



BUREAU
VERITAS

CEH
Certified Ethical Hacker

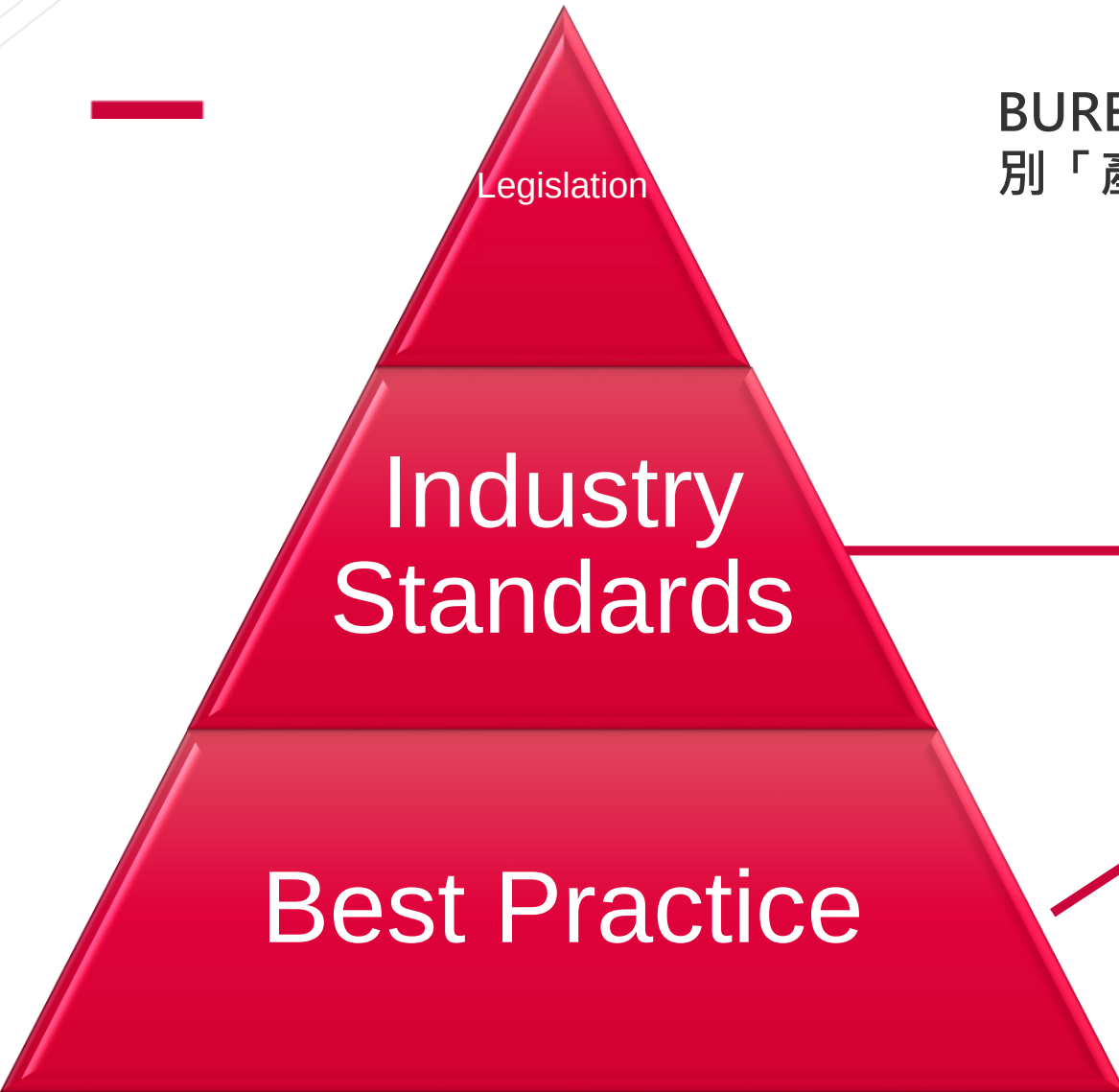


面對車聯網資安挑戰 如何超前部署？

KENNY LEE (CEH , CISSP)

資安法規與驗證

BUREAU VERITAS榮獲2020道瓊永續指數 (DJSI) 專業服務類別「產業領導者」！



BUREAU
VERITAS

Shaping a World of Trust

Organization for
Standardization

公正第三方
驗證機構
資安測試實驗室

全球重要資安法案

持續推出的資安法案

網絡感知法案
管道與液化天然氣設施網路安全準備法案
能源應急領導法案
公私合作加強電網安全法案
提升關鍵基礎設施網路安全的框架
加州裝置資安法
奧勒岡州物聯網裝置資安法

歐盟網路網路安全法案
歐盟網路與資訊系統安全指令
歐盟通用資料保護條例
德國數位化行動綱要
德國能源系統網路安全建議白皮書
英國國家網路安全戰略 (2016-2021)

中華人民共和國國家安全法
關鍵基礎設施安全保護條例
工業控制系統資訊安全防護能力
評估管理辦法
關於加強電力行業網路安全工作的
指導意見
信息安全技術網路安全等級保護
基本要求，測評要求，安全設計
技術要求

日本電信網路安全法

台灣資通安全管理法

巴西金融機構網路安全法

印度電信安全保證要求

新加坡網路安全法

AUTOMOTIVE CYBERSECURITY

Legislation

- UNECE regulations on Cybersecurity and Software Updates

Industry Standard

- ISO 21434

UNECE REGULATION ON CYBER SECURITY AND SOFTWARE UPDATES

- Worldwide organization, including 56 member states
- EU to mandate them from July 2022, Japan from 2021
- Whole life-cycle of the vehicle in scope of the regulation

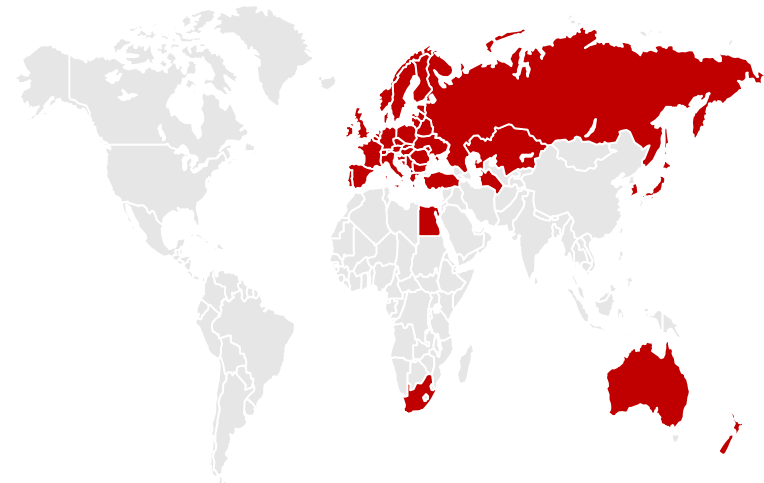


Managing
vehicle cyber
risks

Securing
vehicles by
design to
mitigate risks

Detecting and
responding to
security
incidents

Providing safe
and secure
software
updates



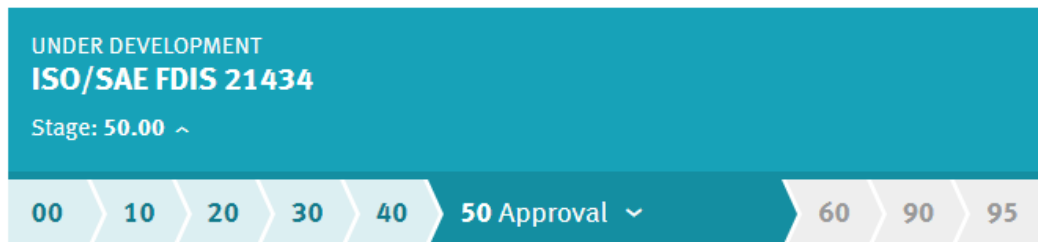
EXPECTED IMPACT



ISO/SAE 21434 AUTOMOTIVE 資安標準

- Industry-backed standard focused on security processes in development, production and post-production
- Useful for both OEMs and Tier 1/Tier 2
- Strong link with the UNECE Cybersecurity regulation

NOW



Scope and references		
Terms and general considerations		
Cybersecurity management		
Continuous cybersecurity activities		
Risk assessment		
Concept phase	Product development (all)	Post-development activities
	Cybersecurity validation	CS incident response
Distributed cybersecurity activities		
Annexes (CALs, use cases, impact ratings...)		

AUTOMOTIVE 重要標準

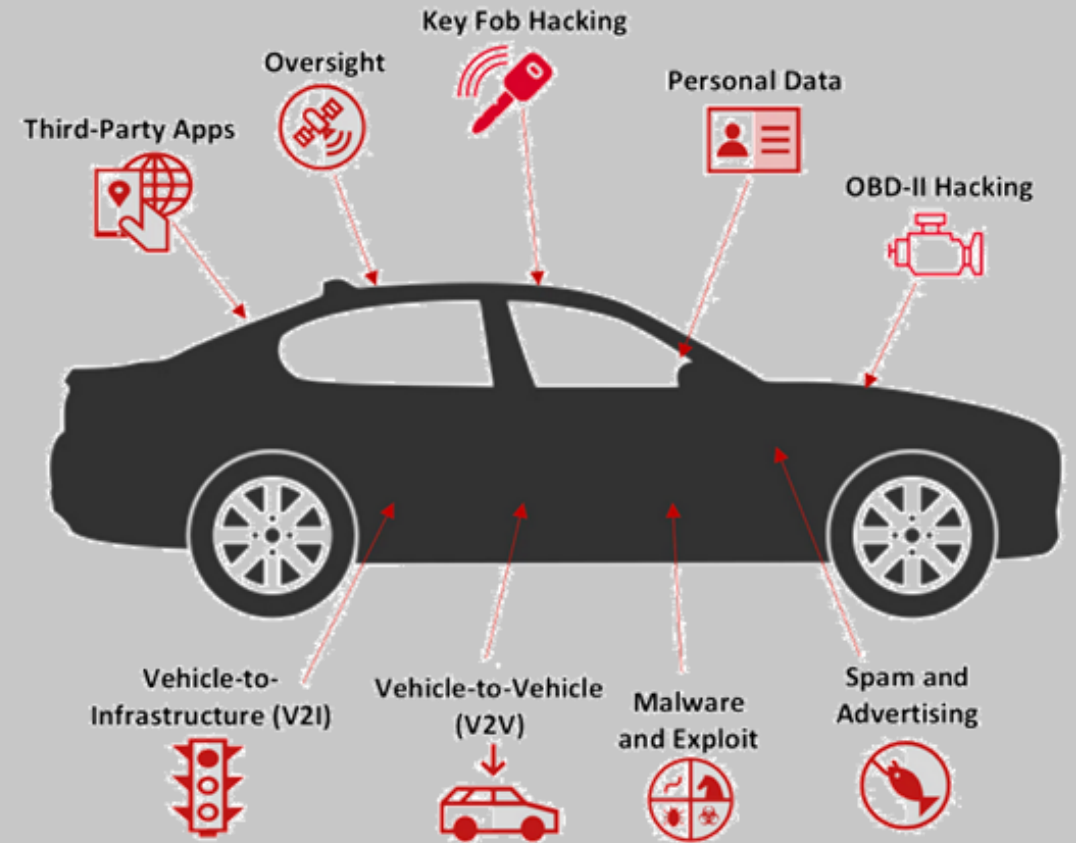


Failure and defects
ISO 26262



Unintended behavior
ISO 21448

System



Cyber threats
ISO 21434

HARMONIZATION OF SAFETY & SECURITY PROCESS



Cyber Security ISO 21434

Concept

Requirement

Design

Implementation

Validation

Update &
Maintenance

Decommissioning

Functional Safety ISO 26262 and Safety of the Intended Functionality ISO 21448

What is TISAX ?

- TISAX (Trusted Information Security Assessment Exchange) audit and exchange mechanism for the ISA was born in 2016
- The German Association of the Automotive Industry (VDA) and ENX, as information security task force, decided to propose a robust and enhanced standard based on ISO 27001 requirements added with the information security assessment (ISA) catalog developed by the VDA.

WHY SHOULD I BE ASSESSED AGAINST TISAX ?

- German automotive companies (BMW, Daimler, and Volkswagen) mandate compliance to TISAX, for suppliers to be ranked as "top reliable" suppliers in term of quality and security of digital information management.
- It shall be enlarged to other OEM and TISAX is becoming the certification reference standard for Automotive Industry and Information security Management.
- TISAX was launched end of 2016 with an instantaneous demand from the automotive industry and after almost 2 years of existence, almost 2000 companies have been already assessed against TISAX.
- Furthermore, the audited company can choose to make its audit results available to other TISAX participants in varying levels of detail, thus avoiding additional audits for other interested participants with the same security requirements. Duplicate and multiple audits are therefore a thing of the past, which helps all those involved to save time and money.

What Complementarity between ISO 27001 & TISAX ?

- Both standards are fully complementary

ISO 27001 focuses on the organization and its structure when TISAX focuses on topics relevant to partners and specific physical sites.

TISAX also considers particularly Customer Specific Requirements from german automotive OEMs or Tier 1 suppliers for what regards information security.

ONE STOP SOLUTION TO EVSE

Security

RF

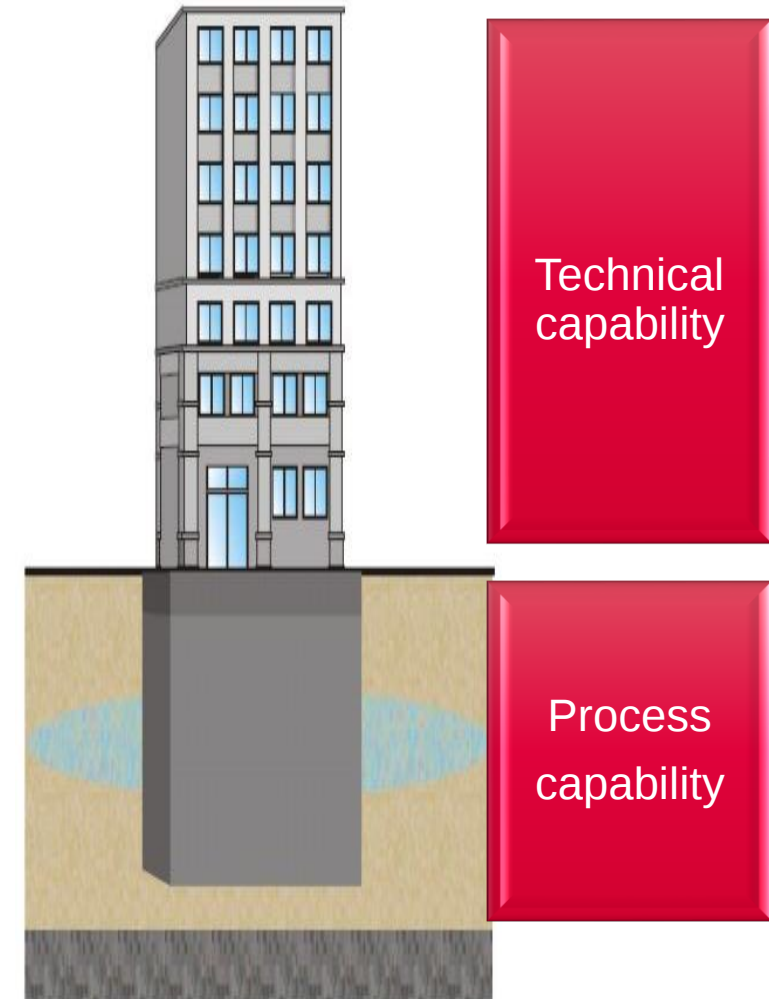
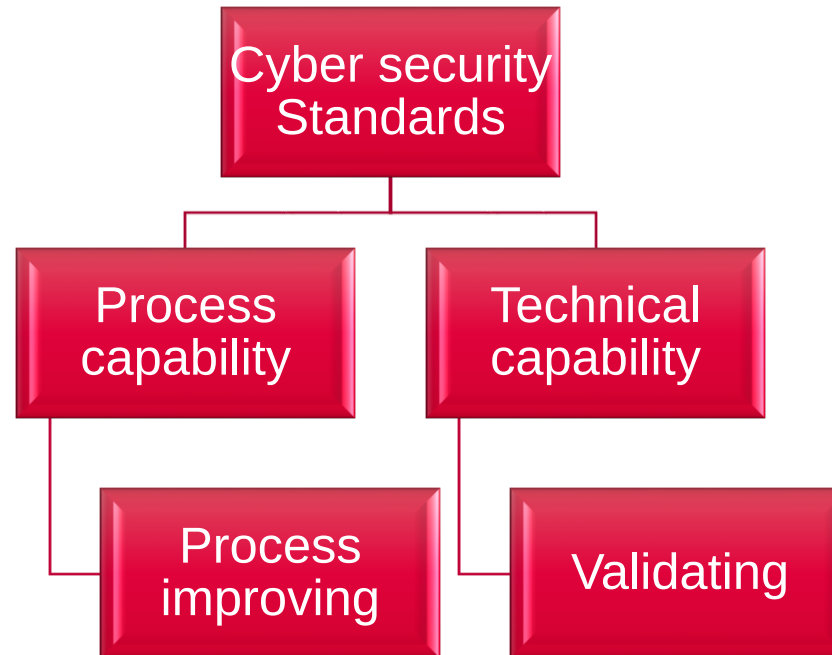
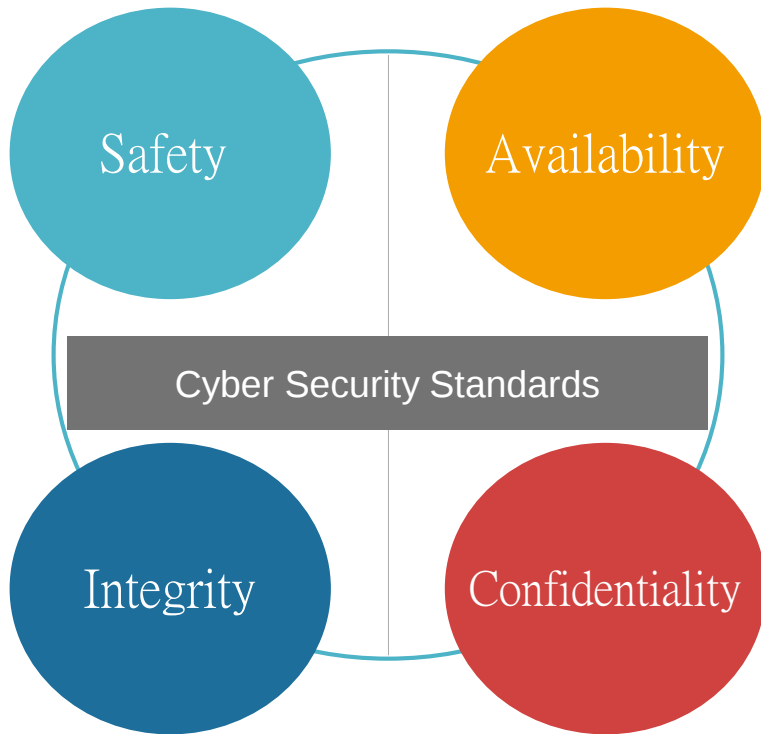


EMC

Safety

IA

SUMMARY



案例分享

客戶	領域	客戶要求	提供服務
保密	歐系車廠	• ISO 26262 認證	• ISO 26262驗證
保密	台灣車用面板廠	• 符合歐洲車廠要求 • 加強網路安全能力	• TISAX驗證
保密	網路基礎設施解決方案	• 產品認證	• 產品與流程驗證 IEC 62443 (4-1 & 4-2)
保密	歐系電動車廠	• 網路安全制度改善 • ISO 26262 認證	• ISO 26262驗證
保密	台灣車用零組件廠	• 增強網路安全成熟度 • 符合歐洲車廠要求	• TISAX驗證

BV資安服務列表

客戶類型	服務內容	服務類型		
		教育訓練	顧問服務 (由BV認可顧問公司提供)	驗證
業主/運營方	建立網路安全計畫 (IEC 62443-2-1)	√	√	▲
系統整合商/維護服務商	安全產品開發生命週期要求 (IEC 62443-4-1)	√	√	√
	IACS服務提供者的安全要求 (IEC 62443-2-4)	√	√	√
	系統安全要求和安全等級 (IEC 62443-3-3)	√	√	√
製造商	TISAX,ISO26262, Common Criteria ISO15408	√	√	√
	ISO21434	√	√	▲
	Eurosmart	√	√	√
	BV IoT,ioXt, IMDA Security Requirements for Residential Gateways, NCC information security testing services , Japan requirement of Article 34-10	√		√
	安全的產品開發生命週期要求 (IEC 62443-4-1)	√	√	√
	IACS元件的技術安全要求 (IEC 62443-4-2)	√	√	√

▲ 等待標準正式發布

MOVE FORWARD WITH CONFIDENCE

