中華資安國際
CHT Security

自駕車運行安全與防護

中華資安國際股份有限公司
洪進福 總經理
2021.03.03

Outline

1. 汽車安全的定義
2. 汽車安全的趨勢
3. 汽車安全的國際標準
4. 從汽車攻擊與檢測案例看汽車資安防護
5. 自駕車實證場域案例分享

中華資安國際
CHT Security

中華資安國際
CHT Security

0. 中華資安國際簡介

公司簡介

2017年成立 | 實收資本額3.09億 | 員工 196人

領先業界之專業能力！

中華資安國際
CHT Security

中華電信集團的**資安專業公司**，服務超過上百家

具備**國家級資安專案建置能力與實績**

2003年開始經營資安業務，**於北中南區有服務據點**

獲獎紀錄

2019

- 工研院民生公共物聯網**漏洞挖掘**邀請賽 第三名
- TWCSA紅色警戒72小時(Red Alert 72) 亞軍

2018

- **HITCON Defense企業資安攻防大賽冠軍** 及情資分享特別獎
- 工研院2018 資安滲透測試攻防國際邀請賽 冠軍

公司成立迄今，連續獲得最新行政院共契之評鑑「全項A級」廠商！

A級資安團隊 (2020)

2020 --- 行政院資安共同供應契約評鑑

序號	受評廠商	SOC 監控服務	資安健診服務	弱點掃描服務	滲透測試服務	社交工程 郵件測試服務
3	中華資安	A 級	A 級	A 級	A 級	A 級

提供事前檢測、事中監控應變、事後事件調查的資安服務

1. **上網資安防護服務**：ISP雲端的入侵防護服務、DDoS防護服務、防駭守門員、APT防護、新世代防火牆、WAF等
2. **資安專業服務**：紅隊演練、滲透測試、IoT檢測、資安健診、金融安全評估、SOC監控、MDR、事故應變與鑑識調查、工控(ICS)資安
3. **資安顧問**：ISMS/PIMS制度導入輔導、資訊安全評估、PKI建置規劃
4. **資安管理平台規劃建置**：資安監控分析通報平台、弱掃管理平台、資安資訊分享與分析系統(ISAC)、網路威脅偵測與應變系統(SecuTex)
5. **身分識別產品與應用**：安全晶片與PKI應用、加密安全通訊解決方案
6. **企業資安整體解決方案**：資安、網路、雲端、軟硬體整體解決方案之規劃及建置

公司簡介

2017年成立 | 實收資本額3.09億 | 員工 196人

紅隊演練/駭客攻防/資安檢測/SOC/事件處理(IR)經驗豐富！

工控場域資安服務實績

通過ISO 17025認證之資安鑑識與檢測實驗室

台灣電力公司 TAIWAN POWER COMPANY　台灣高鐵 TAIWAN HIGH SPEED RAIL　Accton Making Partnership Work　台灣自來水公司 TAIWAN WATER CORPORATION　台灣中油股份有限公司 CPC Corporation, Taiwan

滲透測試與紅隊演練服務實績

國內唯一通過ISO 20000之紅隊演練服務商

中華民國總統府 Office of the President Republic of China (Taiwan)　富邦金控　國泰世華銀行 Cathay United Bank　tsmc　玉山銀行

臺灣證券交易所 TWSE　中華郵政　財金資訊股份有限公司 FINANCIAL INFORMATION SERVICE CO., LTD.　臺灣集中保管結算所 TDCC Taiwan Depository & Clearing Corporation

政府、金融、交通、科技、醫療業及跨國公司資安服務

國內最大的資安服務商

中華民國總統府 Office of the President Republic of China (Taiwan)　AOI APPLIED OPTOELECTRONICS, INC.　NUVOTON DIRECT　ST Electronics　TH INDUSTRIES　tsmc

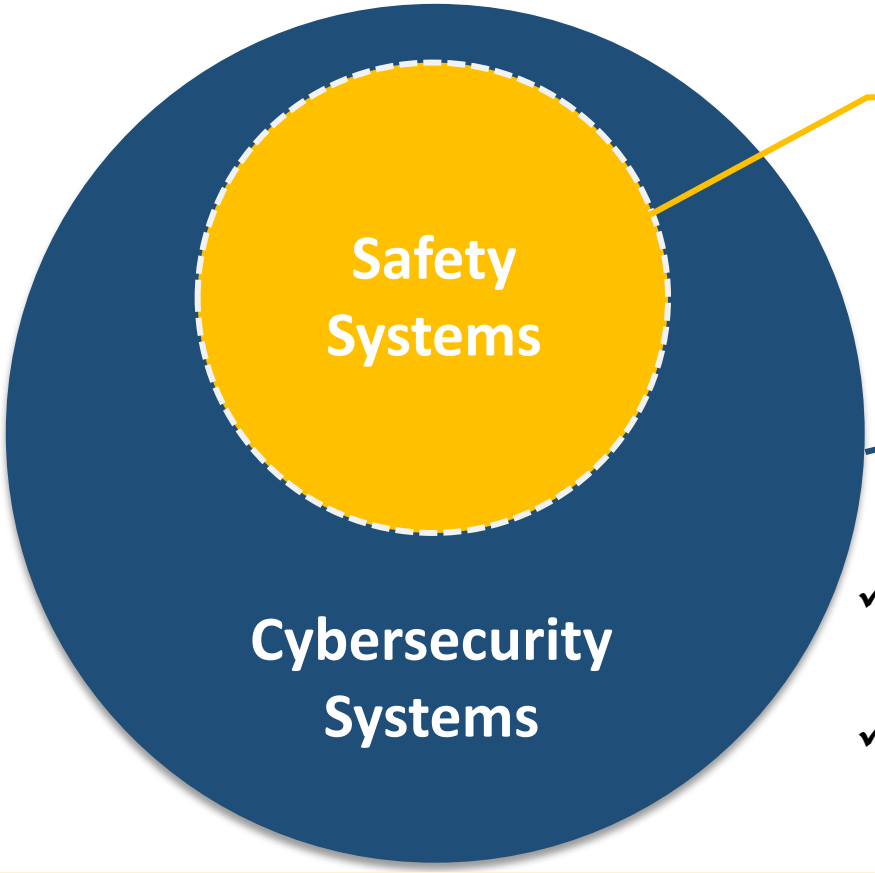
EVA AIR 長榮航空　交通部臺灣鐵路管理局 Taiwan Railways Administration.MOTC 安全、準確、服務、創新、團結、榮譽　winbond 華邦電子　LITEON 光寶科技　中興保全 SECOM

IGS鈊象電子 http://www.igs.com.tw　NUVOTON DIRECT　Panasonic　世界先進 VIS

1. 汽車安全的定義

明確區分功能安全（Functional Safety）與資通安全（Cybersecurity）

汽車安全的 Cybersecurity與 Functional Safety定義



Functional Safety 功能安全

功能安全相關系統失效時，會造成**生命**、**資產**或**環境**面向的傷害

Cybersecurity 資通安全/數位保全

資訊安全相關系統失效時，會造成**財務**、**營運**、**隱私**、**安全**面向的傷害

- ✓ 資訊安全防護的範圍包含功能安全，因為**資安攻擊將直接或間接對功能安全造成危害**。
- ✓ 車聯網的發展趨勢下，「**資通安全**」已和「**煞車功能**」一樣屬於**行車安全的基本需求**。By CEO of Jaguar Land Rover, Sir Ralf D Speth

Functional safety is the part of the overall safety of a system or piece of equipment that depends on automatic protection operating correctly in response to its inputs or failure in a predictable manner (fail-safe).

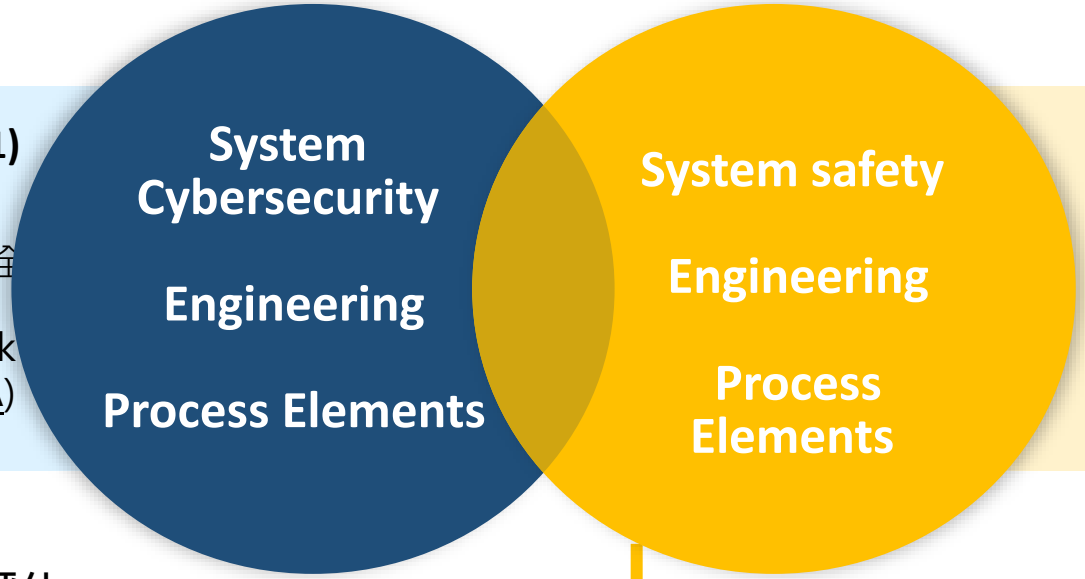
Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

Cybersecurity vs. Functional Safety 比較

ISO/SAE 21434 (prev. J3061)

Cybersecurity **資通安全**/數位保全

Threat Analysis and Risk Assessment (**TARA**)



ISO26262

Functional Safety **功能安全**

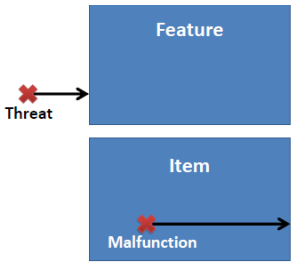
Hazard Analysis and Risk Assessment (**HARA**)

✓ **資通安全風險評估：**

TARA，是將「**外部威脅**」納入評量，針對「**威脅**」所造成的**功能失效**剖析**Safety**、**Privacy**、**Finance**、**Operation**四個面向的風險評估。

✓ **功能安全風險評估：**

HARA，是基於**封閉框架**的假設，針對「**意外**」所造成的**功能失效**進行安全性評估。



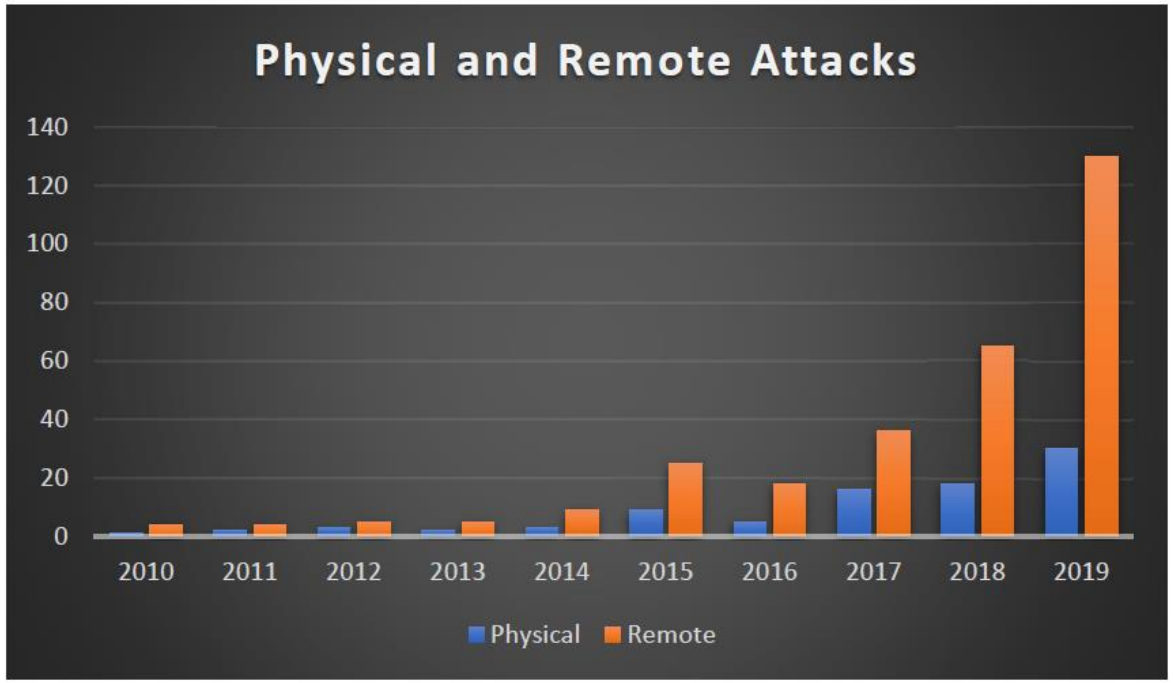
HARA focuses on identifying and categorizing of malfunctions in the item which can lead to a hazard, whereas TARA focuses on threats to a feature

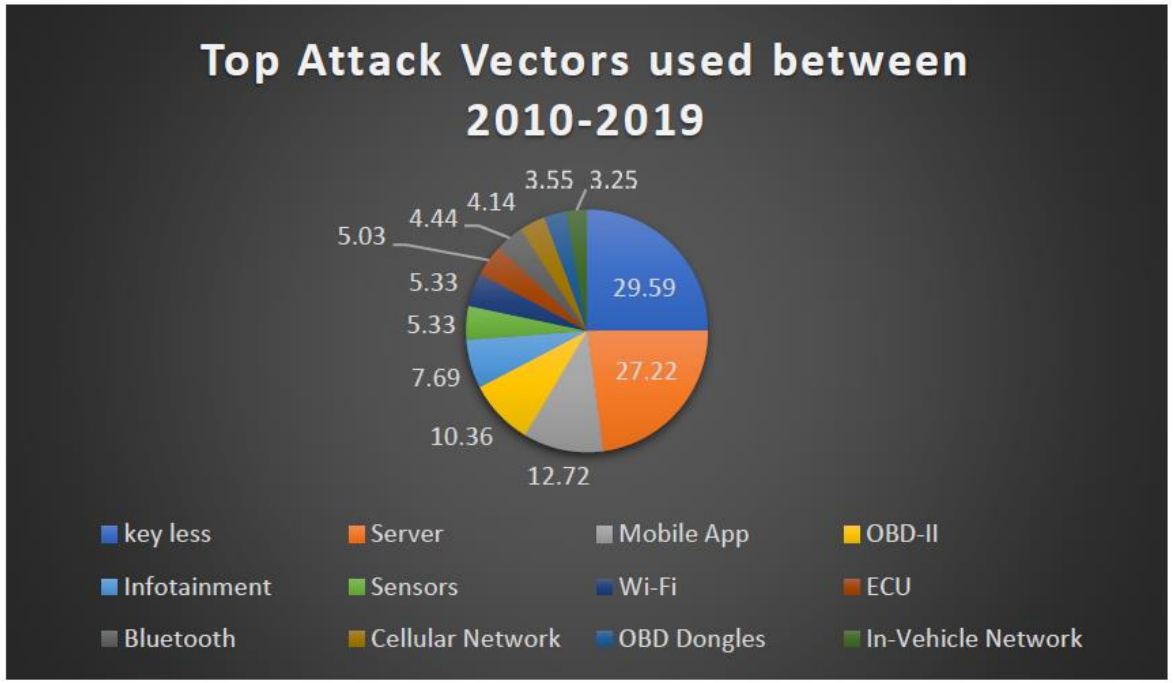
中華資安國際
CHT Security

2. 汽車安全的趨勢

2019汽車攻擊統計數據

- 統計上來看，實體或遠端攻擊次數在近五年內呈現指數成長。
- 伺服器、Keyless、行動App及OBD-2為主要的攻擊向量，總佔比約80%。





Ref: Upstream Security and Global Automotive. UPSTREAM SECURITY's Global Automotive Cybersecurity Report. Technical report, 2020

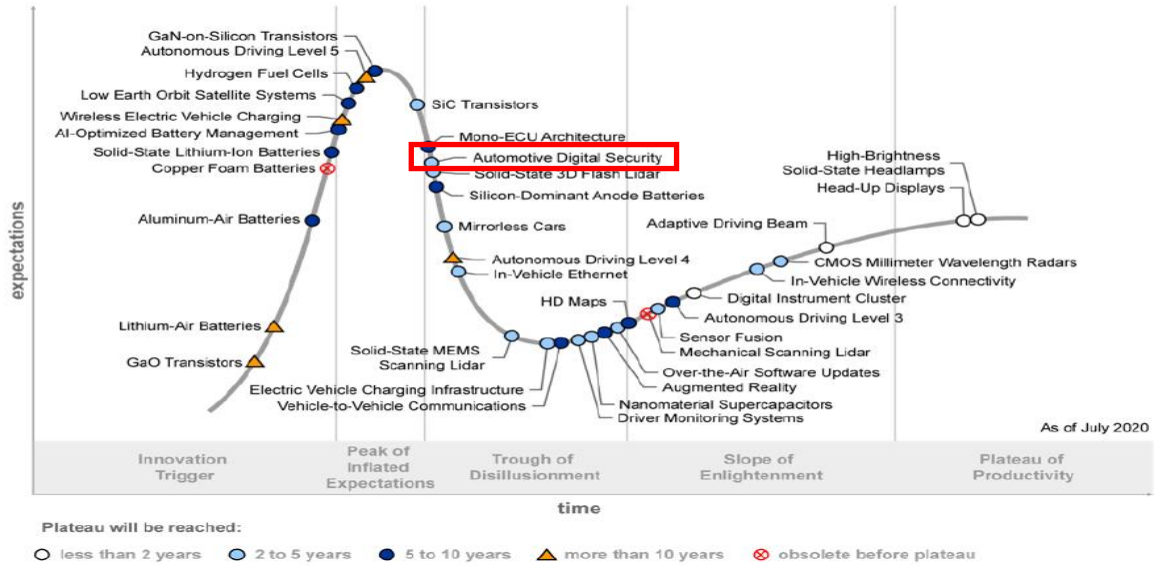
2020汽車優先技術矩陣

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational		Automotive Digital Security	Aluminum-Air Batteries Hydrogen Fuel Cells Low Earth Orbit Satellite Systems Vehicle-to-Vehicle Communications	Autonomous Driving Level 4 Autonomous Driving Level 5 Lithium-Air Batteries
high		In-Vehicle Ethernet In-Vehicle Wireless Connectivity Nanomaterial Supercapacitors Over-the-Air Software Updates Sensor Fusion SiC Transistors Solid-State 3D Flash Lidar Solid-State MEMS Scanning Lidar	AI-Optimized Battery Management Augmented Reality GaN-on-Silicon Transistors HD Maps Mono-ECU Architecture Silicon-Dominant Anode Batteries Solid-State Lithium-Ion Batteries	GaO Transistors
moderate	Head-Up Displays High-Brightness Solid-State Headlamps	CMOS Millimeter Wavelength Radars Driver Monitoring Systems Electric Vehicle Charging Infrastructure Mirrorless Cars	Autonomous Driving Level 3	Wireless Electric Vehicle Charging
low	Adaptive Driving Beam Digital Instrument Cluster			

As of July 2020

- ✓ **汽車數位安全**將在**2~5年內**變得廣泛可行，這項技術本身**不會改變用戶體驗**，但是這項技術的**好處是可轉化**的
- ✓ 要實現**無線軟體更新(OTA)**和**車對車通訊(V2V)**，須確保**汽車有能力緩解網路攻擊**的威脅

Hype Cycle for Automotive Technologies, 2020

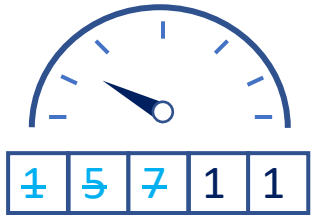


Ref: Gartner Hype Cycle for Automotive Technologies, 2020

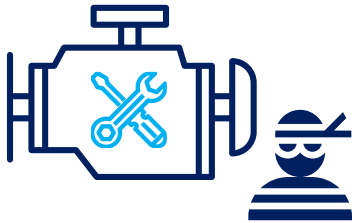
汽車網路安全威脅

Local Attacks

Tampering the odometer

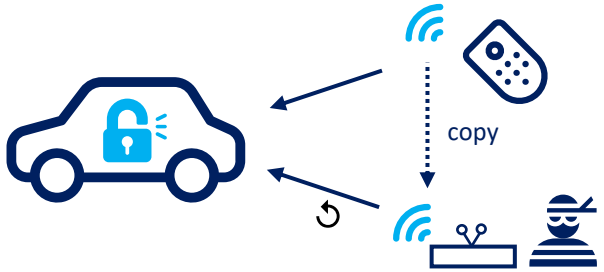


Engine tuning



Remote Attacks

Vehicle theft by relay attack

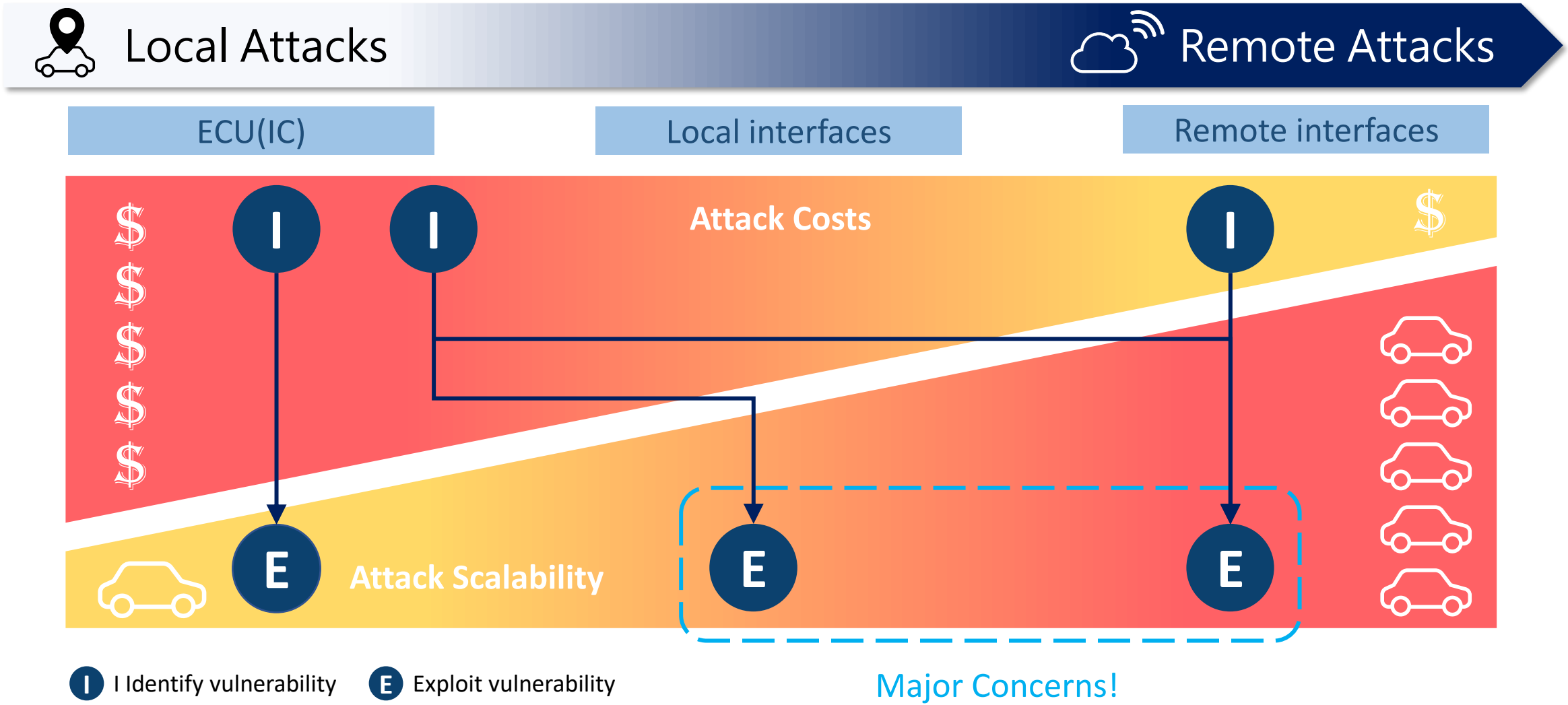


Ransom for a drive

Remote hack of an unaltered car

Ref: . 2019 NXP Tech Day- Automotive Cybersecurity:It's More Than Just Cryptography| 2019-11-21

攻擊成本與影響範圍



Ref: . 2019 NXP Tech Day- Automotive Cybersecurity:It's More Than Just Cryptography| 2019-11-21

中華資安國際
CHT Security

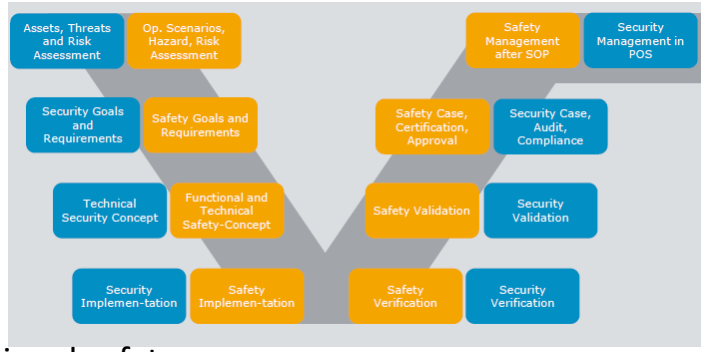
3. 汽車安全的國際標準

功能安全(Functional Safety)與資通安全(Cybersecurity)的國際標準

- 車用電子產品生命週期各個階段，**功能安全**與**資通安全屬於同步進行關係**，各階段包含風險評估、安全目標訂定、功能規格設計與測試以及評級認可等執行項目
- 對於**功能可靠性與可用性**而言，**資通安全是確保功能安全的先決條件**

Functional Safety
(**ISO 26262**, IEC 61508, ISO/PAS 21448)

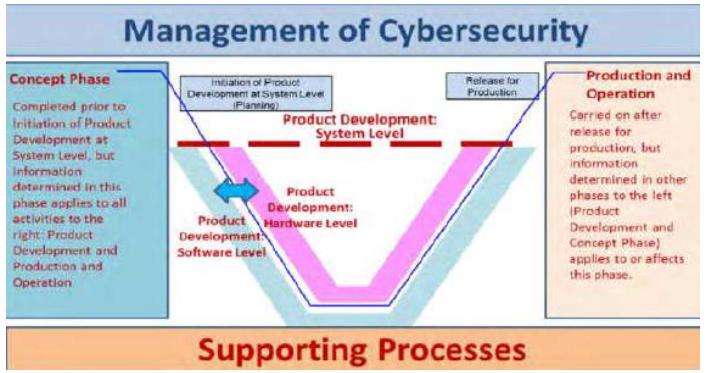
- Hazard and risk analysis
- Functions and risk mitigation
- Safety engineering



ISO 26262:2018 does not address security but requires trade-offs without impact on Functional safety.

Cybersecurity
(**ISO 21434**, **J3061**, ISO 27001, ISO 15408)

- Threat analysis and risk assessment
- Abuse, misuse, confuse cases
- Security engineering



Security and Safety are inter-related and demand holistic systems engineering

汽車電子服務資通安全相關標準

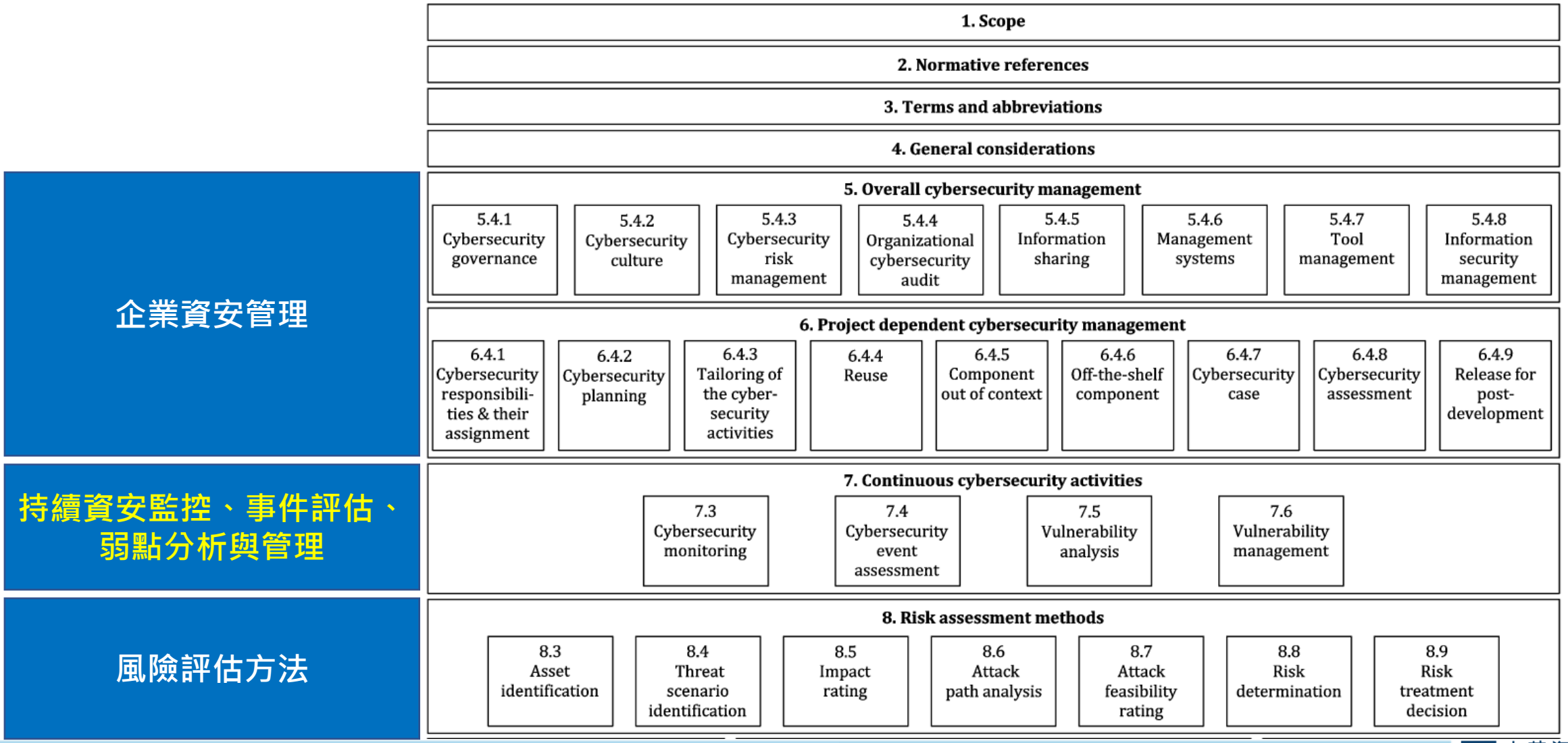
■ 汽車資訊安全

- UN ECE Regulation 155資安規範將成為歐洲車輛及車廠必須遵循的法規
- **ISO/SAE 21434 將取代J3061成為汽車資通安全的主流標準**
- ISO PAS 5112 將作為資安管控與稽核的指南

■ 車用軟體更新

- UN ECE Regulation 156 軟體更新規範將成為歐洲車輛必須遵循的法規
- **ISO/AWI 24089將成為車軟體更新與管理的主流標準**

ISO 21434章節架構



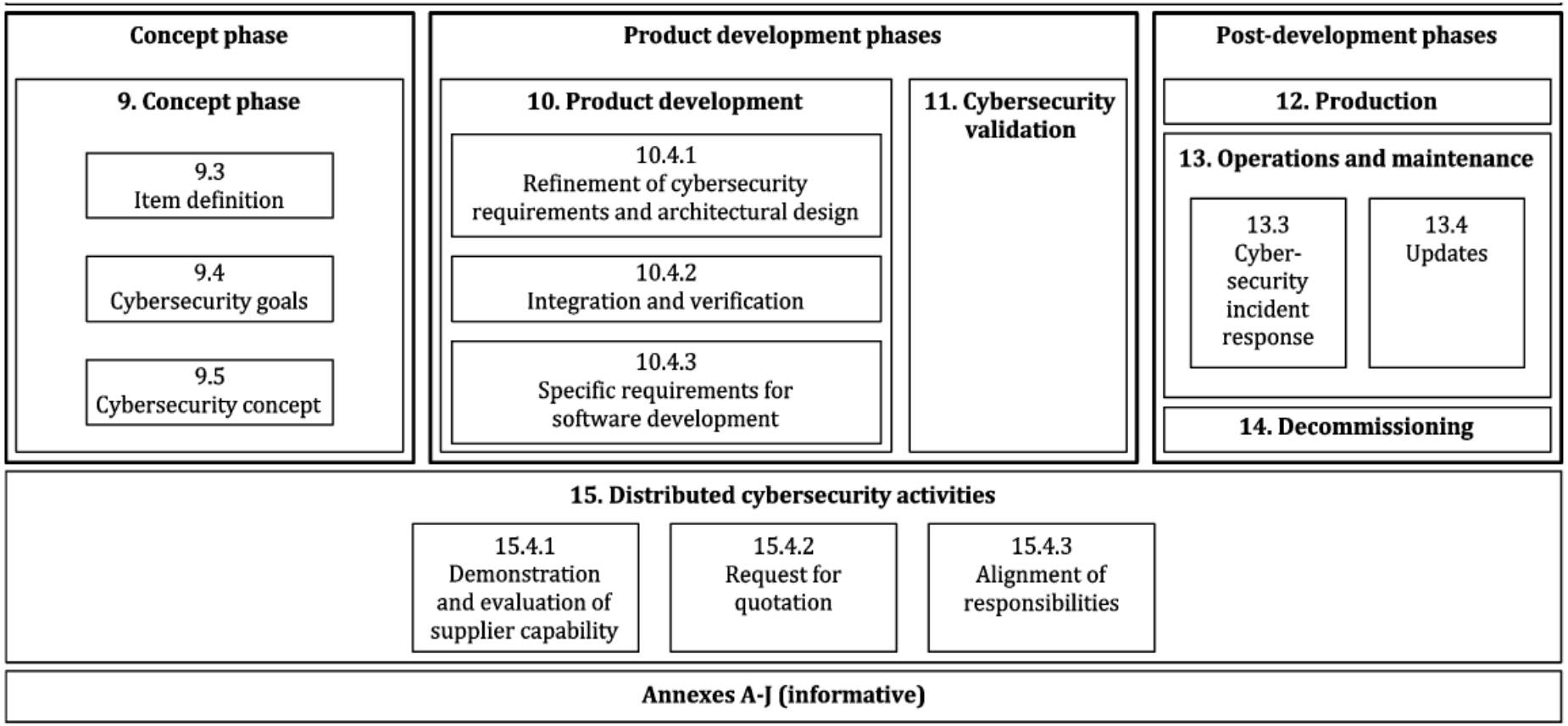
企業資安管理

持續資安監控、事件評估、弱點分析與管理

風險評估方法

ISO 21434章節架構(續)

9. 概念階段：定義資產、資安目標及風險考量
10. 開發階段：資安規格、完成布署資安需求
11.驗證階段：車輛之資安等級
12：生產階段：製程中須考量之資安面向
13：操作及維護：事件回應與更新
14：汰舊/服務終止須考量之資安面向
15：供應鏈管理



ISO 21434 著重於整體企業與產品資安管控的方法論，較無技術面及實際解決方案之論述

Threat Analysis and Risk Assessment (TARA)

1. Threat Assessment

威脅模型

攻擊可行性	評估標準
High	攻擊路徑**可輕易取得網路連線**進而成功執行攻擊活動。
Medium	攻擊路徑**必須避開網路面防護措施**，才可執行攻擊。
Low	攻擊路徑**無法透過網路入侵**的機會，**但可透過開放存取埠**，如USB和記憶卡。
Very low	駭客**必須執行實體破壞**後才有機會發動攻擊。

2. Risk Assessment


Safety


Operation


Finance


Privacy

Risk matrix (example)		**Impact *(S,O,F,P)***			
		Severe	Major	Moderate	Negligible
Attack Feasibility	High	HIGH	HIGH	Medium	Low
	Medium	HIGH	Medium	Medium	Low
	Low	Medium	Medium	Low	Low
	Very Low	Low	Low	Low	Low

V-model產品開發工作流程

[V左半部]

- 整車系統及軟/硬體元件之**架構設計**

[V右半部]

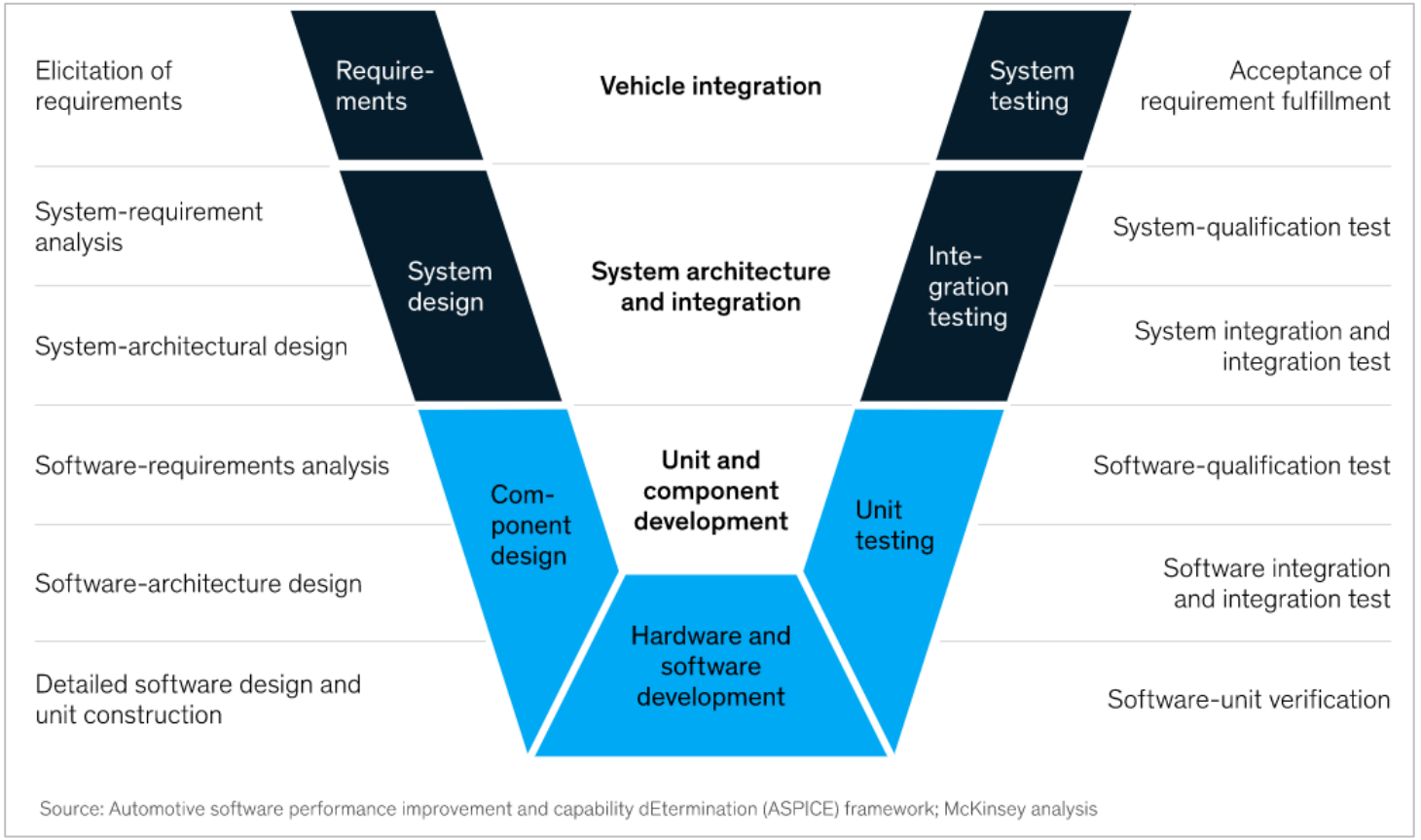
- 整車系統及軟/硬體元件之**架構整合、測試和驗證**

[V上半部]

- **整車系統**層級（OEMs）

[V下半部]

- **軟/硬體元件**層級（Suppliers）



UN – 汽車製造商須具備CSMS合規證明

- 聯合國法律規範將要求**汽車相關製造商**須取得**資通安全管理系統**（CSMS, Cyber Security Management System）之認證
- 第六章要求務必具備**CSMS相關合規證明**，應用範疇須包含**開發階段**、**生產階段**及**生產後期階段**

United Nations ECE/TRANS/WP.29/2020/79 REVISED

Economic and Social Council

Distr.: General
23 June 2020

Original: English

Economic Commission for Europe

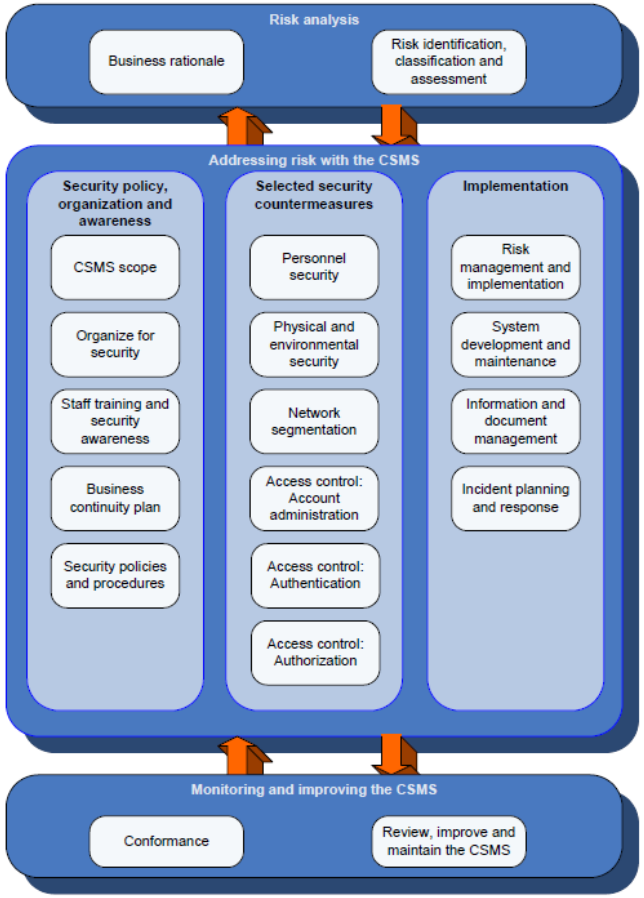
Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

Submitted by the Working Party on Automated/autonomous and Connected Vehicles

如 ISO/SAE 21434 描述，
CSMS 參考IEC 62443 2-1



我們如何協助智慧製造導入 CSMS(IEC 62443) 管理制度

一般
IEC 62443-1系列

定義概念、模型、術語、詞彙、指標、案例等

系統
IEC 62443-3系列

針對工控系統定義安全風險評估及安全需求

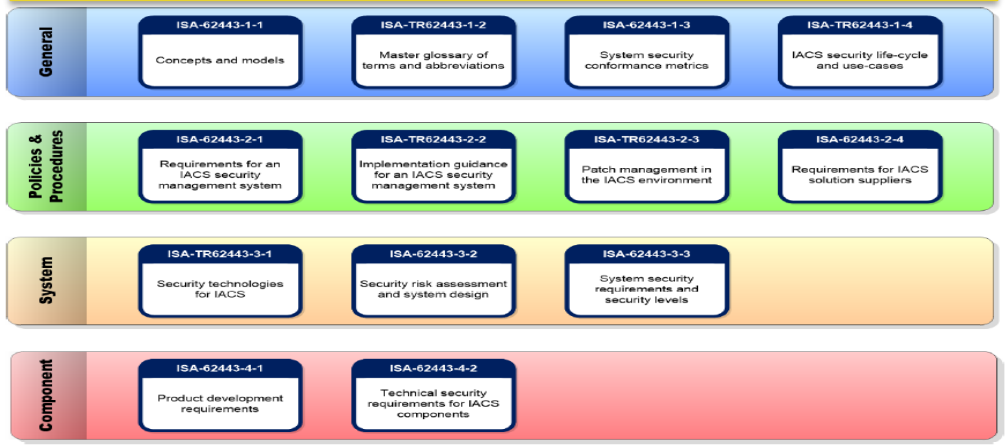
政策與程序
IEC 62443-2系列

針對IACS資產擁有者及IACS服務提供商定義管理系統的相關需求

組件
IEC 62443-4系列

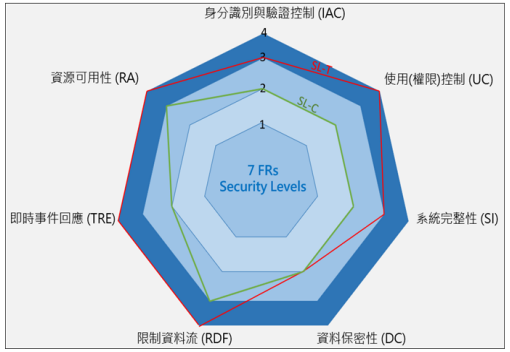
針對產品供應商定義安全產品開發流程及組件安全需求

IEC 62443 系列標準整體架構



IEC 62443 系統基本資安需求控制項實施紀錄

1. 資安水準評估



2. 弱點與威脅建模

[弱點識別與威脅建模]

- 根據資產清單、應用服務及網路行為事件等資訊進行弱點識別並套用威脅模型(如:STRIDE)識別該網區/通道之潛在威脅。

[攻擊路徑模擬]

- 透過該工具模擬新的攻擊路徑，並針對模擬演練所帶來的影響做更進一步分析。

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

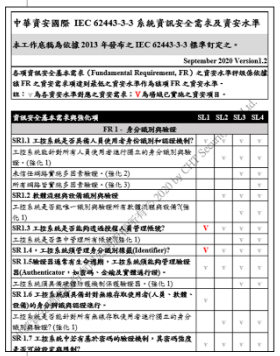
3. 危害性評估

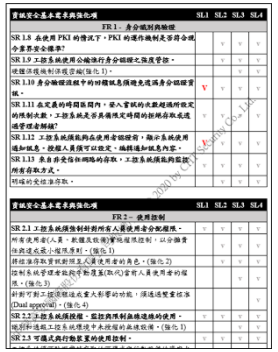
[ISA99危害性矩陣]

- 相較於傳統IT系統使用CIA作為評估工具，工控系統除此之外還需考量HSE面向危害結果。
- 以訪談方式建立企業專屬的危害性矩陣，用以標準化評估資安威脅的危害性。

4. 建議改善方案

- 建議改善方案擬定權重考量風險高低與危害性，逐項針對威脅擬定建議改善方案。





中華資安國際
CHT Security

4.從汽車攻擊與檢測案例看汽車資安防護

案例一：Jeep Cherokee Attack

1 攻擊途徑(一): WiFi連線攻擊

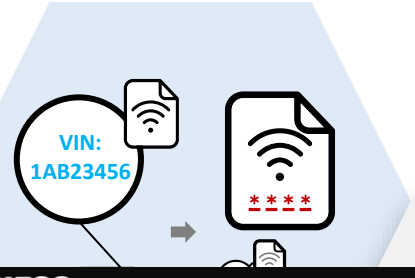
- ✓ **WiFi 密碼**的產生與**VIN碼初始啟動時間**相關
- ✓ **破解密碼產生演算法**，可短時間透過暴力破解WiFi密碼入侵

攻擊途徑(二): 行動網路攻擊

- ✓ Sprint公司對於自家設備之動通訊**毫無管理機制**。
- ✓ 駭客購買**Sprint Airave 2.**
  (Femtocell) 利用其漏洞與機(Uconnect)**建立行動通**

2 執行Port Scan尋找D-B公開的通訊埠

- ✓ 不用**身分驗證**便可連線
- ✓ 具有**命令注入**弱點
- ✓ **取 得 Root 權 限** (Acqui...g Root Privilege)



CNN BUSINESS Markets Tech Media Success Video

Chrysler is recalling 1.4 million vehicles that can be remotely hacked over the Internet.

A flaw in several Chrysler models lets hackers remotely control them, posing an unprecedented danger for American drivers. Hackers can cut the brakes, shut down the engine, drive it off the road, or make all the electronics go haywire.

After the vulnerability was uncovered on Tuesday, Chrysler offered a software upgrade that it recommended customers install "at their earliest convenience."

Chrysler on Thursday upgraded its network, saying the update would prevent the remote hacking from taking place. It said that its update required no action on the part of customers and dealers.

3 竄改攻擊目標之韌體V850

- ✓ **官網下載韌體，逆向**分析
- ✓ 韌體**無數位簽章保護**
- ✓ 原韌體僅具有接收ECU訊息能力，執行**韌體竄改**，使惡意韌體具有**透過CAN BUS對ECU發送控制命令**能力
  系統**D-BUS程式弱點**執行**OMAP**，
  惡意韌體

轉向訊號

N-C 網路當中，發送**控制轉向**的CAN 訊息
(ID: **04f0**)
個位元組(byte)定義**命令優先權**：91為
h speed bus；39為**Medium speed bus**
個位元組(byte)定義**轉向**：01 為**左轉**訊號；
為**右轉**訊號

訊號 LUA script範例：

write(0xf0, 0x02, 91, 0x07, 0x00, 0x00, 0xC0, 0x13, **0x01**, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00)

Turn signal

ref : Remote Exploitation of an Unaltered Passenger Vehicle, Dr. Charlie Miller and Chris Valasek, 2015

案例二：聯網車機的檢測案例

1. 檢測發現汽車車機可以開啟除錯工程模式
2. 發現使用舊版系統，具有已知漏洞，可提升權限；成功入侵至系統底層，安裝任意App且取得最高權限(root)，可以完全掌控、濫用車用網路
3. 雲端平台（北向）與車機連線後，可以完全掌握車子的地理位置，掌握車輛行蹤
4. 車機從晶片、作業系統、應用程式幾乎都留有後門，作為除錯、診斷之用，但幾乎都未妥善管理
5. 原廠未同意提供全車，無法檢測CAN Bus介面（南向），但推論應該有機會完全掌控

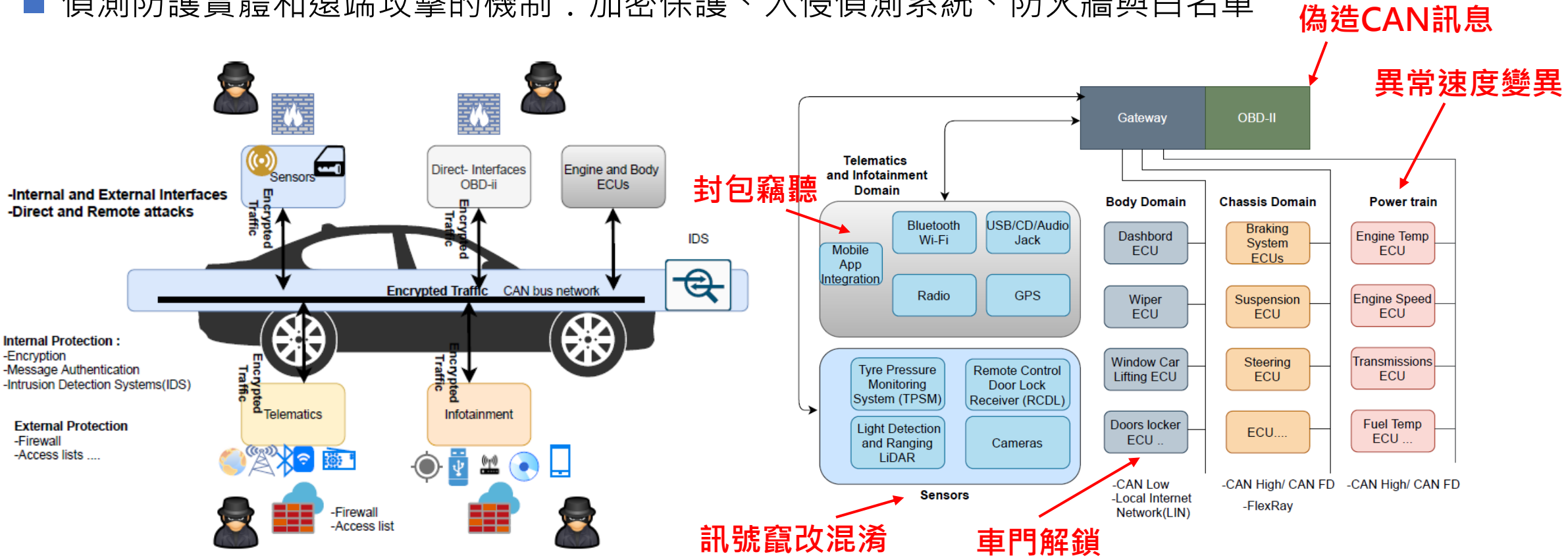
利用工程模式執行系統指令

成功自行安裝App

Source: CHT Security Red Team, Apr. 2020

In-Vehicle Network Attacks

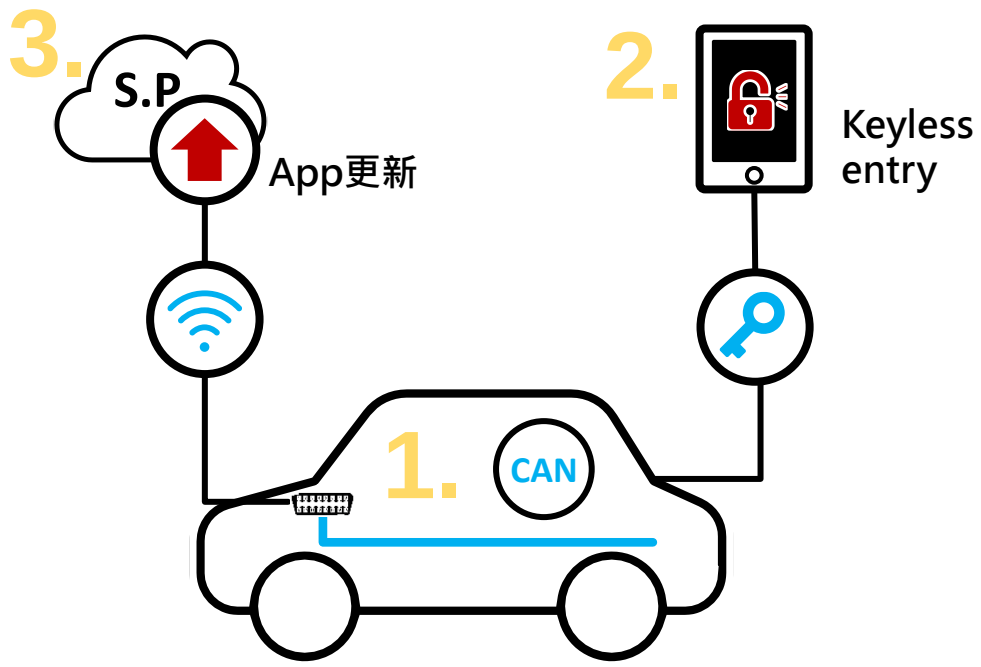
- 目前汽車生產**使用大量的ECU行車電腦**，配備很多**ADAS先進駕駛輔助系統**，產生很多曝險介面
- **入侵點**：車載機(多媒體車用系統)、 資訊娛樂系統、感測器，以及直接對接的介面
- 偵測防護實體和遠端攻擊的機制：加密保護、入侵偵測系統、防火牆與白名單



Ref: Cyberattacks and countermeasures for in-vehicle networks, April 24, 2020

Connected Vehicle Attacks

- 包含**所有 In-Vehicle Network** 攻擊的風險
- 過去車輛通訊技術之發展並未將資安防護納入考量，現今V2X趨勢發展導致聯網通訊的應用增加，車內網路已不具封閉性，**External Network 與 Firmware and Application都是必須面對的資通安全風險**

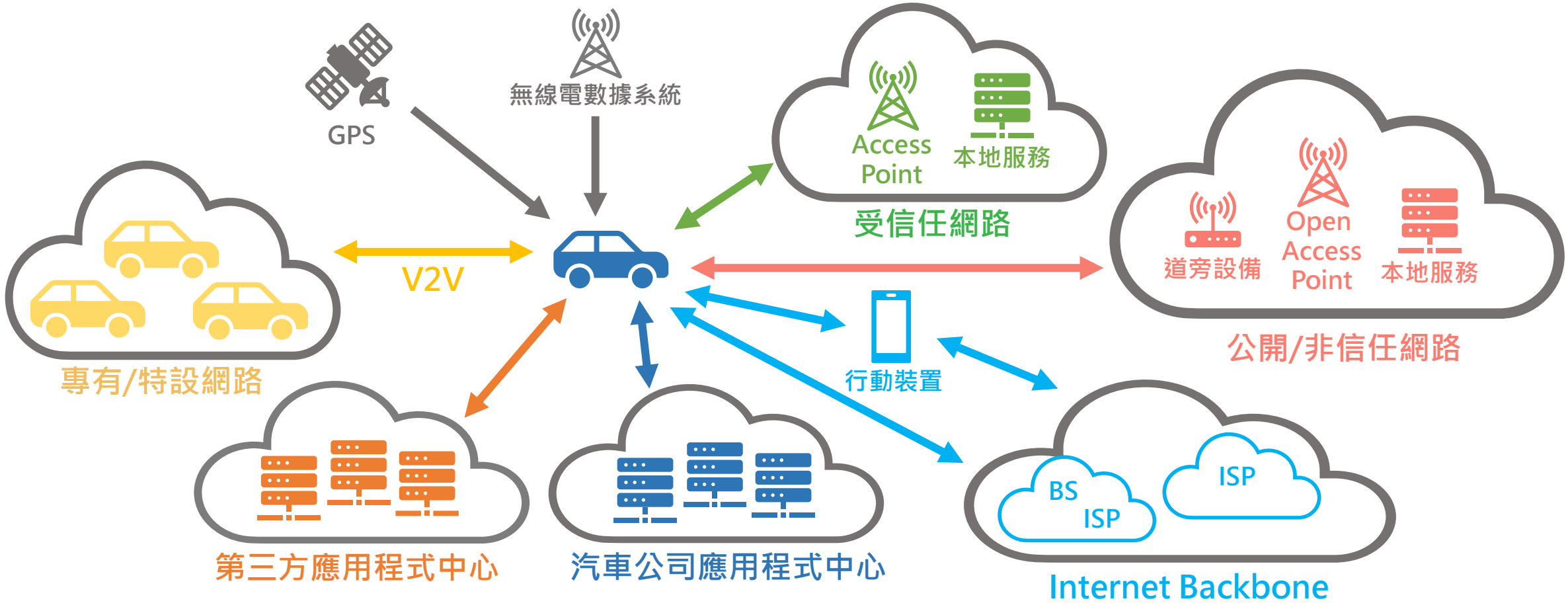


V2X資通安全三大痛點：

1. **In-Vehicle Network**：車內網路骨幹CAN Bus**無資安防護機制**，駭客可偽造控制指令改變車輛狀態，如：關閉頭燈的控制指令。
2. **External Network**：車外通訊**缺乏身分驗證和加密機制**，無法防止竊聽和重送的資安威脅，攻擊情境如：Keyless中間人攻擊。
3. **Firmware and Application**：整車及元件設計僅考量功能性，Over-The-Air **更新無檔案完整性驗證機制**，導致存在更新檔替換和竄改的風險。

自駕車運行的網路基礎建設更複雜

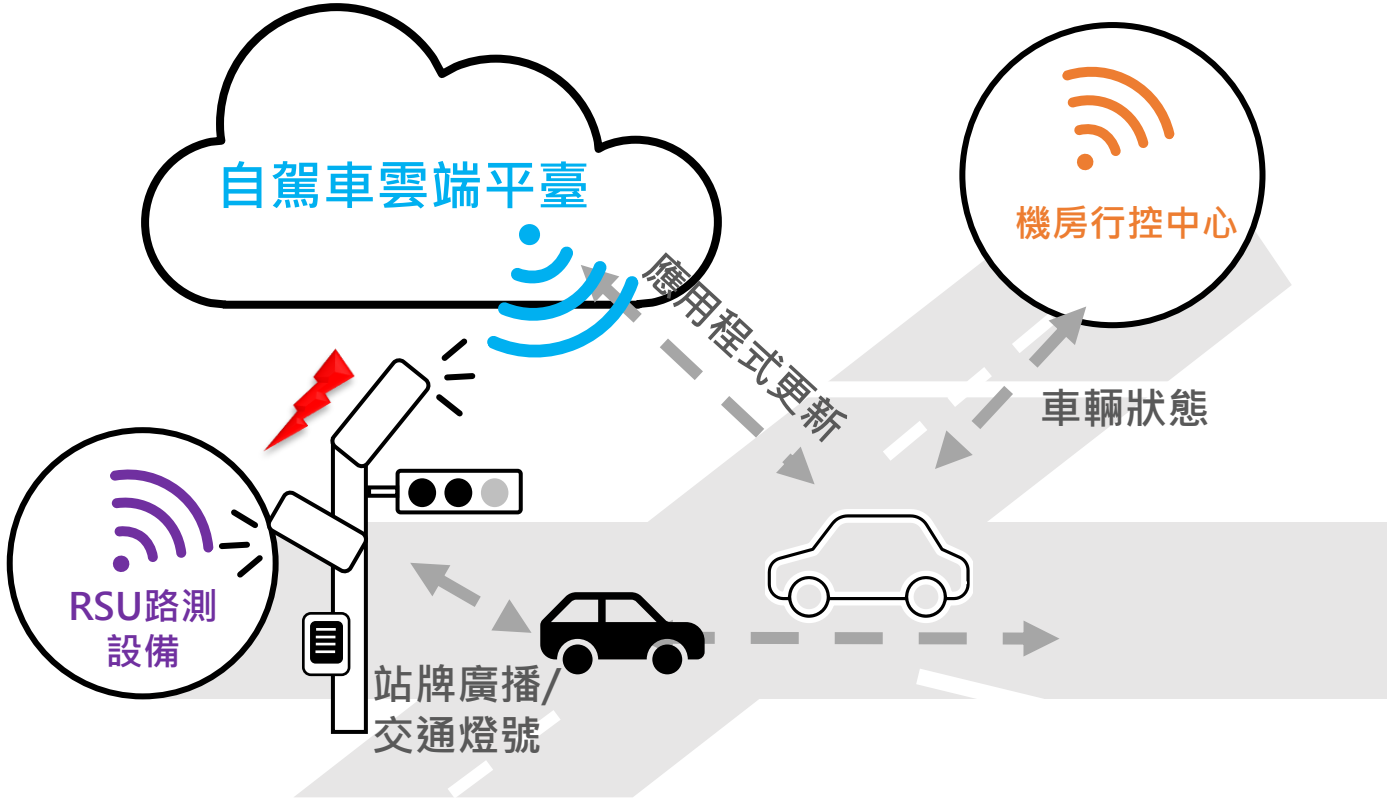
車輛與外部系統互聯化驅動許多新興服務的發展，但在資安面向，卻是資安風險與威脅攻擊面的擴增...



參考資料: SIAeducation @ISC: Will future vehicles be secure(Intel)

Self-Driving Vehicle Attacks

- 包含**所有 Connected Vehicle Network 攻擊的風險**，當然也包含In-Vehicle Network 的攻擊風險
- 自駕車仰賴更多**車上感測設備資料、路側設備、雲端資料、行控中心**的資料，藉以完成自動駕駛功能，所以自駕車運行安全涵蓋車、路、雲、行控中心的協同運作，是一個系統性的安全議題



自駕車運行的資通安全痛點：

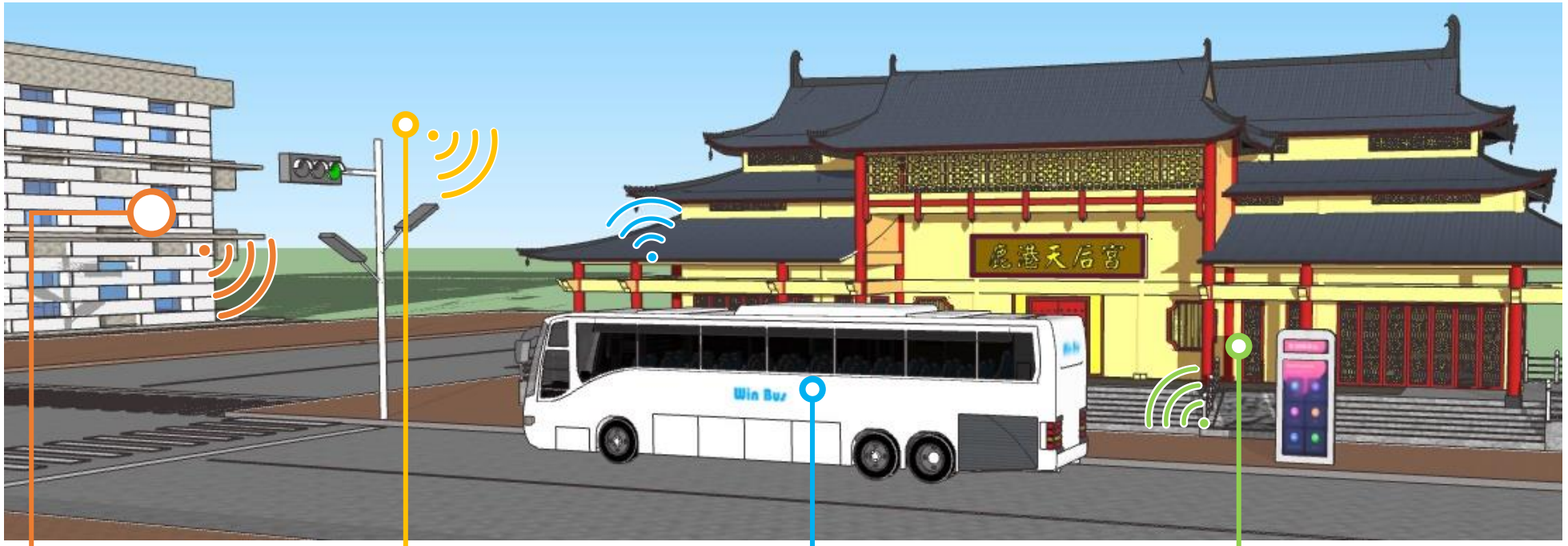
1. **車輛安全**
2. **路側設備**
3. **雲端安全**
4. **行控中心**
5. **整體營運安全**，包含資安檢測、持續監控，緊急應變等
6. **漏洞回報與管理等**

中華資安國際
CHT Security

5. 自駕車實證場域案例分享

自駕車實證場域案例分享

- **自駕巴士彰濱鹿港觀光接駁創新服務計畫整合4G/5G行動網路、C-V2X車聯網環境、智慧路側設施基礎環境。**
- 運行路線總長度**12.6公里**，為目前**全國最長的自駕巴士接駁路線**，沿途經過**台灣玻璃館**、**鹿港天后宮**等彰濱鹿港觀光景點，為遊客提供**自駕接駁服務**。



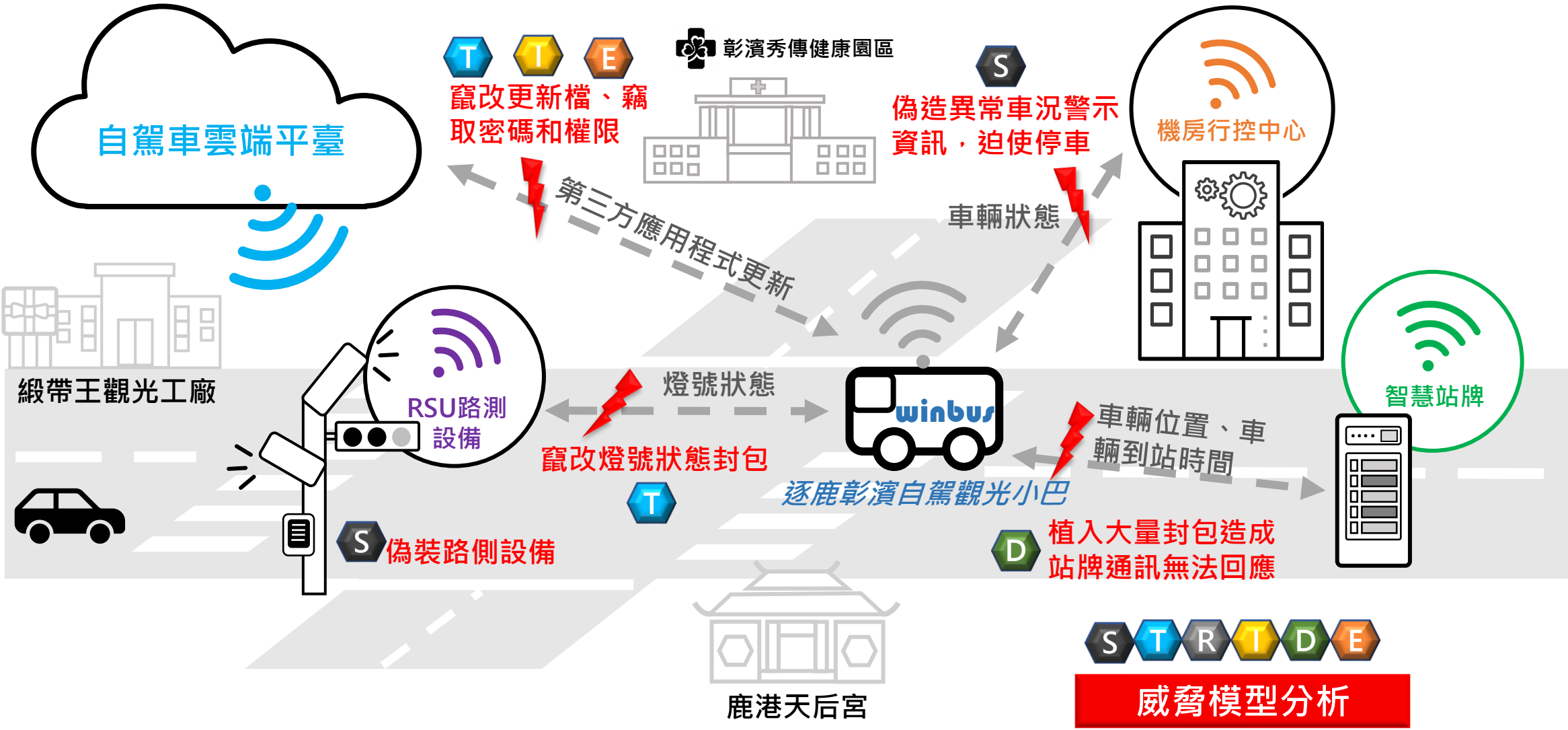
監控後台
- 即時車況
- 遠端監控
- 統計分析資料
- 派遣系統

智慧路口
- 車輛偵測
- 資安防護

自駕小巴
- 全電動化自駕
- 人機介面互動

智慧站牌
- 車輛位置、車輛到站時間與優惠資訊

自駕車實證場域案例**威脅示意情境**



自駕車實證場域STRIDE THREAT MODEL

權限提升 Elevation of privilege

未被授權的使用者獲得授權，並有足夠的權限危害系統及其組件

檢視無人載具架構中所有系統之存取控制及授權設計，評估其機制是否存有漏洞。

身分冒用 Spoofing identity

非法使用他人權限進行存取

檢視無人載具系統架構中設備、通訊管道間遭冒用及攻擊之可能性，並評估是否存有有效之身分驗證及控制程序。

阻斷服務 Denial of service

對有效使用者拒絕服務

評估無人載具架構中每個節點伺服器是否易受DoS攻擊，且是否存有確保持續運作之機制。

竄改資料Tampering with data

包含惡意修改資料及對持續性資料未授權之變更

檢視無人載具架構中資料傳輸途徑是否為安全之傳輸途徑，且有保護資料完整性之復原機制。

資訊洩漏 Information disclosure

資訊揭露給不被預期可存取的他人

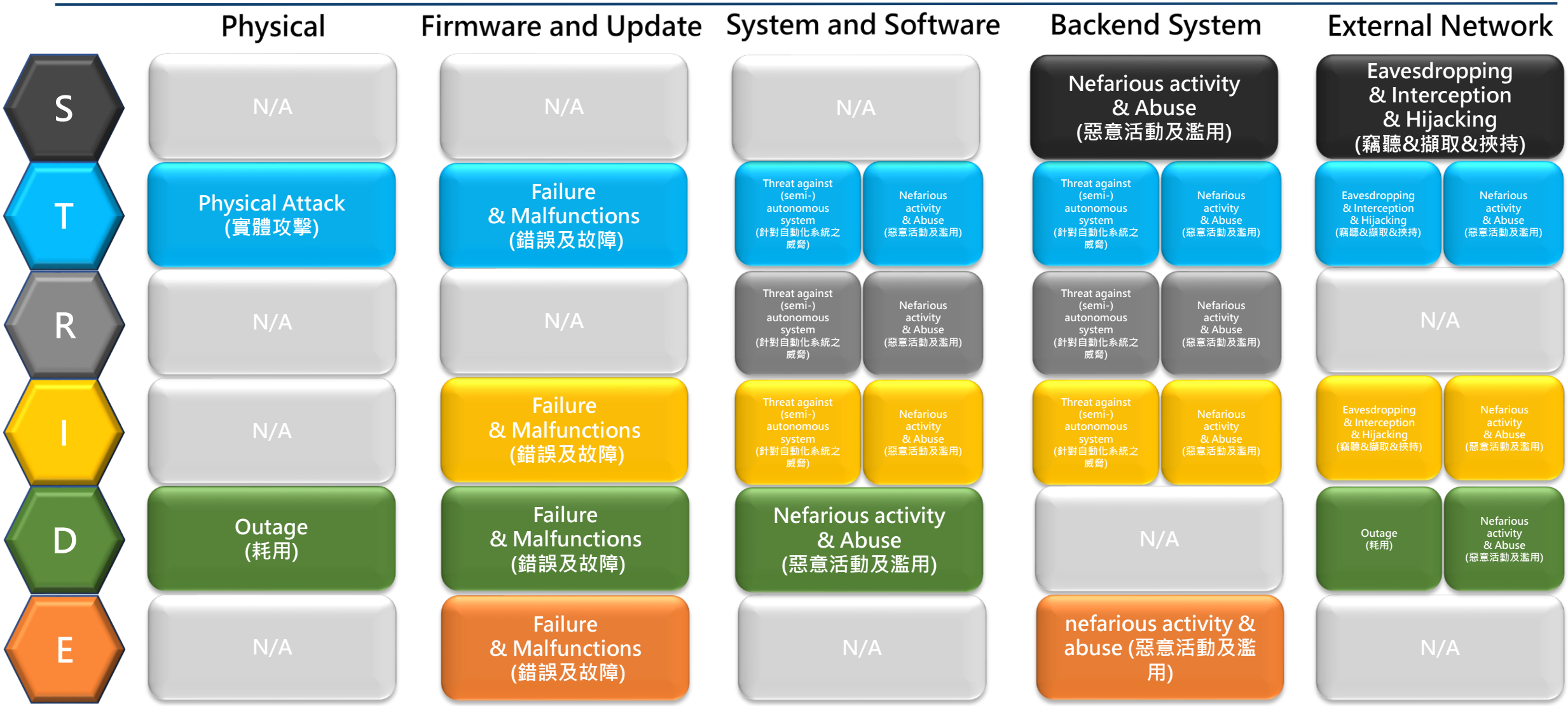
檢視無人載具架構中資料傳輸途徑是否有加密機制，且資料庫之存取是否有存取管控。

否認性 Repudiation

使用者可以否認曾經進行的行為，沒有方法可證明其行為

確認無人載具架構中所有行為活動及資料能皆存有相關軌跡可供證明其合理性。

自駕車實證場域**威脅矩陣**



自駕車實證場域**資安威脅分析**(範例)

項次	資訊系統	STRIDE 威脅模型						評估潛在威脅項目	評估潛在威脅項目說明
		S	T	R	I	D	E		
1	In-Vehicle System and Software Safety		V	V	V	V		A. nefarious activity & abuse (惡意活動及濫用)	流量攻擊CAN Bus導致正常CAN控制指令發生延遲或拒絕服務(DoS)。
									車廠和元件供應商之針對性攻擊:植入特製偽造關閉頭燈的控制指令。
									資料操控(揭露、異動、遺失): 空中編程篡改地圖資料數據中毒、路側裝置資料竄改、偽造的安全性資料、偽造的基本安全訊息注入、資料注入控制器區域網路。
			V	V	V			B. threat against (semi-)autonomous system (針對自動化系統之威脅)	感測器針對性威脅:自動感測器遮蔽、光達及雷達干擾、太多物件以致於難以追蹤)
2	In-Vehicle Firmware and Update Security		V		V	V	V	A. failure & malfunctions (錯誤及故障)	更新無加密和完整性驗證機制，導致存在未授權使用者權限提升、更新檔遭竊聽、替換和竄改的風險。
									軟體漏洞挖掘:不允當參數/過時軟體/已知漏洞之挖掘。
									服務失敗或中斷:原設備製造商服務、第三方服務。

自駕車實證場域整體資安解決方案架構

J3061
ISO 21434
IEC 62443

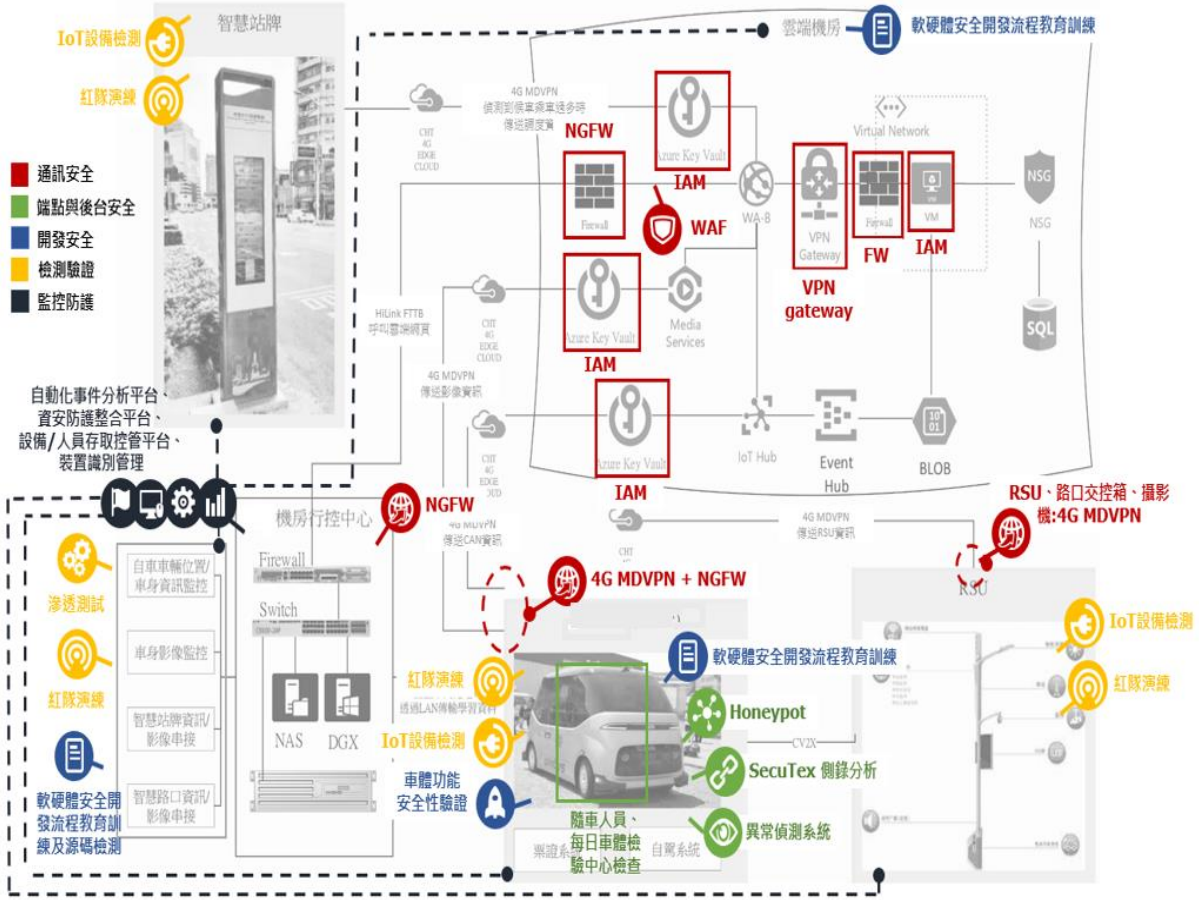
參照國際標準

安全性
網路安全性

風險評估

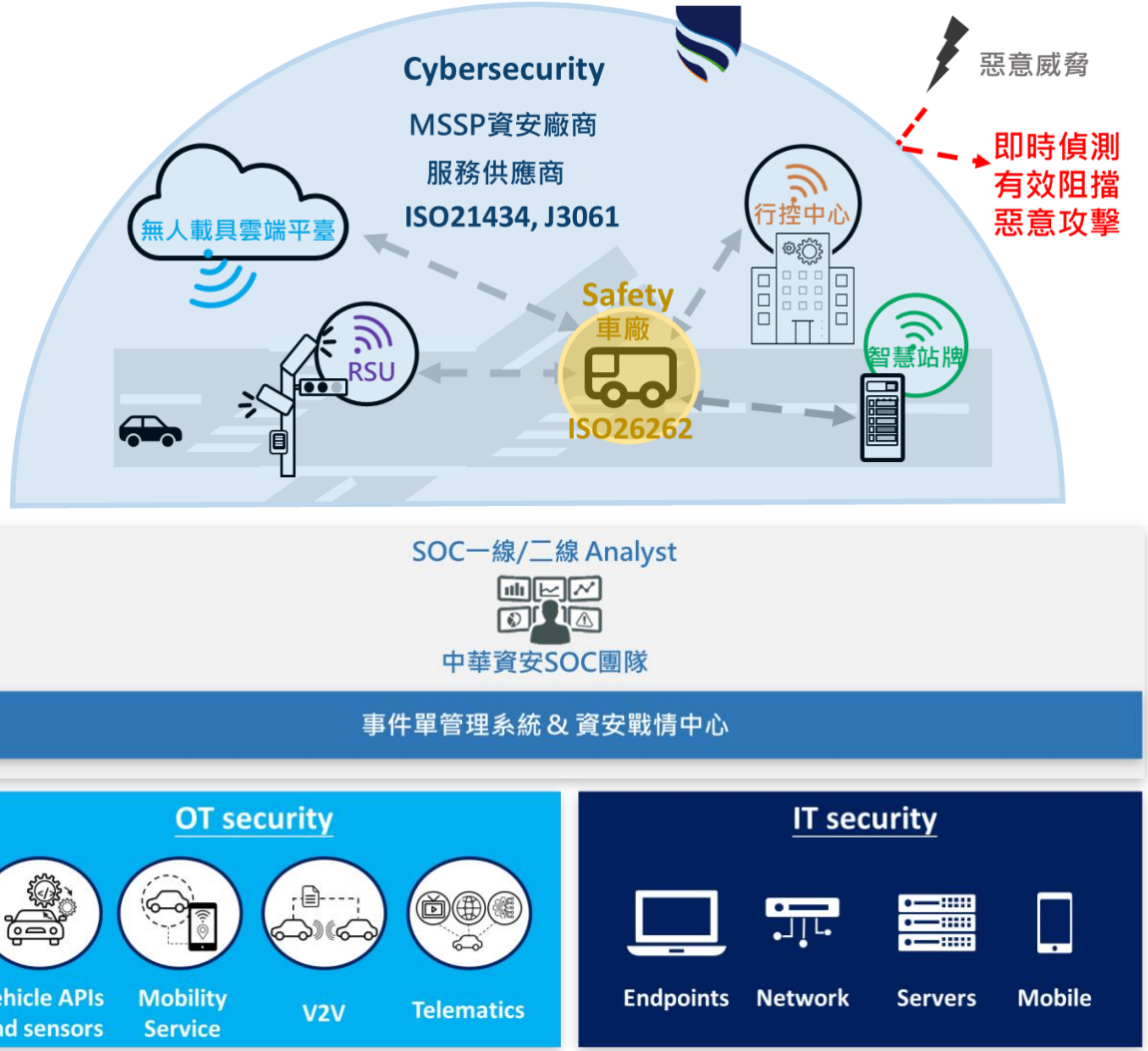
STRIDE
威脅模型

建立威脅模型



Key Takeaways

- **功能安全(Functional Safety)與資通安全(Cybersecurity)**不同，評估方法不同(HARA/TARA)，分別有國際標準(ISO 26262/ISO 21434)
- 車輛智慧化與聯網化造成曝險介面增加，資通安全風險是必須面對的課題，**車廠應考慮納入 CSMS 管理制度**
- 車輛的資通安全**不只涵蓋概念、開發、驗證、生產**，也包含**操作及維護(事件回應與更新)、汰舊或服務終止**
- 自駕車運行場域的資通安全涵蓋車、路、雲、行控中心等系統性問題，預期**車廠與供應商**做安全的車，**車隊或運輸服務商**要營運安全運輸服務，**資安廠商**MSSP協助防護監控應變
- 中華資安國際的技術及經驗，可以協助CSMS**制度導入**、**紅隊資安檢測**、**VSOC資安監控**、**即時事件回應**等專業服務；自主研發**流量側錄與異常分析(SecuTex)**、**惡意程式偵測與防護(Svitania)等**車上資安防護設備有機會合作實證




中華資安國際
CHT Security
Thank you!
Q&A
EMPOWER YOUR SECURITY