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。

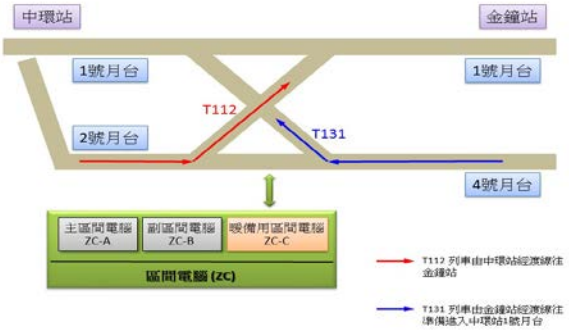

圖 3：事發時列車的行駛情況

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。

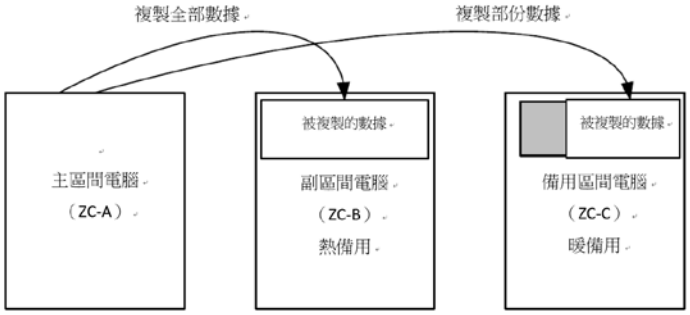

圖 4：三個區間電腦的設計功能

[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。

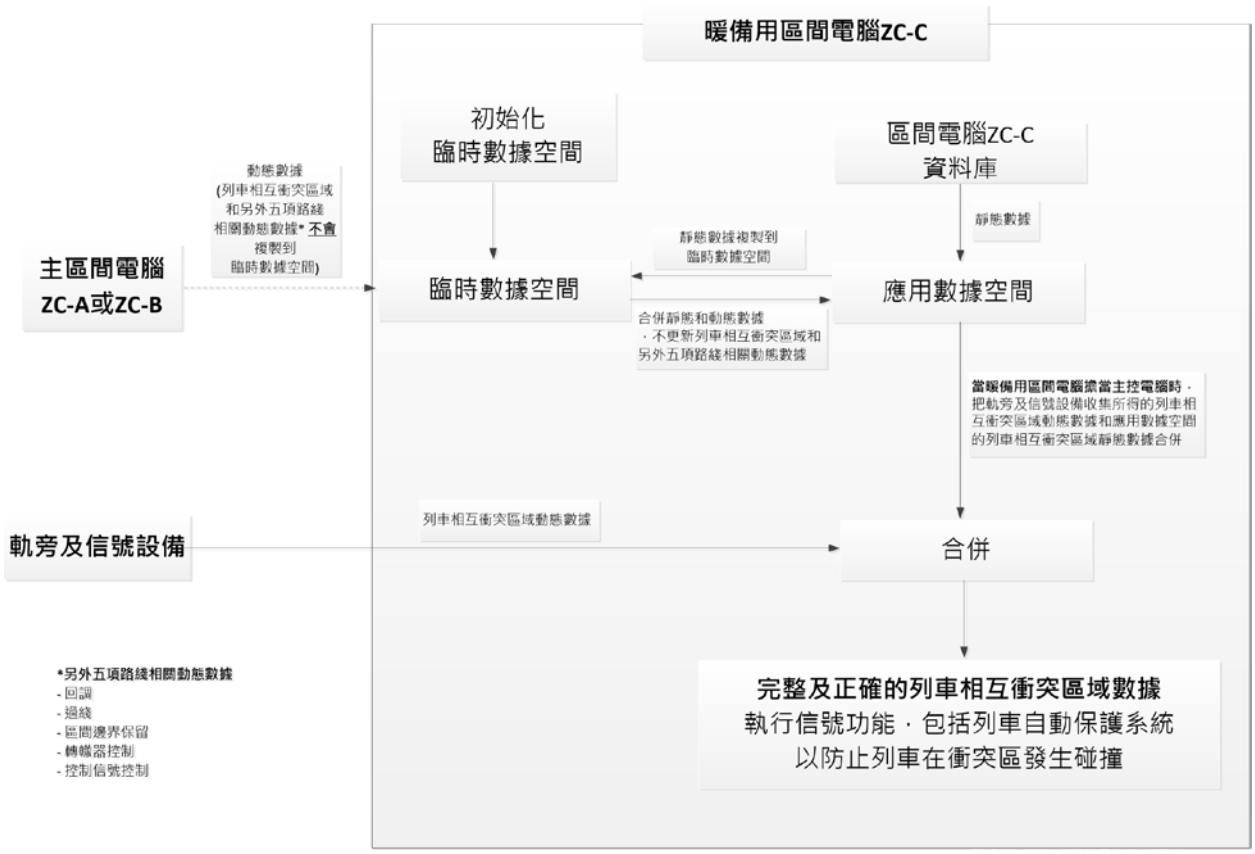

圖 5：主副區間電腦、備用區間電腦及軌旁設備的列車相互衝突區域數據整合方法

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。

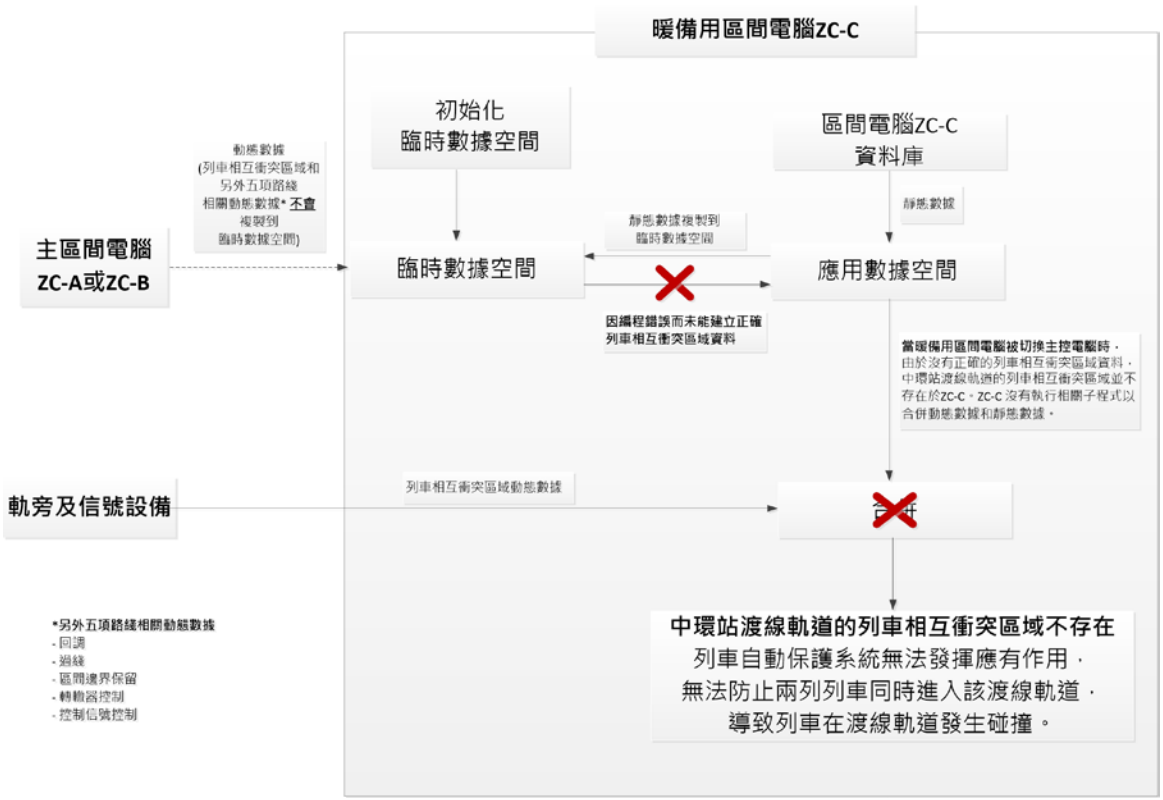

圖 6：暖備用區間電腦沒有執行相關子程式以合併動態數據和靜態數據

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。

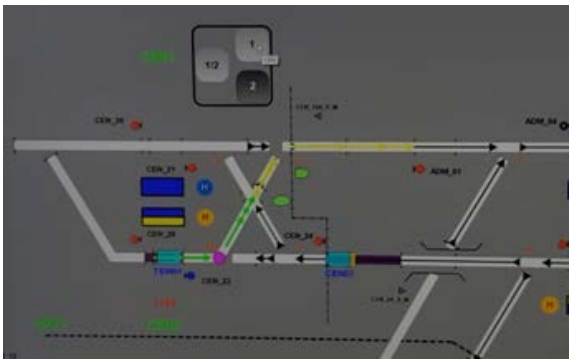

圖 7：ATDJV 香港辦公室模擬器顯示 T112 及 T131 列車同時進入中環站相互衝突區域的路徑設定

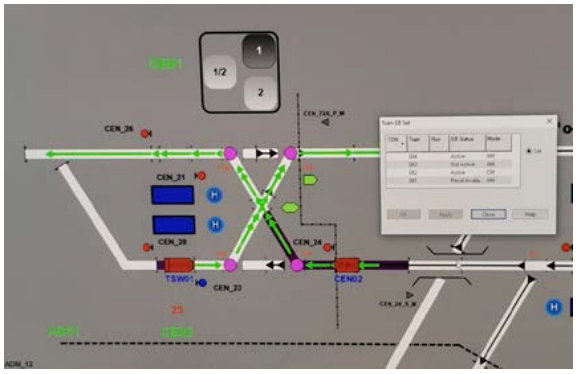

圖 8：ATDJV 香港辦公室模擬器顯示容許兩列列車同時進入中環站的相互衝突區域

[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

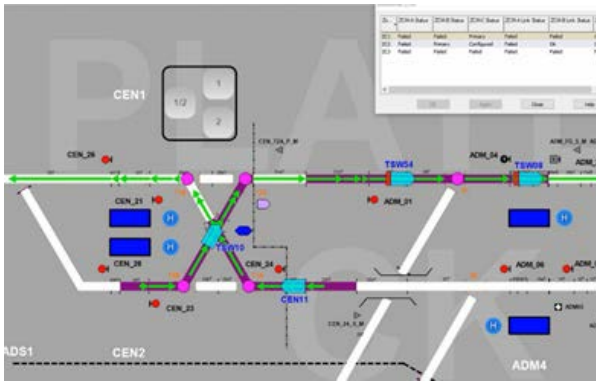

圖 10：模擬結果顯示涉事列車的區間電腦及車載控制器的模擬器容許兩列列車同時進入中環站的相互衝突區域

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。