雖然「相互衝突區域數據」在傳送時被剔除，但這項安排並未於 ATDJV 的內部軟件開發文件中列明。由於沒有在文件中列明，隨後 ATDJV 並無對此進行任何特定測試、風險評估及安全分析，包括在實驗室進行的驗證模擬測試及實地測試，以驗證當 C 電腦系統取代成為主電腦系統時的「相互衝突區域數據」。這是第一項軟件編程的執行錯誤。

5.4 第二， ATDJV 於 A/B 電腦系統數據傳送至 C 電腦系統時剔除了「相互衝突區域數據」，但軟件設計及開發人員在處理需要重新產生的數據時出現了軟件編程的執行錯誤，導致 C 電腦系統未能適當地重新產生「相互衝突區域數據」。這項軟件編程的執行錯誤最後引致 C 電腦系統在並沒有「相互衝突區域數據」的情況下取代成為主電腦系統。

5.5 第三，軟件設計及開發人員建立的軟件邏輯配置，並無阻止 C 電腦系統在沒有「相互衝突區域數據」的情況下取代成為主電腦系統，意味著系統失去了相互衝突區域的防護。沒有執行適當的程式邏輯配置以防止 C 電腦系統在失去相互衝突路綫防護功能的情況下取代成為主電腦系統，被視作為一項軟件編程的執行錯誤。

6. 調查結果

6.1 委員會發現直至事故發生前，ATDJV 在系統核實和驗證過程（包括按進程進行的模擬測試）均未有察覺第 5 章所述的軟件問題。由於 ATDJV 並未察覺有關軟件問題，故此亦無將有關情況告知港鐵營運項目團隊。委員會亦注意到 ATDJV 曾發出有關安全文件，令港鐵營運項目團隊有信心以 C 電腦系統進行演練是安全的。事實上，根據 ATDJV 發出的安全文件，由 2018 年 10 月 15 日起，進行實地測試時已不再就列車數目和列車分隔距離設限。此外，自 2018 年 10 月中起，已經按程序進行多項測試，確定 C 電腦系統（作為備用電腦系統）可取代成為主電腦系統，即是在切換後可由 C 電腦系統持續進行全面操控工作。因此，在此後進行的任何實地測試中，因應各種可容許和可能出現的情境因素組合，當 C 電腦系統取代成為主電腦系統時，有關的軟件問題已可能會浮現。委員會認為 ATDJV 於事故發生前，在進行該次軟件修改過程中出現的三項軟件編程的執行錯誤是造成這次事故的成因。

「WSP 的獨立專家小組認為 ATDJV 有責任向港鐵公司保證其產品是安全的。

就港鐵的演練 / 演習而言，很明顯這些工作是單純為了讓港鐵制定和測試其車務規則手冊及讓其員工熟習正常及有限操作模式的特性而設計，建立對 3036 CBTC 信號系統在可操作性和可靠性方面的信心。」

外間專家

WSP

6.2 同時，委員會認為上述的軟件編程的執行錯誤反映 ATDJV 在軟件程式開發過程中，就該次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。

6.3 委員會認為 ATDJV 有責任釐定模擬測試的範圍，以核實和驗證安裝在 A，B 及 C 電腦系統的共同軟件均按其應有功能發揮作用。ATDJV 應透過其核實和驗證程序，使軟件達至所需的成熟度。委員會亦注意到在實地測試開始之前，ATDJV 已根據其軟件開發文件中的規定，按程序完成其擬定範圍的所需模擬測試。此後 ATDJV 進行了廣泛的實地測試，並用了一年多的額外時間適當地反覆進行模擬及測試，讓軟件漸趨成熟。根據模擬結果以及各項實地測試的結果（包括港鐵鐵路項目團隊見證由 A/B 電腦系統切換至 C 電腦系統的測試），軟件應已具足夠成熟度，可讓車務人員安全地演練，以熟習任何營運情況下各種系統特性。在軟件問題未浮現的情況下，

工程項目遂在 ATDJV 所提供的安全文件確認下進入演練階段。然而，委員會認為就事故後發現的軟件修改的性質而言，ATDJV 應於釐定模擬測試時擴大範圍以涵蓋一些可能影響系統關鍵表現的情境，縱使修改細節或未在軟件開發文件中完全清晰說明。

6.4 港鐵營運項目團隊知悉在演練後將會有一個較新的軟件版本，但委員會認為，由於當其時該軟件的成熟度應能滿足 6.3 段所述的目的，並無任何資料指 2019 年 3 月 18 日的演練需要暫停。

「在沒有確切的理據下，港鐵無理由要片面地決定暫停以軟件版本 8.3.3 進行演練，以等待版本 8.3.4 的推出。」

外間專家

何兆鏗教授

「根據 Thales 提供的文件(即安全證書和 SOR 文件)，於 2019 年 3 月 18 日進行演練是安全的。」

外間專家

WSP

6.5 在使軟件漸趨成熟的過程中，ATDJV 已完成了實驗室模擬以驗證系統的功能是適合進行實地測試。就演練而言，其目的是讓車務人員實地熟習系統特性，並應對實際車務運作中眾多可能會遇到的實地情境。委員會明白到，在安排當日演練之前，已進行了按照軟件開發文件要求而制訂的模擬測試，包括由 A/B 電腦系統切換至 C 電腦系統的測試，但委員會認為在進行模擬測試時，仍可進一步加入額外的情境個案，以加強信心。

6.6 委員會留意到，根據原有資源計劃，2019 年 3 月 18 日所進行的演練程序原先是以 4 列列車擬定的。然而，根據 ATDJV 發出的安全文件，在進行演練時，已不再有列車數目限制。為摸擬早上繁忙時間的狀況，港鐵營運項目團隊透過試車計劃數次通知 ATDJV，於 2019 年 3 月 18 日的演練是以 34 列列車進行，並非 4 列列車。隨後港鐵營運項目團隊和 ATDJV 以 34 列列車進行聯合演練。調查期間證實，由於程序上已經無就列車分隔距離設限，故此在沒有相互衝突路綫防護的情況下，只要有兩列或以上列車均有可能發生事故。委員會因而認為，34 列列車同時運行只是增加了未知的軟件問題浮現的可能性，但絕非事故的成因。委員會亦留意到，參與當日演練的車務人員已恰當地根據正常操作程序處理將來日常營運中可能遇到的車務情境。

6.7 委員會審視了「獨立安全評估顧問」早前就以下幾點關注所提交的評估結果及建議，包括 i) Thales 是否恪守內部程式開發程序；ii) 是否完全恪守國際標準；iii) 其核心產品的開發程序是否不足及有關風險。委員會注意到港鐵營運項目團隊和「獨立安全評估顧問」均已採取額外措施以進行額外評估，包括多次造訪廠房和進行額外模擬測試，並給予 ATDJV 一年多的額外時間，使系統更趨成熟並處

理上述「獨立安全評估顧問」關注的問題。即使根據「獨立安全評估顧問」的職權範圍，有關評估結果及建議只是基於系統最終投入載客服務時的表現而作出，並非針對演練和測試， ATDJV 在事故發生前就部分問題的處理已取得進展。委員會獲「獨立安全評估顧問」確認，按照有關評估結果，他們並沒找到任何特定的情況而需要停止進行實地測試或演練。委員會因此作出結論，認為「獨立安全評估顧問」的評估結果及建議既無發現特定的不安全情況，亦無作出特定建議指出需要終止實地測試或演練。然而，委員會認為港鐵營運項目團隊日後在監察 ATDJV 的項目交付方面，在處理「獨立安全評估顧問」的意見時應提高警覺。

6.8 委員會認為，在事件發生時，並無明確理由終止實地測試 (包括按 ATDJV 提供的安全文件所進行的演練)。儘管如此，委員會認為日後港鐵營運項目團隊在評估「獨立安全評估顧問」提出的關注時應提高警覺，留意對演練會否帶來影響，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。

「基於 Thales 已為演練和測試提供所需的安全保證文件（Specific Application Safety Case [附帶 SOR 限制] ，其後以 Safety Memo 修訂），WSP 獨立專家小組 （設身處地從港鐵的角度）亦會容許演練進行。先前進行的所有工作及提交的文件所逐步建立的保證和信心，均成為支持該項決定的基礎。」

外間專家

WSP

「港鐵一直採取審慎和循序漸進的原則，在安排測試、演練和演習方面取得一定信心。港鐵在收到『獨立安全評估顧問』的意見後亦採取了額外的措施。因此，港鐵相信 3 月 18 日進行的演練是熟習系統的常規演習，實屬合理。」

外間專家

何兆鏊教授

7. 總結

7.1 委員會審視了是次事故的事實以及與事故成因相關的因素，總結認為 ATDJV 在執行是次軟件修改過程中出現以下三項軟件編程的執行錯誤，導致產生軟件問題。

(a) 在軟件開發文件中，沒有清楚列明剔除「相互衝突區域數據」(Conflict Zone Data) 的安排，導致其後並無進行特定測試和安全分析，因而未能發現該未知的軟件問題；

(b) 在軟件編程的執行過程中出現錯誤，導致 C 電腦系統在取代成為主電腦系統後，並沒有適當地重新產生「相互衝突區域數據」；及

(c) 由於軟件邏輯配置沒有阻止 C 電腦系統在沒有「相互衝突區域」防護功能的情況下， C 電腦系統仍繼續運作並切換為主電腦系統，引致失去相互衝突路綫的防護功能。

7.2 委員會亦總結在調查中找到的軟件編程的執行錯誤反映 ATDJV 在軟件程式開發過程中，就該次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。

7.3 因應第 7.2 段所述 ATDJV 的不足之處，委員會亦總結港鐵營運項目團隊日後應對 ATDJV 的項目交付方面，應提高警覺和增加額外的監察措施。

8. 建議

8.1 委員會根據是次事故的成因和從中汲取的經驗作出以下幾項建議。

8.2 為防止因為相同成因導致出現同類事故，委員會建議 ATDJV：

(a) 更換導致有關軟件問題的軟件設計及開發團隊；

(b) 糾正有關軟件修改問題，確保並提供具體證明軟件開發在品質上並無構成其他影響；

(c) 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日後任何可能發生的程式編寫錯誤；及

(d) 制定一系列全面的有效措施，包括但不限於 (i) 聘任外間「獨立軟件評估顧問」，以加強主、副和備用電腦系統的軟件開發過程；(ii) 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；及 (iii) 在委員會專家的協助下，就其軟件編程的執行方面，進行風險評估。

8.3 為協助 ATDJV 落實上述建議，委員會建議港鐵營運項目團隊提高警覺及加強監察，確保 ATDJV 落實有關措施，以重建公眾對新信號系統的信心：

(a) 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；

(b) 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；

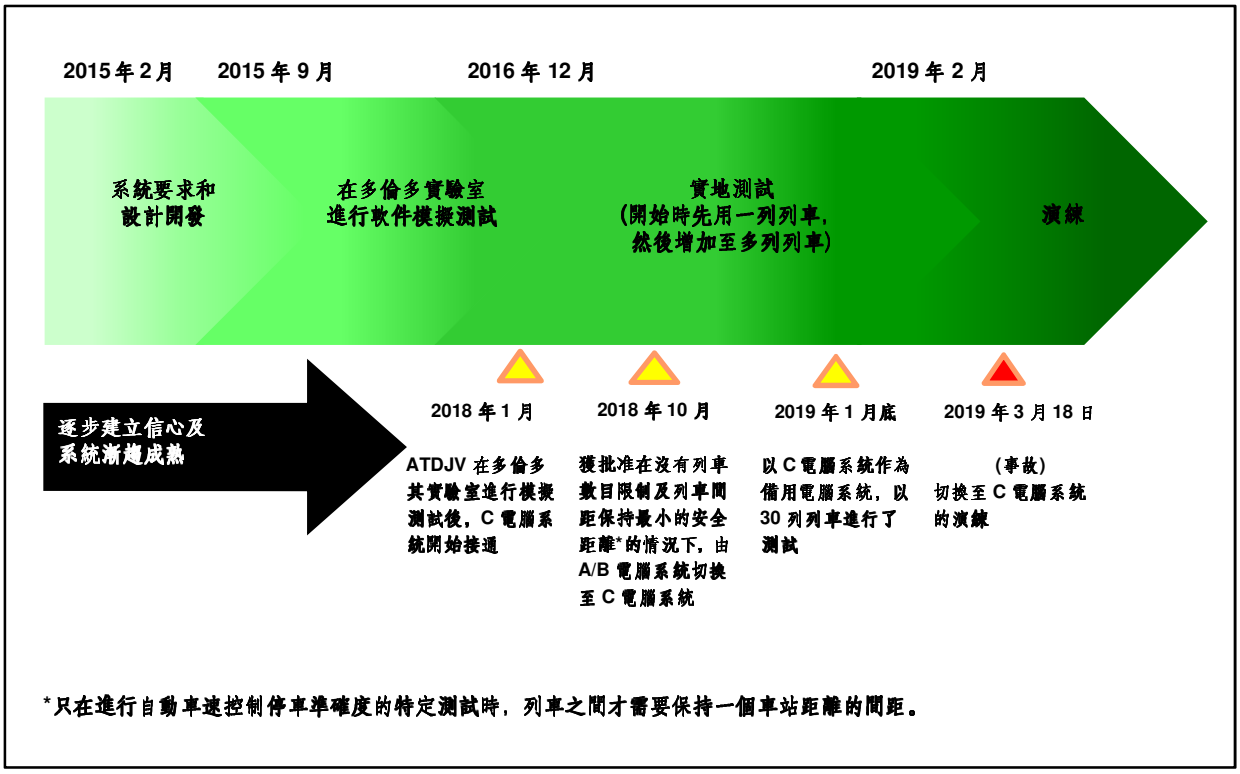
(c) 港鐵與ATDJV共同成立一個信號系統測試及驗收安全委員會，管理實地測試（並納入「獨立安全評估顧問」的意見）；及

(d) 與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，並探究將來其他由 ATDJV 所建議在技術上合適的方案。

8.4 在取得政府同意後，方會恢復在非行車時間內進行新信號系統的列車測試。

附件 1

模擬及測試的整體計劃



重要時序

1. 2016 年 12 月，ATDJV 開始在荃灣綫非行車時間內進行實地列車測試，測試規模由一列列車逐步增加至多列列車。

2. 2018 年 1 月， ATDJV 在其多倫多實驗室進行模擬測試後，C 電腦系統開始接通作為備用電腦系統。

3. 由 2018 年 10 月 15 日起，根據由 ATDJV 發出的安全文件，由 A/B 電腦系統切換至 C 電腦系統可在沒有列車數目限制及列車間距保持最

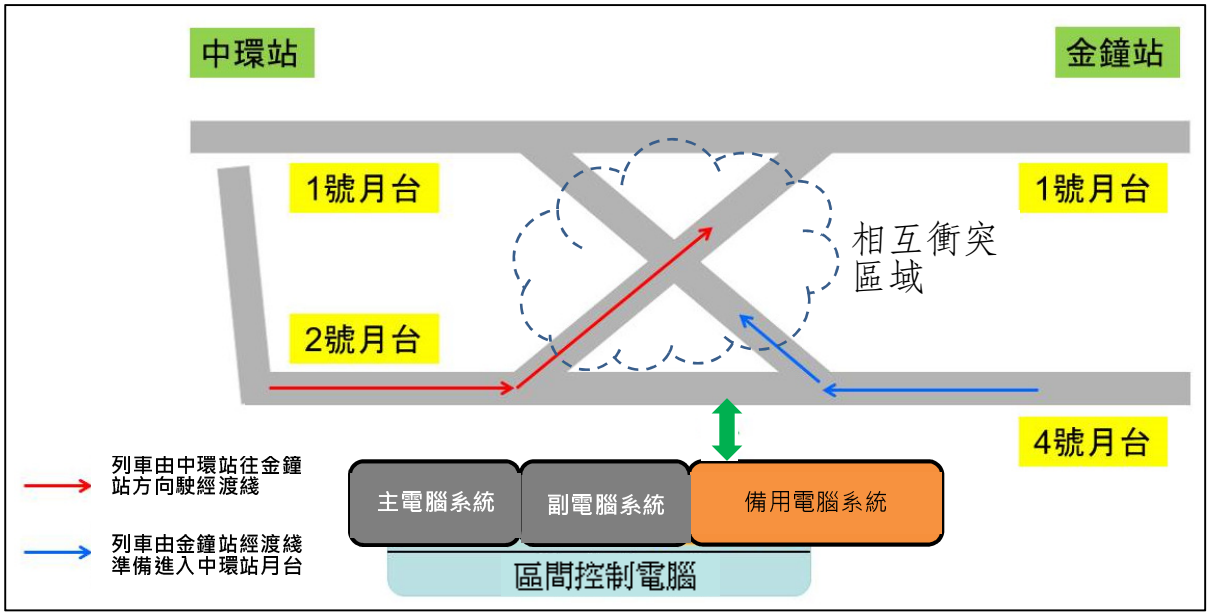
小的安全距離的情況下進行。只有在進行自動車速控制下的停車準確度的特定測試時，列車之間才需要保持一個車站距離的間距。

4. 2019 年 1 月，在沒有測試列車數目限制的情況下，使用了 30 列列車並以 C 電腦系統作為備用電腦系統進行了全綫測試。換言之，當 A 和 B 電腦系統同時失效時，C 電腦系統便會負責控制整體運作。

附件 2

2019 年 3 月 18 日
荃灣綫新信號系統演練事故

情境圖示

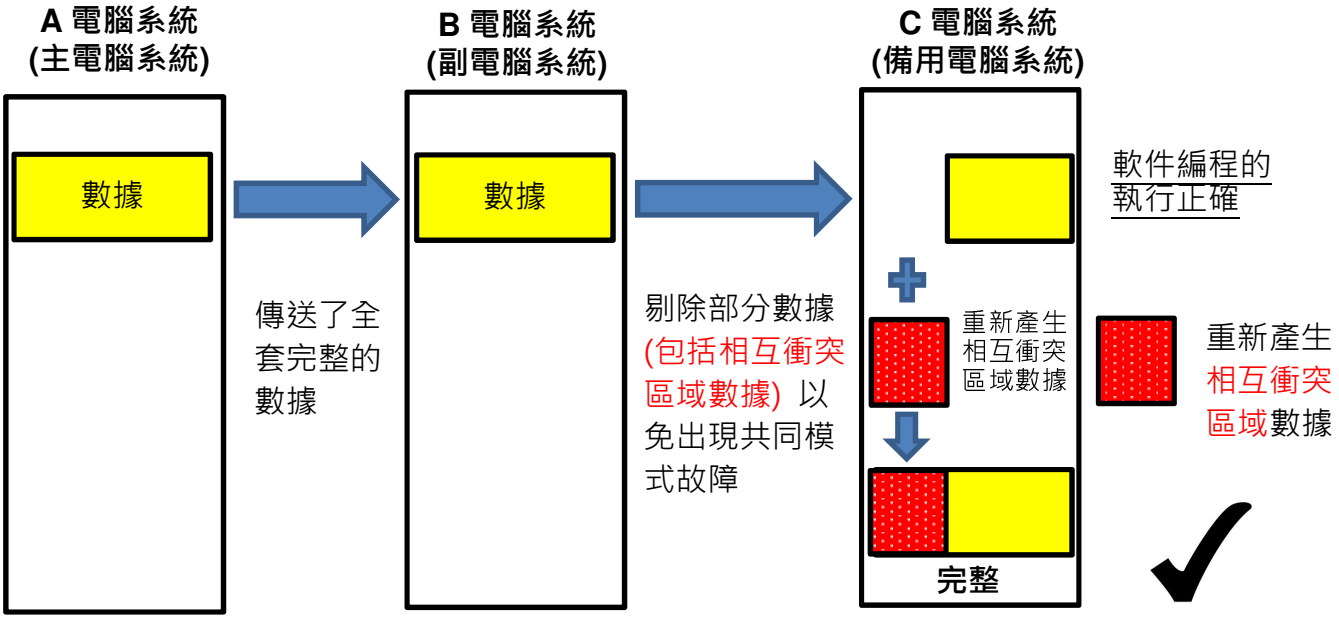


附件 3

A、B 及 C 三套電腦系統之間的數據傳送

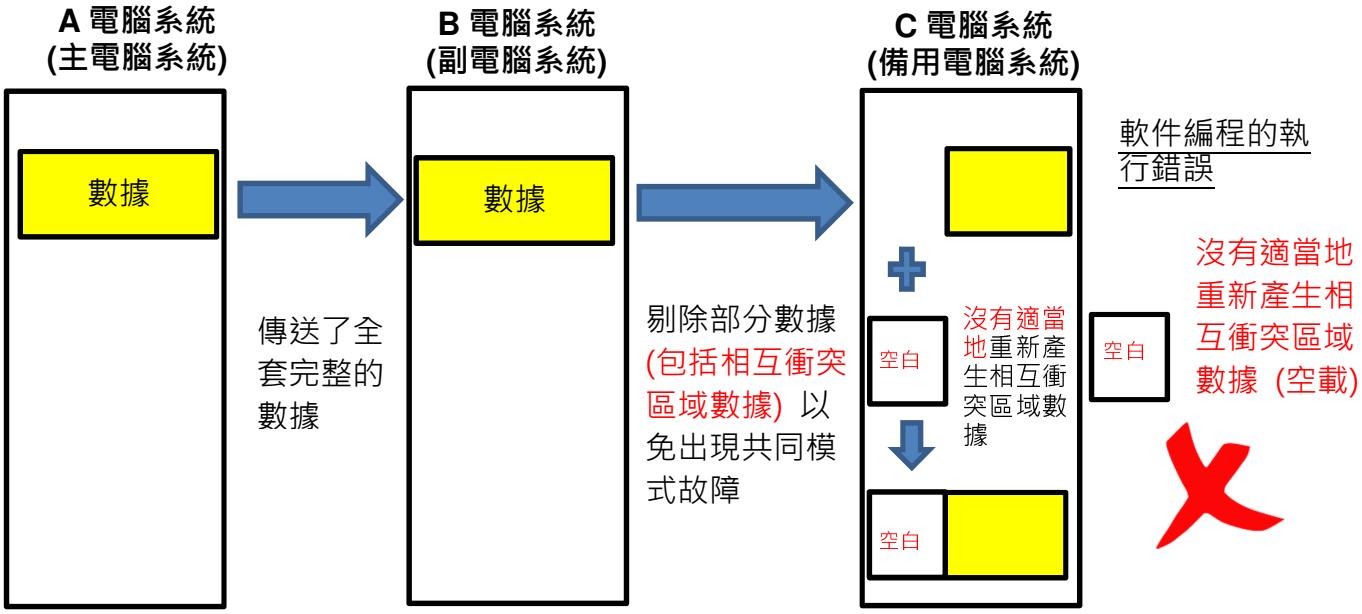
於 3 月 18 日，先關掉作為「主電腦系統」的 A 電腦系統，使 B 電腦系統切換為「主電腦系統」，隨後再關掉 B 電腦系統，使 C 電腦系統切換為「主電腦系統」。

ATDJV 制定的設計目的



過程實況:

軟件編程的執行錯誤導致出現未知的軟件問題



就今年三月十八日港鐵荃灣綫新信號系統測試事故，機電工程署（機電署）進行了獨立、深入和全面調查，並聘請海外鐵路安全專家協助。機電署已完成事故調查，並於今日（七月五日）公布調查結果。

根據調查結果，事故的原因是新信號系統在設計及開發階段，系統承辦商為軟件進行修改期間出現程式編寫錯誤，導致主區間電腦在切換至暖備用區間電腦後無法建立中環站的渡線軌道數據。因此，列車自動保護系統未能發有作用，無法防止兩列列車同時進入中環站的渡線軌道，導致列車相撞。

除了程式編寫錯誤外，機電署認為引入暖備用區間電腦屬承辦商的一項獨特和非標準設計，有別於其現有信號系統，但該非標準設計所帶來的潛在風險並未完全包括在承辦商的風險評估內，而承辦商亦未有在實地測試前，在可行範圍下為暖備用區間電腦作最大程度的模擬測試。因應此新信號系統的重要性及其獨特和非標準設計，機電署亦認為港鐵公司在系統測試過程中應加強警覺性及避免過度依賴承辦商。

機電署亦已仔細審視港鐵公司調查委員會於六月十七日提交的調查報告，信納港鐵公司調查委員會就事故成因的調查結果，即系統承辦商一連串的執行錯誤，令新信號系統軟件出現程式編寫錯誤。此結果與機電署獨立調查的結果吻合。

機電署知悉港鐵公司調查委員會向承辦商及港鐵公司提出的多項建議，認同建議針對修正編程錯誤問題及加強新信號系統的開發及測試過程，以避免同類事故再次發生。本署會密切監察港鐵公司落實改善措施及其成效，在港鐵公司完成改善措施，及本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。