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；

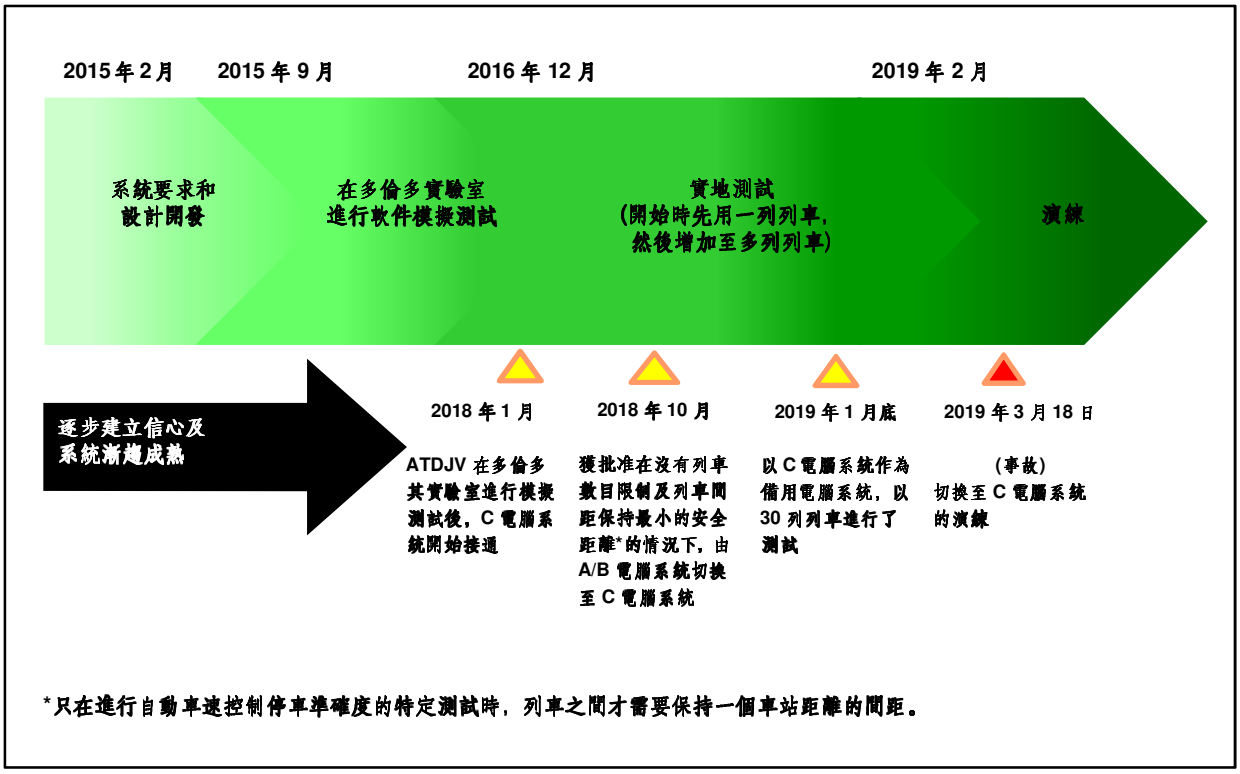
(c) 港鐵與ATDJV共同成立一個信號系統測試及驗收安全委員會，管理實地測試（並納入「獨立安全評估顧問」的意見）；及

(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

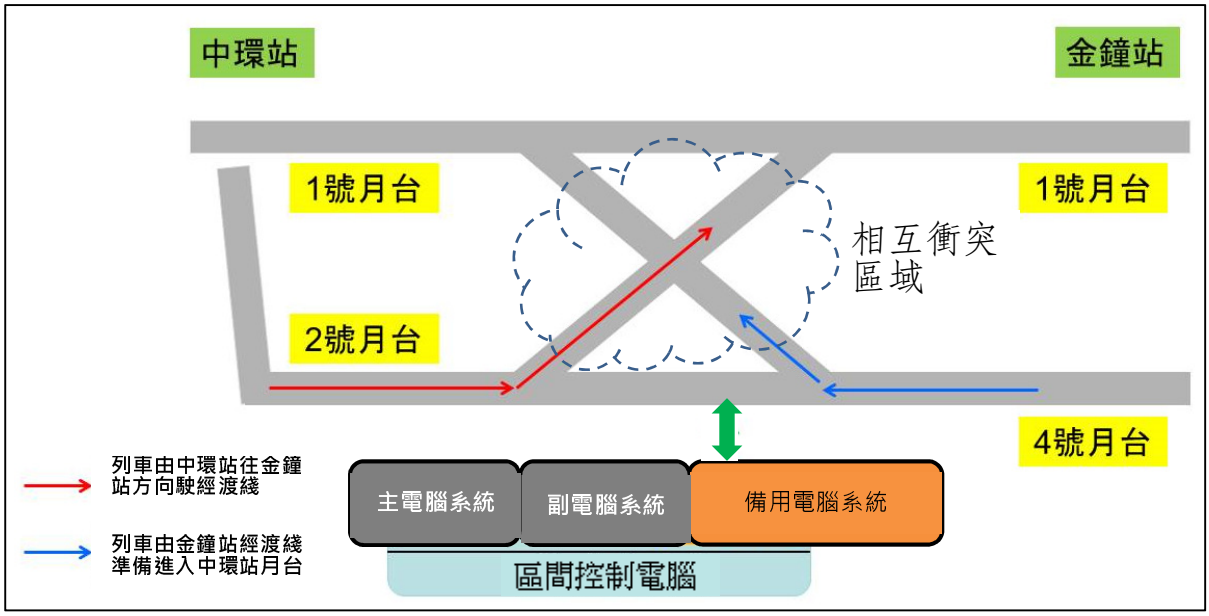
小的安全距離的情況下進行。只有在進行自動車速控制下的停車準確度的特定測試時，列車之間才需要保持一個車站距離的間距。

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

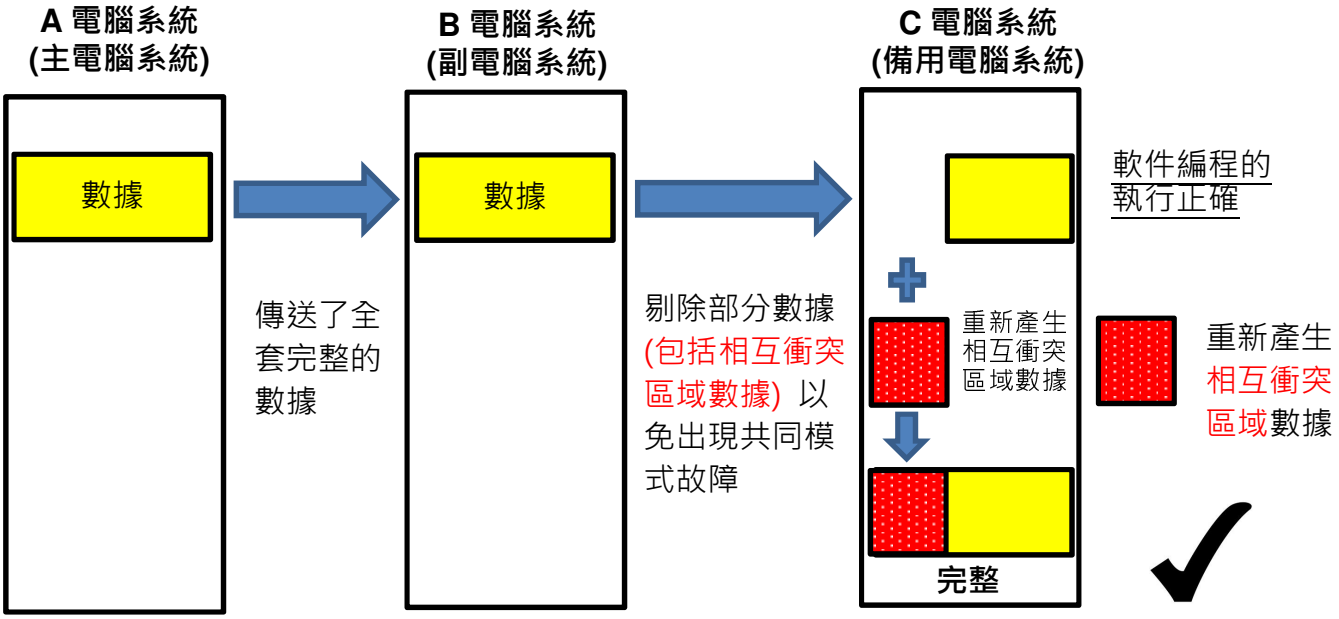


附件 3

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