立法院法制局專題研究報告　　編號：1855

本報告僅供委員參考

鐵道公共運輸關鍵通訊系統資安防護法制問題研析

法制局 林琪蓉　撰

中華民國 115 年 8 月

鐵道公共運輸關鍵通訊系統資安防護法制問題研析

目　　次

摘　　要

近期台灣高速鐵路股份有限公司（以下簡稱高鐵）無線電遭盜接致使列車緊急煞車事件，顯示鐵道公共運輸關鍵通訊系統之資安風險，已由傳統資料外洩或網站癱瘓等資訊安全問題，擴及行車控制、號誌、調度及無線通訊等影響實體運作之操作科技安全風險。我國資通安全管理法第 3 條對資通系統、資通安全事件及關鍵基礎設施已有定義，理論上足以涵蓋鐵道公共運輸關鍵通訊系統；鐵路法第 40 條、第 41 條亦就行車事故、異常事件通報、應變及主管機關檢查權限設有規範。惟現行制度對於操作科技系統之風險特性、資安事件與行車安全之銜接機制、關鍵通訊系統之檢查項目、委外維運及技術基準等事項，仍有進一步明確化及制度化空間。本報告檢視鐵道公共運輸關鍵通訊系統資安防護之現行法制與治理缺口，並參酌國外關鍵基礎設施及運輸資安治理經驗，提出相關建議，以強化鐵路法與資通安全管理法之銜接，提升鐵道公共運輸關鍵基礎設施之資安韌性與營運安全，俾供本院委員問政參考。

鐵道公共運輸關鍵通訊系統資安防護法制問題研析

壹、前言

近年[1]資通安全風險已不再限於資料外洩、網站癱瘓或個人資料保護等傳統資訊科技（Information Technology，以下簡稱 IT）安全問題，逐漸擴及行車控制、號誌、調度、無線通訊等足以影響實體運作之操作科技（Operational Technology，以下簡稱 OT）安全風險。鐵道公共運輸具高度公共性與連續營運特性，其關鍵通訊系統一旦遭未授權接取、身分冒用、訊號干擾或惡意操控，不僅可能造成列車誤點或營運中斷，更可能影響行車安全及社會公共利益。

歐盟網路安全局（European Union Agency for Cybersecurity，以下簡稱 ENISA[2]）指出，網路與資訊安全指令第 2 版（Network and Information Systems 2 Directive, NIS2）係建立歐盟關鍵實體共同資安治理架構，涵蓋能源、運輸、金融、醫療等 18 個關鍵領域，其中運輸部門為重要適用領域之一[3]；歐盟並要求各會員國於 2024 年 10 月完成國內法化，以建立跨領域關鍵基礎設施資安治理架構[4]。由此可見，國際間已逐漸將交通運輸及關鍵基礎設施之資通安全，納入法律及監理制度之一環[5]。

---

[1] 本文有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[2] 其縮寫係依前稱「歐洲網路與資訊安全局」（European Network and Information Security Agency）而取並沿用至今，網址：https://www.nstc.gov.tw/belgium/ch/detail/1057e493-4b52-456d-adb5-bea29b6bf019，最後瀏覽日期：115 年 6 月 29 日。

[3] European Union Agency for Cybersecurity, “Transport,” Cybersecurity of Critical Sectors，網址：https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/transport，最後瀏覽日期：115 年 5 月 14 日。

[4] European Commission, NIS2 Directive: securing network and information systems，網址：https://digital-strategy.ec.europa.eu/en/policies/nis2-directive，最後瀏覽日期：115 年 5 月 15 日。

[5] European Union Agency for Cybersecurity，同註 3。

我國資通安全管理法第3條對於資通系統與安全事件之範疇，已有通則性規範，就法理而言，理應涵蓋鐵道行車控制、號誌、調度及無線通訊等 OT 系統。然而，當前治理瓶頸並非法律定義之漏洞，而是當資安事件實質衝擊列車運行與行車安全時，資通安全管理法與鐵路法兩大體系間的通報應變、聯合演練、跨境檢查及追蹤改善機制，尚未建立緊密的橫向銜接，以致實務運作面臨安全管理的灰色地帶。

交通部鐵道局 111 年「鐵路行車安全通告 111-02」[6]曾指出，通信系統異常可能導致道旁號誌、車上號誌、行車調度無線通訊等行車保安裝置無法使用，並要求鐵路機構做好資通安全防護，避免核心行車控制管理系統遭入侵癱瘓，同時加強行車替代保安方式演練；倘發生資通安全事件，應依行政院資通安全事件通報及應變處理作業程序辦理。此項通告顯示實務上已注意到資通安全與行車安全之連動關係，惟相關要求多見於行政通告或作業程序，宜評估進一步於法律或授權命令層級明確化，值得進一步研析。

尤其鐵道公共運輸關鍵通訊系統多屬 OT 系統，其運作特性與一般資訊系統不同，著重即時控制、穩定運作及安全可靠；一旦遭受資安威脅，可能直接影響列車運行與公共安全。現行制度雖已將相關系統納入資通安全管理範圍，惟針對 OT 之特殊風險，以及委外維運、供應鏈管理、身分驗證、加密管理、異常訊號監測、重大事件認定與第三方鑑識等事項，相關法律及授權命令是否已具充分規範，仍有進一步檢視之必要。

本文爰以鐵道公共運輸關鍵通訊系統資安防護相關問題為研究核心，檢視鐵路法與資通安全管理法之規範銜接，並分析現行法

[6] 交通部鐵道局，〈鐵路行車安全通告 111-02〉，111 年 9 月。

律、子法、技術基準、通報程序、演練規範及主管機關檢查標準間是否存在落差，並參考國外關鍵基礎設施及運輸資安治理經驗，研提我國法制精進方向，以兼顧鐵道營運效率、行車安全、資通安全及大眾公共利益，俾供本院委員問政參考。

貳、我國現行法制與運作概況

一、資通安全管理法建立關鍵基礎設施資安管理之基本架構

我國資通安全管理法係資通安全治理之基本法制。該法第 3 條詳列用詞定義，明文將「資通系統」、「資通安全」、「資通安全事件」、「特定非公務機關」、「關鍵基礎設施」及「關鍵基礎設施提供者」等主客體納入監理範疇。

依據該條文之架構定義，資通系統泛指用以控制、傳輸或處理資訊之系統；資通安全則側重於防止系統遭受未經授權之存取、控制、破壞或竄改，以確保資訊之機密性、完整性與可用性。由此法律定義觀之，鐵道運輸之核心行控、號誌調度及無線通訊等關鍵系統，本質上皆涉及即時資訊傳輸與控制指令之運作，自應屬該法所積極防護之實體範圍。

就管理義務而言，資通安全管理法第 7 條規定公務機關及特定非公務機關應依資通安全責任等級，辦理資通安全防護計畫、稽核及改善等事項；第 10 條並就資通系統或資通服務委外建置、維運時之資安管理設有規範；第 24 條、第 25 條則分別涉及資通安全事件通報、重大資通安全事件調查及應變處理。此一制度已使關鍵基礎設施提供者之資安維護、委外管理及事件通報具有基本法律依據。

然而，上述規範多屬通案性、原則性之抽象要求，面對鐵道公共運輸所涉 OT 之特殊性，現行條文尚未延伸出針對行車控制、無線電調度等工控環境的細緻化風險分級、技術基準或跨系統監測機制，仍有賴後續相關子法、技術規範及主管機關監理措施予以具體落實。

二、鐵路法規定行車事故、異常事件通報及應變演練

鐵路法第 40 條規定，地方營、民營及專用鐵路機構遇有重大行車事故或嚴重遲延，應立即通報交通部鐵道局，並啟動旅客接駁應變計畫；一般行車事故及異常事件亦應按月彙報。該條並授權主管機關訂定重大行車事故、一般行車事故、嚴重遲延及異常事件之定義、通報內容、通報方式及其他相關事項之準則。另鐵路機構應就行車事故及異常事件訂定應變計畫，內容包括現場處置、通報作業、旅客訊息公告、旅客疏散或接駁、人員救護、運轉調度、搶修救援人力調度、危險物品排除、鐵道淨空安全與器材備置，並應定期演練、檢討及改善。

同法第 41 條則規定，交通部鐵道局應定期及不定期派員檢查地方營、民營及專用鐵路之工程、材料、營業、運輸、財務、會計、財產實況及附屬事業經營等情形；必要時，並得命其提出文件、帳冊及其他資料，以掌握鐵路機構營運安全及經營狀況。

綜觀上述，鐵路法已就鐵路行車安全事件之通報、應變、演練與主管機關檢查權限建立基礎制度。惟其規範文字主要仍以行車事故、異常事件、營運及設備檢查為中心，尚未明確列舉因資通安全事件導致行車控制、號誌、調度或無線通訊異常時，應如何納入行車安全事件體系及主管機關檢查事項。

三、交通領域資安整備、聯防及技術強化措施

交通部為配合第 6 期國家資通安全發展方案，曾推動「交通領域關鍵基礎設施資安整備計畫（110 年至 113 年）」[7]，並於新一期「交通領域工業控制系統資安整備計畫（114 年至 117 年）」[8]中，規劃強化交通領域 OT 從業人員資安職能、透過交通領域資安資訊分享與分析中心（Transportation Information Sharing and Analysis Center，以下簡稱 T-ISAC）、交通領域電腦緊急應變中心（Transportation Computer Emergency Response Team，以下簡稱 T-CERT）、交通領域資安聯防監控中心（Transportation Security Operations Center，以下簡稱 T-SOC）等平臺建立資安事件聯防機制，並以實地稽核檢視所管機關之資安合規及成熟度。

根據審計部查核報告指出，交通部前期「交通領域關鍵基礎設施資安整備計畫」係以工業控制系統（Industrial Control System，以下簡稱 ICS）資安防護為重點，透過實地訪談、輔導及交通領域資安資訊分享與分析中心、電腦緊急應變中心、資安聯防監控中心等平臺，提升關鍵基礎設施提供者之防護韌性。惟查核結果顯示，實務上仍有相關人員未持續取得適切資安職能證書、未將 ICS 資安職能訓練規定納入資通安全維護計畫，以及未持續追蹤資安攻防演練弱點改善情形等事項，尚待研謀改善。

就鐵道機構實務而言，國營臺灣鐵路股份有限公司（以下簡稱臺鐵）亦曾與荷蘭資安代表團交流資通安全管理制度與數位轉型

[7] 審計部預決算審核報告查詢平臺，〈交通部推動交通領域關鍵基礎設施資安整備計畫執行情形查核報告〉，112 年，網址：https://auditreport.audit.gov.tw/ServerFile/Get/638257052919488014 2f07b3d40d134ffdb0f8f1351a942f22，最後瀏覽日期：115 年 5 月 19 日。

[8] 立法院預算中心，〈交通部、鐵道局及所屬 114 年度單位預算評估報告〉，113 年 10 月，網址：https://www.ly.gov.tw/Pages/List.aspx?nodeid=55740，最後瀏覽日期：115 年 6 月 29 日。

下風險防範策略[9]。另針對近期媒體報導，臺鐵說明其行調無線電為獨立封閉系統，未連接外網，並已針對資訊設備輸入與輸出進行韌體加密、年度維保時變更無線電終端設備密碼及對使用者操作界面加密，以保護系統設定參數[10]。

上述實務作為顯示，我國交通及鐵道領域已有資安整備計畫、資安聯防平臺、國際交流及技術強化措施。本文後將聚焦於這些措施如何與鐵路法所定行車事故及異常事件通報、應變計畫、定期演練與主管機關檢查制度相互銜接，以及涉及鐵道公共運輸關鍵通訊系統之身分驗證、加密管理、異常訊號監測、弱點改善追蹤及第三方鑑識等事項，是否已有足夠明確之法律或授權命令依據。

四、小結

綜上，我國現行制度已分別就資安治理及鐵路行車安全建立相關規範，惟兩者間之制度銜接及法制整合，仍有檢討精進空間。隨著鐵道公共運輸系統高度依賴行車控制等關鍵系統，資安事件可能直接轉化為行車安全風險。有研究指出，關鍵基礎設施安全維護不僅涉及資訊系統安全，與公共服務持續運作及國家整體安全韌性密切相關[11]。因此，有必要進一步檢視，資通安全事件是否已明確納入鐵路應變計畫範圍；主管機關檢查權是否足以涵蓋關鍵通訊系統之技術防護；鐵路安全管理系統（Safety Management System，以下簡稱 SMS）是否已將資安威脅納入行車危害辨識與

[9] 交通部新聞稿，臺鐵與荷蘭代表團資安交流，強化國際合作及防護韌性，更新日期 114 年 4 月 18 日，網址：https://www.motc.gov.tw/ch/app/news_list/view?module=news&id=14&serno=cf513396-ee06-42e2-a949-34b2578facad，最後瀏覽日期：115 年 5 月 20 日。

[10] 經濟日報，臺鐵駁斥無線電遭駭 強調已韌體加密、變更密碼，115 年 4 月 30 日，網址：https://money.udn.com/money/story/7307/9474922?utm_source=chatgpt.com，最後瀏覽日期：115 年 5 月 20 日。

[11] 柯雨瑞、楊語柔，外國關鍵基礎設施安全維護機制之探討－兼論對臺灣之啟示，柯雨瑞教授網站，網址：https://share.google/hbUUO2elfbyyKh8P0，最後瀏覽日期：115 年 5 月 21 日。

風險評估中；以及資通安全管理法相關子法、技術基準與鐵路法行車安全管理制度間是否已完整連結。

參、國外制度

一、歐盟：以網路與資訊安全指令第 2 版建立關鍵基礎設施資安義務體系

歐盟於 2022 年通過 NIS2，建立跨會員國之關鍵基礎設施資安治理架構，並將運輸部門列為重要及關鍵實體之一，涵蓋航空、海運、鐵路及道路運輸。該指令要求相關實體應採取適當之資安風險管理措施，並建立資安事件通報機制，以確保關鍵服務之持續運作。

ENISA 另於鐵道資安專門報告（Railway Cybersecurity）中指出，鐵道系統之資安防護已不僅涉及資訊系統，亦包括號誌、列車控制、通訊系統、營運科技及供應鏈等面向，並應透過風險管理、安全措施及事件應變機制加以強化[12]。將運輸部門資安納入關鍵基礎設施治理，並透過法律與專門指引明確化相關實體之風險管理、通報及監理責任。

二、美國：以行政命令及監理指引強化運輸資安

美國對於關鍵基礎設施資安治理，係透過行政命令及主管機關指引形成制度。例如 2021 年拜登總統簽署第 14028 號行政命令（Executive Order 14028，簡稱 EO 14028），要求建立資安事件通

[12] ENISA, Railway Cybersecurity–Security Measures in the Railway Transport Sector, European Union Agency for Cybersecurity, 2021，網址：https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Railway%20Cybersecurity.pdf，最後瀏覽日期：115 年 5 月 22 日。

報、軟體供應鏈安全及資安能力提升機制，以強化聯邦政府及關鍵基礎設施資安防禦機制。

在運輸領域，運輸安全管理局（Transportation Security Administration, TSA）針對鐵路及其他運輸業者發布資安指令，要求其建立資安事件通報制度、指定資安負責人、執行資安風險評估及採取保護措施[13]；並透過國土安全部（Department of Homeland Security, DHS）推動關鍵基礎設施保護，強調政府與民間資訊分享、公私協力及跨部會協調，以提升關鍵基礎設施安全韌性[14]。其制度核心特徵包含：

(一)強調即時通報與跨機關合作。

(二)將資安納入運輸安全監理體系。

(三)透過行政命令與監理指引快速因應新興威脅。

另美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）亦提出跨領域關鍵基礎設施資安績效目標（Cross-Sector Cybersecurity Performance Goals, CPGs），強調關鍵基礎設施應建立風險管理、持續監測、事件應變及營運復原等機制，完善整體資安韌性[15]。

三、英國：以國安架構整合運輸與資安治理

英國透過國家網路安全中心（National Cyber Security Centre, NCSC）及交通部建立跨部會合作機制，將資安納入國家安全治理

---

[13] Transportation Security Administration (TSA), Security Directive 1580/82-2021-01C: Enhancing Public Transportation and Passenger Railroad Cybersecurity，網址：https://www.tsa.gov/sites/default/files/security_directive_1580-21-01c_and_memo_508c.pdf，最後瀏覽日期：115 年 5 月 23 日。

[14] 程法彰、洪嫈媛，〈美國在資訊時代中對關鍵基礎設施保護架構與資訊分享議題初探及我國的借鏡〉，《前瞻科技與管理》，第 3 卷，第 2 期，102 年 11 月，頁 120-123。

[15] Cybersecurity and Infrastructure Security Agency (CISA), Cross-Sector Cybersecurity Performance Go*als*, 2023，網址：https://www.natat.org/wp-content/uploads/2023/05/CPGs.pdf，最後瀏覽日期：115 年 5 月 25 日。

體系，並透過網路評估框架（Cyber Assessment Framework, CAF）等機制，協助關鍵基礎設施營運者建立風險管理、持續營運及資安韌性措施，並針對運輸部門發布相關資安指引及風險管理要求，以提升重要基礎設施之防護能力[16]。其制度特色為：

(一)將運輸資安納入國家安全層級管理。

(二)透過指引方式要求業者建立資安風險管理機制。

(三)強化政府與業者間之資訊共享與應變合作。

四、小結

綜合歐盟、美國及英國制度，可歸納下列共通趨勢：

(一) 將運輸系統納入關鍵基礎設施資安治理範圍。

(二)明確要求資安風險管理與事件通報。

(三)強化跨部會及公私協力機制。

(四)逐步將資安責任由政策指引提升至法律或準法律規範層級。

相較之下，我國在鐵道公共運輸關鍵通訊系統資安風險與行車安全管理制度之銜接、OT 系統特性之具體規範、主管機關檢查權限之明確化，以及法律、子法與技術規範間之整合等方面，仍有進一步精進空間。

肆、問題研析與建議

一、強化資通安全事件與鐵路行車安全事件之制度銜接

我國資通安全管理法與鐵路法第 40 條雖各設有通報與應變規範。然而，當資通安全事件已足以影響列車運行、迫使列車緊急停車、導致調度通訊中斷或號誌控制異常時，現行制度仍呈現「雙軌

[16] National Cyber Security Centre (NCSC), Cyber Assessment Framework (CAF) ，網址：https://www.ncsc.gov.uk/collection/cyber-assessment-framework, 最後瀏覽日期：115 年 5 月 26 日。

並行、缺乏橫向交集」之狀態。資安事件在資通安全管理法下固得進行通報，惟其同時作為行車安全事件時，仍宜明確納入鐵路機構之行車事故及異常事件應變計畫、跨領域定期演練及改善追蹤機制，以提升制度一致性。

爰此，建議檢討鐵路行車規則或相關作業規範，於行車異常事件之定義或應變計畫必備內容中，明定「資通系統受破壞、干擾或未授權控制，致影響行車安全者」應納入通報、應變及演練範圍。另宜推動 SMS 與資安治理機制對接，督導鐵路業者於安全管理報告中，將資安威脅列為行車危害辨識（Hazard Identification）之重要項目，據以進行風險評估、改善追蹤及持續檢討，落實行車安全與資安治理整合管理之理念。

二、依操作科技系統特性，具體化資安管理要求

鐵道公共運輸關鍵系統多屬 OT 及 ICS，其功能並非單純處理資料，而係直接支援列車運行、調度指揮及行車保安。其資安風險具有高度即時性、連動性及實體影響性，並非僅止於資料外洩或網站癱瘓，而可能涉及控制訊號異常、參數遭竄改、通訊中斷或設備誤動作等實體運作風險，與一般 IT 之風險態樣與管理需求有別[17]。

工控環境多採全年持續運作架構，設備更新及資安修補作業須兼顧系統持續運轉與營運穩定，相關通訊協定亦可能受相容性及既有設備限制。故後續制度設計不宜僅以一般 IT 之資安要求直接套用於鐵道公共運輸關鍵通訊系統，而應兼顧行車安全、營運持續及資安防護之整體需求。

[17]Joseph Weiss, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, 2010, p.1-15.，網址：https://books.google.com/books/about/Protecting_Industrial_Control_Systems_fr.html?id=ugOsO17iHB8C，最後瀏覽日期：115 年 6 月 30 日。

另就操作科技系統之資安維護而言，補丁管理（Patch Management）亦具有與一般資訊系統不同之特性。一般 IT 系統發現弱點後，通常得透過更新程式或重新開機方式完成修補；惟鐵道號誌、列車控制及調度系統等 OT 環境，係維持列車運行及行車安全之關鍵系統，其設備更新及弱點修補作業須兼顧系統穩定性及營運持續性。一旦更新程序與既有設備發生相容性問題，可能影響列車運行或導致服務中斷[18]。

因此，國際間對於工業控制系統之弱點修補，多強調於正式部署前先於封閉測試環境完成驗證，並於適當維護時段進行更新，以降低對營運之影響。此種風險管理思維與一般資訊系統追求即時更新之模式有所不同，未來鐵道公共運輸關鍵通訊系統之資安管理規範，亦宜將此類操作科技特性納入考量。

三、資安整備計畫、行政規範與法律制度應予整合

交通部雖已推動交通領域關鍵基礎設施及 ICS 資安整備相關計畫[19]，並透過 T-ISAC、T-CERT、T-SOC 等平臺建立資安資訊分享、緊急應變及聯防監控機制；近年亦逐步推動資安治理平臺及風險可視化機制，以協助主管機關掌握轄管機關及關鍵基礎設施之資安風險狀況[20]；鐵道機構亦透過國際交流、硬韌體加密、密碼變更及使用者操作界面加密等技術強化措施。

---

[18] Eric D. Knapp & Joel Thomas Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd ed., Syngress, 2015, p.41-55.，網址：https://www.google.com.tw/books/edition/Industrial_Network_Security/tE7VEAAAQBAJ?hl=zh-TW&gbpv=1，最後瀏覽日期：115 年 6 月 30 日。

[19] 審計部預決算審核報告查詢平臺，〈交通部推動交通領域關鍵基礎設施資安整備計畫執行情形查核報告〉，112 年，網址：https://auditreport.audit.gov.tw/ServerFile/Get/6382570529194880142f07b3d40d134ffdb0f8f1351a942f22，最後瀏覽日期：115 年 5 月 29 日。

[20] 黃彥棻，揭露資安院 2.0 轉型願景，林盈達以 AI 築數位長城，iThome，2026 年 6 月 1 日，網址：https://www.ithome.com.tw/news/175244，最後瀏覽日期：115 年 6 月 15 日。

惟前揭措施多係透過行政計畫、資安整備方案、行車安全通告、業者內部管理措施或個案合作機制推動，其法律位階、適用範圍及持續性仍有不同。相較於資通安全管理法及鐵路法所建立之法定管理機制，部分資安要求尚未完全轉化為鐵路機構應持續遵循之法定義務，相關措施亦可能因計畫期程屆滿、組織調整或資源配置變動而影響執行成效。

為確保政策之長效性，建議交通部依鐵路法第 40 條有關應變計畫及定期演練之規定，配合檢討鐵路行車規則及相關技術規範，將交通領域資安整備計畫所累積之資安管理措施、聯防機制及演練要求，逐步納入法定管理架構。例如關鍵通訊系統之資安演練、異常通報、弱點管理、聯防合作及改善追蹤等事項，建立一致性管理規範，以強化計畫成果之延續性及制度化之成效。

四、明確主管機關對鐵道公共運輸關鍵通訊系統資安檢查權限

鐵路法第 41 條雖授權交通部鐵道局對鐵路機構之工程、材料、營業、運輸、財務、會計、財產實況及附屬事業經營等情形實施檢查。從文義觀察，行車控制、號誌、調度及通訊設備之安全狀態，固可被理解為設備或營運安全之一環，惟條文並未明確列示資通安全防護事項。就鐵道公共運輸關鍵通訊系統而言，主管機關檢查範圍宜包含身分驗證、加密管理、密碼更新、異常訊號監測、弱點修補、委外維運安全、資安演練紀錄及改善追蹤等事項。

國際上對關鍵基礎設施資安治理，已逐漸強調治理、風險辨識、防護、偵測、回應及復原等整體性管理架構，除著重組織治理及風險管理外，亦強調主管機關或監理機關應具備適當之監督及

查核機制，以確認相關措施落實執行[21]。若僅以一般設備或營運檢查概括處理，恐難以反映資安風險之技術性與即時性，故宜評估於鐵路法第 41 條相關授權規範或鐵路安全管理相關子法中，明定主管機關得就關鍵通訊系統之資安防護措施及相關管理機制實施檢查，以提升監督明確性、執行一致性及關鍵系統之整體韌性。

五、強化委外維運及供應鏈資安管理機制

鐵道公共運輸關鍵通訊系統之建置、維護及更新，常涉及設備供應商、系統整合商、通訊服務廠商、軟體維護廠商及資安檢測機構等多重參與者。此類系統一旦因委外維運、遠端連線、弱點修補不及、設備韌體管理不當或供應鏈漏洞而遭入侵，將直接危及行車安全及營運穩定性。相關研究指出，ICS 隨著與資訊網路連結程度提高，設備弱點、通訊協定缺陷及未授權存取等問題，均可能成為攻擊者入侵關鍵基礎設施之途徑，顯示委外維運及供應鏈管理已成為整體資安治理不可忽視之一環[22]。

雖然資通安全管理法第 10 條已就資通系統或資通服務委外辦理之資安管理設有規範，惟現行規範多屬原則性要求，就鐵道公共運輸關鍵通訊系統之特殊風險而言，仍宜進一步具體化委外契約應載事項及相關管理措施（如遠端維護控管、弱點修補時限、第三方測試等）。國際上對關鍵基礎設施資安治理，亦逐漸強調將供應商、委外服務提供者及其他第三方所帶來之供應鏈風險，納入整體資安治理及風險管理架構，並透過契約管理、持續監督及事件通報

[21] National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, February 26, 2024, p.1-3，網址：https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf，最後瀏覽日期：115 年 6 月 18 日。

[22] 傅上哲，《工業控制系統的安全事件風險評估》，中原大學資訊工程學系碩士論文，109 年 6 月，頁 13-18。

機制加以控管[23]。近年實務界亦指出，網路安全不再侷限於資訊部門之技術管理事項，而與供應鏈韌性及組織治理能力密切相關，企業能否有效掌握供應商風險及建立供應鏈透明度，已逐漸成為維持營運與供應鏈韌性的重要因素[24]。

審計機關近年查核更發現，部分關鍵基礎設施提供者於工控資安成熟度評估中，尚有委外廠商資安稽核、弱點評估及資料備份管理等項目未達標準之情形，顯示委外維運及供應鏈安全仍有持續強化之必要[25]。

以鐵道公共運輸系統而言，行車控制、號誌、調度及無線通訊設備之建置與維護，往往涉及設備供應商、系統整合商及維運廠商等多方參與。鐵路機構雖具備行車安全管理專業，惟未必具備充分之資安稽核或供應鏈安全管理能力；倘委外契約未明定資安責任、弱點管理、異常通報或稽核配合事項，相關風險可能透過委外體系擴散至關鍵通訊系統，進而影響行車安全及營運穩定。

因此，除現行資通安全管理法第 10 條所定委外管理要求外，宜就鐵道公共運輸關鍵通訊系統進一步具體化委外契約及管理事項，例如加密與身分驗證要求、遠端維護控管、弱點修補時限、異常事件即時通報、第三方測試、供應商責任及資安稽核配合義務等，建立持續監督、定期檢核及改善追蹤機制，以降低供應鏈風險對行車安全及營運持續性之影響。

---

[23] National Institute of Standards and Technology (NIST)，同註 21，p.13-15。

[24] 黃彥棻，資安不再是 IT 部門的事，供應鏈韌性與 AI 治理成企業存續的核心命題，iThome，2026 年 6 月 15 日，網址：https://www.ithome.com.tw/news/176614，最後瀏覽日期：115 年 6 月 22 日。

[25] 審計部預決算審核報告查詢平臺，〈政府推動國家關鍵基礎設施安全防護執行情形〉，114 年，網址：https://auditreport.audit.gov.tw/ServerFile/Get/638926831626648772f39b695028b7468b92edefd5d27ee0ba，最後瀏覽日期：115 年 6 月 23 日。

六、完善重大資安事件認定及第三方鑑識機制

資通安全管理法第 24 條、第 25 條已就資通安全事件通報、重大資通安全事件調查及應變處理設有規範。然而，在鐵道公共運輸領域，資安事件是否重大，不宜僅以資訊系統受影響程度判斷，亦應納入其對列車運行、旅客安全、調度指揮、通訊可用性及公共秩序之影響。例如無線通訊遭未授權接取、冒用發送緊急煞車訊號、號誌或行控系統發生異常訊號，縱未造成大規模資料外洩，仍可能因影響行車安全而具有高度公共安全風險[26]。

國際上亦曾發生針對關鍵基礎設施控制系統之網路攻擊事件，該停電事故（烏克蘭電網案）並非單純由惡意程式造成，而係攻擊者合法取得控制系統權限後，直接操作控制系統及其軟體所致，其損害結果未必以資料外洩為主要型態，惟仍造成服務中斷、設備失效及公共安全風險。此與鐵道無線電遭冒用之風險具有相似性，行調無線電屬封閉系統，但若終端設備密碼外洩或被冒用，亦可能影響列車運行及行車安全。

未來宜檢討是否於資通安全事件分級或重大事件認定標準中，明確納入「影響鐵道行車安全或營運秩序」之因素，並評估建立第三方鑑識、專家參與、根本原因分析（Root Cause Analysis）、改善追蹤與公開說明之基本程序，以提升社會信任、監理效能及後續風險改善能力。

[26] Robert M. Lee, Michael J. Assante & Tim Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC) & SANS Industrial Control Systems, March 18, 2016, p.3-5. 網址：https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf，最後瀏覽日期：115 年 6 月 24 日。

七、建構鐵路法與資通安全管理法之銜接體系（建議修正鐵路法第40條第4項）

鐵道公共運輸關鍵通訊系統資安防護之核心，在於鐵路法與資通安全管理法雙法體系之銜接。後續制度精進方向，宜避免將所有事項均置於資通安全管理法處理，而應以鐵路法第40條為修法重點；至於第41條，則宜評估透過修法或相關授權子法，明定資安檢查事項。

從法制體系觀察，資通安全管理法係我國資通安全治理之通案性法律，主要規範資通系統之防護措施、資安事件通報、委外管理及資安責任分級等事項；鐵路法則屬鐵路運輸安全之特別法，重點在於行車安全管理、事故通報、應變處置及主管機關監理機制。

因此，鐵道公共運輸關鍵通訊系統之資安防護，並非另行建立獨立法律體系即可解決，而應透過兩法之功能分工與制度銜接加以處理。換言之，資通安全管理法主要負責資安防護措施之建立與執行，例如身分驗證、加密管理、弱點修補、委外管理及資安事件通報等事項；鐵路法則負責當資安事件進一步影響列車運行、號誌控制、調度指揮或無線通訊時之行車安全管理、事故應變、演練及主管機關檢查事項。

準此，未來制度精進方向宜以鐵路法補充行車安全面向之管理機制，並與資通安全管理法既有資安治理架構相互銜接，而非重複建構新的資安管理制度。如此不僅可避免法規重複與權責重疊，亦有助於建立兼顧資安治理與行車安全之整合管理架構。

基此考量，爰建議修正鐵路法第40條第4項規定為：「鐵路機構應就行車事故及異常事件訂定應變計畫，其內容應包括現場處置、通報作業、旅客訊息公告、旅客疏散或接駁、人員救護、運

轉調度、搶修救援之人力調度、危險物品之排除、鐵道淨空安全與器材備置，並應將資通安全事件致行車控制、號誌、調度或無線通訊系統異常之應變處置、危害辨識、復原作業及改善追蹤納入規劃。」，明定鐵路機構應將資通安全事件致行車控制、號誌、調度或無線通訊系統異常之相關情境納入應變計畫，並作為定期演練及鐵路安全管理系統之危害辨識事項，以強化鐵路法與資通安全管理法之制度銜接，並提升鐵道關鍵基礎設施之整體韌性。至於主管機關對鐵道公共運輸關鍵通訊系統之資安檢查事項，宜評估於鐵路法第 41 條或相關授權子法中予以明確規範，以兼顧法制完整性與執行彈性。

伍、結論

隨著鐵道系統行車控制、號誌、調度及無線通訊等關鍵設施高度數位化，資通安全事件已可能直接影響列車運行及公共安全。未來宜通盤檢討鐵路法、資通安全管理法及其相關子法、技術規範與行政措施間之制度銜接，強化技術基準、通報程序、演練規範及監督檢查之整合，以提升鐵道公共運輸關鍵基礎設施之資安韌性、營運安全及服務持續性，俾供本院委員問政及未來修法參考：

一、強化資通安全事件與鐵路行車安全事件之制度銜接。

二、依操作科技系統特性，具體化資安管理要求。

三、資安整備計畫、行政規範與法律制度應予整合。

四、明確主管機關對鐵道公共運輸關鍵通訊系統資安檢查權限。

五、強化委外維運及供應鏈資安管理機制。

六、完善重大資安事件認定及第三方鑑識機制。

七、建構鐵路法與資通安全管理法之銜接體系。

陸、條文對照表

鐵路法第四十條建議修正條文對照表

本報告建議條文	現行條文	說明
第四十條　地方營、民營及專用鐵路機構遇有重大行車事故或嚴重遲延，應立即通報交通部鐵道局，隨時將經過情形報請查核，並啟動旅客接駁應變計畫；其一般行車事故及異常事件，亦應按月彙報。 前項重大行車事故、一般行車事故、嚴重遲延及異常事件之定義、通報內容、通報方式及其他相關事項之準則，由主管機關定之。 交通部鐵道局得就鐵路機構按第一項規定所提報告內容，要求鐵路機構負責人或相關主管說明。 鐵路機構應就行車事故及異常事件訂定應變計畫，其內容應包括現場處置、通報作業、旅客訊息公告、旅客疏散或接駁、人員救護、運轉調度、搶修救援之人力調度、危險物品之排除、鐵道淨空安全與器材備置，並應將資通安全事件致行車控制、號誌、調度或無線通訊系統異常之應變處置、	第四十條　地方營、民營及專用鐵路機構遇有重大行車事故或嚴重遲延，應立即通報交通部鐵道局，隨時將經過情形報請查核，並啟動旅客接駁應變計畫；其一般行車事故及異常事件，亦應按月彙報。 前項重大行車事故、一般行車事故、嚴重遲延及異常事件之定義、通報內容、通報方式及其他相關事項之準則，由主管機關定之。 交通部鐵道局得就鐵路機構按第一項規定所提報告內容，要求鐵路機構負責人或相關主管說明。 鐵路機構應就行車事故及異常事件訂定應變計畫，其內容應包括現場處置、通報作業、旅客訊息公告、旅客疏散或接駁、人員救護、運轉調度、搶修救援之人力調度、危險物品之排除、鐵道淨空安全與器材備置。 鐵路機構應按應變計畫定期實施演練，並作檢討及改善。	現行條文已規定鐵路機構應就行車事故及異常事件訂定應變計畫，並明定其應包括事項。惟近年鐵道公共運輸系統高度數位化，資通安全事件亦可能影響行車控制、號誌、調度及無線通訊系統之正常運作，進而影響列車運行及公共安全。爰修正第四項，增列資通安全事件相關應變處置、危害辨識、復原作業及改善追蹤事項，以強化鐵路行車安全管理與資安治理之制度銜接，並提升公共運輸關鍵基礎設施之整體韌性。

危害辨識、復原作業及改善追蹤納入規劃。 鐵路機構應按應變計畫定期實施演練，並作檢討及改善。 交通部鐵道局得就鐵路機構所訂應變計畫之內容及定期與不定期演練情形予以查核，如認為辦理不善，應命其限期改善。 鐵路機構辦理第一項通報時，並應依運輸事故調查法同時向國家運輸安全調查委員會辦理通報。	交通部鐵道局得就鐵路機構所訂應變計畫之內容及定期與不定期演練情形予以查核，如認為辦理不善，應命其限期改善。 鐵路機構辦理第一項通報時，並應依運輸事故調查法同時向國家運輸安全調查委員會辦理通報。	

參考文獻

一、政府出版品

1、交通部鐵道局，〈鐵路行車安全通告 111-02〉，111 年 9 月。

二、期刊論文

1、程法彰、洪婺媛，〈美國在資訊時代中對關鍵基礎設施保護架構與資訊分享議題初探及我國的借鏡〉，《前瞻科技與管理》，第 3 卷，第 2 期，102 年 11 月，頁 119-137。
2、傅上哲，《工業控制系統的安全事件風險評估》，中原大學資訊工程學系碩士論文，109 年 6 月，頁 13-18。

三、網路資源

1、立法院預算中心，〈交通部、鐵道局及所屬114年度單位預算評估報告〉，113年10月，網址：https://www.ly.gov.tw/Pages/List.aspx?nodeid=55740，最後瀏覽日期：115年6月29日。
2、交通部新聞稿，臺鐵與荷蘭代表團資安交流，強化國際合作及防護韌性，更新日期114年4月18日，網址：https://www.motc.gov.tw/ch/app/news_list/view?module=news&id=14&serno=cf513396-ee06-42e2-a949-34b2578facad，最後瀏覽日期：115年5月20日。
3、柯雨瑞、楊語柔，外國關鍵基礎設施安全維護機制之探討－兼論對臺灣之啟示，柯雨瑞教授網站，網址：https://share.google/hbUUO2elfbyyKh8P0，最後瀏覽日期：115年5月21日。
4、黃彥棻，揭露資安院2.0轉型願景，林盈達以AI築數位長城，

iThome，2026年6月1日，網址：https://www.ithome.com.tw/news/175244，最後瀏覽日期：115年6月15日。

5、黃彥棻，資安不再是IT部門的事，供應鏈韌性與AI治理成企業存續的核心命題，iThome，2026年6月15日，網址：https://www.ithome.com.tw/news/176614，最後瀏覽日期：115年6月22日。

6、經濟日報,臺鐵駁斥無線電遭駭 強調已韌體加密、變更密碼，115年4月30日，網址：https://money.udn.com/money/story/7307/9474922?utm_source=chatgpt.com，最後瀏覽日期：115年5月20日。

7、審計部預決算審核報告查詢平臺,〈交通部推動交通領域關鍵基礎設施資安整備計畫執行情形查核報告〉，112年，網址：https://auditreport.audit.gov.tw/ServerFile/Get/638257052919488014 2f07b3d40d134ffdb0f8f1351a942f22，最後瀏覽日期：115年5月29日。

8、審計部預決算審核報告查詢平臺,〈政府推動國家關鍵基礎設施安全防護執行情形〉，114年，網址：https://auditreport.audit.gov.tw/ServerFile/Get/638926831626648772f39b695028b7468b92edefd5d27ee0ba，最後瀏覽日期：115年6月23日。

9、Cybersecurity and Infrastructure Security Agency (CISA), Cross-Sector Cybersecurity Performance Goals, 2023，網址：https://www.natat.org/wp-content/uploads/2023/05/CPGs.pdf，最後瀏覽日期：115年5月25日。

10、ENISA, Railway Cybersecurity–Security Measures in the Railway Transport Sector, European Union Agency for

Cybersecurity, 2021，網址：https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Railway%20Cybersecurity.pdf，最後瀏覽日期：115年5月22日。

11、Eric D. Knapp & Joel Thomas Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd ed., Syngress, 2015, p.41-55.，網址：https://www.google.com.tw/books/edition/Industrial_Network_Security/tE7VEAAAQBAJ?hl=zh-TW&gbpv=1，最後瀏覽日期：115年6月30日。

12、European Commission, NIS2 Directive: securing network and information systems，網址： https://digital-strategy.ec.europa.eu/en/policies/nis2-directive，最後瀏覽日期：115年5月15日。

13、European Union Agency for Cybersecurity, “Transport,” Cybersecurity of Critical Sectors，網址：https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/transport，最後瀏覽日期：115年5月14日。

14、Joseph Weiss, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, 2010, p.1-15.，網址：https://books.google.com/books/about/Protecting_Industrial_Control_Systems_fr.html?id=ugOsO17iHB8C，最後瀏覽日期：115年6月30日。

15、National Cyber Security Centre (NCSC), Cyber Assessment Framework (CAF)，網址：https://www.ncsc.gov.uk/collection/cyber-assessment-framework, 最後瀏覽日期：115年5月26日。

16、National Institute of Standards and Technology (NIST), The

NIST Cybersecurity Framework (CSF) 2.0, February 26, 2024，網址：https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf，最後瀏覽日期：115年6月18日。

17、Robert M. Lee, Michael J. Assante & Tim Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (E-ISAC) & SANS Industrial Control Systems, March 18, 2016, p.3-5.，網址：https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf，最後瀏覽日期：115年6月24日。

18、Transportation Security Administration (TSA), Security Directive 1580/82-2021-01C: Enhancing Public Transportation and Passenger Railroad Cybersecurity，網址：https://www.tsa.gov/sites/default/files/security_directive_1580-21-01c_and_memo_508c.pdf，最後瀏覽日期：115年5月23日。

附錄：「鐵道公共運輸關鍵通訊系統資安防護法制問題研析」專題研究報告（初稿）座談會紀錄及參採情形

時間：115 年 7 月 17 日（星期五）下午 2 時

地點：立法院法制局 305 會議室

主席：呂組長文玲　　紀錄：林琪蓉

參加人員：

一、學者專家

中央警察大學國境警察學系		柯教授雨瑞

二、交通部

公共運輸及監理司	科長	侯政傑
	技士	余國安
交通科技及資訊司	分析師	陳建宏
鐵道局	分析師	林振芳
	幫工程師	范修誠
台灣高速鐵路股份有限公司	副理	鄒佳樺
國營臺灣鐵路股份有限公司	助理管理師	陳靜慧

三、本局出席人員

蔡研究員琮浩

黃副研究員薇蓉

林助理研究員淑靜

發言要點：

中央警察大學國境警察學系柯教授雨瑞：

本報告體系完整、邏輯嚴密，並具備前瞻性的風險意識，如供應鏈管理與委外治理等，以下針對報告內容及未來制度修正，提出幾點具體建議：

一、強化資安即行安之跨部會雙軌即時通報與聯合演練機制

現行法制下，資安事件由資通安全管理法體系管轄，行車事故則由鐵路法第 40 條管轄，呈現雙軌並行、缺乏橫向交集的治理盲區，當高鐵、臺鐵無線電遭盜接或惡意干擾時，鐵路機構可能僅視為一般通訊異常而按月彙報，無法在第一時間觸發國家級資安聯防與應變機制。具體建議如下：

(一)修正鐵路行車規則：鐵道法規過去偏重實體安全，有關重大行車事故與異常的定義，皆為物理性與實體性事故，如車輛碰撞、脫軌與火災等，缺乏對資安防護之具體規範，建議將關鍵通訊系統受破壞、干擾、冒用或未授權控制，致影響行車安全者，明定為即時通報之異常事件，打破行政通告之法律位階不足問題。

(二)建立跨部會通報：一旦發生該類事件，鐵路機構同步向交通部鐵道局（國家運安會）及數發部資安署（T-ISAC/T-CERT）進行雙軌通報，並由交通部與數發部定期舉辦跨部會的實兵聯合攻防演練，減少實務運作出現灰色地帶。

二、完備 OT 資安管理體系與檢驗授權

現行鐵路法第 41 條僅概括授權鐵道局檢查鐵路機構之「工程、材料、營業、運輸」等項目。鐵道局現有的鐵路檢查員多屬土木、機電、營運專業，普遍缺乏 OT 與 ICS 的資安稽核與技術查核能力，導致資安檢查流於形式或僅能檢查 IT

帳號密碼。具體建議如下：

(一)完備法規授權：於鐵路法第 41 條或相關授權子法中，明確將關鍵資訊及操作科技系統之資安防護措施，列為法定檢查項目，範疇應涵蓋身分驗證、加密管理、異常訊號監測及弱點修補紀錄。

(二)引進外部技術專家與評估架構：為避免臺鐵及高鐵球員兼裁判，鐵道局實施定期或不定期檢查時，建議引進國家資通安全研究院（以下簡稱資安院）或獨立第三方專業機構協同查察，進行客觀資安檢測與完善評估。

(三)導入國際成熟評估工具：參考美國聯邦公共運輸局（Federal Transit Administration, FTA）CATT（Cybersecurity Assessment Tool for Transit, CATT）框架，以及美國國家標準技術研究所（National Institute of Standards and Technology, NIST）所提出網路安全框架（Cybersecurity Framework, CSF），進行動態、即時、可量化之軌道運輸實體專屬評估工具。

三、參考日本安全指令實務作法

建議交通部可參考日本模式，將操作性的技術細節，定義於行政裁量/安全指南中，以保持技術更新的彈性。爰日本國土交通省（Ministry of Land, Infrastructure, Transport and Tourism, MLIT），依據網路安全基本法（サイバーセキュリティ基本法）與 ISO/IEC 27001 標準，訂定鐵道領域確保資訊安全之安全指南（鉄道分野における情報セキュリティ確保に係る安全ガイドライン），其核心重點如下：

(一)管理階層責任：規範管理階層建立資安防禦架構的法定義務，並訂定應急計畫。

(二)專職資安角色：明確設立首席資訊安全官（Chief Information Security Officer, CISO）、資安主導員與電腦資安事件應變小組（Computer Security Incident Response Team, CSIRT）。

(三)供應鏈與委外控制：管理委外廠商與軟硬體供應鏈的資安管控。

參採情形：

一、第一點意見，建立跨部會雙軌即時通報與聯合演練機制部分，與本報告建議強化鐵路法與資通安全管理法銜接體系之方向一致。至於建立跨部會即時通報機制及定期辦理聯合演練，涉及主管機關行政協調及實務運作，相關意見錄供參考。

二、第二點意見，建議完備 OT 資安管理體系及檢查授權部分，現行鐵路法第 41 條第 1 項規定：「交通部鐵道局應定期及不定期，派員檢查地方營、民營及專用鐵路之工程、材料、營業、運輸、財務、會計、財產實況及附屬事業之經營等情形……」，而號誌設備、通訊設備、行控系統等，係屬工程、材料及運輸安全之一環，鐵道局辦理相關資安檢查已有一定法源基礎。惟為強化法制明確性及因應 OT 資安管理需求，建議可評估於第 41 條或相關授權子法中，明定關鍵資訊及 OT 系統之資安檢查事項，並得視需要引進第三方專業機構協助辦理資安稽核或評估，以兼顧法制完整性及保留主管機關制度設計之彈性。另有關導入國際成熟評估工具部分，CATT 及 NIST 網路安全框架可作為主管機關辦理鐵道 OT 資安檢查、風險評估及建立技術指引之參考；惟相關工具之採用及具體評估方式，涉及技術規範及實務執行事項，宜由主管機關依鐵道系統特

性及資安風險評估結果妥為規劃，相關意見錄供參考。

三、第三點意見，建議參考日本安全指引實務作法部分，與本報告主張於鐵路法第 40 條明定資通安全事件應納入應變計畫基本要求之方向一致。至於通報標準、演練情境、危害辨識、復原程序、改善追蹤、資安組織及供應鏈管理等執行細節，後續得由主管機關透過授權命令、安全指引或相關行政規範予以補充，以兼顧法律規範之穩定性及資安技術更新之彈性，相關意見錄供參考。

交通部公共運輸及監理司侯科長政傑：

一、針對近期高鐵無線電訊號受干擾事件，行政院國土安全辦公室、內政部警政署（下簡稱警政署）及數位發展部資通安全署（下簡稱資安署）等相關單位已高度關注並提出專業防範建議。本部後續將積極配合落實相關防治作法並精進緊急應變措施。

二、現行鐵路法及鐵路行車規則已明定鐵路機構須建立安全管理系統，針對潛在事故風險預先訂定防範與應變機制。面對外界關切之「無線電入侵」等新型態資安與通訊風險，本部將持續研析國內外相關經驗與輿情反映，全面盤點檢討並滾動修正防範機制，以充實整體鐵路安全法制規範。

參採情形：

一、第一點意見，主管機關說明已與國安會、警政署及資安署等機關協調研擬後續防治與應變措施，並規劃辦理資安宣導及演練與本報告建議強化跨部會合作及資安演練之方向一致，

相關意見錄供參考。

二、第二點意見，主管機關說明現行鐵路行車規則已要求鐵道機構建立安全管理機制及事故應變措施，並將就無線電受干擾等新型態風險，參考國外經驗及實務運作持續檢討防範機制。本報告問題研析與建議第一點提出將資通安全事件納入鐵路安全管理及應變計畫，並因應無線電干擾等新型態風險，持續精進相關安全管理規範及應變機制，以提升鐵道關鍵通訊系統之韌性，與主管機關持續精進安全管理機制之規劃方向一致，相關意見錄供參考。

交通部交通科技及資訊司陳分析師建宏：

一、有關柯教授建議參考日本安全指令實務作法設置專職資安角色乙節，依資通安全管理法第 23 條規定，特定非公務機關應設置資通安全長，目前臺鐵由副總經理層級擔任，高鐵則由營運副總經理層級擔任，編制上均已符合法規。

二、現行資通安全事件通報應變及演練辦法已將資安事件分為一至四級，其中三及四級為重大資安事件。公務機關知悉資通安全事件後，應於 1 小時內至主管機關指定之系統平臺通報，實務上已有嚴謹的審核與把關機制。

三、有關建議資通安全法明定 OT 領域防護乙節，資通安全責任等級分級辦法第 11 條第 2 項略以，特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。依據前揭規定，本部於 111 年已訂定交通部交通領域工業控制系統資安防護基準，另因應 114 年資通安

全管理法修法，本部於今年已啟動修改前述基準，並請團隊研擬納入與無線電通訊有關之防護基準。

參採情形：

一、第一點意見，主管機關說明目前臺鐵及高鐵均已依資通安全管理法第 23 條規定設置資通安全長，編制上已有相關規範。柯教授建議參考日本制度，主要係作為強化鐵道領域資安治理及安全管理機制之比較法參考，相關意見錄供參考。

二、第二點意見，主管機關說明現行資通安全事件通報應變及演練辦法已建立資通安全事件分級、通報及演練制度，並規定公務機關知悉資通安全事件後，應於 1 小時內完成通報，實務上已有相關通報及應變機制。本報告所提通報制度銜接建議，詳見柯教授雨瑞發言意見項下參採情形之第一點，相關意見錄供參考。

三、第三點意見，依資通安全責任等級分級辦法第 11 條第 2 項規定，交通部已於 111 年訂定交通部交通領域工業控制系統資安防護基準，並已啟動修正作業，規劃將無線電通訊相關防護基準納入規範，顯示交通領域 OT 系統已有專屬防護基準可資依循。本報告建議係認為，未來仍宜持續檢討鐵路法、資通安全管理法及相關技術規範間之制度銜接，並依鐵道 OT 系統特性，採風險導向及分級管理方式，兼顧資通安全與行車安全，相關意見錄供參考。

交通部鐵道局林分析師振芳：

一、引進第三方與演練機制部分，建議未來召開相關會議時，可

邀請數位發展部、資安署及資安院等技術主管機關共同參與。

二、 修法建議部分，目前的資通安全管理法實務執行上，各機關通常仍偏重於 IT 管理，而忽略 OT 系統。以捷運與鐵路系統為例，許多號誌系統與列車控制等營運系統，在設計上屬於封閉式網路，但其使用的可能是極舊的系統，如嵌入式 Windows XP，且幾乎無法更新。建議於鐵路法中強化實體與資安防護外，資通安全管理法也應進一步將 OT 範疇與規範明確化，避免各機關在執行時，僅將資安資源投放於 IT 系統，忽略高行車安全風險的 OT 系統。

參採情形：

一、第一點意見，建議未來召開相關會議時，邀請數位發展部、資安署及資安院等機關共同參與，與本報告建議強化跨部會協調及資安聯防機制之方向一致，相關意見錄供參考。

二、第二點意見，主管機關說明目前資通安全管理法實務執行上，資安管理仍多著重於 IT 系統，鐵路號誌與列車控制等 OT 系統之資安治理及管理範圍尚有明確化空間。另資通安全管理法及相關子法是否明確納入 OT 系統管理規範，以及如何依鐵道 OT 系統特性建立相應管理機制，未來可作為法制檢討之參考，相關意見錄供參考。

台灣高速鐵路股份有限公司鄒副理佳樺：

一、高鐵目前已落實雙軌通報：若發生影響營運事件，一班列車超過 15 分鐘或五班列車超過 5 分鐘，即會立刻通報鐵道局；後若確認為資安事件，亦會於知悉後 1 小時內通報至交通部

的資通安全通報應變網站。

二、高鐵已配合交通部訂定的交通領域工業控制系統防護基準，針對 OT 系統落實控管。但實務上，部分公共系統或封閉式 OT 系統，由於軟硬體系統限制與供應商技術綁定，確實無法隨意變更或更新，這在實務管理上必須予以適度評估。

參採情形：

一、第一點意見，高鐵說明目前已建立資安事件及行車事故雙軌通報機制，對於影響行車之事件及資通安全事件，均已依相關規定辦理通報。與本報告建議強化資安事件與行車安全事件通報及應變機制之方向一致，相關意見錄供參考。

二、第二點意見，高鐵說明已依交通部訂定之交通領域工業控制系統資安防護基準，落實 OT 系統資安管理。至於部分公共系統或封閉式 OT 系統，因軟硬體限制與供應商技術綁定，相關更新及維護措施仍須兼顧系統穩定性及營運持續性；有關交通部交通領域工業控制系統資安防護基準及後續修正方向，詳見交通部交通科技及資訊司陳分析師建宏發言意見項下參採情形之第三點，相關意見錄供參考。

國營臺灣鐵路股份有限公司陳助理管理師靜慧：

一、臺鐵自民國 94 年起導入 ISO 27001 資訊安全管理系統，目前已進入第 7 輪的 3 年期驗證循環，制度運作十分成熟，且定期接受交通部、數位發展部資安署及鐵道局實地稽核。

二、經評估，臺鐵 4 月 30 日發生無線電受干擾事件（無線電發話）僅屬於通訊層面的訊號誤觸/個案干擾，性質上與資安干擾（系

統入侵或數據竄改）不同，且鐵路行車系統具備失效趨於安全（Fail-Safe / Fail-to-Safe）的最高安全設計原則，系統失效時會自動採取最安全的方式(如停車)處理，不致產生重大災害。

三、為因應未來量子電腦發展對密碼學帶來的衝擊，美國情報界已著手因應後量子密碼學（Post-Quantum Cryptography, PQC）之威脅，屆時現有加密算法皆可能被破解，鐵道通訊與資安系統亦須維持前瞻與持續進化的能力。

四、鐵路運轉系統中，許多號誌及通訊系統是向國外系統商（如法商、德商）整套採購的封閉系統，實務上難以由臺鐵單方面進行系統升級，且多數營運單位在盤點資安資產時，往往不自覺地將這類 OT 設備排除在外。這確實是未來在資安管理與修法上需要共同突破的盲點。

參採情形：

一、第一點意見，臺鐵說明自 94 年起導入 ISO 27001 資訊安全管理系統，目前已建立持續驗證及定期稽核機制，並接受交通部、資安署及鐵道局等機關之實地稽核，顯示現行資訊安全管理制度已有相當運作基礎。本報告建議係在既有制度上，進一步強化鐵道關鍵通訊及 OT 系統之風險辨識、檢查與應變機制，相關意見錄供參考。

二、第二點意見，臺鐵說明本次無線電受干擾事件，經評估屬通訊訊號誤觸或個案干擾，與系統入侵及資料竄改等資通安全事件之性質有別；另鐵路行車系統採取失效趨於安全之設計原則，於系統異常時得以停車等安全方式處理。本報告係考量無線電干擾仍可能影響行車調度、資訊傳遞及營運秩序，相關風

險辨識、通報及應變機制宜持續檢討，以提升鐵道通訊系統之整體韌性，相關意見錄供參考。

三、第三點意見，臺鐵指出量子運算技術之發展，可能對現行密碼技術及通訊安全產生影響，鐵道通訊與資安系統宜持續關注後量子密碼技術之發展及國際因應趨勢。鑑於相關技術及標準持續演進，可作為鐵道資安前瞻治理及中長期技術更新規劃之參考，相關意見錄供參考。

四、第四點意見，臺鐵說明部分鐵路號誌及通訊系統係向國外廠商整體採購之封閉式系統，營運機構難以自行升級，且實務上可能未完整納入資通安全資產盤點範圍。至於封閉式 OT 設備之更新限制及補償性安全措施，詳見交通部交通科技及資訊司陳分析師建宏發言意見項下參採情形之第三點；有關 OT 系統管理範圍及相關法制檢討，詳見交通部鐵道局林分析師振芳發言意見項下參採情形之第二點。另供應鏈風險管理及 OT 資產完整盤點，亦可納入後續制度檢討，相關意見錄供參考。

蔡研究員琮浩：

一、報告初稿提及：「歐盟網路安全局（European Union Agency for Cybersecurity，以下簡稱 ENISA）指出，網路與資訊安全指令第 2 版（Network and Information Systems 2 Directive, NIS2）旨在強化運輸部門資安，以保護航空、海運、鐵路及道路運輸等關鍵基礎設施……」，惟查 NIS2 為 NIS Directive 之修正提案，NIS2 旨在加強全體歐盟網路安全，以統一的法律框架維護歐盟 18 個關鍵領域之網路安全；要求歐盟成員國必須要

求監管各國關鍵基礎建設與服務，包括能源、交通、醫療、金融、水資源管理、數位基礎設施、公共電子通訊提供者、數位服務（如社交平臺）、廢棄物與廢水管理、關鍵產品製造、郵政與快遞服務，及中央與區域層級的公共行政甚至太空領域，同時要求中大型企業必須採取適當的網路安全風險管理措施，並在發生重大資安事件時有效通報，運輸部門資安僅為其領域之一。為免造成讀者誤解，建議針對 NIS2 之說明略做補充調整。

二、承上，報告初稿提及 NIS2 將將運輸部門列為重要及關鍵「實體」之一。檢視本報告之內容，亦有多處提及關鍵「實體」，惟關鍵「實體」與關鍵「設施」（infrastructure）是否相同？建議釐清前述二者之異同並予修正。

三、報告初稿之「補丁管理（Patch Management）」為較通俗之慣用語，建議修正為修補程式管理。

參採情形：

一、第一點意見，業針對 NIS2 說明略做補充，已參採修正。

二、第二點意見，NIS2 所稱關鍵實體（Critical Entities）之制度內涵及適用範圍，較我國資通安全管理法所稱關鍵基礎設施更廣，兩者並不完全相同。本報告係以我國法制架構為論述主軸，爰用語與我國現行法規保持一致；另文中所稱實體運作、實體影響性及實體運作風險等，係指系統之實體運作（physical operation）情形，相關意見錄供參考。

三、第三點意見，在 ICS 及 OT 實務領域中，「Patch Management」

常直接譯為補丁管理，修補程式管理亦為常見譯法之一；惟本報告係參酌國際 OT 及 ICS 相關文獻，其多使用補丁管理（Patch Management）之譯法，並於首次出現時併列英文原文，以利讀者理解，爰維持原用語，相關意見錄供參考。

黃副研究員薇蓉：

一、本報告初稿參考歐盟（NIS2 指令與 ENISA 專門報告）、美國（第 14028 號行政命令與 TSA 資安指令）與英國（NCSC 與 CAF 框架）等外國立法例，就其在關鍵基礎設施與運輸部門資安治理之法制與監理實務，以及「強化雙軌法制銜接」與「依操作科技系統特性具體化管理要求」等面向，針對鐵道公共運輸關鍵通訊系統，提出具體務實之建議，非常值得贊同。

二、本報告初稿問題研析與建議第六點，指出未來宜檢討交通部依據資通安全管理法第 24 條、第 25 條所賦予之相關權限，在鐵道主管機關資安分級與重大事件認定標準中，是否納入「影響鐵道行車安全或營運秩序」之因素。然而，就長遠而言，考量鐵道安全之整體系統性風險，爰進一步建議未來可以檢討運輸事故調查法，對第 2 條之重大運輸事故重新定義，打破「造成一定數量之人員傷害、死亡或財物損害才進行調查」之傳統思維，進而將「重大網路攻擊與電磁干擾事件」正式納入國家運輸安全調查委員會的法定調查範圍。

三、本報告初稿問題研析與建議第七點，從鐵路法屬運輸安全之特別法，而資通安全管理法係屬通案性法律；爰認為兩法應採分工與制度銜接，並說明修法應以鐵路法第 40 條第 4 項為重點，以補充行車安全面向之管理機制。此外，亦指出，近年鐵道

公共運輸系統高度數位化，資安事件已可能衝擊行車控制、號誌、調度或無線通訊；爰針對上開問題提出具體修法建議，明文將資通安全事件所致系統異常之「應變處置、危害辨識、復原作業及改善追蹤」納入應變計畫與安全管理系統中，此項具體建議，對於健全我國鐵道資安防護與行車安全之實質銜接，極具參考價值。

參採情形：

一、第一點係贊同本報告論點之意見，錄供參考。

二、第二點意見，本報告係以鐵路法與資通安全管理法之制度銜接為研究核心，暫未擴及運輸事故調查法之全面檢討，相關建議錄供參考。

三、第三點係贊同本報告論點之意見，錄供參考。

林助理研究員淑靜：

一、問題研析與建議第四點既已指出，關鍵基礎設施資安治理涉及治理、風險辨識、防護、偵測、回應及復原等整體性管理架構，若僅以一般設備或營運檢查概括處理，恐難以反映資安風險之技術性與即時性。惟現行鐵路法第 41 條僅就工程、材料、營業、運輸、財務、會計、財產實況及附屬事業經營等事項賦予主管機關檢查權，尚難明確涵蓋關鍵通訊系統資安防護措施及相關管理機制之檢查，尤其此類檢查可能涉及系統設定、身分驗證、加密管理、弱點修補、委外維運紀錄、第三方測試資料及其他資安敏感資訊之調取。故如認為有明定主管機關就關鍵通訊系統資安防護措施實施檢查之必要，似宜評估修

正鐵路法第 41 條或另行明定法律授權依據，而不宜僅以鐵路安全管理相關子法處理。惠請補充說明。

二、問題研析與建議第六點建議建立重大資安事件第三方鑑識、專家參與、根本原因分析、改善追蹤及公開說明等程序。惟鐵道關鍵通訊系統資安事件可能同時涉及資通安全管理法之資安事件處理、鐵路法之行車安全監理，以及運輸事故調查法之重大運輸事故調查。因此，所稱第三方鑑識機制究係置於資安事件通報應變程序、交通部或鐵道局之監理查核程序，或運安會之運輸事故調查程序，似宜進一步釐清，並說明其法源依據、啟動要件、鑑識結果之法律效果及與既有程序之關係。

三、問題研析與建議第七點建議於鐵路法第 40 條第 4 項增訂資安應變之規定，惟該項本來的結構係列舉應變計畫應包括之具體應變事項；資安事件所涉通報、應變處置、系統復原及改善追蹤，與該項所列現場處置、旅客疏散、人員救護、運轉調度及搶修救援等事項性質未盡相同，且「危害辨識」較接近事故前之安全管理或風險評估事項。為避免條文結構過於冗長，是否宜評估將資安事件影響行車控制、號誌、調度或無線通訊系統時之通報、應變處置、系統復原及改善追蹤事項，另列為第 40 條第 5 項，現行第 5 項以下順移？

四、文字及格式體例意見如下：註腳 23「同註 20，P.13-15。」宜修正為「同註 21，p.13-15」；註腳 26、參考文獻 17 之「網址：Analysis of the Cyber Attack on the Ukrainian Power Grid (PDF)」不是完整網址，應補正式 URL 或改成可查得的文件出處；參考文獻數字呈現「1. 2.」及「1、 2、…」宜統一。

參採情形：

一、第一點意見，詳見柯教授雨瑞發言意見項下參採情形之第二點，相關建議錄供參考。

二、第二點意見，本報告所稱第三方鑑識，主要係指重大資安事件發生後，於交通部或鐵道主管機關辦理資安事件應變及監理查核程序中，引進具專業能力之第三方協助資安事件技術鑑識，並非取代運安會依法辦理之事故調查；若後續涉及重大運輸事故，仍應依運輸事故調查法辦理，相關建議錄供參考。

三、第三點意見，本報告係參考SMS採行之規劃、實施、查核與改進（Plan Do Check Act, PDCA）安全管理循環思維，將危害辨識、應變處置、復原作業及改善追蹤，視為資安事件自預防、應變至復原改善之完整管理流程，爰建議將相關事項納入鐵路法第40條第4項之應變計畫內容，相關建議錄供參考。

四、第四點意見，已參採修正。

散會：下午 3 時 5 分