立法會交通事務委員會
鐵路事宜小組委員會

2019年3月18日港鐵荃灣綫新信號系統測試事故
資料文件

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，兩輛列車於新信號系統進行演練期間，在中環站附近發生碰撞的事故。

2. 港鐵公司在事故發生後，迅即成立由本地及海外專家和港鐵公司資深人員組成的調查委員會，從不同方面進行深入調查。調查委員會已完成調查，並於2019年6月17日向機電工程署（機電署）提交調查報告。機電署亦已完成其獨立調查，並於7月5日向運輸及房屋局提交調查報告。

3. 本文件旨在交代港鐵公司成立的調查委員會以及機電工程署分別就事故進行的調查結果及跟進措施。

新信號系統更換工程

4. 港鐵公司在2015年以公開招標形式批出合約予Alstom-Thales DUAT JV（ATDJV）[1]公司，以更新七條港鐵綫（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。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[2]模式，而新的信號系統則採用「通訊為本列車控制」技術[3]，

---

[1] 新信號系統的承辦商是 Alstom Hong Kong Limited (Alstom) 和 Thales Transport & Security (Hong Kong) Limited (Thales)組成的聯營公司 Alstom-Thales DUAT JV，兩間公司總部位於法國，「通訊為本列車控制」技術由 Thales 加拿大技術部門提供。港鐵公司於 2015 年 1 月將有關合約批予這間系統供應商，合約總值 33 億元。

[2] 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。

[3] 新的信號系統利用現代無綫通信技術以列車所發出的信息，將列車位置及

以移動區間原理運作，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。

5. 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、副及備用電腦系統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系統[4]。為進一步提升信號系統的可用性及修復時間表現，港鐵公司於合約中要求多配置一套備用電腦系統[5]。主、副電腦系統以及備用電腦系統的硬件基本上相同並載入共同軟件，及透過硬件識別插頭，按其配置執行主、副及備用電腦系統的功能。

6. 根據合約條款下的設計要求，信號系統承辦商有明確及清晰責任，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。相關的系統開發及評估工作，均屬承辦商的責任。港鐵公司作為系統的使用者及鐵路服務提供者，亦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境，進行實地演練。

7. 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，確保新系統安全及可靠，才投入服務。為了在投入載客服務前進一步確保新信號系統的安全，港鐵公司亦委任了「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，並會在對有關程序評估滿意後，提供安全認可文件。「獨立安全評估顧問」按其工作範疇參與新信號系統更換工程項目，集中檢視新系統在正式啟用載客前的安全審批事宜，惟不包括對演練工作的評估。

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。

[4] 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。

[5] 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。

8. 新信號系統的測試一直以審慎及循序漸進的方式分階段進行。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系統的實地測試，直至2018年初則開始於非行車時間進行全綫測試。整項信號系統更換工程以及持續進行的測試工作，港鐵公司均按照業界標準的要求執行。

事故經過

9. 2019年3月18日，荃灣綫於非行車時間以新信號系統進行演練，讓營運團隊熟習新信號系統的運作，並模擬在主電腦系統及副電腦系統未能如常運作的場境下，系統自動轉至備用電腦系統所需的應變措施、復修程序，及備用電腦系統能否繼續暢順運作。

10. 在演練期間，大約凌晨約2時44分，一列由金鐘站經渡綫[6]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，向金鐘方向駛經渡綫的列車，引致該列車第二至第四卡損壞。請參閱附件一。

11. 受事故影響，3月18日至19日期間荃灣綫中環站及金鐘站的列車服務暫停，而荃灣站至金鐘站之間的服務，在繁忙時間維持3分半鐘一班。荃灣綫的服務在3月20日恢復正常。事故經過時序表見附件二。

12. 事故發生後，港鐵公司為審慎起見，已即時暫停所有新信號系統的行車測試，並就事故展開深入調查。

港鐵公司調查委員會調查結果

13. 根據港鐵公司給予承辦商有關信號系統設計的要求，新信號系統在主、副電腦系統之外，須設有備用電腦系統，以提升系統可用性及在發生事故時能迅速應變。

---

6 渡綫是連接兩條主鐵路軌之間的路軌。

14. 按合約要求，備用電腦系統的軟件程式設計需避免「共同模式故障」(common mode failure) 的問題。換言之，承辦商必須盡量避免主、副電腦系統內有機會導致故障的數據透過數據傳輸直接傳到備用電腦系統的可能性。因此承辦商按其系統設計理應只會將主、副電腦系統的部分數據傳送至備用電腦系統；而備用電腦系統在取代主及副電腦系統控制列車運行之前，亦理應「重新產生」(re-create) 該等沒有傳送的數據，包括防止兩列列車同時行駛相互衝突路綫的「列車相互衝突區域數據」(conflict zone data)。承辦商於2017年6月發現系統的程式未如上述原來設計般編寫，遂於2017年7月就電腦系統的軟件程式作出修改。

15. 鐵路系統一般難以完全避免路軌交叉行走，以便處理事故及調動不同鐵路綫之間的列車。在這些必須設置的交叉位置，在任何時候鐵路的信號系統理應只可以容納一列列車。信號系統內有關這些路軌交叉位置的資料，正是上文所指的「列車相互衝突區域數據」。

16. 有關主、副電腦系統及備用電腦系統的設計見附件三。

17. 調查委員會的詳細調查發現承辦商的軟件設計及開發團隊在上述2017年7月的修改過程中出現了以下三項軟件編程的執行錯誤(software implementation errors)，引致修改後的軟件出現程式問題(programming errors)，引致3月18日的列車碰撞事故。

(一) 承辦商沒有在其內部軟件開發的文件中，清楚列明應該剔除傳輸「列車相互衝突區域數據」的安排，引致承辦商在後續的相關模擬測試、風險評估及安全分析，均沒有針對性測試「列車相互衝突區域」保護是否仍然存在。

(二) 儘管第一項錯誤，承辦商在處理軟件改動時，仍安排剔除「列車相互衝突區域數據」從主、副電腦系統傳送至備用電腦系統。然而，軟件設計及開發人員在處理編碼時出現程式編寫錯誤，令備用電腦系統未能適當地重新產生「列車相互衝突區域數據」。有關程式編寫錯誤見附件四。

(三) 承辦商編寫的系統軟件邏輯，讓備用電腦系統在沒有「列車相互衝突區域數據」的情況下，仍啟動成為主控電腦，即備用電腦系統在沒有路軌交叉位置的資料的情況下控制列車運行，引致兩列列車能夠同時進入渡綫，引致踫撞。

18. 調查委員會認為上述三項軟件編程的執行錯誤反映承辦商就該次軟件修改上，對確保信號系統軟件品質保證的過程、風險評估及模擬測試方面均有所不足。

19. 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，委員會認為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營運鐵路綫發生。

機電署調查結果

20. 機電署就是次事故進行了獨立、深入和全面調查，並聘請海外鐵路安全專家、英國帝國學院教授Professor Roderick Smith及英國伯明翰大學教授 Professor Felix Schmid提供協助。機電署已於7月5日完成事故獨立調查，調查報告於當天提交運輸及房屋局，及上載至機電署網頁，供公眾查閱。調查期間機電署曾經：

(一) 審視超過250份文件紀錄，包括當日控制中心的行車通告、安全簡報紀錄、演練簡報紀錄、肇事列車行車紀錄、及肇事信號系統相關的列車自動監察系統紀錄和區間電腦警報紀錄；

(二) 進行超過65次會面，包括港鐵公司項目工程人員及事故發生時參與測試的車務控制中心人員、車站人員和列車車長，及ATDJV項目工程人員；

(三) 檢視涉及事故的區間電腦和車載列車控制器的軟件程式版本及軟件程式編碼，並用涉及事故的三部區間電腦進行模擬測試。

21. 機電署已仔細審視港鐵公司調查委員會於6月17日提交的調查報告，信納調查委員會就事故成因的調查結果，即承辦商的一連串的執行錯誤，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。機電署的調查亦發現以下引致事故的原因：

(一) 由於系統承辦商沒有就涉事系統軟件的具體設計要求作明確記錄，而其核實和驗證過程不足，使系統承辦商於2017年7月為電腦系統的軟件程式作出修改時出現編程錯誤，而系統承辦商在多次系統測試／軟件升級工作的核實和驗證過程中均未有發現有關錯誤；

(二) 引入備用電腦系統所帶來的潛在風險並未完全包括在系統承辦商的風險評估內；及

(三) 備用電腦系統屬承辦商的的一項獨特和非標準設計，有別於其現有信號系統，但承辦商未有在實地測試前，在可行範圍下為備用電腦系統作出最大程度的模擬測試（特別是有關主、副及備用電腦系統之間的轉換，及有關列車防撞及自動列車保護系統的功能）。

22. 此外，機電署認為港鐵公司的調查委員會報告主要集中於承辦商在軟件開發和系統實施過程中的不足，而沒有提及港鐵公司營運項目團隊在監督項目實施情況方面的角色。無論如何，機電署認為，因應此新信號系統的重要性及其獨特和非標準設計，港鐵公司在過程中亦應加強警覺性及避免過度依賴承辦商。

港鐵公司跟進工作

23. 港鐵公司的調查委員會在調查報告中，向承辦商及港鐵公司提出多項建議。承辦商已逐步執行有關的改善措施，包括：

(一) 事故發生後，承辦商已經撤換引致有關軟件問題的軟件設計及開發團隊。承辦商亦會糾正有關軟件修改問題，並提供相關證明，確保軟件開發在品質上並無構成進一步的影響及提供相關證明；

(二) 承辦商會加強其軟件程式的編程步驟及測試方法，包括增加外聘「獨立軟件評估顧問」，以強化軟件開發程序，以防止同類事件的發生；

(三) 承辦商會審視、重新檢查及證明其軟件開發方式恪守國際標準及安全防護原則，及在調查委員會專家的協助下，就其軟件編寫進行風險評估。

24. 調查委員會明白新信號系統承辦商是有責任確保信號系統安全，包括提供一個安全及可靠的信號系統軟件作測試。調查委員會同時亦建議港鐵公司應提高警覺並加強對承辦商的監督，確保承辦商會落實有關措施，以重建公眾信心。有見及此，港鐵公司將會採取以下措施：

(一) 將現時港鐵公司新信號系統更新工程委任的「獨立安全評估顧問」的工作範圍，由原來投入載客服務前確保系統安全，擴大至涵蓋列車實地測試相關的安全認證；

(二) 提升現時港鐵公司已在本港配置用作培訓之用的信號系統模擬平台的功能，在切實可行的情況下，為更多不同情境進行模擬測試[7]；

(三) 與承辦商共同成立一個測試及驗收安全委員會，並納入港鐵公司按上述(一)項委任的「獨立安全評估顧問」的意見，以管理實地測試。當中，港鐵公司將會與委員會專家

[7] 現時須在承辦商於海外設置的實驗室，方可進行模擬測試。

一同探究不同方案，包括分階段發展備用電腦系統的好處。

機電署跟進工作

25. 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(即上文第26-27段)，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。機電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。

總結

26. 政府及港鐵公司均十分重視今次的事故，港鐵公司會積極落實調查委員會提出的改善措施，而公司必定會在確保安全及獲得政府的同意後，才會重新啟動新信號系統的列車測試。

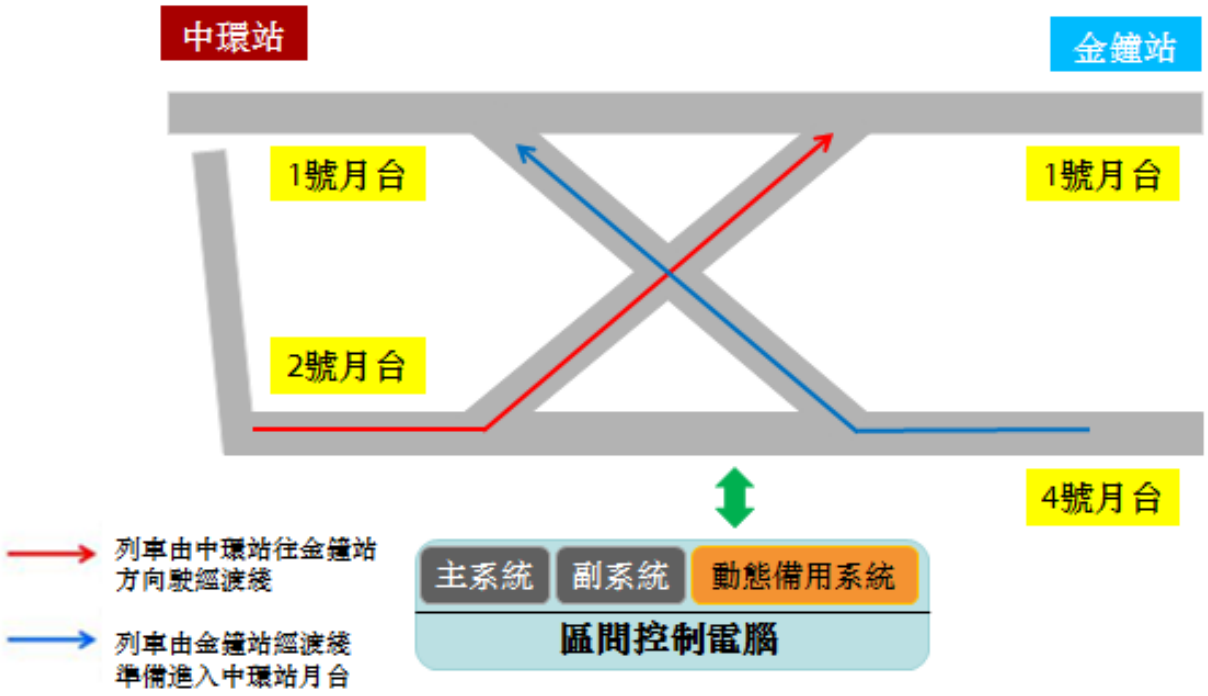
27. 請委員備悉上述文件，以及夾附於附件五港鐵公司調查委員會的調查報告，及附件六機電署的調查報告。

運輸及房屋局
機電工程署
港鐵公司
2019年7月

附件一

2019年3月18日港鐵荃灣綫新信號系統測試事故

事發經過示意圖

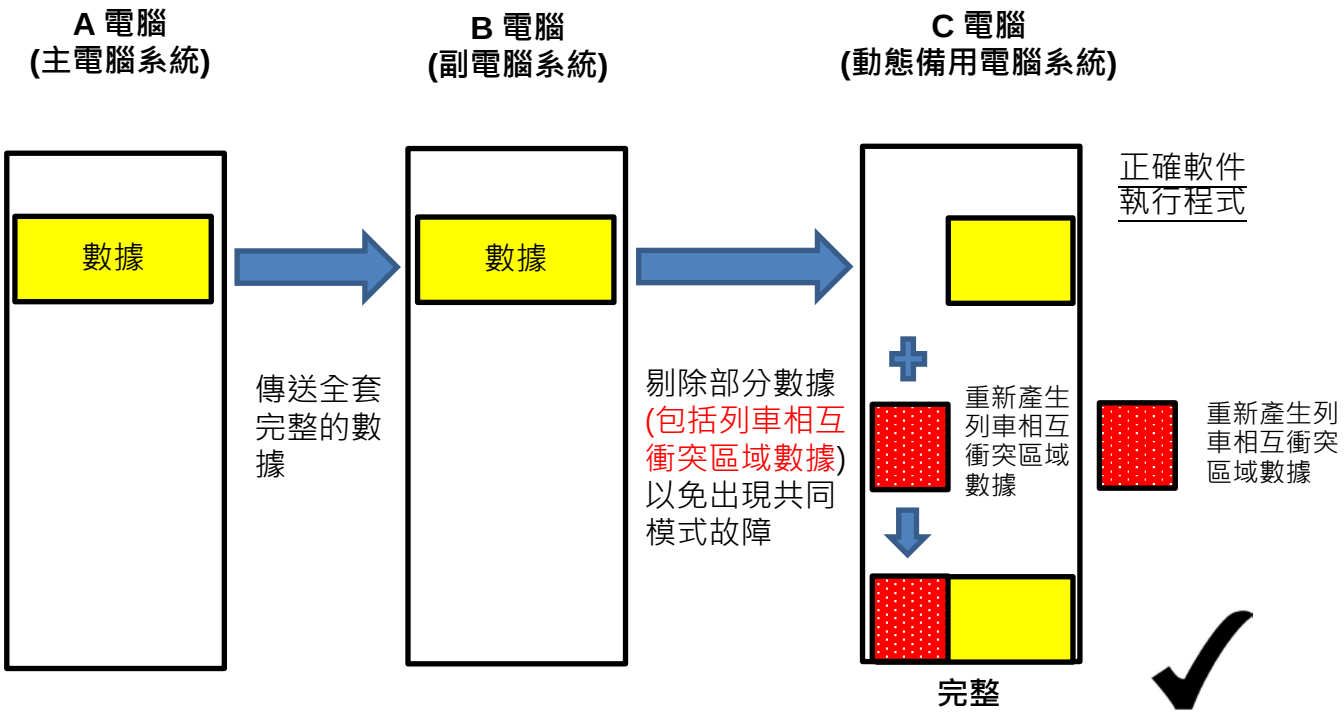


附件二

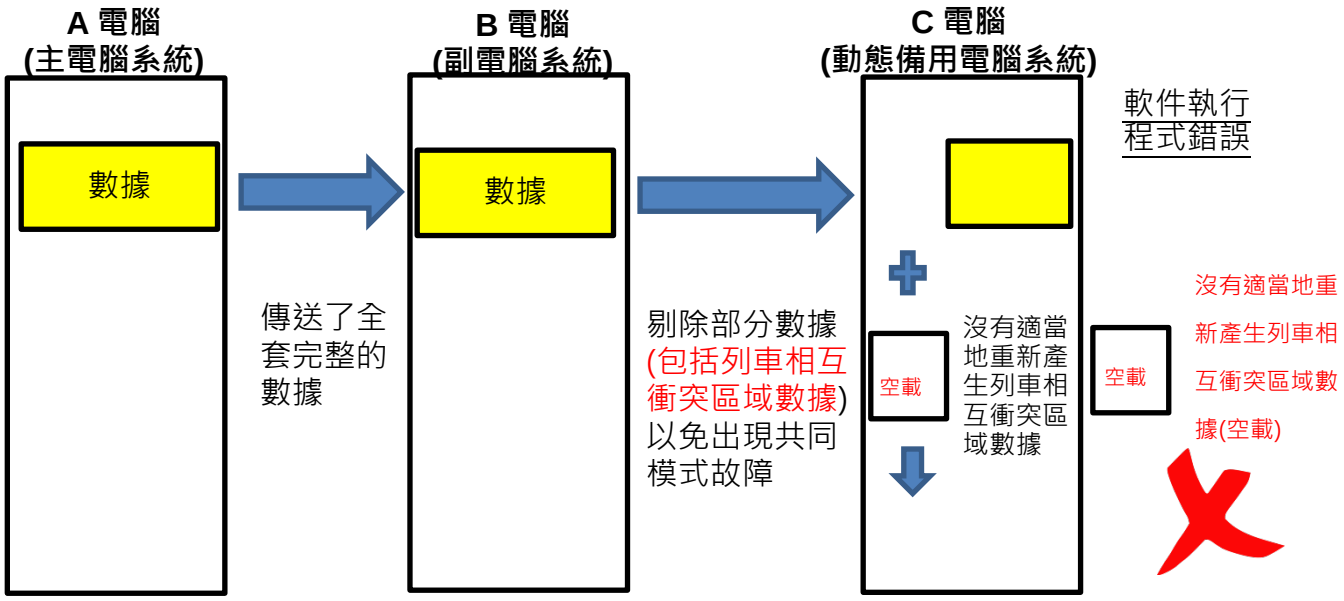
2019年3月18日港鐵荃灣綫新信號系統測試事故

發生時間	事項
3月18日	
凌晨2時44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03分	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。

附件三


A 電腦
(主電腦系統)
B 電腦
(副電腦系統)
C 電腦
(動態備用電腦系統)
數據
數據
傳送全套完整的數據
剔除部分數據(包括列車相互衝突區域數據)以免出現共同模式故障
重新產生列車相互衝突區域數據
正確軟件執行程式
重新產生列車相互衝突區域數據
完整

附件四


A 電腦
(主電腦系統)
數據
傳送了全套完整的數據
B 電腦
(副電腦系統)
數據
剔除部分數據(包括列車相互衝突區域數據)以免出現共同模式故障
C 電腦
(動態備用電腦系統)
空載
沒有適當地重新產生列車相互衝突區域數據
空載
軟件執行程式錯誤
沒有適當地重新產生列車相互衝突區域數據(空載)

機密

2019 年 3 月 18 日非行車時間
中環站（荃灣綫）列車碰撞事故
調查委員會報告

呈交人：

劉天成
車務總監

顏永文
技術工程總監

調查委員會聯合主席

日期： **2019 年 6 月 17 日**

目錄

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習。

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，提供安全審批文件。「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 1 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系統配置，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
何兆鎏教授

「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

何兆鎏教授

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) 由於軟件系統配置沒有阻止 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；

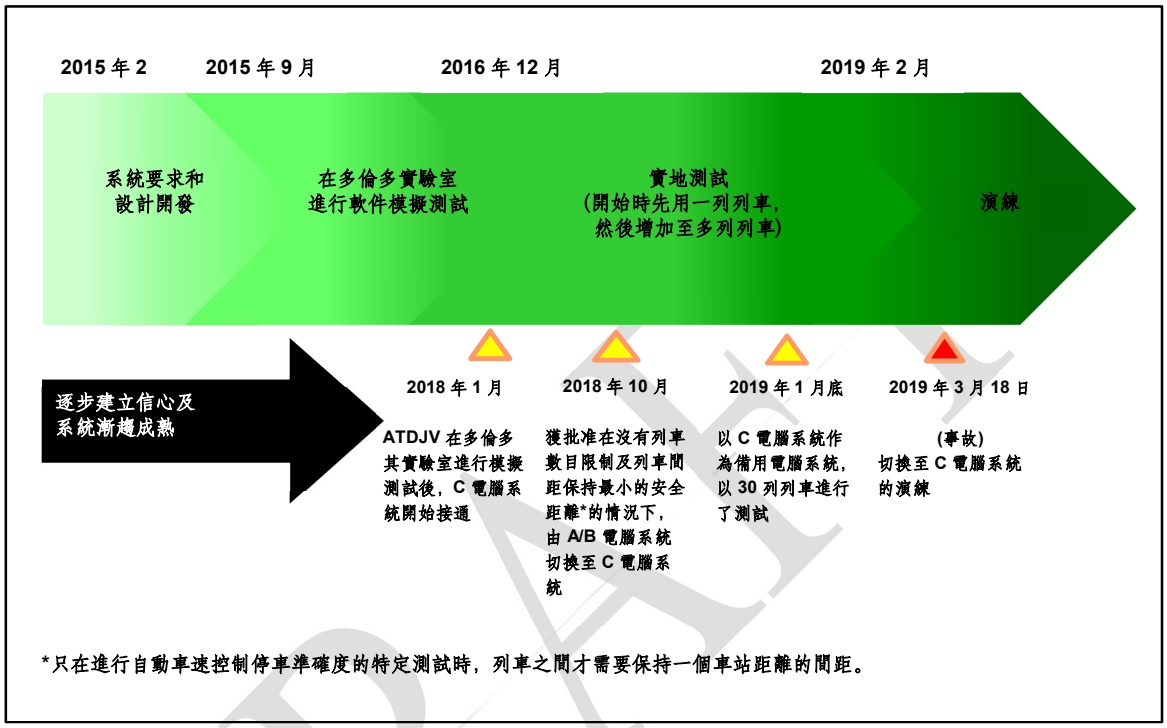
(c) 港鐵與 ATDJV 共同成立一個信號系統測試及驗收安全委員會，管理實地測試（並納入「獨立安全評估顧問」的意見）；及

(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

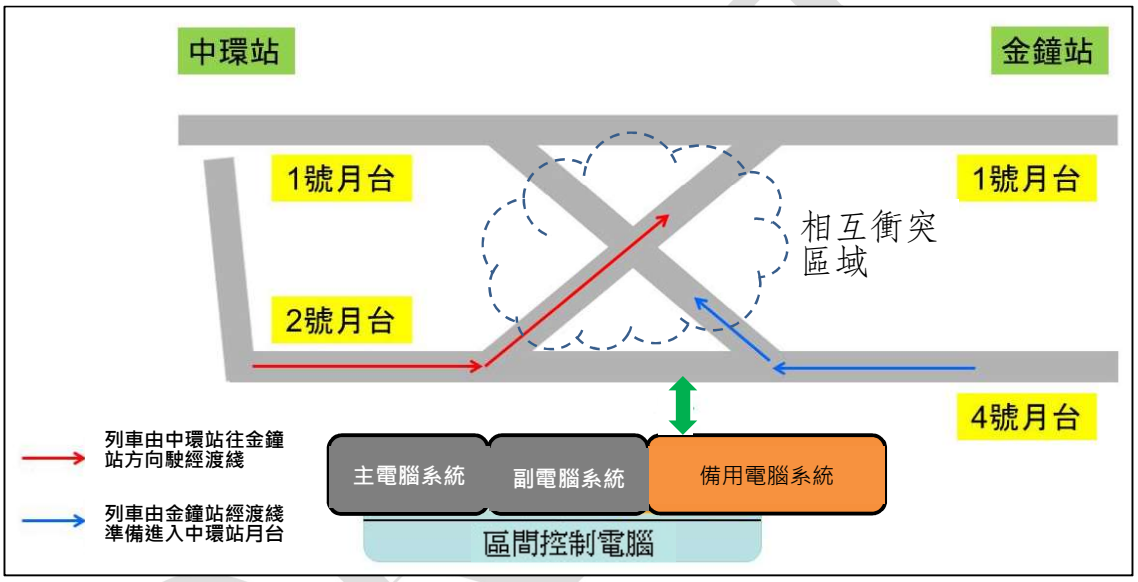
最小的安全距離的情況下進行。只有在進行自動車速控制下的停車準確度的特定測試時，列車之間才需要保持一個車站距離的間距。

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

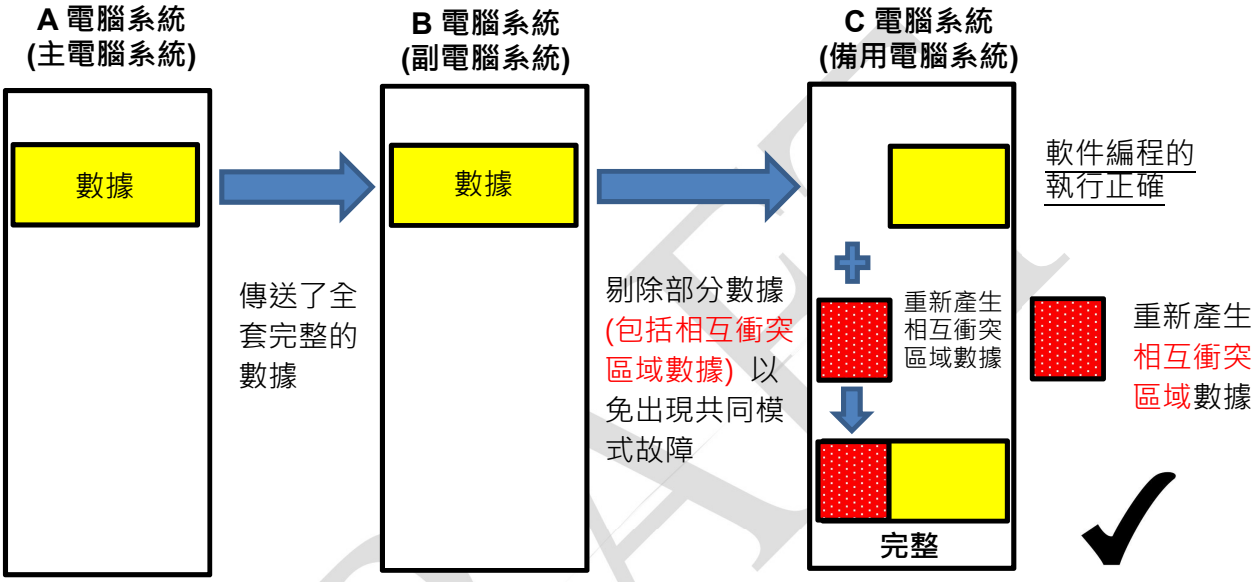


附件 3

A、B 及 C 三套電腦系統之間的數據傳送

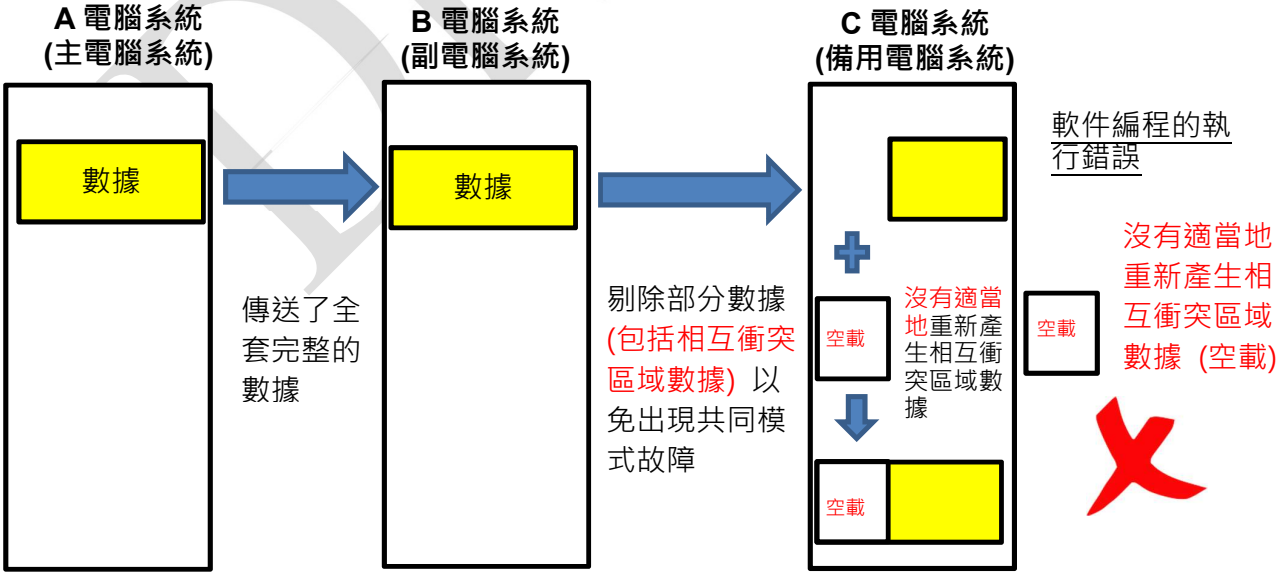
於 3 月 18 日，先關掉作為「主電腦系統」的 A 電腦系統，使 B 電腦系統切換為「主電腦系統」，隨後再關掉 B 電腦系統，使 C 電腦系統切換為「主電腦系統」。

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



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

Chinese Version

中文版

機電工程署 EMSD

Date of Issue: 5 July 2019

出版日期：**2019** 年 **7** 月 **5** 日

目錄

頁

摘要

2019 年 3 月 18 日，荃灣綫新信號系統進行演練期間，發生兩列列車碰撞事故。本報告載述機電工程署(機電署)對事故進行獨立調查後所得的結果。

信號系統承辦商 Alstom-Thales DUAT Joint Venture (ATDJV)是 Alstom Hong Kong Limited (Alstom)及 Thales Transport & Security (Hong Kong) Limited (Thales)組成的聯營公司，自 2016 年年底開始於非行車時間在荃灣綫的不同路段分階段進行新信號系統測試。ATDJV 於 2019 年 2 月完成全綫的測試，香港鐵路有限公司(港鐵公司)在 2019 年 2 月 16 日開始進行演練。

事故發生於 2019 年 3 月 18 日凌晨 2 時 44 分的非行車時間，當時港鐵公司正於荃灣綫以新信號系統進行演練。事發時，一列由金鐘站進入中環站 1 號月台的 T131 列車，與另一列正由中環站開往金鐘站的 T112 列車相撞，導致 T112 列車第二至第四卡車廂損毀，以及 T131 列車第一卡車廂的兩個轉向架偏離路軌。兩列列車的車長送院檢查，並於同日出院。

根據我們的調查結果，事故的原因是新信號系統在設計及開發階段，為軟件進行修改期間出現程式編寫錯誤。這個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重新產生中環站的渡線軌道數據。因此，列車自動保護系統未能發揮應有作用，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。

調查亦發現以下引致事故的原因：

(a) 由於涉事系統軟件的具體設計要求未有作明確紀錄，而其核實和驗證過程不足，使 2017 年 7 月就新信號系統進行軟件修改期間出現的程式編寫錯誤，在系統承辦商多次系統測試／軟件升級工作的核實和驗證過程中均未被發現；

(b) 引入暖備用區間電腦所帶來的潛在風險並未完全包括在系統承辦商的風險評估內；以及

(c) 暖備用區間電腦屬供應商的一項獨特和非標準設計，有別於其現有信號系統，但系統承辦商未有在實地測試前，在可行範圍下為暖備用區間電腦作出最大程度的模擬測試。

碰撞事故發生後，港鐵公司立即暫停對荃灣綫、港島綫和觀塘綫新信號系統的全部測試。此外，港鐵公司宣布，將會繼續暫停於非行車時間為新信號系統進行的所有行車測試工作，政府只會在機電署確定事故原因及糾正工作圓滿完成後，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。

機電署亦審視了港鐵公司調查委員會在 2019 年 6 月 17 日提交的調查報告，機電署的意見載列於 **附錄 III**。

2019 年 3 月 18 日港鐵荃灣綫新信號系統測試事故

調查報告

1. 目的

1.1 是次調查的目的，是找出 2019 年 3 月 18 日荃灣綫新信號系統測試期間發生列車碰撞事故的原因。本報告載述機電署對事故進行獨立調查後所得的結果。

2. 事故背景

2.1 信號系統承辦商 ATDJV 是 Alstom Hong Kong Limited (Alstom)及 Thales Transport & Security (Hong Kong) (Thales)組成的聯營公司，自 2016 年年底開始於非行車時間在荃灣綫的不同路段分階段進行新信號系統測試。ATDJV 於 2018 年年初展開全綫行車測試，並在 2019 年 2 月大致完成歷時超過兩年的實地測試。港鐵公司在新信號系統投入服務前，於 2019 年 2 月 16 日開始進行一連串演練(**附錄 I**)，在 2019 年 2 月 16 日至 3 月 18 日期間共進行九次模擬各不同特殊情境的演練，包括列車故障、轉轍器故障及主副區間電腦故障。

2.2 事故發生於 2019 年 3 月 18 日凌晨 2 時 44 分的非行車時間(**附錄 II**)，當時港鐵公司正於荃灣綫以新信號系統進行第九次演練，參與單位包括港鐵公司的項目人員、車務控制中心人員、車站人員、列車車長及 ATDJV 的工程人員。有關演練的情境為模擬負責控制中環站至深水埗站之間區域的主、副區間電腦發生故障。港鐵公司安排了 34 列列車模擬在繁忙時段主、副區間電腦發生故障，改由暖備用[1]區間電腦負責控制列車運作，藉以訓練港鐵公司人員的應變能力，以在該等情況下維持列車運作。

2.3 根據行車紀錄，事發時，一列由金鐘站進入中環站 1 號月台的 T131 列車，在中環站的渡線軌道(圖 1)以時速 19 公里撞向 T112 列車。當時，T112 列車正以時速 31 公里經該渡線軌道由中環站駛往金鐘站。兩車相撞導致 T112 列車的第二至第四

[1] 暖備用屬冗餘系統設計。當作為主控電腦的主區間電腦運作時，備用區間電腦維持於暖備用模式，並從主區間電腦讀取部分數據。因此，作為主控電腦的主區間電腦與備用區間電腦的數據並不同步。

卡車廂損毀(圖 2)，以及 T131 列車第一卡車廂的兩個轉向架偏離路軌。兩列列車的車長送院檢查，並於同日出院。

圖 1：列車相撞後的情況

圖 2：T112 列車車廂的損毀情況

2.4　根據行車紀錄及與列車車長會面的紀錄，T131 列車的車長曾在列車碰撞前按下緊急停車按鈕，試圖煞停列車，但 T131 列車未能被及時煞停，並與 T112 列車相撞。另外，根據行車紀錄，當時列車自動保護系統未能發揮作用，無法防止該兩列列車同時進入渡線軌道。圖 3 說明事發時列車的行駛情況。

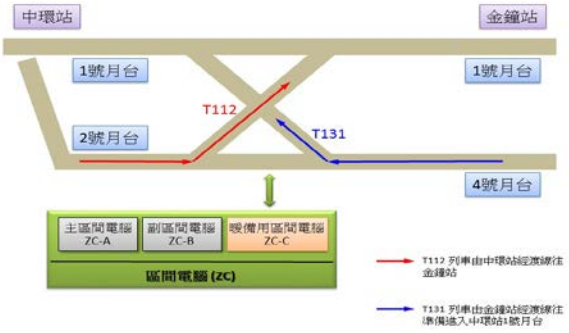


圖 3：事發時列車的行駛情況

2.5　機電署於當日凌晨 3 時 03 分獲通知有關事故，並立即派員到現場調查。

2.6　在 2019 年 3 月 18 日演練進行期間，現有的信號系統被隔離，所有軌旁設備及車載信號設備均由新信號系統控制。有別於現有的信號系統及港鐵公司其他鐵路綫的信號系統，新信號系統配備獨有的暖備用模式的備用區間電腦。因此，是次事故與現有的信號系統無關，現有鐵路綫應不會發生同類事故。

3.　涉事信號系統的技術資料

3.1　在 2015 年，港鐵公司向由 Alstom Hong Kong Limited (Alstom)及 Thales Transport & Security (Hong Kong) (Thales)兩間信號系統承辦商組成的聯營公司(即 ATDJV)批出合約，以更新七條鐵路綫(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。有關工程預期在 2026 年完成。

3.2　信號系統控制鐵路網絡內列車服務的安全運作。鐵路綫劃分成區間，每個區間在任何時間只允許一列列車通過，以確保列車之間保持安全距離。現時，上述七條現有鐵路綫的信號系統採用固定區間設計 [2]，而新信號系統則採用「通訊為本列

[2] 根據固定區間概念，如列車處於某固定區間，信號系統會向下一列列車發出指令，要求該列車不得駛進該區間。

車控制」(Communications Based Train Control)技術[3]，以移動區間的原理運作，確保在加密列車班次和增加各綫載客量的情況下，列車之間仍能保持安全距離。

3.3 在 2019 年 3 月 18 日，港鐵公司為荃灣綫新信號系統進行演練。列車透過無綫通訊，將其位置及車速等資料傳送至主區間電腦，後者計算列車之間的安全距離，以及向列車發送行車許可界限，以實現更高效的行車管理。

3.4 為進一步提升信號系統的可用性，荃灣綫的新信號系統採用三個區間電腦的結構進行列車控制，即主區間電腦(ZC-A)、副區間電腦(ZC-B)和備用區間電腦(ZC-C)。這是供應商的一項獨特和非標準設計，有別於其現有信號系統。這些區間電腦的功能如下(圖 4)：

(a) 主區間電腦 ZC-A 為指定軌道路段信號系統的主控電腦，負責列車控制；

(b) 副區間電腦 ZC-B 處於熱備用狀態，與 ZC-A 時刻保持同步，當 ZC-A 發生故障時，ZC-B 會取代 ZC-A 作為主控電腦，負責列車控制；

(c) 備用區間電腦 ZC-C 處於暖備用狀態，當 ZC-A 和 ZC-B 同時發生故障時，ZC-C 會取代 ZC-A 和 ZC-B 作為主控電腦。為免出現共同模式故障[4]，ZC-C 的部分數據與 ZC-A 和 ZC-B 的數據並不同步。這些數據會在 ZC-C 擔當主控電腦後，在 ZC-C 重新產生。

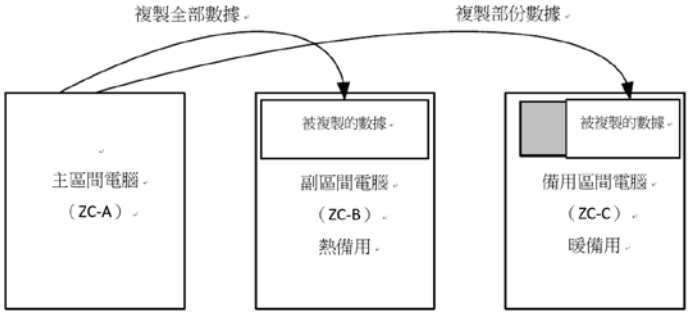


圖 4：三個區間電腦的設計功能

[3] 新信號系統利用無綫通訊技術，把列車發出的信號(例如列車位置及車速)傳送至控制電腦，然後由電腦運算出列車之間所需的安全距離。

[4] 共同模式故障是指當暖備用區間電腦取代主區間電腦及副區間電腦作為主電腦時，仍然出現與主區間電腦及副區間電腦相同的故障。

在新信號系統加設 ZC-C 作為暖備用配置屬嶄新設計，其切換模式相對傳統信號系統只採用兩個區間電腦作為主控及熱備用配置的設計較為複雜。

3.5 在任何情況下，信號系統中只有一個區間電腦為主控電腦，負責列車控制。主控電腦會時刻接收行駛列車及軌道的資料，包括列車的位置、車速、行駛方向，以及列車於某路段、道岔及渡線位置的車速限制。主控電腦不僅計算和維持列車之間的安全距離，亦會防止多於一列列車同時進入道岔或渡線，以確保鐵路運作安全。

3.6 在正常情況下，主控電腦為 ZC-A 或 ZC-B。主控電腦定期每 100 毫秒向暖備用區間電腦 ZC-C 傳送動態數據，但為了盡量減低出現共同模式故障，根據摘錄自供應商所提交的事故調查報告的資料，下列六個路綫相關動態數據項目不會由主控電腦(即 ZC-A 或 ZC-B)複製至暖備用區間電腦(ZC-C) (圖 5)：

- 相互衝突區域
- 回調
- 過綫
- 區間邊界保留
- 轉轍器控制
- 信號控制

3.7 當 ZC-A 及 ZC-B 均出現故障，暖備用區間電腦 ZC-C 會擔當主控電腦。在處理相互衝突區域的路綫相關數據時，暖備用區間電腦 ZC-C 應先初始化其內部數據空間，然後利用軟件的子程式把相應的軌旁及信號設備收集所得的動態數據與儲存在 ZC-C 數據庫的相應靜態數據合併，供 ZC-C 執行信號功能。這些動態數據包括：

- 相互衝突區域物體數量
- 相互衝突區域是否與非通訊物體重疊
- 相互衝突區域在上一個周期是否與非通訊物體重疊
- 相互衝突區域使用者數量
- 使用者列車識別碼
- 使用者路綫識別碼

從軌旁及信號設備收集上述的相互衝突區域動態數據後，有關數據會與 ZC-C 的下列兩項相互衝突區域靜態數據合併：

- 相互衝突區域識別碼
- 相互衝突區域設定的路徑數量

ZC-C 會以上述動態數據及靜態數據為基礎，重新產生完整而正確的列車相互衝突區域數據資料，由此 ZC-C 方可執行信號功能，包括列車自動保護系統以防止列車在相互衝突區域發生碰撞。

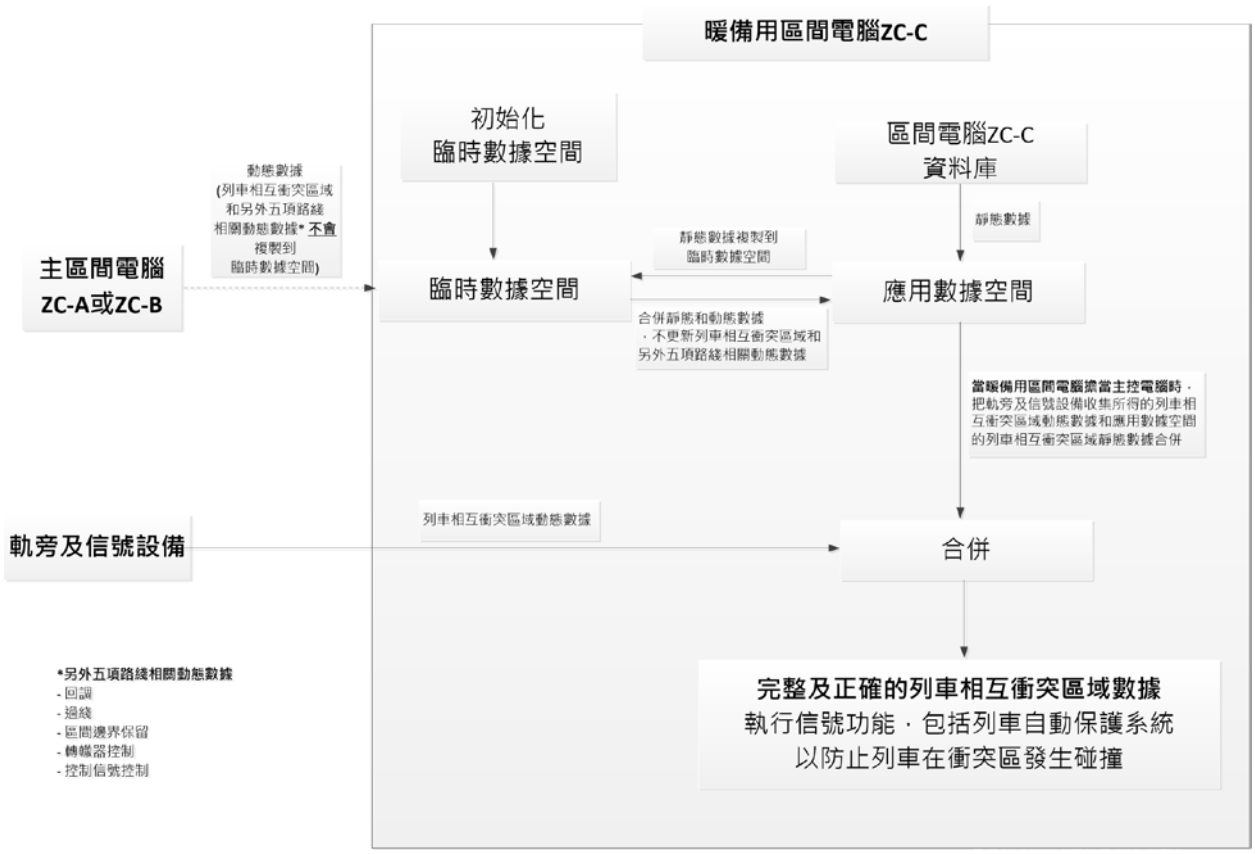


圖 5：主副區間電腦、備用區間電腦及軌旁設備的列車相互衝突區域數據整合方法

3.8 然而，在碰撞事故中，上述負責列車相互衝突區域數據整合的軟件子程式因程式編寫錯誤而無法於暖備用區間電腦 ZC-C 擔當主控電腦時執行，因此 ZC-C 的列車相互衝突區域數據未能正確重新產生。這個錯誤容許兩列列車同時進入涉事的相互衝突區域並發生碰撞。

4. 調查方式

4.1 機電署就是次事故進行了獨立、深入和全面的調查，並委聘三個獨立單位提供專家意見，即專長為事故調查、安全管理及系統和程序風險評估的鐵路安全顧問公司 TPD System Asia Limited (TPDSA) 的海外專家、帝國學院教授兼鐵路安全專家 Roderick Smith 教授及伯明翰大學教授兼鐵路信號系統專家 Felix Schmid 教授。機電署進行調查期間，曾經：

(a) 舉行超過 65 次會議，檢視逾 250 份文件和紀錄，當中涵蓋 16 類不同文件，包括工程項目合約文件、設計文件、調試計劃、調試報告、測試證書、演練程序、安全證書、軟件程式編碼、會議紀錄、港鐵公司委聘的獨立安全評估顧問及獨立審核機構的建議、行車通告、安全簡報紀錄、演練簡報紀錄、行車紀錄及調查報告；

(b) 檢視事發當日車務控制中心的行車通告、安全簡報紀錄、演練簡報紀錄、涉事列車的行車紀錄、涉事列車的車載信號紀錄，以及涉事區間電腦的警報紀錄；

(c) 檢視事發前後月台及大堂範圍的閉路電視片段；

(d) 檢視涉事區間電腦和車載信號設備的軟件程式版本，並以涉事的三個區間電腦進行模擬測試；

(e) 檢視相應的軟件程式編碼；

(f) 檢視港鐵公司和 ATDJV 的調查報告；

(g) 會見港鐵公司的 106 名人員，包括 53 名項目人員、 4 名車務控制中心人員、11 名車站人員及 38 名列車車長；

(h) 會見 ATDJV 的 27 名項目人員；

(i) 會見獨立安全評估顧問(Arthur D Little Limited)的 2 名代表；以及

(j) 會見獨立審核機構(Kusieog Limited)的 2 名代表。

5. 機電署的調查結果

5.1 事故成因

根據機電署的調查，新信號系統的表現與第 3.7 段所描述的預期運作情況有所不同。事發當日，港鐵公司進行實地演練，模擬控制中環至深水埗各站的主、副區間電腦在繁忙時間發生故障，藉以訓練港鐵公司人員處理有關故障。演練情境是主區間電腦 ZC-A 及處於熱備用模式的副區間電腦 ZC-B 同時發生故障，而信號系統需要切換至處於暖備用模式的備用區間電腦 ZC-C 以維持列車運作。

調查發現，當 ZC-C 被切換為信號系統的主控電腦時，負責處理列車相互衝突區域數據的電腦程式沒有執行相關的子程式，以合併動態數據和靜態數據，因而沒有重新產生正確的相互衝突區域資料(圖 6)。由於沒有正確的相互衝突區域資料，中環站渡線軌道的相互衝突區域並不存在於 ZC-C。最終，列車自動保護系統未能發揮應有作用，無法防止兩列列車同時進入該渡線軌道，導致列車在渡線軌道發生碰撞。

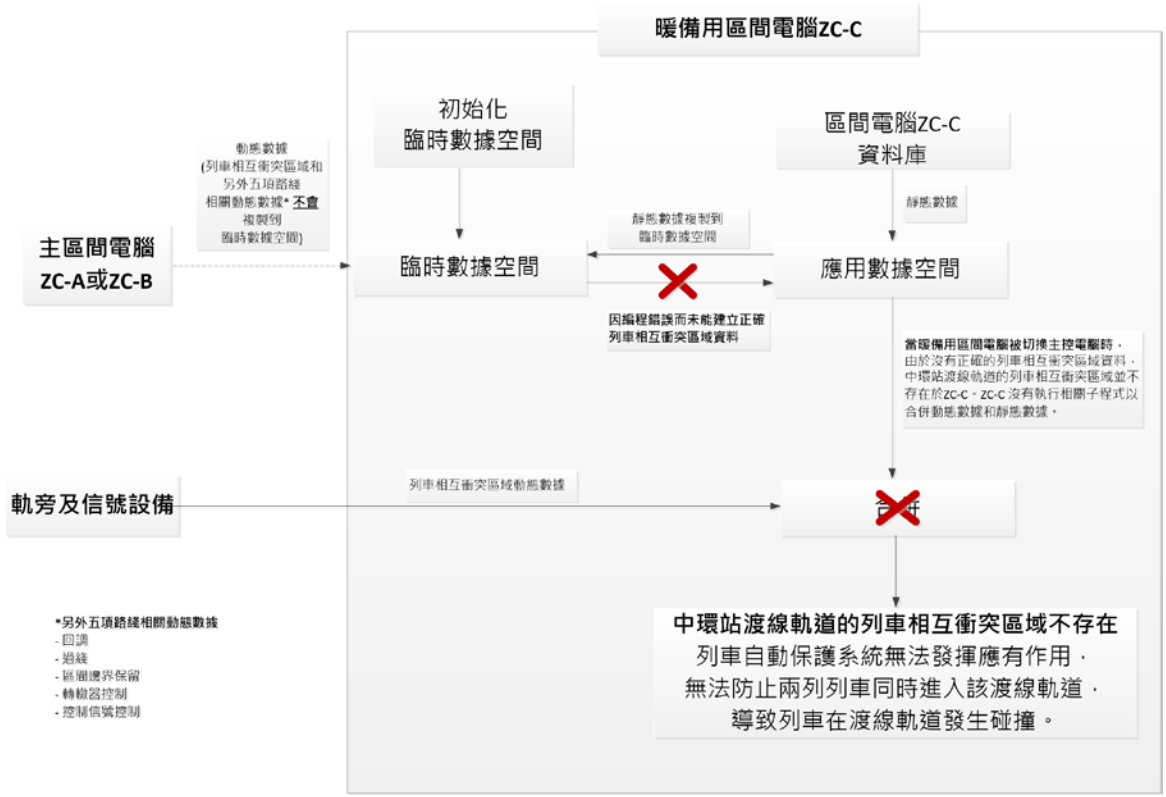


圖 6：暖備用區間電腦沒有執行相關子程式以合併動態數據和靜態數據

5.1.1 測試項目

事故發生後，機電署及其委聘的鐵路顧問在九龍灣車廠、何文田站[5]、ATDJV 香港辦公室及 ATDJV 位於加拿大多倫多的軟件開發中心進行了多項測試。有關測試如下：

(a) 為涉事列車進行制動系統測試

在九龍灣車廠為涉事 T131 列車進行了一系列制動系統測試，旨在測試制動系統的運作情況，以確定事故是否與列車的制動系統有關。測試結果顯示，制動系統運作正常，因此與事故無關。

(b) 為信號系統進行電腦模擬測試

使用與事故中的列車相同版本的軟件，並以相同地點及情況，在何文田站、ATDJV 香港辦公室及 ATDJV 位於多倫多的軟件開發中心進行電腦模擬測試(圖 7 及圖 8)，以確保情境完全相同。模擬測試結果顯示，在模擬器中使用相同版本的軟件同樣會發生相同的碰撞情況。

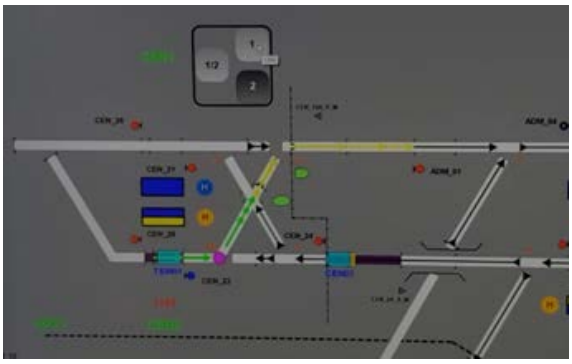


圖 7：ATDJV 香港辦公室模擬器顯示 T112 及 T131 列車同時進入中環站相互衝突區域的路徑設定

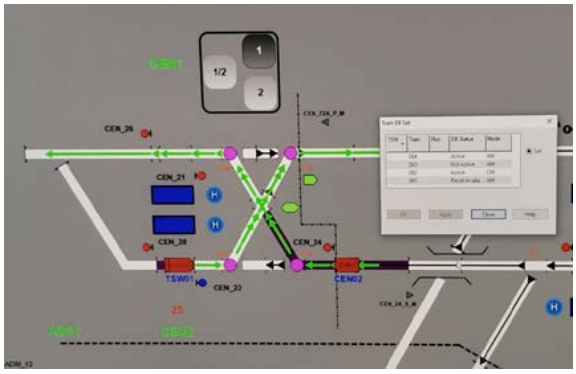


圖 8：ATDJV 香港辦公室模擬器顯示容許兩列列車同時進入中環站的相互衝突區域

[5] 何文田站配置了為新信號系統培訓之用的模擬平台。

(c) 為涉事區間電腦及車載控制器進行模擬測試

使用涉事列車的區間電腦及車載控制器，並以相同地點及情況，在何文田站進行模擬測試(圖 9 及圖 10)，以確定事故是否由涉事的區間電腦及車載控制器造成。模擬測試結果顯示，在模擬器中使用涉事的區間電腦及車載控制器同樣會發生相同事故。

圖 9：何文田站的新信號系統模擬平台

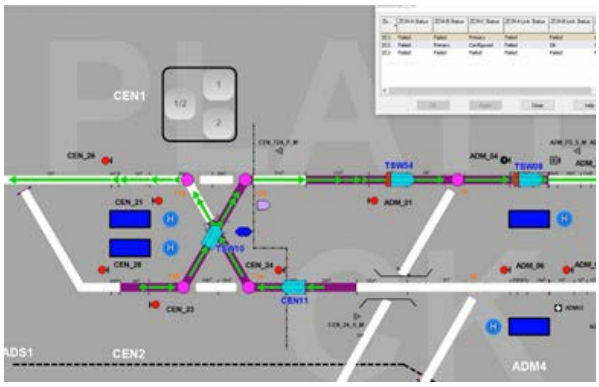


圖 10：模擬結果顯示涉事列車的區間電腦及車載控制器的模擬器容許兩列列車同時進入中環站的相互衝突區域

5.2 信號系統的開發、核實及測試與演練

5.2.1 區間電腦的程式編寫錯誤

調查顯示，在 2017 年 7 月軟件編碼經修改後，區間電腦的信號系統軟件出現程式編寫錯誤。這個程式編寫錯誤使 ZC-C 被切換為主控電腦後，負責處理列車相互衝突區域數據的電腦程式沒有執行相關的子程式，以合併動態數據和靜態數據，因而中環站的列車相互衝突區域數據未能在 ZC-C 正確重新產生。

列車自動保護系統未能發揮應有作用，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。

5.2.2 軟件程式的開發流程

國際標準 BS EN 50128 (鐵路應用—通訊、信號及處理系統—鐵路控制及保護系統軟體)訂明，在軟件的開發流程中，軟件的規格、功能要求及程式編寫邏輯應妥為記錄，讓軟件開發商得以在其後的核實及驗證過程中制訂相關測試和檢視。調查顯示，軟件設計並無妥善記錄 2017 年 7 月就列車相互衝突區域數據為備用區間電腦 ZC-C 進行的軟件編碼，因此在其後的核實及驗證過程中未能察覺相關的軟件編碼錯誤。

這反映軟件設計及相應的變更要求均未有訂明應如何妥善處理在 ZC-C 重新產生列車相互衝突區域數據。有關設計及變更控制文件僅訂明與現有的行車路綫請求、路綫授權及行車許可界限有關的數據不會複製至 ZC-C，並無提及列車相互衝突區域數據亦不會複製至 ZC-C。如軟件開發商對軟件的全部規格、功能要求、程式編寫邏輯及所作出的改動予以妥善記錄，則或可能在其後的核實及驗證過程中發現和修正編碼錯誤。

5.2.3 信號系統的風險評估

一般信號系統通常採用兩個區間電腦(即主區間電腦 ZC-A 及副區間電腦 ZC-B)，用以在主控及熱備用模式之間進行切換。荃灣綫新信號系統加設處於暖備用模式的備用區間電腦，屬供應商的一項獨特和非標準設計，有別於其現有信號系統。調查發現，在信號系統的開發過程中，沒有針對 ZC-C 的獨特設計進行全面的風險評估。就 ZC-C 合併相互衝突區域的動態和靜態數據的設計而言，如曾適當地進行以下全部活動，包括詳細的風險評估、識別安全要求、核實設計文件中的安全文件、實施設計安全要求、檢視設計、實施編碼要求、檢視編碼，以及相應的全面模擬測試或實地測試，則或能可發現軟件的編碼錯誤。

5.2.4 核實及驗證過程

因應港鐵公司委聘的獨立安全評估顧問所提出的疑問及意見，在 2018 年 10 月至 2019 年 2 月進行了額外的軟件核實及驗證檢查工作。大部分額外的核實及驗證檢查工作已於 2019 年 3 月 1 日完成，惟未能發現軟件編碼錯誤。原訂於 2019 年 2 月進行的獨立軟件審核工作未能如期完成。如有關審核工作能按

計劃於 2019 年 2 月完成，則或可能發現軟件的編碼錯誤。然而，機電署委聘的顧問認為，該程式編寫錯誤或仍未能於上述獨立軟件審核工作中被發現。

5.2.5 信號系統測試

國際標準 IEEE 1474.4 (通訊為本列車控制系統功能測試的建議做法)訂明，應在出廠前驗收測試階段進行最大程度的模擬測試。另外，實地功能測試亦應包括整個信號系統(即包括 ZC-C)的功能，以證明有關系統能滿足通訊為本列車控制的功能要求。根據紀錄，在出廠前功能測試階段及實地功能測試階段，均沒有就事故情境(即 ZC-A 和 ZC-B 同時出現故障，而須把 ZC-C 切換為主控電腦)進行全面的衝突路綫模擬測試。如曾以最大程度進行全面的模擬測試及實地功能測試，則或可能發現程式編寫錯誤及 ZC-C 未能重新產生列車相互衝突區域數據的問題。

5.2.6 信號系統模擬測試

荃灣綫信號系統加設處於暖備用模式的備用區間電腦，屬供應商的一項獨特和非標準設計，有別於其現有信號系統，合約文件的特殊規格部分已訂明有關具體要求。系統設計訂定的設計要求，僅訂明行車路綫請求、路綫授權或行車許可界限不會複製至 ZC-C。如設計文件涵蓋 ZC-C 擔當主控電腦後處理列車相互衝突區域數據的詳細資料，並在實地測試前曾為此非標準設計進行更全面的模擬測試，則或能可及早發現和修正在涉事渡線軌道列車相互衝突區域數據出錯的問題，而 2019 年 3 月 18 日的事故可能不會發生。

5.2.7 安排實地演練

港鐵公司在新信號系統投入服務前，委聘了獨立安全評估顧問核證該系統的安全性。基於新信號系統原定按早前的計劃於 2019 年年中投入服務，獨立安全評估顧問於 2018 年 10 月 19 日向港鐵公司匯報，信號系統的安全保證系統的缺陷或會導致不安全事故發生，需要作出改善。顧問於 2019 年 2 月 6 日提出以下意見，並於 2019 年 3 月 5 日重申有關事項：

(a) 顧問不相信信號系統完全符合認可的國際標準；

(b) 顧問十分關注系統是否符合系統供應商的軟件開發程序；以及

(c) 顧問不相信供應商所採用的開發流程與信號系統的複雜程度相符。系統的核心軟件(Convergence 3.2)在獲發安全認證後，仍發現許多潛在的安全異常情況，顯示基礎流程存在弱點，因此而導致不安全事故的可能性高得令人無法接受。

因應獨立安全評估顧問的意見，有關各方於 2019 年 2 月 19 日至 25 日進行多次三方研討會，以討論顧問的關注事項及系統的開發進度。港鐵公司於會後把新信號系統計劃投入服務的日期延期六個月至 2019 年第四季，讓 ATDJV 有時間回應顧問的關注事項及改善新信號系統。ATDJV 表示，新版信號系統 Build 8.3.4 將於 2019 年 5 月 24 日發布，而事故中所使用的軟件版本為 Build 8.3.3。根據紀錄，參與演練的 ATDJV 及港鐵公司均知悉新版軟件定於 2019 年 5 月發布及當中變更的內容。雖然引致事故的上述程式編寫錯誤僅在事故後才被發現，而該程式編寫錯誤亦未有包括在 ATDJV 於 Build 8.3.4 軟件中計劃更新的項目，但我們認為 ATDJV 仍有些微機會於新版本或由其獨立軟件團隊進行軟件評估或審核期間發現該程式編寫錯誤。我們委聘的鐵路專家則認為，當時並無清晰意見引使港鐵公司在等待新軟件發布期間暫停演練，亦沒有證據顯示在任何情況下該程式編寫錯誤會被發現和於新版軟件中予以修正。

5.2.8 實地演練程序

演練由 2019 年 2 月 16 日開始進行，事故在第九次演練期間發生，當時動用了 34 列列車進行實地演練，但並無參照任何相關的演練程序。

6. 機電署委聘的鐵路專家的調查結果

6.1 鐵路顧問公司(TPDSA)的調查結果

6.1.1 在委聘鐵路顧問公司 TPDSA 之前，機電署已確定碰撞的直接原因是用以控制列車行駛的備用區間電腦(ZC-C)編碼出現軟件錯誤。TPDSA 認同這是直接原因，並已就軟件缺陷作出詳細調查。TPDSA 亦作出進一步調查，以確定出現錯誤的原因，並找出以下相關的成因：

(a) 在簡單審查軟件開發過程後，發現重大缺陷，未被發現的軟件錯誤仍然存在。

(b) ZC-C 的需要或效益沒有顯明，這削弱了經驗證的核心軟件效益。

(c) 在子系統層面沒有訂立軟件規定，也沒有對規定詮釋進行獨立檢視。

(d) 直到後期，獨立安全評估顧問表示軟件開發及安全工程過程有不足之處，並會影響製成品的完整性。

(e) 儘管承辦商已出示安全案例和安全證書，獨立安全評估顧問的評估範圍太窄，並不涵蓋「測試就緒狀況」(不論是一列或多列列車)。

(f) 鐵路測試的管理不善，欠缺正式溝通，以致出現各種關乎測試限制的假設和混亂情況，因此也沒有施加足夠管制。

(g) 承辦商的機構內部及其與客戶之間的溝通欠缺坦誠。儘管安全案例和安全證書有限制，由於溝通不足，以致一份 PowerPoint 簡報被錯誤詮釋為進行演練的授權。

(h) 與演練有關的安全案例和安全證書有欠清晰而且無法追溯，而引入 ZC-C 也導致安全分析出現差距，因此不符合 EN50129(鐵路應用 - 通信、信號和過程控制系統 - 信號用安全相關電子系統)的要求。

(i) 受到計劃和商業壓力而展開測試，忽略了需要有穩健的過程才能研發出合適的軟件這一點，涉及的各方未能全面理解其重要性。

(j) 在核心軟件內所發現的潛在安全缺陷，以及施加於核心軟件的安全限制，並未被理解為程序欠妥及軟件差劣的先兆。有關決定是基於對核心軟件可靠性的假設而作出，而這些假設顯然是沒有事實根據的。

(k) 不能合理地期望操作人員(車務控制中心人員及列車車長) 能採取更多措施，防止或緩解該事故。

(l) 雖然獨立軟件評估小組來自供應商的另一組別，但被認為不夠獨立。

(m) 儘管有定期舉行會議，但港鐵公司仍與機電署保持距離，並沒有與機電署分享當中的困難，例如獨立安全評估顧問的新評估結果。

6.1.2 概括而言，軟件出現未被察覺的錯誤，是由於要求管理、安全管理和軟件開發過程均不符合國際標準 EN50128 和 EN50129 的規定，這些規定已在合約中訂明，並且是國際公認的信號系統規定。

6.1.3 是次事故的促成因素，是獨立安全評估顧問多次發出意見，指有關軟件並不可靠，但這些意見在事發前並未完全解決。此外，獨立安全評估顧問的職權範圍並不涵蓋「測試就緒狀況」(儘管供應商已出示安全案例和安全證書)，其狹隘的職權範圍，導致測試演練時使用了未經驗證而且缺乏足夠安全管制的軟件。

6.2 Roderick Smith 教授的調查結果

6.2.1 是次事故是因控制軟件的缺陷所致。當模擬首兩個控制器發生故障而進行測試時，該控制軟件未能執行所需的交換資料程序。有關各方都同意這個結論，認為言之成理。Roderick Smith 教授毫無保留地支持這個主要結論。

6.2.2 獨立安全評估顧問早於 2018 年 10 月已表示質疑，並在 2019 年 2 月 6 日及 3 月 5 日重述有關疑問。這些疑問包含了一些意見，例如不相信該信號系統完全符合國際標準，以及認為軟件中的「潛在異常情況」可能導致不安全事故的風險高得令人無法接受。在 2019 年 2 月 19 日至 25 日進行多次三方研討會後，港鐵公司把新系統正式投入服務的日期延至 2019 年第四季。這已是一連串延期的第四次，原定目標日期為 2018 年 5 月。這清楚證明各方都意識到在引入新系統前進行測試所面對的困難。供應商答應在 2019 年 5 月提供新版本的軟件。在 2 月 16 日至 3 月 18 日肇事當天期間，港鐵公司再進行了八次演練，期間沒有出現任何問題。在 3 月 18 日肇事當日，有 34 列列車牽涉其中。沒有任何一方曾向項目倡議者發出清晰意見，扼述進一步測試的情況會構成不可接受的風險，也沒有任何一方曾指示在新版軟件備妥前需暫停測試。

6.2.3 隨着軟件日趨複雜，並應用於眾多不同情況，要離綫測試複雜軟件以知悉一切可能發生的事並不容易，甚或不可能。這類軟件通常是團隊長時間努力編製而成，具有多個版本，極難確保連續性。模擬測試情境恰當與否，取決於編製者在軟件投入服務前進行風險評估時所想像的情況。在測試和驗收軟件的過程中，必須有降低概率的元素，目標是在合理切實可行的範圍內減低風險，而這絕非百分百肯定的。在這個案中，新信號系統正在突破新領域。

6.3 Felix Schmid 教授的調查結果

6.3.1 持份者未能清楚了解實施暖備用而非熱備用配置，以減低全部三個區間電腦發生由數據導致的共同模式故障風險的重要性。事實上，設有 ZC-A、ZC-B 和 ZC-C 三個區間電腦的暖備用系統，屬供應商的一項獨特和非標準設計，有別於其現有信號系統。有關設計是港鐵公司特別要求的，以滿足其嚴格的可用性目標。

6.3.2 於目前正在運作的鐵路實施通訊為本列車控制系統，以及引入備用區間電腦 ZC-C，兩者分別會被視作重大變動。持份者沒有意識到把這兩個變動結合的關鍵程度。

6.3.3 列車相互衝突區域數據不複製至備用區間電腦 ZC-C，應在系統設計文件及其後制訂的模擬和實地測試中詳細說明。

6.3.4 系統設計文件未有詳述列車相互衝突區域數據不複製至備用區間電腦 ZC-C。因此，除了程式編寫(邏輯)存在疏漏外，系統設計文件差劣及制訂模擬和實地測試的不足均為促成因素。

7. 總結

根據調查結果，機電署得出的結論是，2019 年 3 月 18 日於非行車時間在荃灣綫中環站的渡線軌道進行演練期間發生的列車碰撞事故，原因如下：

(a) 涉事的暖備用區間電腦軟件存在程式編寫錯誤，導致主區間電腦在切換至暖備用區間電腦後無法重新產生中環站渡線軌道的列車相互衝突區域數據。因此，列車自動保護系統未能發揮應有作用，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；

(b) 由於涉事系統軟件的具體設計要求未有作明確紀錄，而其核實和驗證過程不足，使 2017 年 7 月就新信號系統進行軟件修改期間出現的程式編寫錯誤，在系統承辦商多次系統測試／軟件升級工作的核實和驗證過程中均未被發現；

(c) 引入暖備用區間電腦所帶來的潛在風險並未完全包括在系統承辦商的風險評估內；以及

(d) 暖備用區間電腦屬供應商的一項獨特和非標準設計，有別於其現有信號系統，但系統承辦商未有在實地測試前，在可行範圍下為暖備用區間電腦作出最大程度的模擬測試。

8. 事故後採取的措施

8.1 碰撞事故發生後，港鐵公司立即暫停對荃灣綫、港島綫和觀塘綫新信號系統進行的全部測試。此外，港鐵公司宣布，將會繼續暫停於非行車時間為新信號系統進行的所有行車測試工作，直至查明事故原因。

8.2 機電署知悉港鐵公司調查委員會向系統承辦商及港鐵公司提出多項建議，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過程及測試，以避免同類事故再次發生。機電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。

– 報告完 –

附錄 I – 2019 年 2 月 16 日至 3 月 18 日的演練

日期	演練
2019 年 2 月 16 日	演練 1 模擬轉轍器故障及列車故障
2019 年 2 月 21 日	演練 2 模擬車務控制中心停電、疏散車務控制中心人員及其他操作演習
2019 年 2 月 23 日	演練 3 模擬信號系統故障及列車救援
2019 年 2 月 28 日	演練 4 模擬供電故障及列車不能停靠月台
2019 年 3 月 9 日	演練 5 模擬供電故障及列車不能停靠月台
2019 年 3 月 12 日	演練 6 模擬信號系統故障
2019 年 3 月 15 日	演練 7 模擬車務控制中心停電、疏散車務控制中心人員及其他操作演習
2019 年 3 月 17 日	演練 8 模擬列車救援
2019 年 3 月 18 日 (事發當日)	演練 9 模擬區間電腦故障

附錄 II – 事件時序表

時間	描述
3月18日	
凌晨0時15分	ATDJV向港鐵公司人員進行簡報，接着由港鐵公司的演練主管向港鐵公司人員進行簡報。
凌晨2時44分	兩列列車在中環站相撞。
凌晨2時54分	通知消防處及警方有關事故。兩名車長送院檢查，並於同日出院。
凌晨2時56分	通知運輸署有關事故。
凌晨3時03分	通知機電署有關事故。
凌晨3時17分	通知運輸署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應用程式及傳媒通知乘客荃灣綫列車服務將受影響，而荃灣綫金鐘至中環站的列車服務需要暫停。
3月19日	
全日	進行復修工作。
晚上11時	把其中一列列車的兩個轉向架移回路軌。
3月20日	
凌晨0時至 1時15分	進行復修工作。
凌晨1時15分	復修工作完成後，把涉事列車移到金鐘站的側綫，並進行安全檢查。

附錄 III – 機電署對港鐵公司的調查委員會的報告的意見

機電署的調查報告與港鐵公司的調查委員會的報告的調查結果並無分歧。然而，機電署認為下列其他事實和因素與事故有關：

(a) 處於暖備用模式的備用區間電腦屬供應商的一項獨特和非標準設計，有別於其現有信號系統，因此不應受限於軟件開發文件內容，而應進行全面的風險評估；以及

(b) 因應備用區間電腦的獨特和非標準設計，在出廠前驗收測試階段不應受限於軟件開發文件內容，而應參照國際標準 IEEE 1474.4 以最大限度為備用區間電腦進行模擬測試。

此外，港鐵公司調查委員會的報告主要集中於供應商在軟件開發和系統實施過程中的不足。報告沒有提及港鐵公司營運項目團隊在監督項目實施情況方面的角色。機電署認為因應此新信號系統的重要性及其獨特和非標準設計，港鐵公司在過程中應加強警覺性及避免過度依賴承辦商。

機電署注意到港鐵公司委員會的報告向 ATDJV 及港鐵公司營運項目團隊提出多項改善措施，以修正程式編寫錯誤問題及加強新信號系統的開發過程及測試，以避免同類事故再次發生。其中，港鐵公司承諾會採取以下措施：

(a) 將「獨立安全評估顧問」的工作範圍，由原來的投入載客服務前確保系統安全，擴大至涵蓋列車實地測試相關的安全認證；

(b) 提升現時港鐵公司已在本港配置用作培訓之用的信號系統模擬平台的功能，在切實可行的情況下，為更多不同情境進行模擬測試；

(c) 與承辦商共同成立一個測試及驗收安全委員會，並納入「獨立安全評估顧問」的意見，以管理實地測試；以及

(d) 與委員會專家一同探究分階段發展備用電腦系統的好處，或由ATDJV建議在技術上合適的其他方案。

機電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。