

出國報告：（出國類別：考察）

「考察鐵道系統數位化資安技術發展趨勢」 出國報告

服務機關：交通部鐵道局

姓名職稱：	總工程司室	總工程司	彭家德
	營運監理組	副組長	賴美孜
	機電技術組	副組長	李開熙
	機電技術組	科長	林育賢

派赴國家：德國

出國期間：113年7月22日至113年7月31日

報告日期：113年10月

摘要

系統識別號: C11301572

因應 5G 發展、數位化需求以及國際趨勢，為了因應新的挑戰，特別是在數位轉型和智慧鐵道系統快速發展的情形下，傳統資訊安全的技術已明顯不足，本次考察目的是為了藉由收集國外營運技術(Operation Technology, 簡稱 OT)與資訊技術(Information Technology, 簡稱 IT)資安之作法，發展我國關鍵基礎設施相關資安規範及應用、並瞭解資安產業新的趨勢以及標準並國際接軌。

本次赴德國考察的主要目的是研究鐵道系統的資訊安全技術，透過學習德國的先進技術與經驗，希望在發展臺灣智慧鐵道系統時，能更快速與精確地接軌國際資訊安全技術，此次考察將深入探討和學習以下幾個面向：

首先，了解德國的鐵道基礎設施，這議題同時涉及 OT 及 IT 資訊安全技術。藉由探討德國 OT 及 IT 技術狀況，學習德國的 OT 及 IT 架構及相互技術搭配之結合及發展。我們希望能夠在臺灣發展智慧鐵道技術基礎上，強化國內鐵道系統的資安教育訓練以及資安防護能力。

其次，考察內容亦著重於相關國際法規、標準及管理等應用(例如 IEC 62443、TS 50701、IEC63452 等)，這一類的國際標準有些已在歐洲國家全面應用並有廣泛影響力，且德國相關法規之制定亦依循這類國際標準。通過對國際法規的深入探討，我們計畫未來在臺灣智慧鐵道系統的資訊安全推動時，亦須依循相關國際法規來提升資訊安全管理要求。

另外，我們將透過參訪供應商西門子交通股份有限公司公司(SIEMENS Mobility GmbH)，實際了解該公司在智慧鐵道系統的資訊安全方面最新技術與相關解決方案，以作為臺灣未來鐵道資訊安全發展的參考，並與德國的專家進行深度交流，學習他們在應對資訊安全所面臨的挑戰、經驗與策略。

最後，本次赴德國考察將為臺灣智慧鐵道系統推動時，參考引入最新的國際標準、知識、技術及法規，為國內鐵道資訊安全推動帶來先進的安全管理知識與發展機會

目錄

1. 考察概述	1
1.1 考察緣由與目的	1
1.2 考察行程與人員	1
2. 考察過程紀錄	3
2.1 德國西門子交通運輸公司(Siemens Mobility GmbH)	3
2.2 Die Autobahn 公司	26
2.3 楚格峰齒軌鐵路和索道纜車	34
<u> 2.4 德國鐵道系統其他觀察</u>	41
3. 考察心得與建議	48
3.1 考察心得	48
3.2 考察建議	52

附錄

附錄 A1 西門子鐵道資安介紹簡報.....	附錄-1
附錄 A2 資安脆弱性管理說明簡報.....	附錄-7
附錄 A3 鐵路設備安全授權說明簡報.....	附錄-9
附錄 A4 Railigent 介紹.....	附錄-11
附錄 A5 電氣化公路介紹簡報.....	附錄-15

1. 考察概述

1.1 考察緣由與目的

本考察係緣於本局刻執行「建立 5G 智慧鐵道運輸及監理環境計畫」，計畫訂定國內智慧鐵道技術標準規範，將國內鐵道系統相關傳輸標準一致化，並利用 5G 無線傳輸技術作資訊傳遞。為確保資訊傳遞安全及配合未來全國智慧鐵道推動政策方向，爰訂定本次參訪計畫至鐵道系統資訊整合具豐富經驗的德國企業，並針對其系統發展上資訊安全的標準、資訊整合應用與現場實際建置成果為主軸進行深度訪談，為未來我國相關智慧鐵道建設推動策略提供明確方向。

1.2 考察行程與人員

本考察為 113 年 7 月 22 日至 113 年 7 月 31 日共計 10 日行程，各考察單位規劃與議題詳表 1.2-1，本次考察團由本局彭總工程司家德帶隊，率營運監理組賴副組長美孜、機電技術組李副組長開熙及林科長育賢，併同台灣世曦電機部王翔正工程師及台灣西門子公司張尹駿產品與解決方案資安長等 6 人出訪。

表 1.2-1 考察行程與議題

日期	時間	參訪機關	拜訪議題內容
07/22 (一)	22:50	台灣 (航班:華航 CI61)	辦訪行程整理及參訪行前準備作業
07/23 (二)	06:55 13:00	西門子公司 產品與服務資安部 門 (布藍茲維 /Braunschweig)	1. 拜會西門子產品資安部門，了解德國政府在智慧鐵道領域的資安政策及相關法規 2. 調查歐盟鐵道資安標準及相關法規的實施細節。 3. 鐵道資安標準政策及相關法規執行情況。 4. 教育訓練體系分享。 5. 說明我國鐵道業近期的發展以及所面臨的挑戰。
07/24 (三)	10:00	西門子公司 產品與服務資安部 門 (布藍茲維 /Braunschweig)	1. 歐盟法規與軌道資安趨勢分享。 2. 軌道號誌資安、入侵偵測。 3. 單向閘道器於鐵道上的應用案例。 4. 瞭解德國如何參與 ISO、IEC 等國際標準組織的提案及國際標準的協調情況
07/25 (四)	13:00	西門子公司 車輛部門	實地參訪鐵道號誌系統產品的檢測及標準化作業。

		(愛爾朗根 /Erlangen)	
07/26 (五)	13:00	西門子公司 車輛部門 (愛爾朗根/Erlangen)	<ol style="list-style-type: none"> 1. 拜訪車輛部門總部，探討車輛設計暨資訊安全的議題。 2. 數位化產品 Railigent 以及軌道資料平台介紹，相關防護以及經驗分享。 3. 瞭解相關數據分析工具，如何幫助鐵路營運商、維護人員和資產所有者更好地理解和分析資產數據。 4. 瞭解廠商在智慧鐵道應用 Railigent、系統雲端整合、方面的新創技術與資安服務。 5. 針對資安教育訓練，瞭解培育相關人員的過程。
07/27 (六)	09:00	(慕尼黑/Munich)	楚格峰齒軌鐵路和索道纜車體驗與考察
07/28 (日)	09:00	(慕尼黑/Munich)	人員移動行程
07/29 (一)	13:00	Die Autobahn (法蘭克福 /Frankfurt)	因應永續經營與淨零的世界趨勢，參訪德國電動高速公路的實際運作，瞭解如何採用鐵道電力設備應用於運輸卡車上，減少對石油的依賴，以達到低排放的替代方案。
07/30 (二)	11:20	法蘭克福機場 (航班:華航 CI62)	回國
7/31 (三)	06:10	台灣	

2. 考察過程紀錄

2.1 德國西門子交通運輸公司(Siemens Mobility GmbH)

Siemens Mobility GmbH 是西門子集團旗下專注於交通運輸解決方案的子公司，其沿革發展、業務範圍、產品與服務涵蓋了鐵路基礎設施 (Rail Infrastructure)、鐵路車輛 (Rolling Stock)、統包專案 (Turnkey Projects)、電氣化 (Electrification) 及軟體解決方案 (Software Solutions) 等各種與交通事業領域相關業務，並提供廣泛的產品和服務，涵蓋鐵路和公路系統各方面。

此次參訪首個地點為西門子公司產品與服務資安部門，由西門子交通運輸公司之產品與解決方案資安長(Principle Product and Solution Security Officer) - Christian Paulsen 帶領其各專業同仁，分別針對資訊技術發展、現今資安威脅、國際標準、教育訓練及政策管理方法之實務經驗與觀點，進行深度交流，有助於我國對於未來各項鐵道建設推動，能有更全面與更長遠的規劃。Christian 是 SMO 處理歐盟資安韌性法 (EU Cyber Resilience Act, CRA) 的主要窗口，他的協助對於未來台灣軌道資安與歐盟新標準接軌至關重要。本次交流主題重點彙整如下：

(1) IT 與 OT 的差異與合作

傳統上，資訊技術 (IT) 主要專注於數據處理、軟體開發與網路連結，而營運技術 (OT) 則涉及實物控制和系統營運，如鐵路營運中的列車控制、號誌系統等。生命週期也是一大差異，一般 IT 產品生命週期約為 3 到 5 年、軌道 OT 則為 20 至 40 年。這對於營運機構是個非常艱巨的挑戰。

隨著工業物聯網 (IIoT) 的發展，IT 與 OT 的合作將更加緊密，界線變得模糊，如何結合兩種領域的技術，達成數位轉型目標及確保資訊安全極為重要，這種合作需要 IT 和 OT 專業人員相互理解對方的需求和挑戰，尤其是在防範工業控制系統 (ICS) 中的網路攻擊時尤為重要。

德國藉由下列方法來縮小 IT 和 OT 之間的差距，提高整體系統的安全性和可靠性：

建立共同的安全目標

將 IT 和 OT 的安全需求整合統一的安全目標中，確保兩者之間的

安全策略和措施一致。

提升溝通與協調

定期的跨部門會議，確保 IT 和 OT 團隊之間的溝通順暢。分享資訊和安全事件，以便快速回應潛在威脅。

實施網絡分段

將 IT 和 OT 網絡進行邏輯分段，以減少潛在的安全風險和跨界攻擊的可能性。同時，使用適當的防火牆和安全設備保護兩者之間的接口。

制定緊急應變計劃

制定包含 IT 和 OT 的綜合緊急應變計劃，以確保在發生安全事件時，兩個團隊能夠協同工作，快速恢復系統正常運行。

培訓與意識提升

定期對 IT 和 OT 團隊進行培訓，提升對對方領域的理解。增強全員對資訊安全的意識，確保所有人員了解相關的風險和應對措施。OT 資安很重視產業知識的培養，這也是一般資安無法直接跨到軌道 OT 的主要門檻。

使用現代技術

採用現代的安全技術和工具，如入侵檢測系統、威脅情報平台和數據分析工具，來保護 IT 和 OT 環境中的數據和系統。

(2) 全球資訊安全挑戰

當前的全球資訊安全環境愈發複雜，駭客技術不斷演進，攻擊手段日趨精細。特別是在鐵路行業中，關鍵基礎設施的數位化使其成為具高價值攻擊目標。隨著勒索軟體攻擊和進階持續性威脅（APT）的頻繁發動攻擊，促使鐵路營運商不得不加強其網路防禦措施。

歐洲的 NIS2 資安指令等法規不僅對資訊安全提出了更高要求，也迫使企業進行合規性更新，這不僅是技術挑戰，更是法律與經濟層面的壓力，各企業應儘早納入長期規劃。

(3) 標準化與合規的重要性

有關保證鐵路系統安全營運方面的議題，標準化的資訊安全措施至關重要。歐盟的標準，如 NIS2(Network and Information Security)、IEC 62443、TS 50701 甚至最新的 IEC 63452 正在推動鐵路產業全面實施這類安全措施。

標準化不僅有助於確保系統的一致性和可靠性，還能在跨國營運中提高系統的相互操作性。例如，標準化的通訊協定可以確保來自不同供應商的設備無縫協作，避免受限特定廠商，降低了系統整合的難度，並加強其系統的安全性。安全等級的定義，也幫助營運商能更簡便的瞭解軟硬體的防護能力，讓日後的採購與維護作業更簡化。

目前歐盟主要推動的法規為 IEC 62443、TS50701，相關內容簡述如下：

IEC 62443 是一系列專門針對工業自動化和控制系統 (IACS) 資安的標準和規範，由國際電工委員會 (IEC) 制定。該標準旨在幫助企業和組織保護其工業控制系統免受網路威脅。IEC 62443 系列分為四個主要部分，每部分涵蓋不同的資安領域。

TS 50701 是一針對鐵路系統設計的資安標準，基於 IEC 62443 標準框架，專注於鐵路營運環境中的網路安全。它適用於鐵路基礎設施、列車控制系統和其他相關的鐵路電子和通信系統。涵蓋了鐵路系統運行中的關鍵網路安全問題，針對鐵路應用進行了調整，重點強調風險管理、多層防護、通信安全等。該標準在智慧鐵道的發展中至關重要，為列車自動控制、遠程監控和數位化營運提供了可靠的安全保障，確保智慧鐵路系統能夠安全運行，防範日益增長的網路威脅。

(4) 國際合作的重要性

國際合作有助於台灣提升自身的資訊安全結構、強化資訊安全基礎設施，台灣可以從歐洲國家的資訊安全合作實踐中學習(例如:德國和法國在鐵路營運中的資訊安全標準和法規實施經驗)，通過共享威脅情報和安全技術來增強防禦能力。可以與歐洲廠商討論，評估其意願，與台灣學界合作，培養在地學生，一起在台成立針對本地軌道產業的資訊安全營運中心(Security Operation Center / SOC)。藉由此合作，參與國際標準的制定，台灣能更快參與全球鐵路營運的安全體系，除了能持續不斷的培養在地人才外，並能確保本地系統持續在國際市場上維持競爭力。

(5) 國際與跨領域的標準化之影響

以德國為代表的鐵路安全管理標準，已經在歐洲乃至全球產生了

廣泛影響。這些標準為跨國鐵路網路的互操作性提供了可依循的目標，使得不同國家的鐵路系統能夠無縫銜接。例如，歐盟標準（EN 系列標準）中的資訊安全要求，已經成為各國參考的範本，未來可能進一步擴展至亞洲市場。此外，跨領域的協作，特別是在涉及 IT 和 OT 技術並存的領域中，能夠有效解決複雜的資訊安全問題，確保系統的整體安全性。

(6) 政府專責單位擔任督導職責

德國聯邦鐵路機構（Eisenbahn-Bundesamt, EBA）是負責監督和管理德國鐵路系統的政府機構，其職責涵蓋鐵路基礎設施的安全性和營運，包括資訊安全（cybersecurity）在內。隨著現代鐵路系統依賴於數字化和網路技術，EBA 在網路安全方面的監督和管理也變得日益重要。以下是 EBA 在德國鐵路系統有關資訊安全的監督管理職責和作業程序。

EBA 負責確保德國鐵路系統的網路安全，包括：

合規性查核與監管：EBA 會要求鐵路營運商和基礎設施提供商提交定期的網路安全合規報告(包括如風險管理、保護措施、應變計畫、供應鏈安全和事故回應等)，對其網路安全措施進行定期審查或隨機審查，可以包括文件審查、現場查驗和技術測試，確保其遵守與網路安全相關的法規和標準，例如 TS 50701、IEC 62443 等工業控制系統(ICS)的網路安全標準，以及歐盟網路安全指令(NIS Directive)。

評估：對鐵路系統中的網路安全風險進行評估，確保系統設計、操作和維護過程中的網路風險得到了充分的考慮。EBA 可要求營運商提供風險評估報告，依據該報告進行審查和分析，並視結果要求進一步改善；EBA 亦可要求對關鍵基礎設施進行專門的風險評估，以識別和防範潛在的網路威脅。

認證：雖然 EBA 自身並不頒發網路安全認證，但它負責對鐵路系統中的關鍵系統和供應商的合規性進行審查，確保第三方認證符合德國和歐盟的法規要求。營運商和供應商需要向 EBA 提供已取得的網路安全認證或符合性證明，如 ISO 27001 或 IEC 62443 的認證。

安全事件管理與緊急應變：當鐵路系統發生重大網路安全事故時，EBA 也負責對事故的應對進行監督。營運商需要按照規定的流程向 EBA 報告網路安全事故，並提供詳細的調查報告。

EBA 會對事故應對過程進行評估，確保事後的補救措施有效，並

評估系統是否需要進一步強化安全措施。

(7) 政府部門跨單位擔任督導職責

EBA 與德國的聯邦資訊安全局（BSI）合作，確保德國鐵路系統符合德國國家網路安全要求。BSI 提供技術支持，協助 EBA 實施網路安全監管。

有關交流過程紀錄詳圖 2.1-1 至 2.1-12。



圖 2.1-1 資安長 Christian Paulsen 與本次參訪人員合照



圖 2.1-4 西門子交通工廠參訪



圖 2.1-5 西門子交通工廠參訪早期閘柄式轉轍器

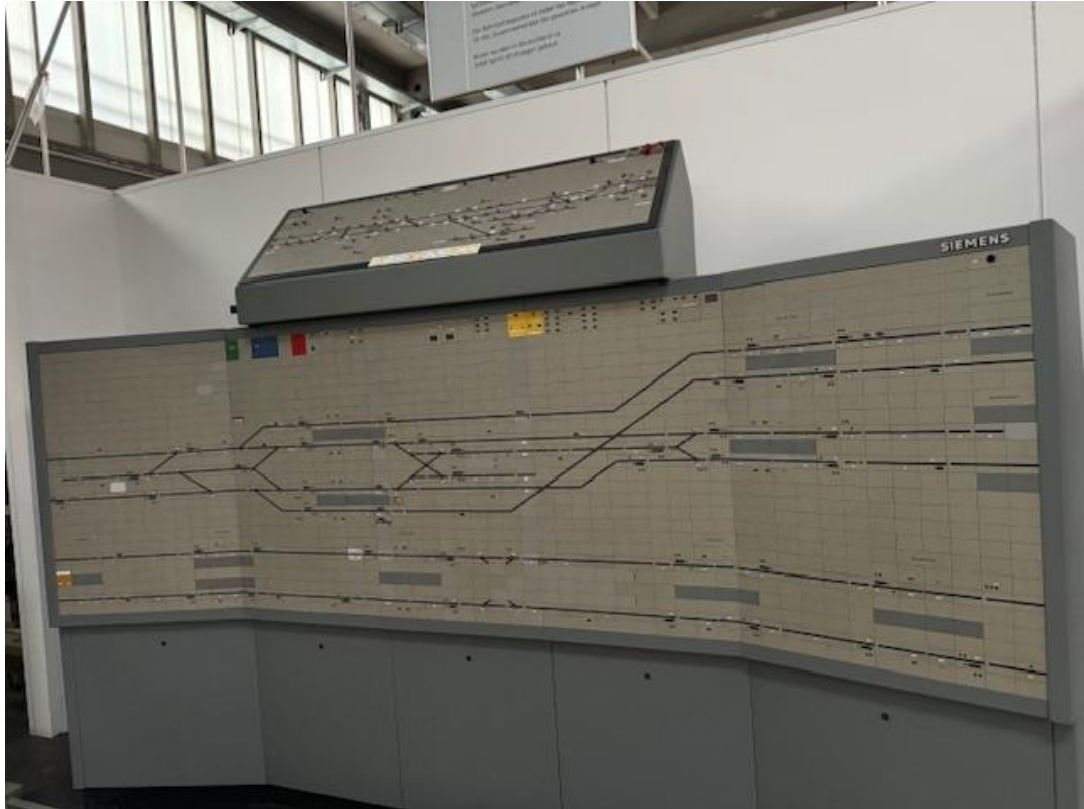


圖 2.1-6 西門子交通工廠參訪早期行車控制盤



圖 2.1-7 禮品相互致贈(Christian Paulsen)

IT Security		OT Security	
Confidentiality			Availability
3-5 years	Asset lifecycle		20-40 years
Forced migration (e.g. PCs, smart phone)	Software lifecycle		Usage as long as spare parts available
High (> 10 "agents" on office PCs)	Options to add security SW		Low (old systems w/o "free" performance)
Low (~2 generations, Windows 7 and 10)	Heterogeneity		High (from Windows 95 up to 10)
Standards based (agents & forced patching)	Main protection concept		Case and risk based

圖 2.1-8 IT 與 OT 主要之差異

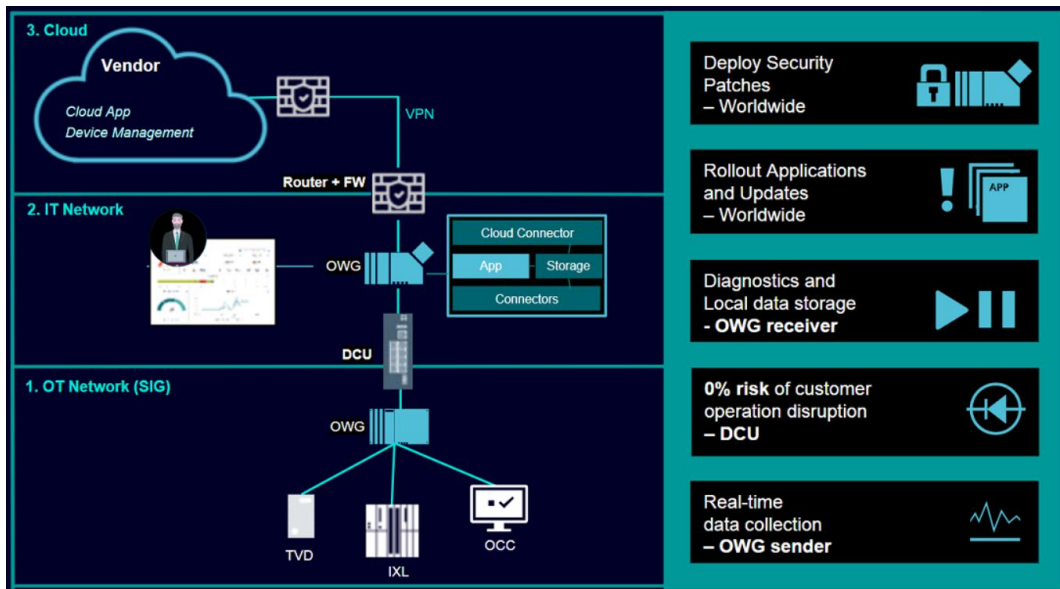


圖 2.1-9 軌道 OT 資安概念圖



圖 2.1-10 測試軌道旁設備介紹(Smart Wayside Object Controller(SWOC))



圖 2.1-11 SMO 布藍茲工廠參訪(內部無法拍照)



圖 2.1-12 高雄黃線設備測試(廠內無法拍照，此為廠區介紹之圖片)

拜訪第 2 個行程位於愛爾朗根的西門子研發基地，該研發基地著重有關能源、醫療、工業自動化和數位化技術領域之核心競爭能力研究。本次由西門子車輛部門成員 Martin Kunz 等人，對於該公司 Railigent 產品之資訊整合應用、資安制度落實與導入、檢測與監控的重要性進行說明，相關重點整理如下：

(1) Railigent 產品特色介紹

Railigent 是西門子基於其 MindSphere 物聯網系統開發專為鐵路行業設計的數位化平台，目的在於提升鐵路系統的營運效率和資產管理。這個平台的核心功能包括預測性維護、資產管理與優化、即時數據分析，以及對鐵路系統的全面監控。

Railigent 能夠利用先進的數據分析技術和機器學習算法，提前預測潛在的設備故障，從而避免營運中斷，並延長設備的使用壽命。平台還能集中管理鐵路網路中的各種資產，通過深入分析來優化這些資產的使用效率，協助營運商制定更明智的維護和更換策略，進一步降低營運成本。Railigent 的模組化設計允許營運商根據自身需求靈活配置不同功能模組，如車輛診斷、軌道監測和能效管理等，從而實現客製化的解

決方案。根據西門子的資料，衍生的效益還有減少延誤成本最多達 15%、提升可用性和可靠性外，藉由數位化也提高了運量。

此外，Railigent 的開放式架構支持與第三方系統和設備的無縫整合，使營運商能夠充分利用現有的技術基礎設施。這對於國內想跨足海外市場的公司是個不錯的機會。藉由在該平台上架的概念，能讓更多國家看到台灣廠商的能力。該平台還提供雲端和本地部署選項，以滿足不同營運商對靈活性和安全性的需求。數據安全是 Railigent 的另一大特點，平台內建的高級安全措施和對國際標準的合規性，確保了敏感數據在傳輸和存儲過程中的安全性。除了提升安全性，Railigent 也關注能源管理，通過對列車運行數據的精確分析，提出降低能耗的建議，幫助營運商減少碳足跡，降低能源成本。此外，隨著全球分工以及法規日趨嚴格，Railigent 也符合目前非常嚴格的資安法規 - European General Data Protection Regulation(GDPR)，嚴格定義哪些個人資訊可以保留、儲存以及運用。西門子對 Railigent 提供持續的技術支持和更新服務，使其始終處於技術領導者，並能夠應對不斷變化的市場需求和技術挑戰。這些特性使得 Railigent 成為全球鐵路營運商提升營運效率和確保安全的關鍵數位化工具。

(2) OT 安全人員培訓的重要性與經濟效益

在工業控制系統 (ICS) 的背景下，針對營運技術 (OT) 人員的專業培訓是保障系統安全營運的基礎。雖然許多企業願意在技術和流程上投入大量資源發展，但如果操作人員缺乏相應的軌道技能和意識，這些投資將無法有效轉化為實際威脅的防禦能力。因此，企業應定期提供針對不同層級的員工與主管培訓課程，從基礎知識到高級應用，以及特定的認證課程，如德國技術監督協會 (TÜV) 的認證課程，這些都能顯著提升員工的資訊安全技能。

目前台灣處理資安大多為資訊相關部門人員主導，但該部門通常不瞭解實際現場的運行狀況，這對於軌道 OT 資安推行是一大挑戰。必須藉由不斷的教育訓練，才能減少兩者的落差。討論的過程中，資安業務經理 - Martine Kunz 也分享了 Network & Information Systems (NIS2) 需注意的義務與責任，例如違反相關資安規定，最高可達 1,000 萬歐元甚至是全球年度營業額的 2%。公司針對新發現的漏洞需要進行協調一致的漏洞披露。管理階層除了需要負責遵守網絡安全風險管理措施外，

也需留意安全事件報告義務，並對報告程序、內容和時間做出處理，這些都在 NIS2 內有更詳細的規定。我國廠商日後如果要進入歐盟市場，這些都是需要提早準備的議題。

(3) 產品和供應鏈安全

在當前的資訊安全環境下，確保產品開發過程中符合資訊安全要求十分重要。然而，關注產品本身的安全性並不足夠，企業還必須確保供應鏈中的每一個環節都符合安全標準。這包括硬體供應商、軟體開發商以至於物流合作夥伴的安全協議落實。隨著供應鏈的全球化，管理供應鏈中的資訊安全風險變得愈發複雜，這包括進行持續的漏洞管理和安全審核，確保供應鏈中的每個元件在整個生命週期內保持安全，尤其是面對老舊且無法汰換的舊系統（Legacy Systems）漏洞時，如何有效管理成為一大挑戰。

參訪期間也介紹了 Charter of Trust 這個協議，這是西門子於 2018 年在慕尼黑安全會議上發起的全球性網絡安全倡議，旨在應對日益增長的數字化威脅並提高數字經濟中的安全標準。由多個跨國企業和政府機構共同簽署，強調建立全球性的網絡安全框架，以確保數位轉型的安全性和信任。Charter of Trust 將網絡安全視為企業與政府的共同責任，倡導公私合作以應對全球網絡安全挑戰。其中一個主要議題便是數位供應鏈安全，旨在確保整個數位供應鏈符合嚴格的安全標準，防範從生產到使用過程中的安全漏洞。另外由於西門子在台灣有執行中的專案，這部分該部門也有針對台灣資安法律進行研究，相關落差日後也需持續討論，便於日後與國際接軌。

(4) 安全與網路安全的協調與平衡

在鐵路營運中，安全性（Safety）和網路安全（Cybersecurity）是兩個互補但又有所區別的概念。安全性通常關注於系統操作的可靠性和穩定性，而網路安全則側重於防範外部攻擊。然而，這兩者在實際操作上經常存在衝突，例如在處理緊急停車指令時，安全性要求系統快速反應，而網路安全則需要進行認證以防止惡意攻擊。因此，企業需要制定協調策略，確保在不影響安全性的前提下，實施必要的網路安全措施。

(5) 管理系統的建立與風險管理

在建立資訊安全管理系統時，企業應將其與現有的工程管理流程緊密結合，而非獨立設立。這樣可以在專案執行中保持一致性和可控性。

風險管理應涵蓋整個產品生命週期，從設計階段的風險識別到營運階段的風險緩解。企業可以採用分層級的風險管理方法，確保風險在各個層級上都得到適當的處理。例如，從單個組件的安全評估，到整個系統的風險分析，這種多層級的方法可以有效降低系統的整體風險。討論過程當中，Christian 也分享了西門子內部 PSS(產品與解決方案資訊安全) 對於風險評估的手法 – TRA(Threat & Risk Analysis)，主要用於系統性地識別安全弱點和漏洞，分析可能利用這些弱點的威脅，並評估由此產生的風險。這對於管理階層，能夠很快的明瞭目前資安的風險點以及是否該從何處投入資源。

(6) 持續更新與管理階層的支持

無論是安全性還是網路安全，系統的需求規範和應用條件都需要隨著技術和威脅的演變而進行持續更新。企業應定期審查和更新其安全政策，以確保其能夠應對最新的安全挑戰。同時，管理階層的參與和支持對於成功實施資訊安全管理至關重要，尤其是在資源分配、策略制定和跨部門協作方面，高層的積極參與能夠大幅提升安全措施的有效性。

(7) 鐵路資安的檢測與監控

A. 事件監測與回應與復原

於鐵路環境建立資安營運中心 (SOC) 或資安卓越研究中心(CoE) 進行資通行為的集中監控和管理網路安全尤其重要。結合產官學一起合作，除了能夠穩定的培養本國的工控資安人才外，與歐洲等資安法規較先進的國家也能長期合作。本國資訊背景數量與能力有一定的優勢，藉由工控能力的提升，有機會在整個軌道工控的人才產業鏈中扮演到關鍵地位。資安營運中心可以全天候監測系統狀態，並在發現異常情況時，及時啟動應急備案，減少潛在威脅對系統的影響。

B. 滲透測試與安全掃描

資安的核心過程包括幾個重要階段：識別 (Identify)、保護 (Protect)、偵測 (Detect)、回應 (Respond) 與復原 (Recover)。首先，通過識別關鍵資產和風險來源，確保企業了解其潛在的威脅。接著，透過保護措施加強防禦，減少弱點被攻擊的機會。一旦威脅出現，偵測技術能快速發現異常，並在回應階段立即採取行動。最後，復原過程確保在攻擊後能迅速恢復營運，減少業務中斷並提升韌性。回應與復原在前一節提到，至於偵測則是各個領域較難的部分，因為會需要融合既有

的產業知識，避免在偵測的過程中，觸發不必要的反應，影響車輛營運。為確保系統安全，可透過滲透測試與安全掃描來檢測系統安全性。這些測試不僅僅是在開發階段進行，而應該貫穿系統的整個營運流程。通過這些測試，可以及時發現並修補潛在的安全漏洞，防止攻擊者利用這些漏洞發起攻擊。另一個重要議題是事後報告的解讀，這角色需要具備鐵道以及資安背景，討論中也拿出 IEC 62443 Part:2-1 (Management) + Part:3-3 (Security-Level) 相關的實際報告進行案例經驗交流。

C. 自動化與工具的使用

在處理大量數據和監控系統安全時，自動化工具的使用變得越來越重要。這些工具可以幫助安全專家聚焦於最具威脅的安全漏洞，提高工作效率，並減少人為錯誤的風險。西門子的產業特性，每天需要在不同工控領域中與多種不同的設備和軟體應用程式合作。由於任何軟體都可能出現漏洞，所以西門子產品開發部門開始思考如何定位和封堵安全漏洞，開始發展工控資安自動化工具，其目標是降低整個資安運作的門檻，西門子使用「SiESTA®」(西門子可擴展安全測試裝置)來測試其產品的安全性，包括已知和未知的漏洞。原本是進行自己內部工廠安全測試，目前現在也將其作為服務提供給終端客戶，來應對其複雜的鐵路系統安全需求。

D. 與雲端技術的整合

此外，Siemens 利用雲端平台 (如 AWS) 提供的強大資訊基礎設施來支持其服務應用運行，這不僅提升了系統的可擴展性和靈活性，也在數據傳輸和存儲過程中提供了強大的安全保護。雲端技術的整合使得 Siemens 的產品能夠更高效地管理和保護其分佈在全球各地的鐵路系統。

有關本次交流過程詳圖 2.1-13 至 2.1-29。



圖 2.1-13 鐵道資訊整合與應用說明簡報



圖 2.1-14 鐵道資訊安全技術說明簡報



圖 2.1-15 禮品相互致贈(Juergen Sept 與 Dr. Michele Barletta)

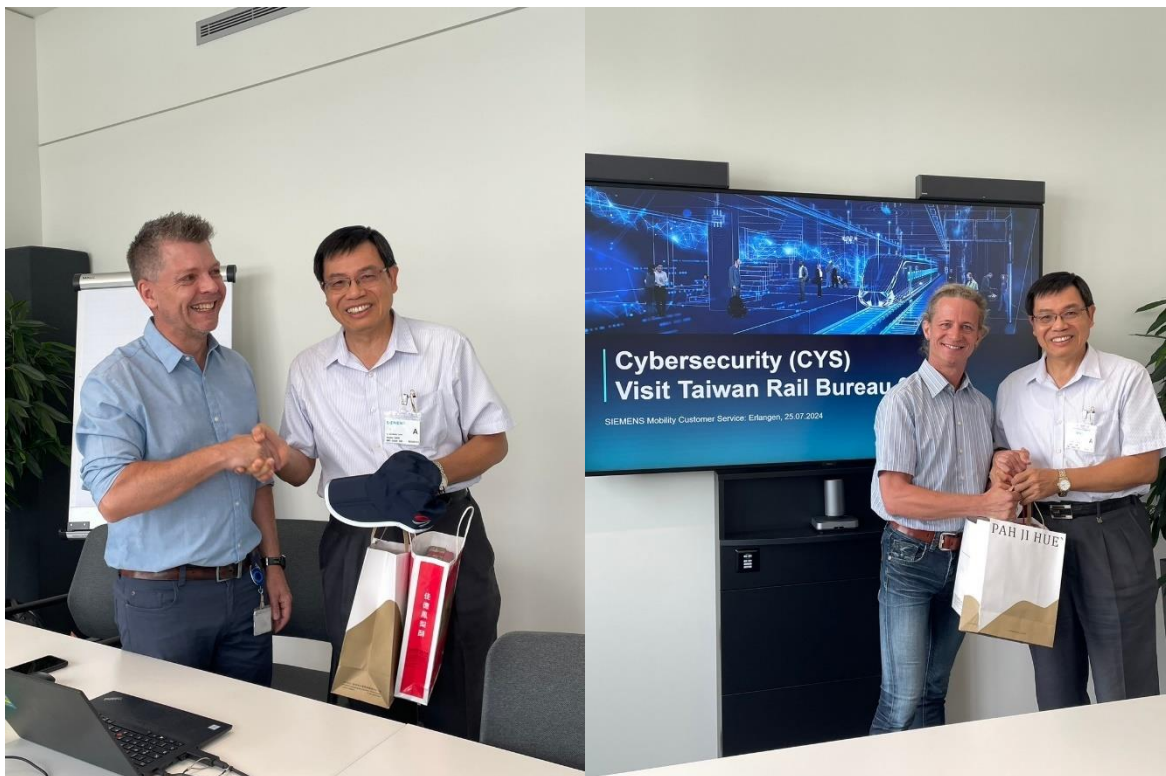


圖 2.1-16 禮品相互致贈(Martin Kunz 與 Christian Kunze)

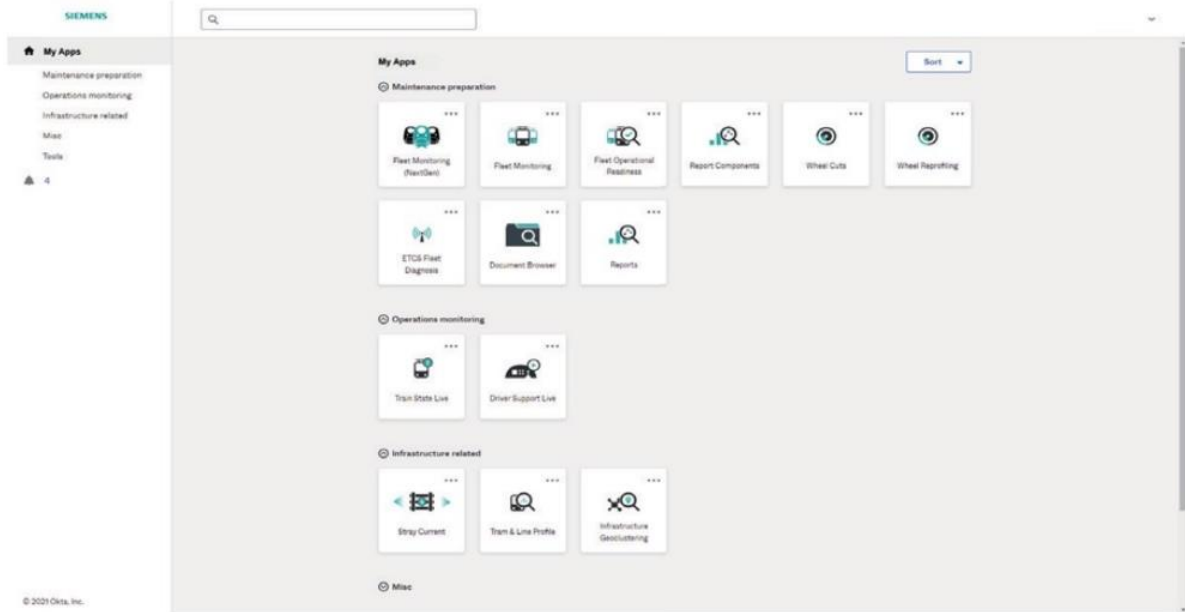


圖 2.1-17 Railigent Application Suite

↓
🔖

Key principles

- 01 Ownership of cyber and IT security
- 02 Responsibility throughout the digital supply chain
- 03 Security by default
- 04 User-centricity
- 05 Innovation and co-creation
- 06 Education
- 07 Certification for critical infrastructure and solutions
- 08 Transparency and response
- 09 Regulatory framework
- 10 Joint initiatives

Charter of Trust

圖 2.1-18 Charter of Trust 協議之主旨

Trend: New regulations, standards and guidelines
 Cyber regulations for critical infrastructure are becoming increasingly stringent



New Directive Network & Information Systems (NIS2)- proposed on 16 December 2020



- Higher fines of up to €10 million or 2% of annual global turnover
- Mandate for information exchange and cooperation
- Coordinated vulnerability disclosure for newly discovered vulnerabilities
- Basic security requirements with a list of targeted actions, including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption
- Focus on cybersecurity in the supply chain
- Responsibility of management for compliance with cybersecurity risk management measures
- Security incident reporting obligations, with more detailed provisions on the reporting procedure, content and timing

圖 2.1-19 NIS2 發布後的相關趨勢

Similar regulations and requirements on standards globally

Taiwanese Cybersecurity Requirement: "Schedule 4: Level-B Cyber Security"

全國法規資料庫

Table: Regulations on Classification of Cyber Security Responsibility Levels

Attachment: History of Rights Affairs (歷史紀錄)

- Schedule 1: Matters to be controlled by the government agency of cyber security responsibility level 1-ppt
- Schedule 2: Matters to be controlled by the government agency of cyber security responsibility level 2-ppt
- Schedule 3: Matters to be controlled by the specific non-government agency of cyber security responsibility level 3-ppt
- Schedule 4: Matters to be controlled by the government agency of cyber security responsibility level 4-ppt
- Schedule 5: Matters to be controlled by the government agency of cyber security responsibility level 5-ppt
- Schedule 6: Matters to be controlled by the specific non-government agency of cyber security responsibility level 6-ppt

圖 2.1-20 針對各國法規的分析

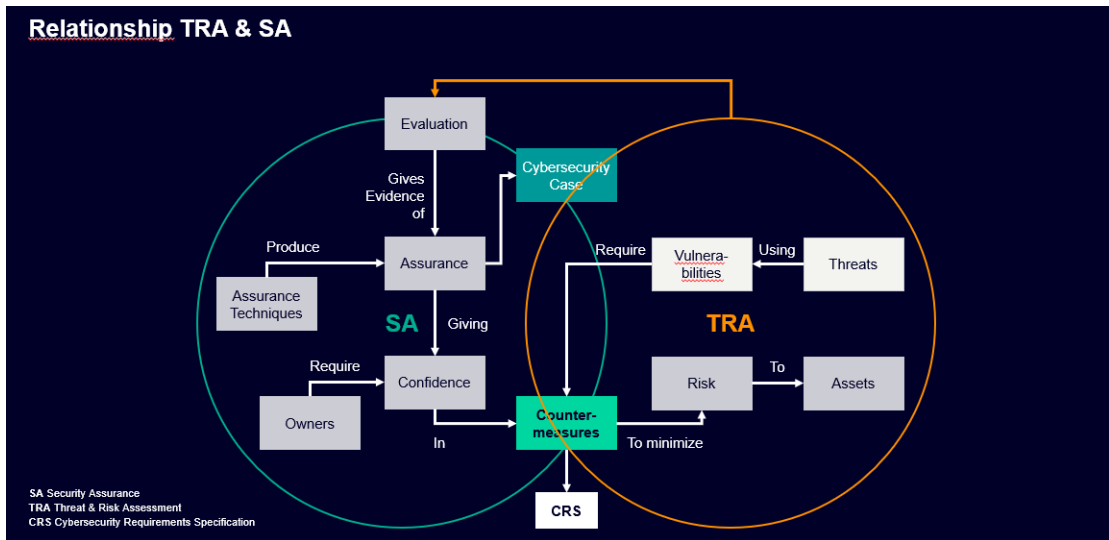


圖 2.1-21 Threat & Risk Analysis 與其他介面的關聯

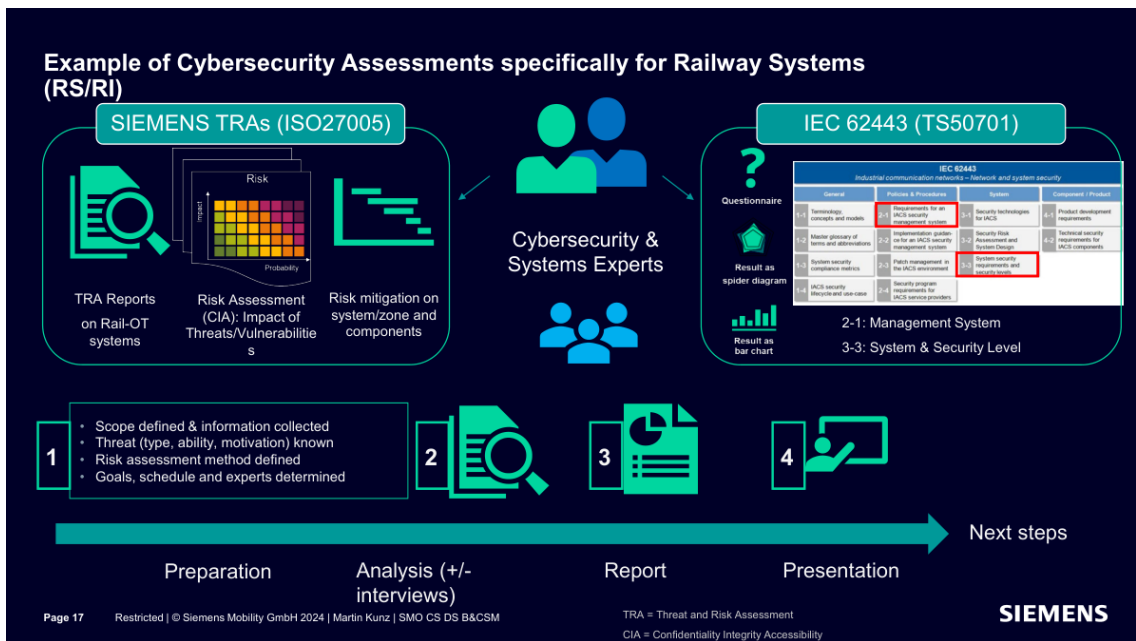



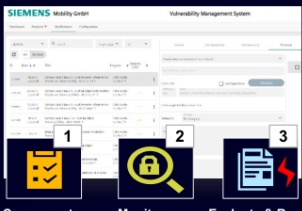
圖 2.1-22 軌道資安安全評估範例

Security Scanning, Vulnerability Management and Intrusion Detection (IDS)




Security Scanning

- Expert-supervised scanning
- Detection of software components, configurations and vulnerabilities
- Detect changes to baseline and security policies
- Reusable scans and "single" report



Vulnerability Management

- Automated tracking of software vulnerabilities
- Risk assessment of exploitability based on system know-how
- Report and risk-based measures Recommendation from experts



Intrusion Detection (IDS)

- SIEMENS OSA for OT Infrastructure
- SecurityGateway and/or RazorSecure for Rail Vehicles
- Signature and AI-based recognition

Page 18 Restricted | © Siemens Mobility GmbH 2024 | Martin Kunz | SMO CS DS B&CSM

SIEMENS

圖 2.1-23 安全掃描、弱點管理與入侵偵測

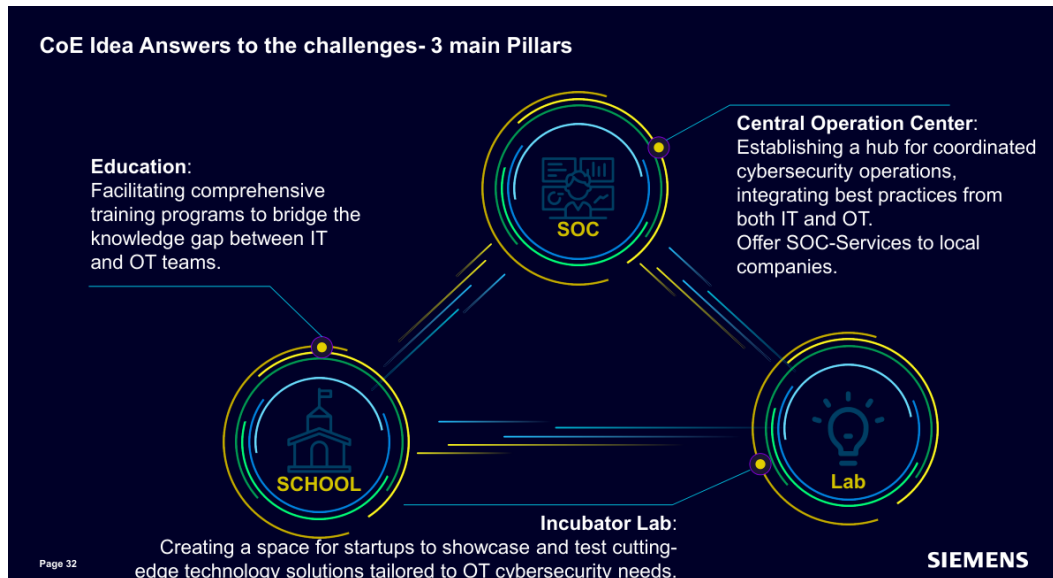


圖 2.1-24 資安卓越中心(CoE)的三大主要角色

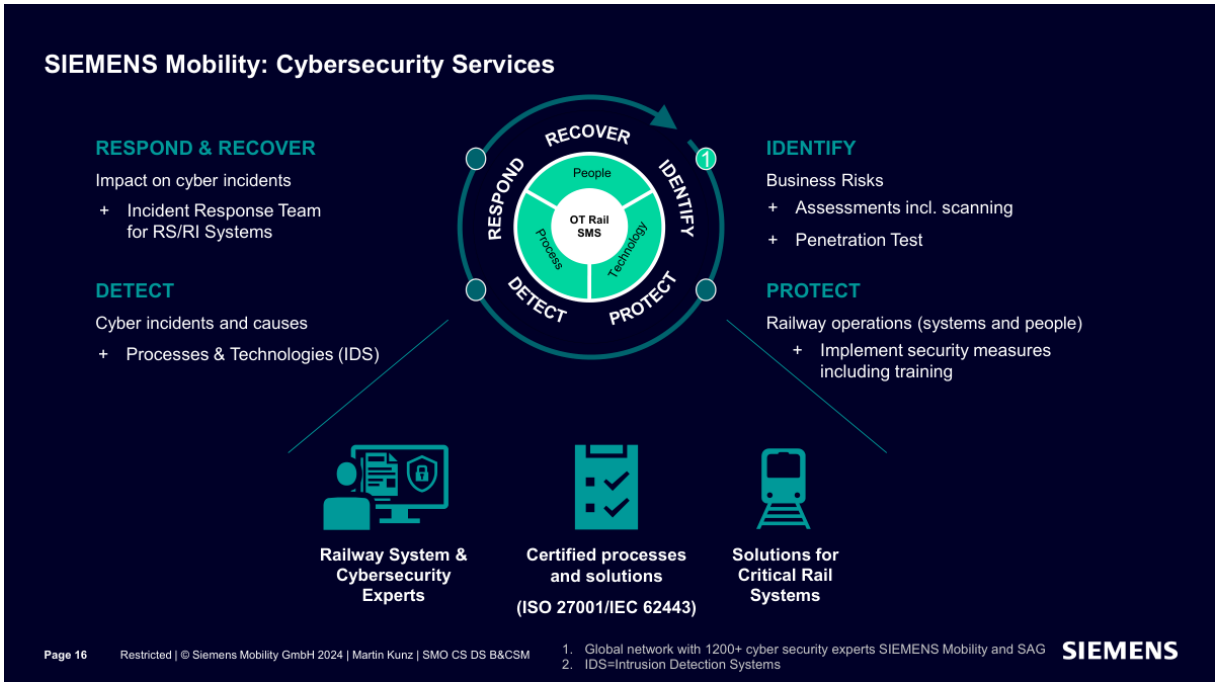


圖 2.1-25 資安服務的主要循環

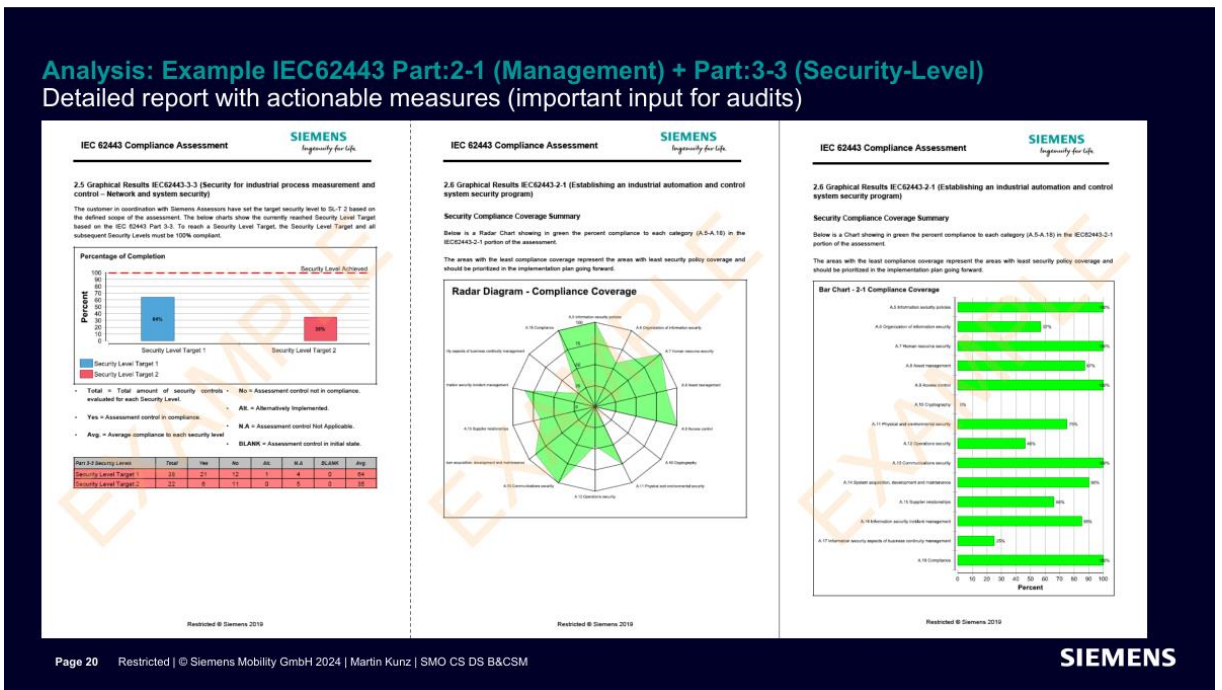


圖 2.1-26 基於 IEC 62443 標準的案例分析

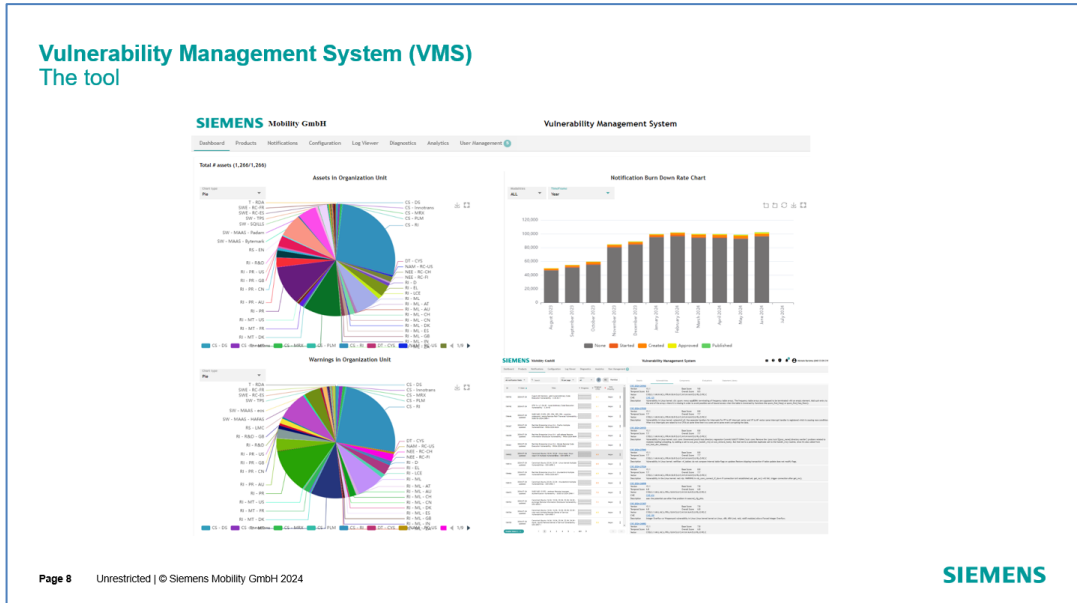


圖 2.1-27 弱點管理案例(Dr. Michele Barletta)

SiESTA® enables Digitalization by addressing typical OT security challenges



Typical OT characteristics	Possible OT security challenges	SiESTA® value contribution
<p>This is OT, not IT</p> <p>OT differs from centrally managed IT and needs a different protection philosophy</p>	<ul style="list-style-type: none"> ▪ Lack of tools, e.g. IT vulnerability detection mechanisms are not designed for OT. ▪ Lack of IT know-how in OT environments, different processes in IT and OT areas. 	<ul style="list-style-type: none"> ▪ A large number of top-of-the-line security tools (both common and commercial) are integrated within a single user interface.¹ ▪ Largely automated processes based on the profound experience of Siemens Cybersecurity experts.
<p>It wasn't built in a day</p> <p>factories have grown to comprise large varieties of hardware & software</p>	<ul style="list-style-type: none"> ▪ Limited transparency since there is hardly ever a complete central register of OT assets. ▪ Complex heterogeneous environment with many different system types and vendors. 	<ul style="list-style-type: none"> ▪ Highly performant non-harmful active scans for rapid asset discovery (performed on-site within 1-2 days). ▪ Detailed asset list with vendor, product model, hardware and software version (with in-depth data for Siemens OT products).
<p>If it's not broken, use it</p> <p>lifecycles of 20+ year lifecycles, frequently beyond end of life dates</p>	<ul style="list-style-type: none"> ▪ Dated, fragile devices may be negatively affected by regular security scans or tools. ▪ Unclear, if it is safe since keeping track of all published vulnerabilities can be overwhelming. 	<ul style="list-style-type: none"> ▪ Excluding devices from asset and/ or vulnerability scans is possible as additional safeguard. ▪ Detection of known vulnerabilities; for Siemens OT products with lifecycle/ patch information & recommended patches.
<p>Availability is key</p> <p>only running OT earns money and one doesn't simply reboot a factory like a PC</p>	<ul style="list-style-type: none"> ▪ Fix what matters most, not every single finding to strike a sound cost-risk-ratio. ▪ Rare patching windows (if any) to avoid both downtimes and updating to a new set of bugs. 	<ul style="list-style-type: none"> ▪ Comprehensive reporting with findings by criticality for risk-based decisions and key findings summarized for management. ▪ Siemens Security Advisories for Siemens OT products (linked in reports) show the software version required for fixing.

¹ License clearing of commercial tools currently in discussion with vendors.



圖 2.1-28 SiESTA 主要的效益

Analysis: Example Security Scanning/Vulnerability Assessment (SIESTA) Detailed report with actionable measures (important input for audits)

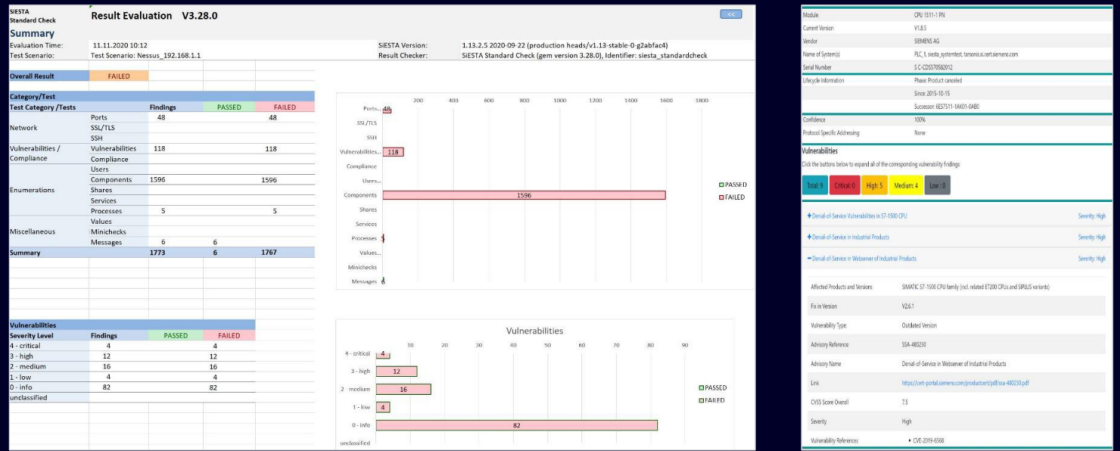


圖 2.1-29 SiESTA 報表演示

2.2 Die Autobahn 公司

德國的高速公路系統「Autobahn」，是世界上最著名的公路網之一，因其部分路段無限速而聞名。Autobahn 的管理和營運由德國聯邦政府的 Autobahn GmbH 負責，該公司成立於 2018 年，專注於維護、營運和未來的基礎設施發展。

本次參訪第 3 個地點為 Autobahn GmbH 公司，負責維運德國高路公路相關設施，本次參訪電氣化高速公路(eHighway)的背景、發起構想、階段成效與未來發展，相關重點整理如下：

(1) 計畫背景

德國推動 ELISA 計畫的背景源於多方面考量。過去 30 年 (1990-2021)，德國的公路貨運量激增 198%，未來 30 年預計還將增長 52%。根據聯邦氣候變遷法，德國運輸部門須在 2030 年前將溫室氣體排放量減少至 8500 萬噸，而商業用車輛約佔 CO2 排放量的三分之一。此外，未來 72.3%的貨運仍將依賴公路運輸。

(2) ELISA 計畫概述

ELISA (電氣化高速公路與創新重型貨運) 計畫自 2017 年啟動，目的在於利用架空線路技術對重型貨物運輸的提升，以實現淨零碳排目標。該計畫包括德國第一條電氣化高速公路 (eHighway) 的建設，並

已分三階段推進。自 2019 年起，測試路段開始運行，2022 年起進行路段延伸。測試主要關注架空電力線的運行可行性、CO₂ 減排效果及安全性等方面。

(3) eHighway 工程與技術合作

eHighway 位於德國 A5 高速公路上，這段繁忙的路段為技術測試提供了理想條件。2023 年，ELISA III 計畫延伸至達姆斯塔特方向，測試路段總長度增至 17 公里。計畫涉及 4 家主要合作夥伴，包括德國聯邦高速公路公司、e-netz Sudhessen AG、Darmstadt 技術大學及 Siemens Mobility GmbH，並有 9 家物流公司參與。這些卡車配備了集電弓和混合動力系統，在實際貨運環境中進行測試，以評估系統的可靠性和能源效率。

(4) eHighway 系統技術概述

ELISA 計畫的測試軌道設有 4 座變電站，提供標稱電壓 670VDC 的電力以支持架空電車線的運行。在 eHighway 上，卡車通過集電弓從架空電車線獲取電力，驅動電動馬達並為車載電池充電。當卡車離開架空線路或變換車道時，可以依靠已充電的電池或混合動力車輛的內燃機繼續駕駛。目前，eHighway 系統中使用三種類型的架空線路卡車：

Type 1：40 噸混合動力卡車，配備 130kW 電動機、18.5kWh 電池，以及柴油內燃機（2019 年投入使用）。

Type 2：40 噸插電式混合動力卡車，配備 260kW 電動機、99kWh 電池，以及柴油內燃機（2022 年投入使用）。

Type 3：26 噸純電池驅動卡車，配備 230kW 電動機及 297kWh 電池（2023 年投入使用）。

eHighway 系統結合了動態充電的效率與公路貨運的靈活性，避免了長時間的固定充電需求。如果使用 100% 可再生能源，該系統有望成為碳中和公路。電力驅動卡車的能量利用效率達 71%，顯著優於氫燃料電池和柴油內燃機，這顯示純電動技術在能量轉換過程中的損失較小。

(5) 動機與挑戰：

隨著德國道路運輸需求的持續增長，特別是在貨運方面，政府即使大力推廣鐵路運輸，道路貨運的需求仍將上升。因此，確保道路貨運的可持續性和低碳化成為當前的主要議題。本專案的主要挑戰在於如何

解決重型卡車的電氣化問題。由於重型卡車需要運載大量貨物，這導致所需電池的體積和重量過大，從而佔用貨物空間並增加運輸成本。因此，專案團隊探索了能否在不依賴大型電池的情況下，通過直接供電來實現卡車的電氣化，以滿足未來交通需求並達到減碳目標。

(6) 技術實施：

專案中提出的技術核心是架空電纜系統，這是一種已在鐵路中廣泛應用的技術。該系統可以讓卡車在行駛過程中通過架空電纜進行充電，這樣不僅能減少對大型電池的依賴，還能保留更多的車輛空間來運輸貨物。本專案探討了如何將這一技術應用於道路運輸，並對比了其他可能的選項，如路面軌道供電和感應充電技術。架空電纜系統的優勢在於它對道路的侵入性較小，施工期間可以維持交通流暢，並且系統易於維護。此外，卡車的「集電弓」技術使得車輛在行駛時可以靈活連接或脫離電纜，這提高了運輸的靈活性和效率。

(6) 初步成果：

自 2017 年專案啟動以來，團隊成功建設了 10 公里長的架空電纜系統，並對其進行了全面測試。在 A5 高速公路的現場試驗顯示，使用 eHighway 系統的重型貨車可以實現無廢氣排放。架空線路卡車能融入物流公司的日常運作流程，並且系統運行安全、堅固且可靠，可用度超過 98%。在 ELISA III 計畫中，長距離充電行為、交接處整合以及隔音牆等問題仍在研析中，並對三種類型的架空線路卡車進行運行評估。

該系統在德國高速公路上運行穩定且安全，並未對交通流量或事故率產生負面影響。專案在營運初期面臨多項挑戰，包括法律問題和施工許可的獲取，但最終成功解決。初步數據顯示，當卡車在行程的 40% 時間內處於架空電纜下方時，能夠實現完全淨零碳排的行駛。同時，動態充電技術允許使用較小的電池，減少了對固定充電設施和停車位的需求，這對解決德國高速公路上貨車停車位短缺的問題具有重要意義。

根據現有測試結果，未來 eHighway 系統有可能擴展至更廣泛的高速公路網，為減少道路貨運部門的碳排放做出重要貢獻。

(7) 未來計劃：

在初步成功的基礎上，專案已進入第三階段，目標是在現有 10 公里的基礎上再延長 7 公里，並進一步測試不同路段和充電技術的整合。未來計劃包括擴展系統的規模，涵蓋更多的高速公路路段，並探索與其

他技術（如氫能和混合動力系統）的結合。此外，專案團隊正在研究如何在更大規模的應用中保持高效營運，包括分段關閉系統以進行維護，而不影響整體交通流量。最終，專案的發現將有助於推動在德國乃至全球範圍內更大規模的「電氣化高速公路」技術應用。

有關本參訪情形詳圖 2.2-1 至 2.2-12。

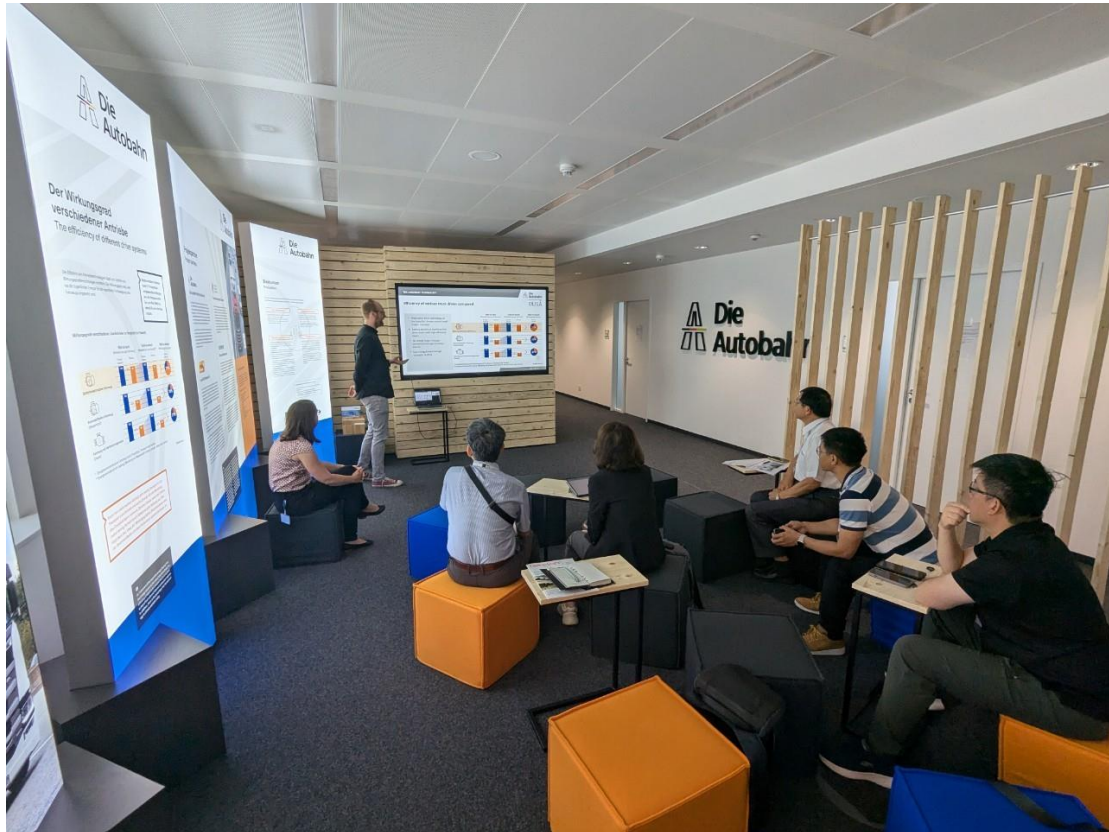


圖 2.2-1 eHighway 說明簡報



圖 2.2-2 eHighway 成員合影(Bianca Martin 與其團隊成員)

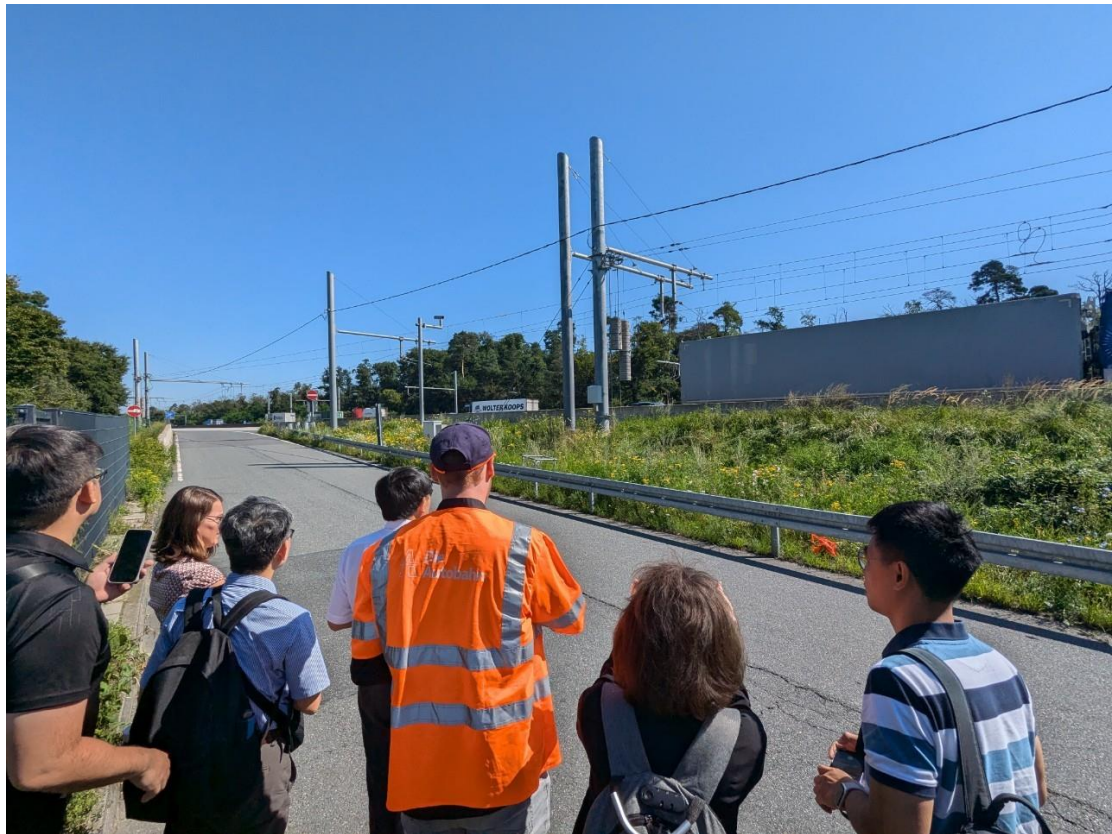


圖 2.2-3 現地參訪



圖 2.2-4 eHighway 於公路上設施配置情形



圖 2.2-5 eHighway 於公路上設施配置情形



圖 2.2-6 eHighway 實際使用的卡車



圖 2.2-7 具集電弓卡車行駛在 eHighway(與一般汽車共用車道)



圖 2.2-8 電氣化高速公路 A5 路段



圖 2.2-9 eHighway 道旁變電站外觀

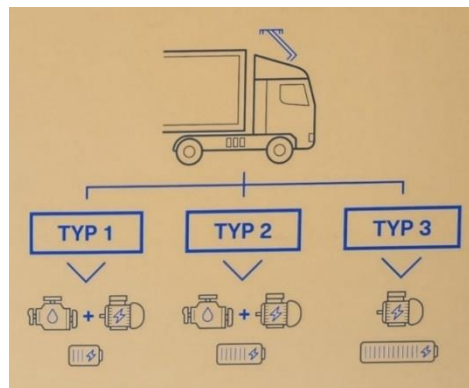


圖 2.2-10 架空線路用之三種類
型之卡車驅動系統



圖 2.2-11 電車線提供電力經車頂集電弓提供電動馬達之動力源



圖 2.2-12 eHighway 貨車的集電弓

2.3 楚格峰齒軌鐵路和纜車

7月27為周末自由參訪行程，主要瞭解德國對於觀光地區開發結合鐵道、纜車系統之應用、對於觀光地點特色發展之構想。

(1) 齒軌鐵路

楚格峰齒軌鐵路是德國著名的齒軌鐵路，連接巴伐利亞州的加米施-帕滕基興(Garmisch-Partenkirchen)與德國最高峰楚格峰(Zugspitze)。這條鐵路是齒軌與普通鐵路相結合的系統，使其可讓列車能夠安全地攀登這座海拔 2,962 米的高山。

該鐵路的建設始於 1928 年，並於 1930 年正式啟用。其主要功能是将遊客從山下的加米施-帕滕基興帶到楚格峰的山頂。這條鐵路的部分路段是普通鐵軌，而在陡峭的山坡上，則採用齒軌技術，以確保列車能夠負擔較大的爬升角度，鐵路全長約 19 公里，齒軌段 11.5 公里中，列車速度較慢，但能夠穩定地爬升至山頂 2,600 米處，終點站楚格峰車站。

(2) 纜車

楚格峰纜車(Zugspitze Cable Car)是世界上技術最先進的纜車之一，以其卓越的工程技術和創新設計而著稱。以下是這條纜車的主要技

術特色：

A. 世界最高的纜車支撐塔

楚格峰纜車的支撐塔高度達到 127 米，這是目前世界上最高的纜車支撐塔。這座支撐塔的設計和施工極具挑戰性，必須在確保結構穩定性的同時，抵抗強風和雪崩等極端氣候條件。

B. 最大的單跨距離

纜車在艾伯湖站與山頂站之間的單跨距離達到 3,213 米，這表示纜車在這段距離內沒有任何中間支撐結構。這樣的設計不僅減少了对自然環境的影響，還提供了無阻擋的視野，使乘客能夠盡享阿爾卑斯山的壯麗景色。

C. 最大的高差

楚格峰纜車從艾伯湖站到山頂站的垂直高差達到 1,945 米，這也是世界紀錄。纜車在短短的 10 分鐘內完成了這一驚人的海拔變化，為乘客提供了快速且舒適的登山體驗。

D. 高承載能力與穩定性

每個纜車車廂可以容納 120 名乘客，並且整條纜車每小時能運送 580 名遊客。這得益於其先進的驅動系統和鋼索技術，鋼索的直徑達到 72 毫米，是目前世界上最粗的纜車鋼索之一，確保了纜車在運行過程中的穩定性和安全性。

E. 全景玻璃車廂

纜車的車廂設計採用了全景玻璃，讓乘客在旅途中能夠享受 360 度無遮擋的視野。車廂玻璃經過特殊處理，可以抵抗高海拔的紫外線輻射，同時提供良好的隔熱性能，保證乘客在任何季節都能舒適地享受景觀。

F. 頂尖的驅動與控制系統

纜車的驅動系統採用了最新的電機技術，能夠提供精確的速度控制和平穩的運行。控制系統配備了多重冗餘設計，以確保即使在極端條件下，纜車仍能安全運行。除此之外，纜車還配備了先進的風速監測系統，可以在風速超過安全限度時自動停止運行，確保乘客安全。

G. 耐候性與環境友好設計

纜車設計考慮了阿爾卑斯山區的極端天氣，所有材料和結構都經過特殊處理，以抵抗低溫、強風和雪崩等自然威脅。此外，纜車的建設

和運行對環境的影響最小化，施工過程中採用了多種環保技術，以保護楚格峰的自然生態。

有關本參訪圖像記錄詳圖 2.3-1 至 2.3-7。



圖 2.3-1 齒軌鐵路及其列車



圖 2.3-2 齒軌鐵路轉轍器



圖 2.3-3 齒軌鐵路轉轍器



圖 2.3-4 齒軌鐵路結構



圖 2.3-5 齒軌鐵路結構

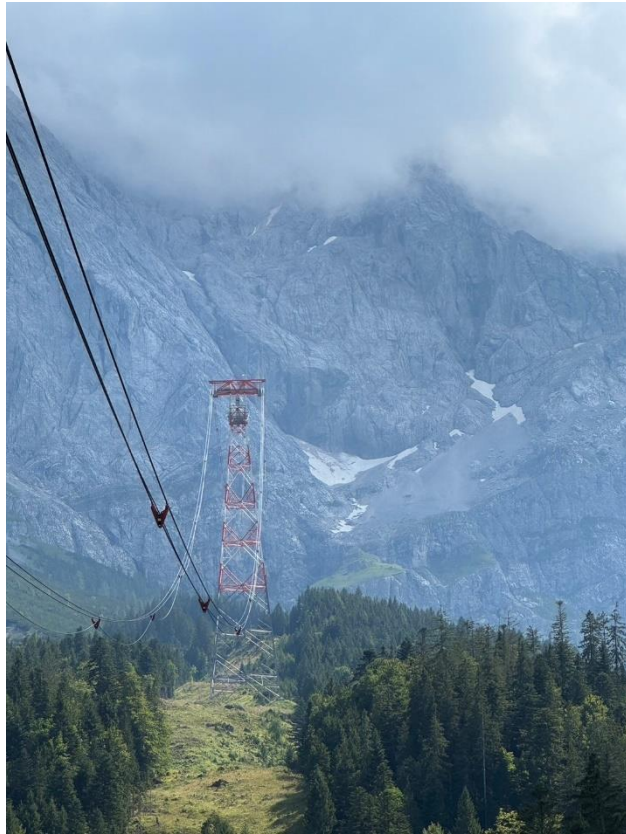


圖 2.3-6 纜車全景



圖 2.3-7 纜車電機驅動系統

2.4 德國鐵道系統其他觀察

2.4.1 車站與月台設施

本次考察德國鐵路現況，觀察其德國鐵路車站未採用月台門和收票閘門的設計，分析原因來自多重因素，包括歷史文化、營運效率、安全考量及社會信任度等方面，說明如下：

(1) 月台門

A. 歷史與文化保護：

德國的鐵路系統擁有悠久的歷史，許多車站甚至被列為歷史建築。這些車站不僅是交通樞紐，還是文化遺產的一部分。月台門的安裝通常需要對現有結構進行大規模改造，這可能會影響車站的外觀和歷史風貌。因此，保護這些歷史建築成為了優先考量，月台門的推廣受到限制。

B. 高效營運與技術：

因月台門的主要功能是防止乘客跌落軌道並確保安全，但在德國，由於列車停靠的精度高，並且乘客的安全意識強，這種風險相對較低。此外，月台門的安裝和維護成本較高，對於營運成本的控制也成為考量之一。

C. 車站設計的靈活性：

德國許多車站的設計強調開放性和靈活性。開放式的月台設計允許乘客在不同月台之間自由移動，減少了換乘時間，提高了乘客的整體體驗。月台門的引入可能會限制這種靈活性，導致乘客流動性降低。

(2) 收票閘門

A. 營運效率與乘客便利性：

德國鐵路系統採用開放式進站模式，乘客可以自由進出車站而不需經過閘門，這大大提高了通行效率。特別是在尖峰時段，開放式車站能夠有效緩解人流壓力，避免因閘門擁擠導致的堵塞。此外，這種開放式設計也為乘客提供了更舒適和便捷的體驗，減少了乘車過程中的不必要等待。

B. 信任與社會責任：

德國社會對個人責任和守法意識有較高的期望，鐵路系統依賴這一點來確保營運的順暢。儘管沒有收票閘門，德國鐵路系統通過車上查票的方式來確保乘客持有有效車票。這種隨機抽查的方式，結合高額的罰款，對逃票行為形成了強有力的威懾。因此，德國鐵路能夠在沒有收

票閘門的情況下，依然有效抑制逃票行為。

C. 經濟考量：

設置和維護收票閘門需要高昂的成本，尤其是在大型車站或換乘樞紐。德國鐵路選擇將資源投入到其他更能提高營運效率和乘客體驗的方向，例如列車的準點率和服務質量，而非在收票閘門上。

德國鐵路車站未採用月台門和收票閘門的原因，是多方面考量的結果。這既反映了德國對歷史文化的重視，也體現了其在技術與經濟上的理性選擇。此外，德國社會對公共秩序和個人責任的高度重視，使得這種開放式設計得以成功運行，並在全球鐵路系統中形成了獨特的模式。有關德國車站配置現況詳圖 2.4-1~2.4-3。



圖 2.4-1 大型車站月台配置圖



圖 2.4-2 車站無閘門收費柱



圖 2.4-3 小型車站月台配置圖

2.4.2 列車準點率議題

德國鐵路系統過往以其高效和準時著稱，然而近年來，德國鐵路列車的準點率已不如以往，這已成為一個備受關注的問題，本次考察亦多次因列車誤點而影響行程，影響德國鐵路列車準率的原因經討論可歸納如下：

(1) 基礎設施老化與維護不足：

德國鐵路系統已有超過一個世紀的歷史，部分路段和設施已經老舊，長期未進行大規模的升級改造。這導致基礎設施在應對現代列車營運需求時出現瓶頸，進而影響列車的準點率。

(2) 運輸需求增加：

隨著德國及歐洲各國之間的經濟聯繫加強，鐵路運輸需求不斷增長，尤其是貨運需求的增加，使得運輸網絡承載著過大的壓力。這種高負荷營運容易引發延誤，尤其是在繁忙時段。

(3) 運行調度複雜：

德國的鐵路網絡非常繁複，涵蓋城際、區域、城市和國際運輸線路。不同類型列車的運行速度和優先權不同，這加大了調度的複雜性，也容易導致誤點。

(4) 人力資源不足：

德國鐵路公司（Deutsche Bahn）長期面臨人力資源短缺問題，特別是在維修和運行調度等關鍵崗位上，這使得即時應對突發狀況的能力不足，影響列車準點。

2.4.3 地面電車運行

德國的地面電車（Straßenbahn）在許多城市中扮演了重要角色，不僅為居民和遊客提供了便捷的公共交通服務，也成為城市生活中不可或缺的一部分。本次參訪針對其架空線、車輛對於城市交通、行車安全、市容之影響，提出幾個方面的感想：

(1) 城市交通的便捷性與可持續性：

德國的地面電車系統廣泛覆蓋城市各個區域，使居民和遊客能夠輕鬆到達市中心、商業區、住宅區和其他重要場所。與私家車相比，地面電車可減少城市交通擁堵，有助於降低城市碳排放。且架空線為電車提供了持續的電力支持，確保了系統的穩定性和可靠性，進一步促進了城市的交通可持續性發展。

(2) 行車安全：

地面電車在德國有嚴格的安全標準，確保了行人和其他用路人的安全。關於地面電車路線的規劃通常會考慮到行車安全並設有專門的軌道區域和號誌系統，以減少與其他車輛的碰撞風險。此外，地面電車行駛速度相對較慢，能夠有效應對緊急情況，進一步提高了安全性。

(3) 市容的影響：

架空線在德國城市中是地面電車不可或缺的一部分，雖然其對市容有一定影響，但設計和規劃經過精心考量，盡量減少對城市美觀的影響。許多城市採取了融合城市歷史和現代設計的方式，使架空線與周邊建築和景觀相協調。此外，地面電車車輛本身的設計也注重美觀與功能的結合，許多車輛採用現代化設計，與城市環境相得益彰。

(4) 文化與歷史的融合：

在一些歷史悠久的城市，地面電車系統已成為城市文化和歷史的一部分。地面電車不僅是交通工具，也承載了豐富的歷史記憶，成為了城市文化的象徵。這種文化與歷史的融合使得地面電車成為城市旅遊的一部分，增強了城市的魅力和吸引力。

德國的地面電車在維護城市交通便利、安全的同時，通過精心的規劃和設計，將其對市容的影響降到最低，並且成為了城市文化和歷史的一部分。這樣的系統不僅促進了城市的可持續發展，還提升了城市的整體形象。有關地面電車運行情形詳圖 2.4-4~2.4-6。



圖 2.4-4 地面電車路口設施配置情形圖



圖 2.4-5 地面電車乘車站相關配置圖



圖 2.4-6 地面電車轉轍器

3. 考察心得與建議

3.1 考察心得

此次考察可帶給我國未來智慧鐵道發展多樣參考，特別是在了解德國如何在交通運輸、鐵路系統資安管理的整體規劃方面展現出的創新與實踐能力。德國展示了其在全球科技領域的領導地位，特別是在資訊技術（IT）與營運技術（OT）融合方面的突破，可瞭解到數位轉型在工業和交通運輸中勢在必行趨勢。

西門子對於全球資訊安全挑戰的應對以及其在國際標準化推動中的積極參與，為我們提供了寶貴的參考，特別是在鐵路資安領域中，德國的標準化措施和法規執行經驗，對於提升系統穩定性、互操作性以及應對未來技術變革具有重要意義。

參考德國針對資安的推動方式，我們未來在執行我國智慧鐵道推動時，亦可依循下列方向逐步執行：

(1) 依循國際標準推動資安遵循方向

標準化是資安推動的核心，無論是歐盟的 NIS2 指令還是 IEC 62443 標準甚至未來的 TS50701 以及 IEC 63452，都明確指出標準化的措施有助於提升系統的穩定性和互操作性，確保在不同國家和供應商的跨國合作中，系統能夠無縫運行。另應隨時掌握國際最新標準制定及技術演進，如軟體供應資安商管理、人工智慧(AI)以及量子計算加密技術的潛在影響，以保持標準化的前瞻性和適應性。

(2) 與國際鐵路資安單位協同合作

在推動鐵路資安標準的過程中，台灣可以參考歐洲各國家相互合作經驗。這些國家在標準化、法規共同研擬、訂定並遵循和國際合作方面都積累了豐富的經驗，值得台灣學習。

首先，台灣應積極參與國際資安標準的制定，確保本地標準與國際標準接軌，提升台灣鐵路系統在全球市場中的競爭力。其次，台灣可以學習歐洲國家在資安法規方面的成熟經驗，將資安要求納入法規體系，強化合規性管理，確保企業在技術和法律層面都能有效應對資安挑戰。此外，台灣應加強跨國和跨領域的合作，與國際社會共享威脅情報和安全技術，通過成立資訊安全營運中心(SOC)或資安卓越中心(CoE)引進外部鐵道資安專業知識來提升本地防禦能力。

(3) IT 和 OT 應有密切合作

在現今數位化和全球化的背景下，鐵道系統的資安標準推動必須遵循多層次、多領域的協作原則。首先，IT 與 OT 的深度合作是不可避免的趨勢。隨著工業物聯網（IIoT）技術的廣泛應用，鐵道系統的數據處理、網路連結與實物控制的邊界逐漸模糊。為了有效應對這一趨勢，資安標準應涵蓋 IT 與 OT 的協作需求，強化兩者在資訊安全上的共識與協同機制。

(4) 持續推動鐵道資訊整合平臺

隨著全球鐵道運輸系統的不斷發展，資訊整合平臺的建立成為提升營運效率與安全性的關鍵。未來，鐵道資訊整合平臺將朝著數位化、智慧化和模組化的方向發展。

數位化是推動鐵道系統資訊整合的基礎。透過雲端技術、物聯網（IoT）及大數據分析，鐵道資訊整合平臺將能夠有效地收集、分析並應用龐大的營運數據，從而提升整體系統的營運效率。其次，智慧化發展將使鐵道系統維運更具預測性和主動性，透過機器學習和人工智慧技術的應用，平臺可以提前預測設備故障並自動調整營運策略，避免營運中斷。最後，模組化設計將提供靈活性，使得鐵道營運商可以根據自身需求進行客製化配置，從而達成最佳的資源利用與風險管理。

(5) 統一數據標準及通訊協定

在推動鐵道資訊整合的過程中，需採取多方位的策略，確保平臺的落地與實效性。首先，標準化是推動資訊整合的關鍵。透過建立統一的數據標準和通訊協定，可以確保來自不同供應商和系統的數據能夠無縫整合，實現資訊共享與系統互操作性。其次，跨部門合作不可或缺，鐵道資訊整合涉及多個部門與領域，需建立有效的協作機制，確保技術開發、數據管理與營運需求之間的協調一致。此外，資訊整合的推動需要管理階層的強力支持。管理階層應提供資源並制定長期策略，確保資訊整合項目能夠順利推進並達成既定目標。最後，安全性也是資訊整合中不可忽視的部分，隨著數據的集中化管理，系統面臨的資訊安全威脅增加，因此必須同步推動資安措施，保障平臺的安全運行。

楚格峰齒軌鐵路與索道纜車的整合模式，展示了如何將先進交通技術與自然景觀和旅遊資源緊密結合，成功打造出一個兼具便捷性和吸引力的全方位旅遊體驗。這種模式不僅提升了旅遊區的吸引力，還在保護自然環境的同

時，實現了可持續發展，對於台灣的山區旅遊規劃和發展具有重要的借鑒意義。

針對德國楚格峰與艾伯湖的觀光整合模式，台灣在觀光發展上可以考慮以下幾點心得：

(1) 交通系統整合與升級：

台灣的多山地形類似德國巴伐利亞州，可以借鑒齒軌鐵路和索道纜車的設計，特別是在攀登高度較大的旅遊景點如阿里山、太魯閣等地區。這種交通設施不僅提升了旅遊便利性，還能增加景區的可達性和吸引力，特別是對於老年人和外國遊客。

(2) 無縫的旅遊體驗：

德國的觀光整合展示了如何在自然景觀與交通之間實現無縫連接，台灣可以在熱門景點之間建立類似的整合系統，如在日月潭與阿里山之間開發高效的交通連結(不限鐵路或纜車)，讓遊客能在一天之內輕鬆遊覽多個景點。

(3) 文化與歷史融入旅遊：

台灣擁有豐富的文化和歷史遺產，可通過設置文化展示區和解說牌來提升遊客的體驗。這種做法不僅可以增加旅遊地點的吸引力，還能加強遊客對當地文化的理解與認同。

(4) 智慧旅遊技術應用：

台灣可以引入更多智慧旅遊技術，例如即時資訊平台、虛擬導覽與擴增實境（AR）等，提升旅遊的互動性和便利性。這對於吸引年輕遊客和外國遊客尤為重要，因為他們更傾向於使用數位工具來進行事前計劃。

(5) 可持續發展與環境保護：

在推動觀光發展的同時，應注重環境保護與可持續性。德國的經驗表明，在建設旅遊基礎設施時，選用環保材料、減少對自然景觀的破壞，並設立生態保護區，這些做法都能夠在旅遊業發展與環境保護之間取得平衡。

(6) 全季節旅遊推廣：

台灣的氣候多樣且自然景觀豐富，應考慮開發適合不同季節的旅遊活動，使各地景區能夠全年吸引遊客。這將有助於平衡淡旺季的遊客流量，提升當地經濟收益。

德國鐵路系統在高效營運和開放性設計方面的成功經驗也讓人印象深刻。德國鐵路車站採用無月台門和收票閘門的設計，既體現了其對歷史文化的尊重，也反映了德國社會對公共秩序和個人責任的高度重視。這種開放式的設計在提高通行效率和乘客便利性的同時，保持了鐵路系統的高效和安全營運。

雖然德國鐵路與我國傳統鐵路類似，正面臨系統老舊、人員知識無法傳承等一系列困境，導致列車準點率不佳等問題，但德國鐵路營運公司仍積極著手下列改善方式：

(1) 加強基礎設施投資：

德國政府和鐵路公司應加大對鐵路基礎設施的投資，進行必要的升級和現代化改造，包括加強對關鍵路段的維修和更新，以及備用路線規劃，確保運行順暢。

(2) 提升調度效率：

利用先進的技術手段，如人工智慧和大數據分析，優化列車調度系統，以提高調度效率，減少因調度不當引起的延誤。

(3) 提升運能：

適當增加列車班次或加大列車編組，於尖峰時段，緩解運輸壓力，確保更高的運行效率和準點率。

(4) 強化員工培訓與招募：

增加鐵路行業的人力資源投入，提高薪資待遇與改善工作環境，加強員工的專業技能培訓，並積極招募新員工，以提升對突發事件的應對能力。

另外，德國的 eHighway 電氣化高速公路項目不僅顯示了未來道路運輸低碳化的可能性，也顯示了德國在推動淨零碳排的決心，即使在實施過程中面臨多項需克服的技術和經濟挑戰，但德國仍在這一計畫展示了如何在現有基礎設施上進行技術創新，並通過國際合作和多方參與來推動實驗性項目的落地，這為我們在考慮未來交通電氣化時提供了有力的參考。

3.2 考察建議

根據此次考察心得，我們建議台灣在以下幾個方面進行改進和提升：

(1) 加強鐵路系統資安標準化推動與國際接軌：

台灣應積極參與國際鐵路資安標準的制定，特別是在參考歐盟 NIS2 指令、IEC 62443、TS 50701 以及 IEC 63452 標準的基礎上，制定符合本地需求的資安標準。這些標準應涵蓋 IT 與 OT 的深度融合，確保在數位化和工業物聯網（IIoT）背景下，鐵路系統的數據處理、網路連結以及實體設備控制系統都能得到全面保護。與此同時，台灣應與國際社會加強合作，學習德國等國家的資安實踐，借助這些國家在標準化、法規遵循和技術創新方面的經驗，提升自身的鐵路資安能力。另外隨著供應鏈數位化程度的提升，供應鏈中的網路威脅也越來越多，這對企業組織構成了巨大的挑戰。應該如何建立一個強大的現代化供應鏈，確保營運的安全並提高網路安全？轉型為數位供應鏈是否能保證資訊安全，是否會衍伸出其他問題？技術驅動的新型態是否能同時提供安全的營運環境？從企業的角度來看，儘管供應鏈是相當關鍵的功能，但在防禦潛在網路威脅方面並未得到應有的重視。德國在鐵道資安議題上，目前正在討論這個新議題，我們應該持續關注，未來在台灣發展出對應的規範。

(2) 推動鐵路建設中資安技術的前瞻性應用：

在未來的鐵路建設中，台灣應特別關注資安技術的前瞻性應用。例如，隨著量子計算技術的發展，現有的加密技術可能面臨挑戰，台灣應提前佈局，在鐵路資安標準中融入量子加密技術等先進手段。同時，台灣應推動人工智慧和機器學習技術在鐵路資安中的應用，利用這些技術進行即時威脅檢測和預測性維護，以提高鐵路系統的整體安全性和營運效率。

(3) 推動我國鐵道系統專屬資訊平台

推動我國鐵道系統專屬資訊平台刻不容緩。在全球數位化浪潮中，鐵路營運和維護的智慧化成為發展趨勢。以 Siemens Railigent 平台為例，其透過物聯網、人工智慧與大數據分析，實現鐵道系統的預測性維護與營運優化，顯著提升系統效能與可靠性。類似的平台可讓我國特鐵道系統更為精準地監控列車與基礎設施，並即時應對潛在問題，減少非預期停運，進一步確保運輸安全與穩定。

專屬資訊平台的建置不僅能促進本土鐵路數位化轉型，更可優化列車運行調度、減少延誤，並提升能源利用效率。透過數據驅動的決策支持，我國鐵道系統將邁向更智慧、安全與高效的未來，滿足日益增長的運輸需求，並增強國際競爭力。此外也能評估是否與原廠開放平台合作，除了節省資源浪費外，也能在該平台上行銷國內的廠商，跨足其他以前我們無法觸及的市場。相關合作方式也可以在日後進行討論。

(4) 增加鐵路基礎設施投資，提升資安防護能力：

鐵路基礎設施是確保系統安全營運的關鍵。台灣應加大對鐵路基礎設施的投資，特別是在老舊設施的更新改造和現代化升級方面。這不僅包括實際基礎設施的升級，還應加強對資訊基礎設施的投資，確保在數位化過程中，鐵路系統的各個環節都具備足夠的資安防護能力。這些投資應包括建立高效的資安監控系統，並在關鍵設施中部署縱深防護措施，以防範日益增長的網路威脅。初期可以從單向閘道器(以西門子為例為 DCU)等標準設備開始，先阻擋大部分的入侵路徑，日後再對系統進行縱深防禦的強化。

(5) 建立強化鐵路資安的專業培訓和事件應變機制：

台灣應加強對鐵路系統相關人員的資安專業培訓，確保從技術人員到管理階層都具備應對資安威脅的能力。這些培訓應涵蓋最新的資安技術和國際標準，並包括針對工業控制系統（ICS）和營運技術（OT）的專業課程。鐵道業是一個很特殊的行業，這行業有著高安全性，高穩定度以及進入門檻極高的特性，該如何進入這一個封閉型產業是極大的挑戰。縱使台灣過去在全球資通訊(Information and Communication Technology, ICT) 產業有著不錯的成績，然而在鐵道資安領域甚少有機會觸碰。

此次參訪接觸到了西門子軌道資安核心成員，對方除了介紹未來歐盟軌道資安發展趨勢外，也分享了內部的教育訓練方式以及架構。訓練一個資安產品與解決方案工程師 PSSE(Product and Solution Security Engineer)需要投入大量的資源。該角色除了接受 IT 訓練外，還需要兼具軌道運轉的領域知識。國內在這方面的資安訓練除了需要落實在設計規劃的單位外，日後稽核以及負責營運的角色都需要有對應的能力，還有一條很長遠的路要走。在當前國際競爭日益激烈的環境下，時間就是最大的競爭優勢。

為了縮短學習曲線並迅速提升市場競爭力，我們應積極評估與國際大廠的合作，這不僅能加快技術吸收速度，瞭解產業趨勢與規範，還能有效縮短產品上市時間，確保我們在激烈的全球競爭中搶佔先機。此外，台灣應建立健全的事件應變機制，確保在發生資安事件時能夠迅速有效地應對，將潛在損失降至最低。借鑒德國的經驗，台灣應設立鐵路專門的資安營運中心（SOC），實施全天候的資安監控，並與國際資安社群保持密切聯繫，共享威脅情報和應對策略。

(6) 推動資安技術與鐵路建設的同步發展：

在新鐵路項目的規劃和建設過程中，資安技術應與基礎設施建設同步推進。這表示在設計階段就應考慮資安要求，確保新建鐵路在投入營運時已經具備強大的資安防護能力。例如，在引入新的鐵路控制系統和自動化技術時，應提前進行全面的資安測試和評估，並部署先進的滲透測試和安全掃描工具，以確保系統在整個生命周期內的安全性。

(7) 促進跨領域協作，提升鐵路系統整體安全性：

鐵路系統的資安保障需要跨領域的協作，包括交通運輸部門、資訊技術（ICT）部門以及產業部門的共同努力。台灣應建立跨部門協作機制，確保在鐵路建設和資安推動過程中，各方能夠緊密配合，共同制定和實施資安策略。這種協作應包括資安標準的共同制定、資安技術的整合應用以及資安事件的聯合應對，從而提升鐵路系統的整體安全性和抗風險能力。

(8) 促進可持續發展與環境保護：

台灣在發展觀光業的同時，應堅持可持續發展的理念，學習德國在保護自然景觀和減少環境影響方面的經驗。這包括在旅遊基礎設施建設過程中選用環保材料，減少對生態環境的影響，並設立保護區域，避免遊客對敏感地區的過度干擾。這樣不僅可以保護台灣的自然資源，還能提升台灣在全球旅遊市場中的形象。

附錄 A1 西門子鐵道資安介紹簡報

Cybersecurity (CYS)
Visit Taiwan Rail Bureau 07/24
 SIEMENS Mobility Customer Service: Erlangen, 25.07.2024
SIEMENS

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: **Introduction and Expectations**

9:15 AM - 10:30 AM: **SMO CS and Cybersecurity Services**
 Presenter: Martin Kunz
Cybersecurity Trends and Role of SMO CS:
Cybersecurity Services:
 - Audits and Overview of Services
 - Penetration Testing and Security Scanning (incl. SIESTA demo)
 - Vulnerability Management (incl. VMS demo)

10:30 AM - 10:45 AM: **Break**

10:45 AM - 11:30 AM: **CSOC Support and Cloud Security**
 Presenter: Martin Kunz
CSOC Support:
 - CSOC integration example project
 - Challenges and lessons learned
 - CoE Idea with City of Kaohsiung
Cloud Security:
 - Example: Railigent X

11:30 AM - 12:00 PM: **Q&A and Wrap-Up**
 - Questions and Next Steps

12:00 PM: **Lunch**

CSOC: Cybersecurity Operation Center
 SMO CS: Security Model/Event Management
 ES: Intrusion Detection System
 CoE: Center of Excellence
 VMS: Vulnerability Management System

SIEMENS

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: **Introduction and Expectations**

9:15 AM - 10:30 AM: **SMO CS and Cybersecurity Services**
 Presenter: Martin Kunz
Cybersecurity Trends and Role of SMO CS:
Cybersecurity Services:
 - Audits and Overview of Services
 - Penetration Testing and Security Scanning (incl. SIESTA demo)
 - Vulnerability Management (incl. VMS demo)

10:30 AM - 10:45 AM: **Break**

10:45 AM - 11:30 AM: **CSOC Support and Cloud Security**
 Presenter: Martin Kunz
CSOC Support:
 - CSOC integration example project
 - Challenges and lessons learned
 - CoE Idea with City of Kaohsiung
Cloud Security:
 - Example: Railigent X

11:30 AM - 12:00 PM: **Q&A and Wrap-Up**
 - Questions and Next Steps

12:00 PM: **Lunch**

CSOC: Cybersecurity Operation Center
 SMO CS: Security Model/Event Management
 ES: Intrusion Detection System
 CoE: Center of Excellence
 VMS: Vulnerability Management System

SIEMENS

Role and Responsibility of SMO CS Responsible for Cybersecurity during Operation & Maintenance

Cyber Security Services for Rail systems

DESCRIPTION:
 Responsible for cyber security in all greenfield projects for the tracks, stations and control and the extended "digital backbone" of cyber security improvements to existing rail systems for upgrades.

A comprehensive set of cyber security services to protect the rail and its infrastructure from malicious attacks. All cyber security analysis and penetration tests, all cyber security implementation in a patch management, continuous monitoring (incl. Intrusion Detection, BSI) of all cyber security and cyber security testing.

Customer Services
 Services for Turnkey, Rolling stock and Rail Infrastructure. From end-to-end lifecycle. Products and solutions. Digital Services (Railigent X), CMSS (CERT.MU), VMS, BSI/IX.

Secure design, Secure architecture, Secure implementation, Verification & testing, Secure operation, Secure decommissioning

Page 4 | Restricted | © Siemens Mobility GmbH 2024 | Martin Kunz | SMO CS | DB | B&W | VMS: Vehicle Equipment - Measurement Systems | **SIEMENS**

Global Trends in Cybersecurity
 Having a Secure Solution is good, but maintenance is getting more important

Cyber Incidents & Compliance

New Standards & Regulations

Page 5 | Restricted | © Siemens Mobility GmbH 2024 | Martin Kunz | SMO CS | DB | B&W

Trend: ENISA Transport Threat Landscape (21. March 2023)

Figure 6: Prime Incidents in the Transport sector (January 2020 to October 2022)

Consequences: Data related Breach, Malware, DDoS, Phishing, Supply chain attacks, Breach/divulgence, Fraud, Vulnerability exploitation

Incidents (Jan-Oct 2022)

Individual Actor (7%), State Actors (18%), Hacktivist (23%), Cybercriminals (52%)

Page 6 |

Trend: Rail operators face fines for non-compliance with regulations Example operators with insufficiently protected systems

Operator	Country	Regulation	Compliance Status
DB	Germany	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
SNCF	France	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
Trenitalia	Italy	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
CP	Canada	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
RZD	Russia	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
Korail	South Korea	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
KTM	Austria	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
CNR	China	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
JR	Japan	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed
UIC	International	EN 50126	Not Assessed
		EN 50128	Not Assessed
		EN 50129	Not Assessed
		EN 50159	Not Assessed

Legend: Not Assessed, Achieved, Partially Achieved, Not Achieved, Not Relevant

Page 8 | Restricted | © Siemens Mobility GmbH 2024 | Martin Kunz | SMO CS | DB | B&W | **SIEMENS**

Trend: New regulations, standards and guidelines Specially developed by and for the railway industry

Directive: CLC/TS 50701:2021 (in preparation IEC63452)
 Title: Railway Applications - Cybersecurity

- This document is intended for railway operators, system integrators and product suppliers in the areas of communication, signalling and processing, rolling stock and fixed installations.
- It connects the systems engineering lifecycle (EN50126) with the processes for cybersecurity
- It links cyber security activities with safety management processes (Safety Case EN50129)
- It also provides examples of measures in rail transport.
- It proposes railway-specific measures from the IEC 62443 standard.

ISO 27001, KE 62443, TS 50701

Page 9 | Restricted | © Siemens Mobility GmbH 2024 | Martin Kunz | SMO CS | DB | B&W

Trend: New regulations, standards and guidelines
Cyber regulations for critical infrastructure are becoming increasingly stringent

New Directive Network & Information Systems (NIS2)- proposed on 16 December 2020

- Higher fines of up to €10 million or 2% of annual global turnover
- Mandate for information exchange and cooperation
- Coordinated vulnerability disclosure for newly discovered vulnerabilities
- Basic security requirements with a list of targeted actions, including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption
- Focus on cybersecurity in the supply chain
- Responsibility of management for compliance with cybersecurity risk management measures
- Security incident reporting obligations, with more detailed provisions on the reporting procedure, content and timing



Page 10 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

Similar regulations and requirements on standards globally



Taiwanese Cybersecurity Requirements: Schedule 4: Level-B Cyber Security



Page 11 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

Schedule 4: Measures to be undertaken by the specific government agency of other security responsibility Level-B

Item	Item	Item
1. The government agency shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4, and shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4, and shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4.	2. The government agency shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4, and shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4, and shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4.	3. The government agency shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4, and shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4, and shall ensure the security of its information systems and information assets in accordance with the requirements of this Schedule 4.

Page 12 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: Introduction and Expectations

9:15 AM - 10:30 AM: SMO CS and Cybersecurity Services

10:30 AM - 10:45 AM: Break

10:45 AM - 11:30 AM: CSOC Support and Cloud Security

11:30 AM - 12:00 PM: Q&A and Wrap-Up

12:00 PM: Lunch

CSOC: Cybersecurity Operation Center
SIEM: Security Incident Event Management
IDS: Intrusion Detection System
UE: Center of Excellence
VMS: Vulnerability Management System

Page 13 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

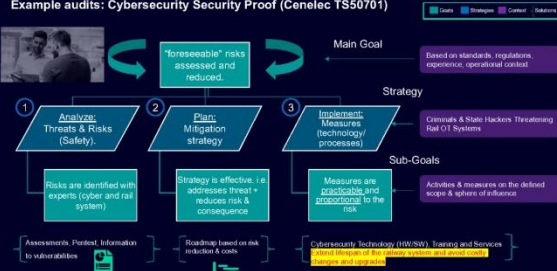
SMO CS and Cybersecurity Services
Audit Support: Risk Analysis Evidence & Effective Measures Implementation



- Cybersecurity Technology (HW/SW), Training and Services
- Upgrades of railway systems


Page 14 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

SMO CS and Cybersecurity Services
Example audits: Cybersecurity Security Proof (Cenelec TS50701)



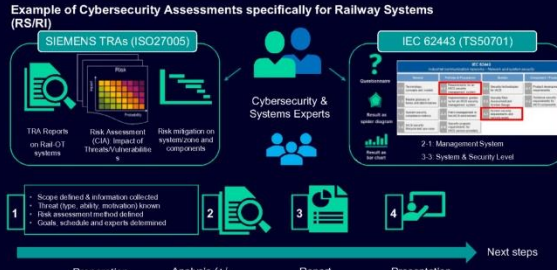
Page 15 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

SIEMENS Mobility: Cybersecurity Services




Page 16 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

Example of Cybersecurity Assessments specifically for Railway Systems (RS/R)




Page 17 Restricted | © Siemens Mobility GmbH 2024 | Mario Kruj | SMO CS DR BAC200

Security Scanning, Vulnerability Management and Intrusion Detection (IDS)




Security Scanning

- Expert-supervised scanning
- Detection of software components, configurations and vulnerabilities
- Detect changes to baseline and security policies
- Reusable scans and "single" report



Vulnerability Management

- Automated tracking of software vulnerabilities
- Risk assessment of exploitability based on system know-how
- Report and risk-based measures
- Recommendation from experts



Intrusion Detection (IDS)

- SIEMNS OSA for OT Infrastructure
- SecurityGateway and/or RadarSecure for Risk Vehicles
- Signature and AI-based recognition

Page 18 | Restricted | © Siemens Mobility GmbH 2024 | Mainz, Kassel | SMO CS DB BA20M | SIEMENS

Sample Reports



Assessments (IEC62443 and SIEMNS TRA)



Penetration & Scanning




Vulnerability Management


Page 19 | Restricted | © Siemens Mobility GmbH 2024 | Mainz, Kassel | SMO CS DB BA20M

Analysis: Example IEC62443 Part:2-1 (Management) + Part:3-3 (Security-Level)


Detailed report with actionable measures (important input for audits)



IEC 62443 Compliance Assessment



IEC 62443 Compliance Assessment




IEC 62443 Compliance Assessment

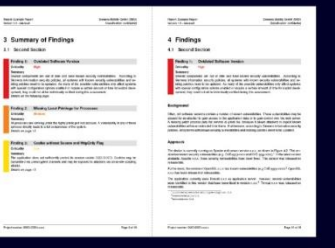
Page 20 | Restricted | © Siemens Mobility GmbH 2024 | Mainz, Kassel | SMO CS DB BA20M | SIEMENS

Analysis: Example penetration test

Detailed report with actionable measures (important input for audits)



Report
Security Assessment Example Report



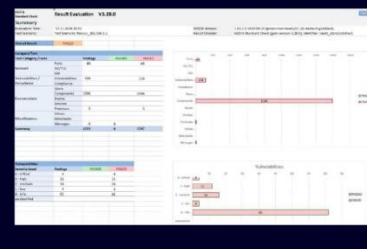
3 Summary of Findings

4 Findings


Page 21 | Restricted | © Siemens Mobility GmbH 2024 | Mainz, Kassel | SMO CS DB BA20M | SIEMENS

Analysis: Example Security Scanning/Vulnerability Assessment (SIESTA)

Detailed report with actionable measures (important input for audits)




Search Evaluation: 13.8.2023



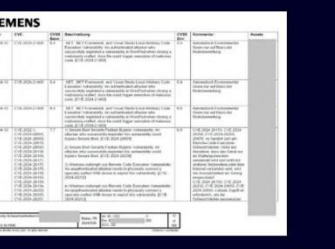
Page 22 | Restricted | © Siemens Mobility GmbH 2024 | Mainz, Kassel | SMO CS DB BA20M | SIEMENS

Analysis: Vulnerability Management Service Example

Detailed report with actionable measures (important input for audits)



Contents



SIEMENS

Page 23 | Restricted | © Siemens Mobility GmbH 2024 | Mainz, Kassel | SMO CS DB BA20M | SIEMENS

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: Introduction and Expectations

9:15 AM - 10:30 AM: SMO CS and Cybersecurity Services

Cybersecurity Trends and Role of SMO CS:

- Audits and Overview of Services
- Penetration Testing and Security Scanning (incl. SIESTA demo)
- Vulnerability Management (incl. VMS demo)

Presenter: Christian Kuntze

10:30 AM - 10:45 AM: Break

10:45 AM - 11:30 AM: CSOC Support and Cloud Security

CSOC-Support:

- CSOC integration example project
- Challenges and lessons learned
- CoE: Ideas with City of Kassel

Cloud Security:

- Example: Railigent X

11:30 AM - 12:00 PM: Q&A and Wrap-Up

- Questions and Next Steps

12:00 PM: Lunch

CSOC: Cybersecurity Operation Center
SIEM: Security Incident Event Management
ECS: Intrusion Detection System
CoE: Center of Excellence
VMS: Vulnerability Management System

SIEMENS

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: Introduction and Expectations

9:15 AM - 10:30 AM: SMO CS and Cybersecurity Services

Cybersecurity Trends and Role of SMO CS:

- Audits and Overview of Services
- Penetration Testing and Security Scanning (incl. SIESTA demo)
- Vulnerability Management (incl. VMS demo)

Presenter: Michele Baratta

10:30 AM - 10:45 AM: Break

10:45 AM - 11:30 AM: CSOC Support and Cloud Security

CSOC-Support:

- CSOC integration example project
- Challenges and lessons learned
- CoE: Ideas with City of Kassel

Cloud Security:

- Example: Railigent X

11:30 AM - 12:00 PM: Q&A and Wrap-Up

- Questions and Next Steps

12:00 PM: Lunch

CSOC: Cybersecurity Operation Center
SIEM: Security Incident Event Management
ECS: Intrusion Detection System
CoE: Center of Excellence
VMS: Vulnerability Management System

SIEMENS

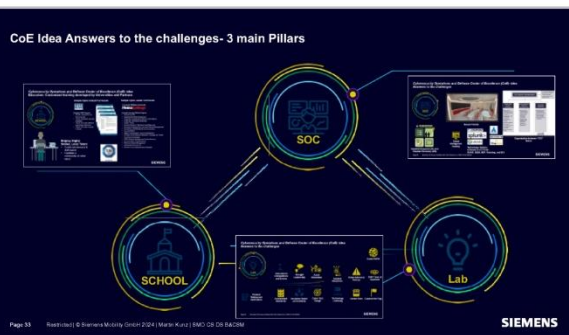
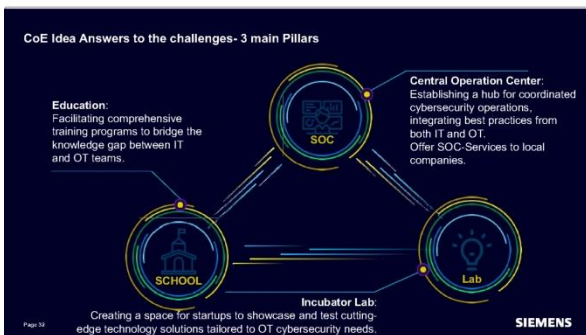
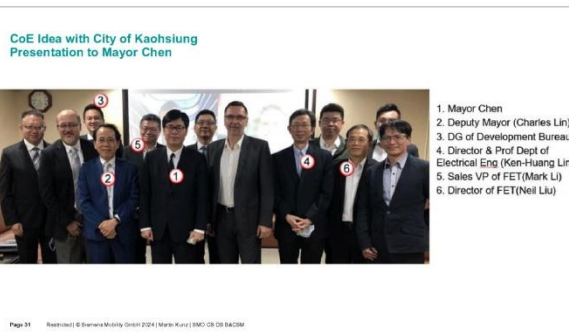
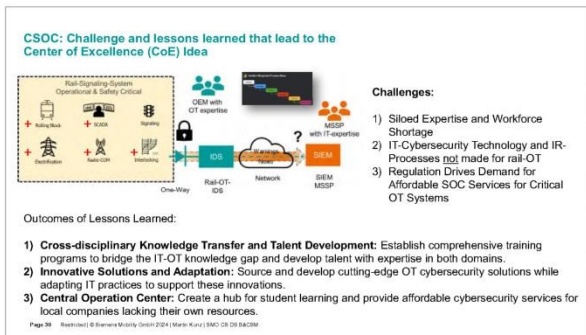
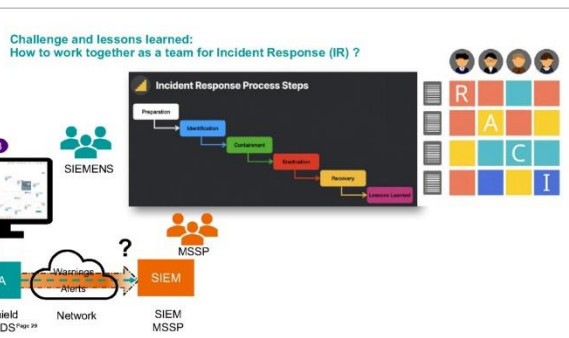
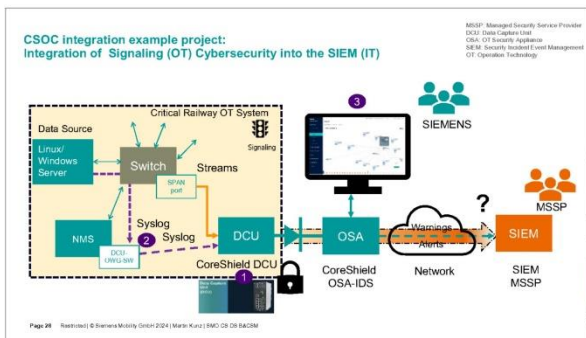


Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM:	Introduction and Expectations	10:45 AM - 11:30 AM:	CSOC Support and Cloud Security
9:15 AM - 10:30 AM:	SMO CS and Cybersecurity Services	Presenter: Martin Kunz	<ul style="list-style-type: none"> CSOC integration example project Challenges and lessons learned CoE Idea with City of Kaohsiung
	Cybersecurity Trends and Role of SMO CS: Cybersecurity Services: <ul style="list-style-type: none"> Audits and Overview of Services Penetration Testing and Security Scanning (incl. SIESTA demo) Vulnerability Management (incl. VMS demo) 	11:30 AM - 12:00 PM:	Q&A and Wrap-Up
10:30 AM - 10:45 AM:	Break		<ul style="list-style-type: none"> Questions and Next Steps
		12:00 PM:	Lunch

CSOC: Cybersecurity Operation Center
 SEM: Security Event Management
 IDS: Intrusion Detection System
 CoE: Center of Excellence
 VMS: Vulnerability Management System

© Siemens 2021 | 2021.11.11



Cybersecurity Operations and Defense Center of Excellence (CoE)- Idea
Education: Customized training developed by Universities and Partners

Sample Cyber Analyst Curriculum

Example: SANS Program

- SEC401: Introduction to Cyber Security
- KS400: KIS/CISSA Security Essentials
- KS500: KIS Active Defense and Incident Response
- KS600: KIS Cyber Security in Organizations

Example: Carnegie Mellon University Heinz College

- Role of the CISO
- Applied Cyber Risk Management
- Cyber Risk Quantification with the FAIR Method
- SCRM and Operational Resilience
- Insider Threat
- Security Strategy, Operations and Assessment
- Business of Cybersecurity, Security Financial Management
- Storytelling and CISO Board Communications
- Security Metrics
- Digital Transformation: Security Implications
- Evaluation of the Network Defender's Strategy and Toolkit
- Cloud Security Strategy
- CISO's Guide to Software and Product Security
- Security Center Physical Systems
- Efficient Incident Management
- Information Security Law
- Effective Crisis Communications Strategies

Employ Highly Skilled, Local Talent

- Create job demand & skill export
- Facilitate a community of cyber talent

Lab

Product Testing and Verification

Assessment Standards

Incubator Model (Investment)

Cyber Test Range

Technology Licensing

Career Fairs

Capture the Flag

Cyber EXPO

SIEMENS

Cybersecurity Operations and Defense Center of Excellence (CoE)- Idea
Answers to the challenges

SOC

Secure Facility

Organization between IT/OT Teams

Incident Response (IR) and Disaster Recovery (DR)

Threat Intelligence/Hunting

Technology Options: In-house or COTS for: SOAR, SIEM, MDR Ticketing, and IDS

SIEMENS

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: **Introduction and Expectations**

9:15 AM - 10:30 AM: **SMO CS and Cybersecurity Services**

Cybersecurity Trends and Role of SMO CS:

Cybersecurity Services:

- Audits and Overview of Services
- Penetration Testing and Security Scanning (incl. SIESTA demo)
- Vulnerability Management (incl. VMS demo)

10:30 AM - 10:45 AM: **Break**

10:45 AM - 11:30 AM: **CSOC Support and Cloud Security**

CSOC-Support:

- CSOC integration example project
- Challenges and lessons learned
- CoE Idea with City of Kachszung

Cloud Security:

- Example: Railigent X

11:30 AM - 12:00 PM: **Q&A and Wrap-Up**

- Questions and Next Steps

12:00 PM: **Lunch**

SIEMENS

Cloud Security: Example: Railigent X

SIEMENS

Meeting Agenda: 9:00 AM - 12:00 PM

9:00 AM - 9:15 AM: **Introduction and Expectations**

9:15 AM - 10:30 AM: **SMO CS and Cybersecurity Services**

Cybersecurity Trends and Role of SMO CS:

Cybersecurity Services:

- Audits and Overview of Services
- Penetration Testing and Security Scanning (incl. SIESTA demo)
- Vulnerability Management (incl. VMS demo)

10:30 AM - 10:45 AM: **Break**

10:45 AM - 11:30 AM: **CSOC Support and Cloud Security**

CSOC-Support:

- CSOC integration example project
- Challenges and lessons learned
- CoE Idea with City of Kachszung

Cloud Security:

- Example: Railigent X

11:30 AM - 12:00 PM: **Q&A and Wrap-Up**

- Questions and Next Steps

12:00 PM: **Lunch**

SIEMENS

Questions?

Martin Kunz
Sales for Cybersecurity services
Siemens Mobility GmbH
SMO CS DS DO
Siemenspromenade 7
91058 Erlangen, Germany
Mobile: +49 1520 953 8074
martin.kunz@siemens.com

Christian Kunze
Lead Cybersecurity services
Siemens Mobility GmbH
SMO CS DS CVR CTR
Klausius-Muller-Str. 2
80567 Munchen, Germany
Mobile: +49 (162) 2502466
christian.kunze@siemens.com

Michele Berletta
Lead Vulnerability Management
Siemens Mobility GmbH
SMO CS DS DO
Siemenspromenade 7
91058 Erlangen, Germany
Mobile: +49 (173) 5676984
michele.berletta@siemens.com

SIEMENS

OT cybersecurity standard IEC 62443 is also used for railway

IEC 62443 Industrial communication networks - Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements IACS service providers		

Similar Areas such as - 27001

OT Cybersecurity Standard IEC 62443 Example: Part 3-3 (SL= Security Level for Systems)

FR>	IAC	UC	SI	DC	RDF	TRE	RA	tot	Protection Against
SL 1	10	8	5	2	4	1	7	37	Casual or Coincidental Attacks
SL 2	6	4	5	2	2	1	3	23	Intentional Attacks With Simple Means
SL 3	6	9	6	1	4	1	3	30	Attacks With Sophisticated Means
SL 4	2	3	3	1	1	0	0	10	Attacks With Extrem
tot	24	24	19	6	11	3	13	100	

SL = (IAC UC SI DC RDF TRE RA)
SL = (2 2 2 1 1 1 2 1)

Number of system requirements given in IEC 62443-3-3:2019, per FR groups and SL values

Confidentiality Integrity Availability

CSOC integration example project: Incident Analysis and Response Workflow (High-Level)

Precondition:

- Alert triggered in SIEM - hypothesis it could be an OT incident

Step 1: MSSP: Contact OT Site Lead

- Role: SOC Tier 1 Analyst
- Action: The analyst initiates contact with the OT Site Lead to discuss the alert details

Step 2: OT Site-Lead Investigation

- Role: OT Customer Site Lead
- Action: The OT Site Lead performs a site investigation to gather more context about the incident and its potential impact on OT systems

Step 3: OT Decision

- Critical Alert with Known Mitigation (Branch)
- Yes Branch:
 - Action: Follow established Internal Incident Response (IR) procedures (SOC Tier 2 & OT Incident Handler)
 - Role(s): SOC Tier 2 Analyst and OT Incident Handler work collaboratively
 - Outcome: Resolve the incident by implementing known mitigation steps

Step 4: MSSP: Decision

- Critical Alert with Unknown Mitigation (Branch)
- Yes Branch:
 - Action: Utilize threat intelligence platforms to gather further information and potential mitigation strategies (OT Incident Handler)
 - Role: SOC Tier 2 Analyst and OT Incident Handler work collaboratively
 - Outcome: Update the knowledge base with the new threat information and identified mitigation steps
- No Branch:
 - Outcome: The incident may be deemed non-critical or a false positive. Further investigation or analysis might be required depending on the context

Post-Condition:

- The OT security incident is resolved or contained
- The knowledge base is updated with new threat information (if applicable)
- Lessons learned are documented and incorporated into future response procedures

Cyber security center of excellence to attract companies, cyber startup incubator and encouraging high school students to study cyber security.

Siemens to open global cyber security centre of excellence in Production

The new center will be located in Eindhoven, Netherlands. It will focus on the development of new products and services for the industrial sector. The center will also serve as a hub for talent development and innovation in the field of industrial cybersecurity.

The center will be led by Dr. Ralf Schmitt, who will be responsible for the overall strategy and execution of the center. He will be supported by a team of experts in industrial cybersecurity, including Dr. Ingrid Isenhardt and Dr. Gernot Heiser.

The center will be a key part of Siemens' commitment to digitalization and cybersecurity in the industrial sector. It will provide a platform for collaboration between academia, industry, and government to address the challenges of industrial cybersecurity.

附錄 A2 資安脆弱性管理說明簡報

Vulnerability Monitoring and Management (VMM) & Vulnerability Management System (VMS)

SMO Cybersecurity Services

Visit Taiwan Rail Bureau 07/2024
Dr. Michele Barletta (SMO CS DS CVS CYS)

Monitoring of known security vulnerabilities throughout the lifecycle Cyber security services: Vulnerability monitoring and management

Vulnerability monitoring and management	Scope and approach	Your benefits	What's more?
<ul style="list-style-type: none"> Monitoring software vulnerabilities in rail systems (rail infrastructure, rolling stock, rail electrification & auxiliary including 3rd party systems) Alerting customers in case of major vulnerabilities Prioritization, evaluation of software vulnerabilities and proposal of mitigation measures 	<ul style="list-style-type: none"> Mitigation of potential cyber security risks and thus supporting the availability of services and reducing potential reputational damage Supporting all component types (independent of vendor), entire rail system can be monitored Compliance with laws, regulations and standards Enabling customers to plan the potential updates/major upgrades in advance 	<ul style="list-style-type: none"> Integration into Cyber Security Management System Support for 100% system availability 	

Monitoring of known vulnerabilities throughout an entire rail system life-cycle Our solution to secure your rail systems

Vulnerability monitoring and management is a comprehensive process for continuously identifying, assessing, classifying, remedying and reporting on security vulnerabilities over the entire lifecycle.

It requires a holistic view to identify all vulnerabilities of various rail systems (independent of vendor) and make informed decisions on how to mitigate vulnerabilities.

A seamless approach to minimize your attack surface and your risk from cyberattacks Implementation of vulnerability monitoring and management

- Define scope:** Define scope to be monitored and managed with customer. Update configuration data if necessary.
- Monitor:** Siemens Mobility monitors vulnerabilities and EOL information from multiple sources.
- Alert and report:** Siemens Mobility provides information to target groups (multiple ways).

Vulnerability Monitoring Systems

SMO OT vs IT/Cloud Security Monitoring Tooling

Product & Solution Security (PSS)

↑

VMS
Siemens Mobility Cyber Vulnerability Management System

Vulnerability Management System (VMS)

Cybersecurity Services: Tooling

MOTIVATION

Holistic View
of the security risk in the installed base products

Quick Access
to accurate product security information

Efficient Solution
to fulfil rail (cyber)security regulatory requirements

Centralized Platform
to drive and support security related workflows

Rail Business Specific
Cybersecurity risk evaluation

Continuous Support
in customer's security risk management

Transparency
of the security posture of the customer products

Fully-Managed
Vulnerability Monitoring and Risk Analysis

Direct Communication
of risks incidents to the customers

Compliant
with Rail Business specific norms and standards

Vulnerability Management System (VMS)

Vulnerability Management Process

Siemens Mobility Process

Component Scanner

SW Clearing

SVM

Vulnerability Management System

Implementation & Patching creation

Publication

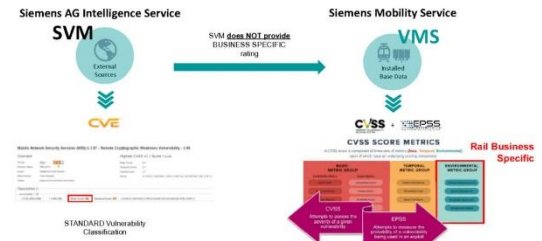
Vulnerability Management System (VMS)

The tool

VMS Killer Features (... among others)
Cyber security services



Standard Evaluation vs Business Specific Evaluation
SVM versus VMS



SMO VMM - VMS Contacts
Cyber security services



Dr. Michèle Barietta
michela.barietta@siemens.com
Technical Product Owner
Cybersecurity Services
SMO CS DS CVS CYS



Rail cyber security

附錄 A3 鐵路設備安全授權說明簡報



Authorisation of IT security equipment in railways sector – a proposal

Frank Weber, Deputy Head of IT Security Task Force

Eisenbahn-Bundesamt (EBA) (Federal Railway Authority, Germany)

EBA's Responsibilities

- According to **German General Railway Act (AEG)** and related laws
- Supervisory, licensing and safety authority for **railways and railway undertakings**
- "... avert danger resulting from railway operation or being emanated by operational facilities ..."

→ **Safety (also involving IT Security)**




2

Railway Infrastructure^(*) Authorisation


- Both individual and generic authorisation processes according to legal act (also as basis for supervision)
- **Generic infrastructure authorisation:**
 - **Approval for (generic) market placing and application** (per system type)
- National sector guideline (executive regulation), established in 2021
 - Processes for generic systems' authorisation assessment
 - Signalling, Telecommunication, and Electrical power supply

(*) Rolling stock authorisation based on TSI legal basis



What about IT Security?


- **S? T? E? IT Security!**
- Digitisation requires interconnected railway infrastructure equipment
- Interconnection via IT/OT networks → IT security required
- „Security for Safety“
- Logical functional elements vs. functions-combining products
- „Special case“ electrical power supply (energy industry act)



4


How to assess IT security for railways?

- Sector guideline section „IT security“
- General rules and preconditions
- Three phase validation model
- Additional partial process „IT security patch“



General rules and preconditions


- Derive IT security requirements from safety requirements specification
- „Generally accepted rules of technology“ vs. „State of the Art“
- TS 50701 → Cyber Security Case (CSC)
- Roles (Asset Owner, IT Security Integrator, Operator)



6


Three phase validation model

- Requirements specification
- Target specification
- Product



IT security requirements specification

- Initiated by operator
- Compile requirements spec (both IT security and system related requ.)
- Evaluation (clearance officer) → authority informed
- Significance decision and resulting process (in case of deviation from rules)
- Partial verification statement
- Partial CSC
- Provision of documents to IT security integrator



8

IT security target specification

- Initiated by IT security integrator
- Compile target specification
- Partial CSC
- Frequent security patching required? → Initiate patch process generation
- Assessment (authority-licensed IT security assessor) → authority informed
- Significance decision and resulting process (in case of deviation from rules)
- Inspection report (requirements hand-over to patch process if applicable)
- Provision of documents (incl. requirements coverage)

Product phase

- Initiated by IT security integrator
- Product development / establishing / provision
- Significance decision and resulting process (in case of deviation from rules)
- Partial CSC
- Assessment (authority-licensed IT security assessor) → authority informed
- Provision of documents to operator
- Inspection report
- Verification certificate (based on inspection report)

Partial process „IT security patch“

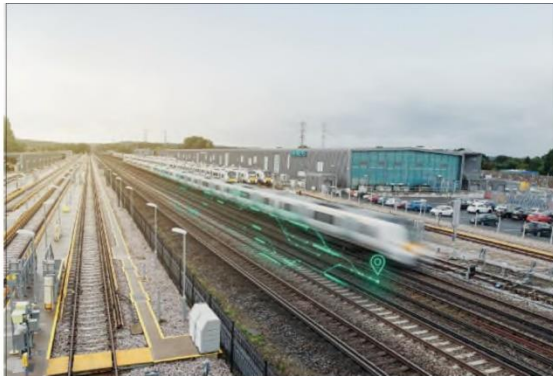
- Generic process to **define a specific process** to handle IT security patches available for the developed IT security product
- Initiated by IT security integrator
- Define **specific IT security patch process** (or verify given patch process)
- Assessment (authority-licensed IT security assessor)
- Inspection report
- Hand-over of documents to product phase

Summary

- Introduced new section of national railway sector guideline for generic authorisation assessment of IT security systems
- IT security systems/functions assessed and authorised independent of functional railway systems (signalling, telecommunication, electrical power)
- Additional partial process „IT security patch“
- Goal / benefit: Way to authorise fast-moving IT security technology (incl. security patching) for application in long-lasting railway safety systems

Thank you for your attention!

附錄 A4 Railigent 介紹



SECURITY ON THE RAILIGENT PLATFORM

Efficient and certified security for Railigent

Security is not just made on one layer and has multiple aspects to take care of. Within this document we give you an overview of typical aspects and mechanism we take care of to provide you as our customer with proper security in all our Software as a Service products on the Railigent® platform.



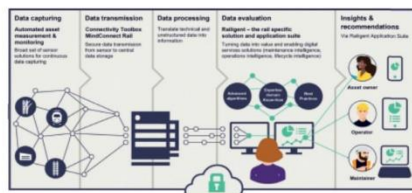
RAILIGENT

The Application suite that leverages IoT and AI for rail assets

Railigent makes intelligent use of rail asset data to create added value. It empowers rail operators, maintainers, and asset owners to understand their railway data, generate valuable information, and acquire deeper insights about the performance of their assets. The analysis of the rail asset data provided by these apps leads to improved operation, optimized maintenance, higher cost-efficiency, and ultimate 100% availability of rolling stock and wayside assets.

Railigent applications make use of our proven application platform, Amazon Web Services (AWS) public cloud services and IT infrastructure enhanced by build and deployment pipelines. They are integrated into a central User Portal, with security in mind, and share similar design and user experience to optimize business value.

How railigent works, step by step



Content

What is Railigent®?	3
ISO 27001 certification	4
Central User Portal	5
Privacy	6
Data encryption and communication policies	7
Secure application design and change process	8
Rail cyber security services	10
Contact	11

ISO 27001 certification

Ensure secure and state-of-the-art management

Railigent operations and support processes are externally certified to the ISO 27001 standard to ensure secure and state-of-the-art management of customer data and applications. Centralized support processes ensure in-time support of our customers, fully aligned with corporate and ITIL best practices.

ISO 27001 is a globally accepted standard for information security management. The scope of our ISO 27001 certification is defined as: Hosting and operation of Software as a Service (Railigent) for internal and external customers. This includes monitoring of the hosted environment, provisioning of ITIL-driven service processes (e.g. Change and Incident Management), user management, configuration of customer projects in the context of Railigent and vulnerability and patch management for the hosted software applications.

For this purpose, we are audited by an independent external organization on a yearly basis.

Operation Excellence

Railigent operation and support processes are within scope of our ISO 27001 certification to ensure secure and state-of-the-art management of applications and customer data. Centralized support processes ensure in-time support of our customers, fully aligned with corporate and ITIL best practices.



Central User Portal

Manage security policies centrally for a seamless user interaction

Railigent provides a central user portal as landing page for all our applications. There, the user can access the assigned application tiles only. All applications use single-sign-on (SSO) technologies to give the user a seamless experience and grant the correct role within the application automatically.

The central user portal within Railigent manages the security policies centrally and offers SSO for a seamless user interaction in between applications.



Railigent Application Suite

User and password policies

Access to this portal and dedicated applications is provided on a need-to-know basis via well-defined processes. A user account can only access and interact with applications assigned to the account. The user accounts and corresponding access rights are reviewed on a yearly basis. A user must be a natural person and account sharing is prohibited. The portal possesses global policies for authentication retries and will lock the account on a reached threshold. Such events also trigger notifications to the user and events in our security monitoring.

The central user portal allows us to enroll global password policies to ensure password complexity meets state of the art security requirements.

Currently we enforce:

- minimum 12 characters,
- maximum validity of 180 days
- complexity: lower, upper, number symbols,

Passwords are of course solely stored as a hashed value to ensure they are only known by the user and cannot be misused in any form.

5

User Privacy

General Data Protection Regulation (GDPR)

Within Railigent user portal we comply with the European General Data Protection Regulation. This privacy and security law regulates, for example, what kind of (personal) data may be kept, stored and processed.

We follow a strict policy regarding data encryption at rest and in transit.

EU GDPR

EU GDPR does not specify a strict retention period for personal data. Instead, it states that personal data may only be kept in a form that permits identification of the individual for no longer than is necessary for the purposes for which it was processed. Once the purpose vanished the data must be deleted.

Retention time

In our Railigent user portal the retention time of logs containing personal data is conform to EU GDPR requirements and is currently deleted after 90 days.

We review on a regular basis if the periods are still valid or should be adjusted.

Besides that, project specific retention times of project data can be agreed.

7

Multi Factor Authentication

The user portal supports a variety of multi factor types. A user shall configure at least one MFA method during the user onboarding and activation process. Of course, a user can configure all of them and choose the preferred method at every login by dropdown. The portal will auto-suggest the last used method.

The current supported methods are:

- SMS
- Voicecall
- Google Authenticator
- Okta Verify App (incl. Push)

Whenever an application is integrated in our portal, we ensure through our processes that based on the criticality of the applications, a decision is made if an MFA is enforced or not. Enforced MFA means that the usage of the application is solely granted when the MFA was successfully passed. A successful MFA is typically valid for a workday.

Single sign-on

All of the applications within our Railigent user portal make strict usage of single-sign-on (SSO) technologies based on industry standards like openid or SAML.

With this mechanism we ensure that the user authenticates only once and accesses all assigned applications with the correct role automatically. Just one click away.

User management

We ensure that user management is defined, documented, and audited on a regular basis. User authorization is defined on a need-to-know basis and guarantees that each person solely can access applications and data required for working tasks in the least applicable role assignment. Such assignments are further reviewed on a regular basis. On- and offboarding of users is handled with care and is prioritized. Each change on grants is documented for audit reasons and requires approval from assigned user managers (e.g., the superior or a project responsible).

6

Data encryption and communication policies

Secure communication and data storage

Within Railigent we have strict data encryption rules and maintain these rules globally within each application where data is transferred, stored, or processed. We apply state of the art encryption for all our Railigent applications and interfaces to ensure confidentiality is handled with care.

Encrypted communication

At all applications and interfaces within Railigent, regardless of whether these are used for user interaction or data transfer, solely encrypted communication is used. We further use state of the art encryption technologies, aligned with current best-practice recommendations issued e.g., by the ISO, NIST, or other respected entities. For machine-to-machine communication certificates are used and have an adequate lifecycle management behind them.

Data at rest

All our databases and file storages use additionally encryption per global policy to ensure confidentiality of all data stored. Retention time of data in general is also processed by global policies.

EU projects

Regarding EU GDPR we ensure that such data is solely stored within the EU and solely if we are legally allowed to store it.

Security over the whole process



8

Secure application design and change process

Focus on security by design

Ensuring application security for the whole lifecycle is a challenging task. Within Railigent and Siemens we have strict processes regarding application development, operation, and lifecycle. We focus on security by design to ensure all your applications have security build in from the start.

We focus on security by design to ensure application security during the whole lifecycle.

Application blueprints and design principles

Within Railigent we make use of application blueprints to ensure OS, databases, and services are hardened and configured in a secure way directly from the start. Services and components are running with least privileges, have a centralized logging and monitoring included and a predefined secure network zone concept.

Deployment automation

A DevOps tool chain is in place for all applications in Railigent. This includes a fully automated build pipeline, artifact repository, code quality testing and analysis, robot framework for testing automation together with additional tools. The tool chain is mandatory for managing production workloads and is the basis for efficient secure and reproducible software builds, deployments, and operations. Additionally, it does support restore and recover procedures.

Product and Solution Security within Siemens

During the creation of an application or service we ensure that defined security and design principles are fulfilled, by standard processes and quality gates. For each application threat modelling methods are used where security experts engage with developers and architects. This ensures confidentiality, integrity, and availability for each data asset, component, and service for the application. We further analyze the trusted communication and involved interfaces to limit the attack surface for each component and service. This also includes regular reviews of the secure network zone concept.

Penetration testing

We make use of penetration testing teams to test the security of all involved components, application design and role grant definition under realistic attack scenarios and to make sure that the applications meet the required security requirements. Such penetration tests are typically carried out in a non-productive environment to ensure only secure applications are deployed to production and we avoid service outages as side effect of a penetration test activity.

Application and service review

Before an application is handed to our operation and service team and released into the production environment a final review is conducted by security and operation experts. This review verifies that all quality gates and service definitions have been finalized before a customer can access an application or service. We want to ensure everything is ready for our customers. Not just the application but the whole service.

Continuous monitoring

For each application we monitor the availability of each component and service involved. We ensure availability and performance requirements per service level agreement with our customers.

Secure application lifecycle process

To ensure security through the whole lifecycle of an application we have a defined vulnerability monitoring and patch management process. Depending on the application we might make use of a defined patch windows to rebuild our application infrastructure automated to the latest software version.

Railigent operators and support processes in scope of our ISO 27001 certification to ensure secure and state-of-the-art management.

Incident Management

Preparedness is important as, regardless of how well cybersecurity is implemented on a technical and organizational level, incidents might still occur. Siemens Mobility is prepared and has implemented Incident Management across the organization to ensure a fast reaction on such events.

If a customer encounters a suspicious event, she can always reach out to the Siemens Product CERT by mail (productcert@siemens.com).

Further details, also related to Siemens' responsible disclosure process for vulnerabilities in our products and services, are available on the Internet¹.

¹ https://www.siemens.com/global/en/products/mobility/secure_cert.html

Rail cyber security services

Ensuring sustainable rail security

Availability, reliability, and security: These are the challenges every rail operator is faced with – concerning both rail infrastructure and rolling stock. Gaps in cyber security can prevent these targets from being met or even damage the operator's reputation. For this reason, ensuring sustainable cyber security for all rail systems is a fundamental requirement for smooth and safe operation. With cyber security services, we help you to analyze your systems, identify potential vulnerabilities, and define and implement measures to protect your assets.

Cyber-attacks on industrial systems are becoming increasingly common and can cause devastating damage. Also, rail systems are potential targets for hackers. Their typical lifecycles of 20 years or more make them even more vulnerable. Only a regular review of the security status can protect them. Governments and public institutions have recognized the importance of cyber security for critical infrastructures and therefore also for rail transport. Laws and initiatives that stipulate minimum standards and regular reviews have already been adopted by many countries. New international standards (such as IEC 62443 and ISO 27001) lay the foundations for cyber security in systems and organizations.

To ensure sustainable cyber security for rail operators, we have developed Cyber security services. The multilevel service comprises the following modules:

Rail security gap analysis

- Assessment of the current system architecture and processes
- Identification of security gaps
- Risk evaluation
- Recommendation of measures to minimize the risks
- Optional: penetration tests

We assess the status quo using a test catalog specially tailored to rail systems in accordance with IEC 62443. As well as technical systems, we also consider internal operational workflows.

If required, we perform penetration tests to simulate cyber-attacks. This means that our security specialists carry out a hacker attack in agreement with our customers. Based on the results of the analysis, we propose measures to improve cyber security.

Rail security concepts and implementation

- Implementation of measures such as system hardening
- Optimization of processes, etc.

We work with you to implement the tailored rail security concept.

Continuous monitoring of rail security

- Ongoing review of the rail security status
- Proactive threat reporting
- Support if incidents occur

The system data flows are monitored automatically in real time. Irregularities and potential threats are detected quickly and reported reliably.

Rail security training

- Standardized training courses, e.g., as web-based trainings
- Customer-specific training

Employee conduct is a decisive factor in rail security. We train your staff and turn them into key allies in the fight against cyber-attacks.



Assess the current situation and identify risks

The first step towards cybersecurity in railway systems is a precise status analysis.

Provide the utmost security

The assessment of possible risks and evaluation of required protective measures is followed by the implementation of your individual protection concept for cybersecurity.

Always be alert and ready to react

Cybersecurity in railway systems can only be maintained permanently if the continually changing threat situation is constantly and closely monitored.

OPEN QUESTIONS?

Contact

Hopefully we could give you an introduction in our security practices. In case you have additional questions please contact your local SMO representative or approach our global security team.

Cybersecurity (general):
Michael Dietz
dietzmichael@siemens.com

Railigent sales:
Gerhard Paal
gerhard.paal@siemens.com

Rail cyber security portfolio:
Swantje Weiss
swantje.weiss@siemens.com

Rail cyber security sales:
Martin Kunz
martin.kunz@siemens.com

Published by
Siemens Mobility GmbH
Otto-Hahn-Ring 6
81739 Munich, Germany
contact.mobility@siemens.com

Dokumentnummer MOCS-810079-00-7600
Depo.Nr.: Z1716

Subject to changes and errors

The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Further information is available at: www.siemens.com/mobility.

附錄 A5 電氣化公路介紹簡報




An update on the Dutch ERS developments

Arjan.van.viet@mni.nw.nl
Vienna June 2024



AGENDA

1. Why ERS?
2. Update on ERS studies
3. Work in progress
4. Questions




Wegen vrachtwagenheffing

Heavy Duty Vehicle Charge in The Netherlands

- > The law was passed in parliament and the senate last year and is now being implemented.
- > The expected start of the toll is 2026.
- > Trucks pay an average of €0.15 per kilometer (price level 2019) on the toll network.
- > The toll rate is differentiated according to weight and CO₂ class.
- > All trucks will have a GPS box. The system is interoperable with German and Belgian systems.


Return of Heavy Dutch Vehicle Charge

- > Part of these revenues is reserved for the sustainability and innovation of road transport. This is approx €400 million per year.
- > Spending in consultation with the road transport sector.
- > Approx 100 mln. EUR reserved for ERS



Electrification of Heavy Goods Vehicles

Grid capacity slows down the climate ambitions

Four Dutch studies on ERS finalised



And more TU Delft studies

Prospects for Electric Road Systems on the Dutch freight corridors: results of 5 projects

Lári Tavassy, Mahnam Saeednia, Janske Otten, Ximeng Liao, Kevin Duijn, Mo Wang + Universiteit Antwerpen

TU Delft, October 2023

Recent studies on ERS for NL

5 MSc students of TU Delft & connected work from University of Antwerp

- **Policy options:** Cost-Benefit Analysis of Energy options (Janske Otten, Port Authority Rotterdam) + Impacts for Small and Medium Sized Enterprises (Roxana de Nie, IenW – ongoing)
- **Network vision:** What is optimal ERS network size? (Ximeng Liao, DAF)
- **Concrete projects:** Trajectory choice R'dam-Antwerp corridor (Kevin Duijn, Siemens + University Antwerp)
- **Technology assessment:** Overhead lines or induction? (Mo Wang, TUD)

The Dutch E-CORE connection

- › TNO and TU Delft are selected
- › Mid term results delivered
- › Final report November 2024

TNO/TU Delft objective

Assess the potential of ERS in reducing costs and improving efficiency for the logistics sector compared to a stationary charging-only scenario.

TNO/TU Delft interim result

- › Very sensitive to assumptions
- › A negative net present value.
- › When more positive assumptions are made the CBA can turn positive easily
- › More detailed analysis to limit the uncertainties.

Community building

- › 15 interviews with potential users
- › Presentation on the national transport association
- › Community meeting on the 24th of June

If we start..then finding the right financial tooling

- › Open procedure
- › Restricted procedure
- › Competitive negotiated procedure
- › Competitive dialogue
- › Innovation partnership
- › Design contest

Financial options


- › National funds
 - Return flow truck toll 100 million
 - Climate fund 20 million
- › European funds: European investment Bank
- › Private
 - Banks and companies
 - Pension funds

The Dutch Road authority RWS

- Current focus on the quality of the existing networks
- Ongoing discussion sustainable networks versus today's needs
- Several concerns that need to be addressed.

Electric Road Systems: Where do we want to go?

Electric Road Systems (ERS) enable electric trucks to charge while driving. This is done using an overhead line and a current collector (pantograph), similar to a train or trolleybus.



2024 - 2025 start of the construction phase

2026 start of the construction phase

2028 (completed) Rotterdam - Antwerp road - truck test

2032 (completed) Rotterdam - Vlissingen - coast lane

2040 open to all vehicles

Advantages


- High energy efficiency: Charge and drive without mechanical transmission, resulting in 90% energy efficiency.
- Low efficiency due to the conversion of energy from electricity to mechanical energy.
- Additional electrification of heavy transport: Low efficiency due to the conversion of energy from electricity to mechanical energy.
- Low and medium capacity: existing networks are not suitable for heavy transport.
- High capacity: existing networks are not suitable for heavy transport.
- High capacity: existing networks are not suitable for heavy transport.

Attractive Business Case

- Low energy and low maintenance costs: High energy efficiency and low maintenance costs.
- High energy efficiency: High energy efficiency and low maintenance costs.
- High energy efficiency: High energy efficiency and low maintenance costs.
- High energy efficiency: High energy efficiency and low maintenance costs.
- High energy efficiency: High energy efficiency and low maintenance costs.

Status

- Rotterdam - Vlissingen - coast lane: High energy efficiency and low maintenance costs.
- Rotterdam - Antwerp road: High energy efficiency and low maintenance costs.
- Rotterdam - Vlissingen - coast lane: High energy efficiency and low maintenance costs.
- Rotterdam - Antwerp road: High energy efficiency and low maintenance costs.
- Rotterdam - Vlissingen - coast lane: High energy efficiency and low maintenance costs.



Ministerie van Infrastructuur en Waterstaat

Thank you for listening!