智慧交通安全嗎？

德國萊茵TUV檢測認證集團

趙斌 Bin.Zhao@tuv.com

010-65666660-104

TÜVRheinland®
Precisely Right.

議程

1 案例分析

2 智慧交通系統安全要求

3 汽車資訊安全分析

4 SAE J3061

5 萊茵TÜV資訊安全服務

6 客戶及證書範例

議程

1 案例分析

2 智慧交通系統安全要求

3 汽車資訊安全分析

4 SAE J3061

5 萊茵TÜV資訊安全服務

6 客戶及證書範例

汽車資訊安全事故案例 1

克萊斯勒-吉普 切諾基(Jeep Cherokee) 遭駭客攻擊

- 據《華爾街日報》官網報導，2014年7月，兩位網路安全研究人員公開展示了如何通過數公里以外的筆記型電腦來控制一輛吉普·切諾基汽車的空調、音響裝置甚至傳動系統和發動機系統。這一車型使用了克萊斯勒公司的UConnect車載資訊系統，該系統可以為使用者**提供娛樂、導航、WiFi熱點服務，同時也為駭客提供了可乘之機。**這也許是近年來汽車暴露出的最嚴重的與互聯網(網際網路)有關的資訊安全問題。

摘自:„http://auto.qq.com/a/20150824/022443.htm “

克萊斯勒-JEEP 切諾基 遭駭客攻擊

摘自:„http://auto.qq.com/a/20150824/022443.htm “

TÜVRheinland®
Precisely Right.

- 2014年7月菲亞特克萊斯勒(Fiat Chrysler) 宣佈，召回140萬輛存在軟體漏洞的汽車。這是第一起因為網路安全而發起的召回！汽車資訊安全受駭客威脅不再只是危言聳聽，汽車廠商準備好如何應對了嘛？

摘自:„http://auto.ifeng.com/pinglun/20150727/1044337.shtml “

汽車資訊安全事故案例 2

用OBD控制雪佛蘭-克爾維特(Chevrolet-Corvette)

據報導，美國加利福尼亞大學聖地牙哥分校的網路安全研究員在雪佛蘭-克爾維特(Chevrolet-Corvette)的OBD-II端口插入了一個裝置，以此來侵入汽車的安全系統，在低速行駛狀態下實現雨刷控制器的開關並且干預剎車系統的動作。與克萊斯勒事件相同，在這起案例中，“犯人”有兩個，一個是Mobile Devices的OBD設備，一個是克爾維特的車輛CAN匯流排。

Mobile Devices的OBD問題一是開發者模式與使用同樣的金鑰讓駭客們可以輕鬆獲取最高許可權，二是通過簡訊方式下發指令，簡訊不用經過任何驗證的手段給駭客大開方便之門。

摘自:„http://www.sinocars.com/autocar/2015_hyxw_0814/41980.html “

汽車資訊安全事故案例分析

上述兩起汽車資訊安全事故具有下列特徵：

▪1、首先汽車上具有大量的電子控制模組(ECU),它們之間可以通過匯流排傳遞資訊，且不同汽車上的ECU網路往往結構不同；

▪2、駭客通過遠端獲取進入汽車內部網路的許可權，使得駭客向汽車網路注入資訊（好的或者不好的）成為可能，直接或者間接控制目標ECU；

▪3、現代汽車除了ECU往往還具有部分智慧功能，即資訊物理系統；

此外，現有的研究表明：不同數量的ECU、不同拓撲結構的網路以及資訊物理系統，其資訊安全性均具有很大的差異，並且首先反映在遠端攻擊介面（remote attack surface）上。

議程

1 案例分析

2 智慧交通系統安全要求

3 汽車資訊安全分析

4 SAE J3061

5 萊茵TÜV資訊安全服務

6 客戶及證書範例

預見Security發展

- 汽車被駭客攻擊甚至操縱的事件，這不是第一起，也絕不是最後一起，以後還將越來越多。不論是無人駕駛汽車還是車聯網，一部智慧手機加上幾個輪子，成為公認的汽車發展方向。汽車智慧化的首要代價就是安全威脅，不但有傳統的資訊、財務等安全問題，更有可能威脅生命。在安全技術沒有突破前，沒有任何廠商和用戶能夠倖免，但這同時也預示著一個更大規模的汽車安全產業的出現。

摘自:„http://auto.qq.com/a/20150824/022443.htm “

功能安全和資訊安全

思考：

智慧交通的信號系統出現問題，或被駭客攻擊，危險嗎？

功能安全和資訊安全同等重要，是智慧交通未來發展的重要要求

功能安全標準：ISO26262 ， IEC61508

資訊安全標準： IEC62443， SAE J3061……

其它：如電氣安全要求、電磁相容要求、環境測試要求……

德國萊茵能夠為您提供：
人員資質的培訓，功能安全管理體系審核，產品認證評估

其他安全要求

- **電氣安全(Electrical Safety):**

電力動能車輛須符合歐洲經濟委員會(Economic Commission for Europe, ECE)所發佈的法規Regulation 100 Part 1，以符合歐洲市場對於電力動能車輛電器安全的要求，例如: E-mark認證。

- **電磁相容性(Electromagnetic Compatibility, EMC):**

整車及電機/電子產品須符合歐洲經濟委員會(Economic Commission for Europe, ECE)所發佈的法規Regulation 10，以符合歐洲市場對於產品EMC的要求，例如: E-mark認證。

- **環境測試(Environmental Test)**:

根據車廠所提出的測試規範或標準，或是ISO、IEC、SAE、ASTM、DIN、JIS等標準。

議程

1 案例分析

2 預見智慧交通系統安全要求

3 汽車資訊安全分析

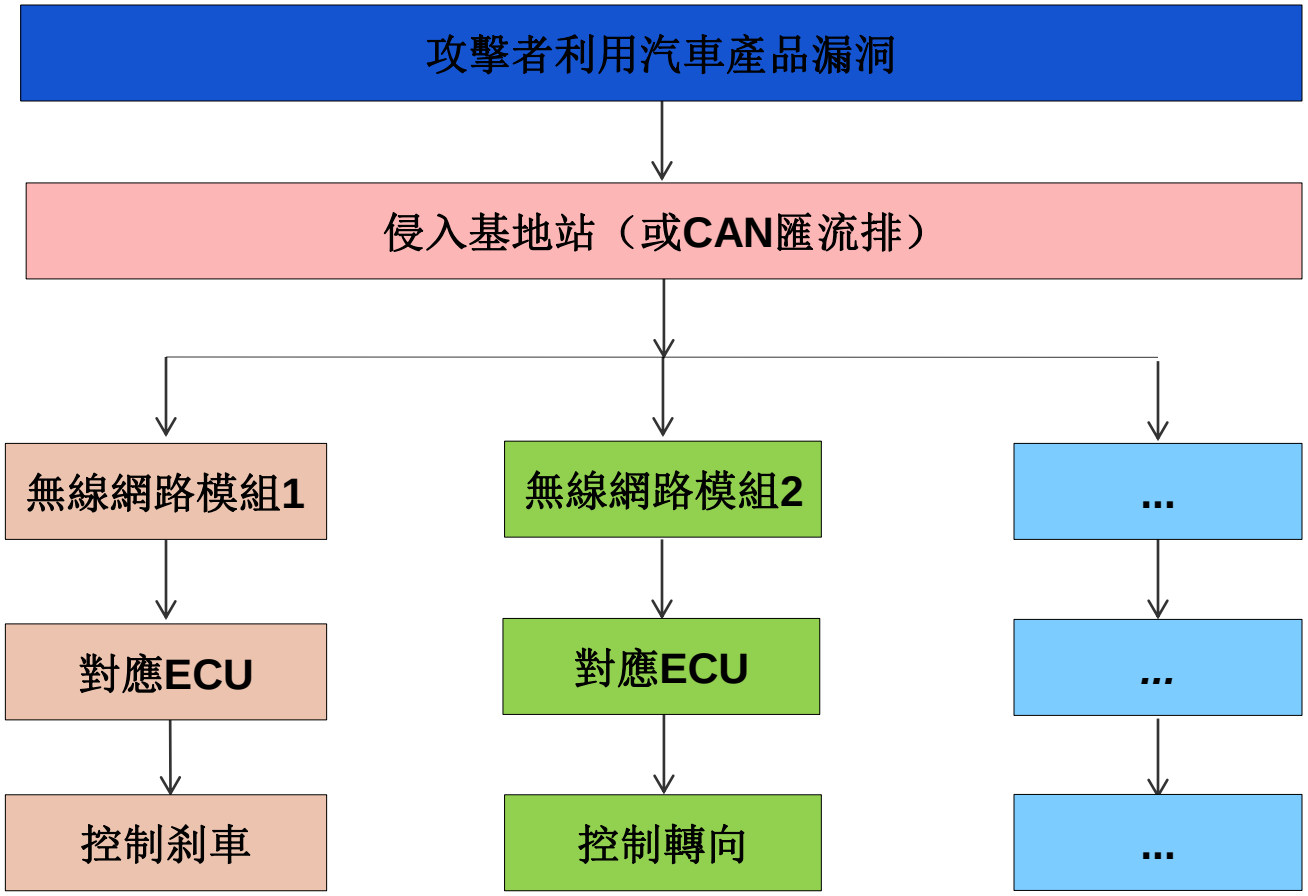
4 SAE J3061

5 萊茵TÜV資訊安全服務

6 客戶及證書範例

汽車在Security上需要考慮的幾個方面

常見入侵途徑

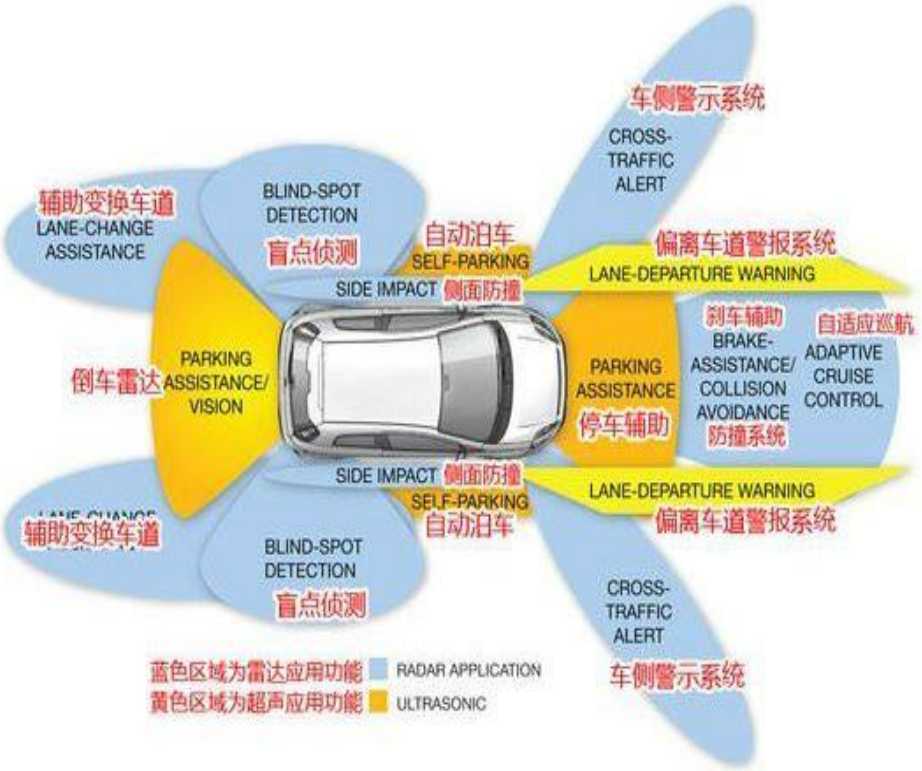


漏洞類型分析

- **軟體設計漏洞**：吉普 切諾基的WPA2密碼設置很弱，以及D-BUS允許匿名登入等
- **系統間物理結構連接存在問題**：吉普 切諾基的 Uconnect（資訊娛樂系統:可連接到移動運營商）直接連接到汽車的CAN匯流排上...
- **韌體(firmware)缺失**：缺少安全隔離網閘（air gap:不同功能的ECU間可能存在閘道以攔截非法資訊的傳遞）

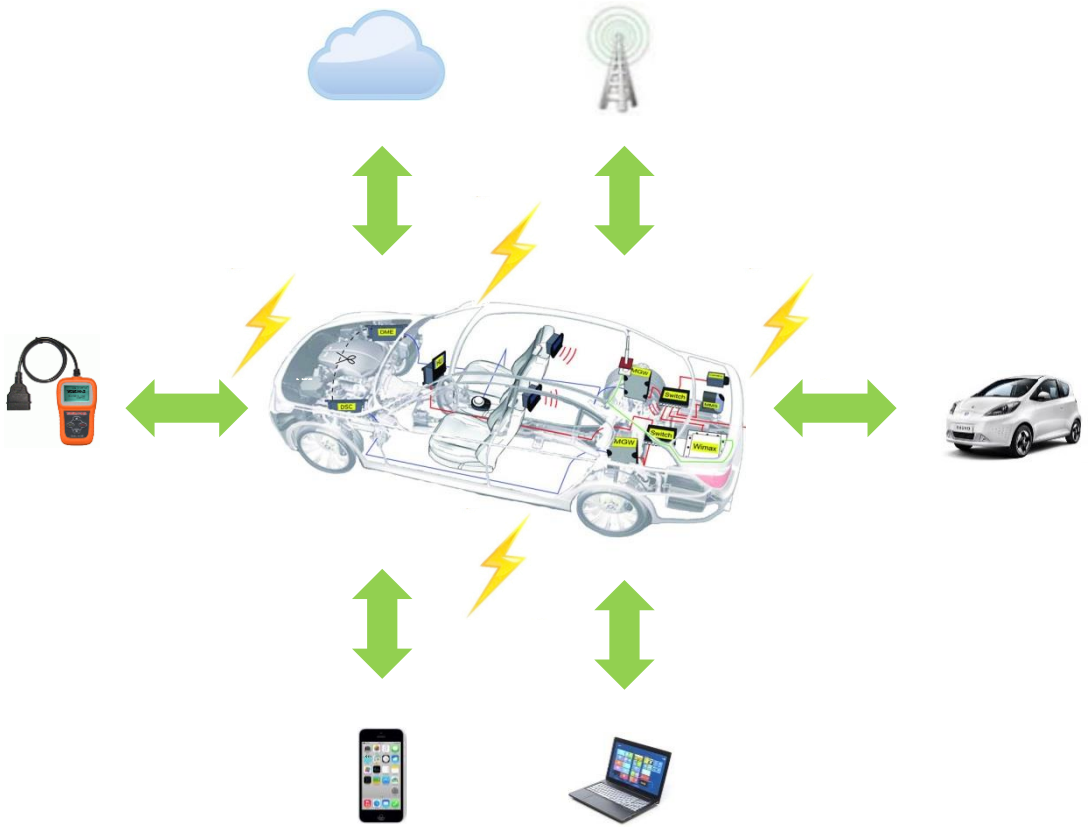
產品資訊安全測試

- 資訊娛樂系統 (e.g. Uconnect)
- 安全隔離網閘(AIR GAP)的設定
- 藍牙系統
- 車載自動診斷系統(e.g. OBD)
- 車載App網路應用程式許可權及驗證方式設置
- CAN匯流排安全性原則的設定
- 無線網路模組、ECU判斷正確指令的功能
- …….



系統資訊安全測試

- 通信識別驗證
- 應用軟體安全
- 嵌入式系統韌體/軟體安全
- 通信協議安全
- 端到端(End-to-End)穿透測試
- 代碼評估



議程

1 案例分析

2 預見智慧交通系統安全要求

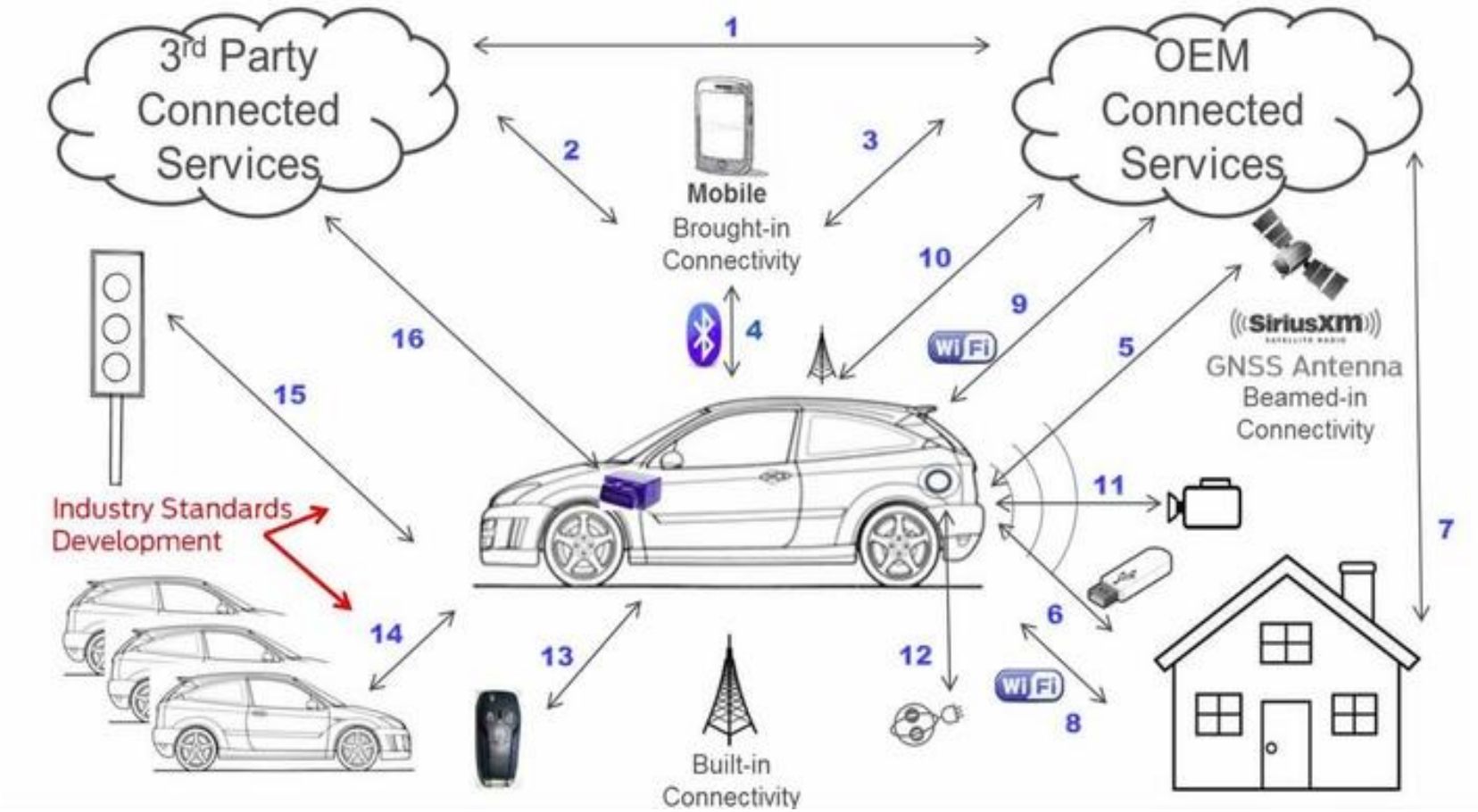
3 汽車資訊安全分析

4 SAE J3061

5 萊茵TÜV資訊安全服務

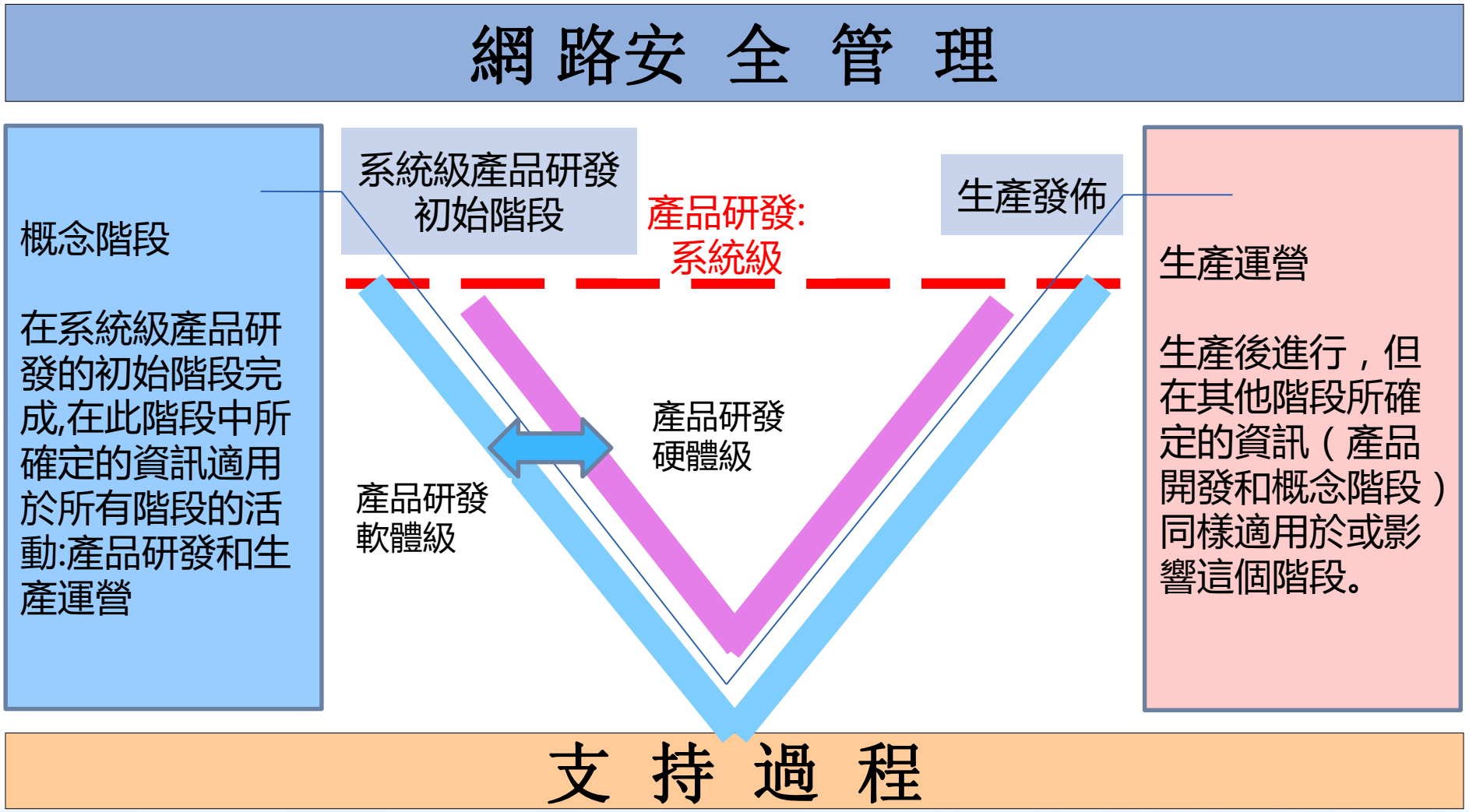
6 客戶及證書範例

車聯網系統



摘自:„http://www.wtoutiao.com/p/143spLE.html “

網路安全過程整體框架



汽車資訊安全技術要求

- 網路安全系統的開發必須從車輛**設計階段**就開始進行
- 設計團隊盡可能尋找潛在威脅，並採取措施消除或降低風險
- 汽車廠商必須採用**系統工程的方法**保護網路安全
- 汽車安全和網路安全之間的交集越來越多，入侵者可通過某些方法影響車輛的關鍵功能
- 網路攻擊的目標可能是車輛安全系統、資訊娛樂系統，也可能是其他電子系統
- 作為整車廠，所制定的規劃須包含一個能夠準確判斷事件性質的**響應機制**
- 設計團隊可以採取一些措施，為車輛提供**多重保護**
- 網路安全系統一般採用**縱深防禦**技術，即使某層防禦被突破，其他程式也能補上缺口
- 整個汽車行業應建立一個**資訊共用的分析中心**
- 汽車網路系統只有**不斷升級**才能有效保持防禦能力
- ...

議程

1 案例分析

2 預見智慧交通系統安全要求

3 汽車資訊安全分析

4 SAE J3061

5 萊茵TÜV資訊安全服務

6 客戶及證書樣例

我們的資訊安全服務

Data and Endpoint Security

- (1) 通用標準服務- ISO 15408
- (2) 數據遺失/ 洩漏預防(DLP)
- (3) 移動設備安全
- (4) 電子郵件加密
- (5) 資料安全TTP加密
- (6) 硬碟和資料加密
- (7) 資訊技術取證/鑒證
- (8) 藍圖和實施測試

IT Security in Production

- (9) 管理和自動化技術：技術檢驗審查/認證

Network Security

- (10) 管理控制
- (11) 資訊安全、事件管理和日誌管理
- (12) 資訊技術安全管理服務&支持
- (13) 資訊安全快速檢查測試 / 認證
- (14) 區域網路資訊安全
- (15) 資料中心評估審查/認證
- (16) 電子郵件內容安全過濾
- (17) 漏洞掃描– 資訊安全監控
- (18) 資訊技術安全藍圖
- (19) 滲透測試和資訊技術安全分析
- (20) 電腦安全應急小組(CSIRT)

我們的資訊安全服務

Online Security and Quality

- (21) 資訊技術可用性測試
- (22) 資料安全性及資料隱私性
- (23) 原始程式碼審計測試/ 認證
- (24) 功能性品質保證
- (25) 測試管理
- (26) 負載和性能測試

Strategic Information Security

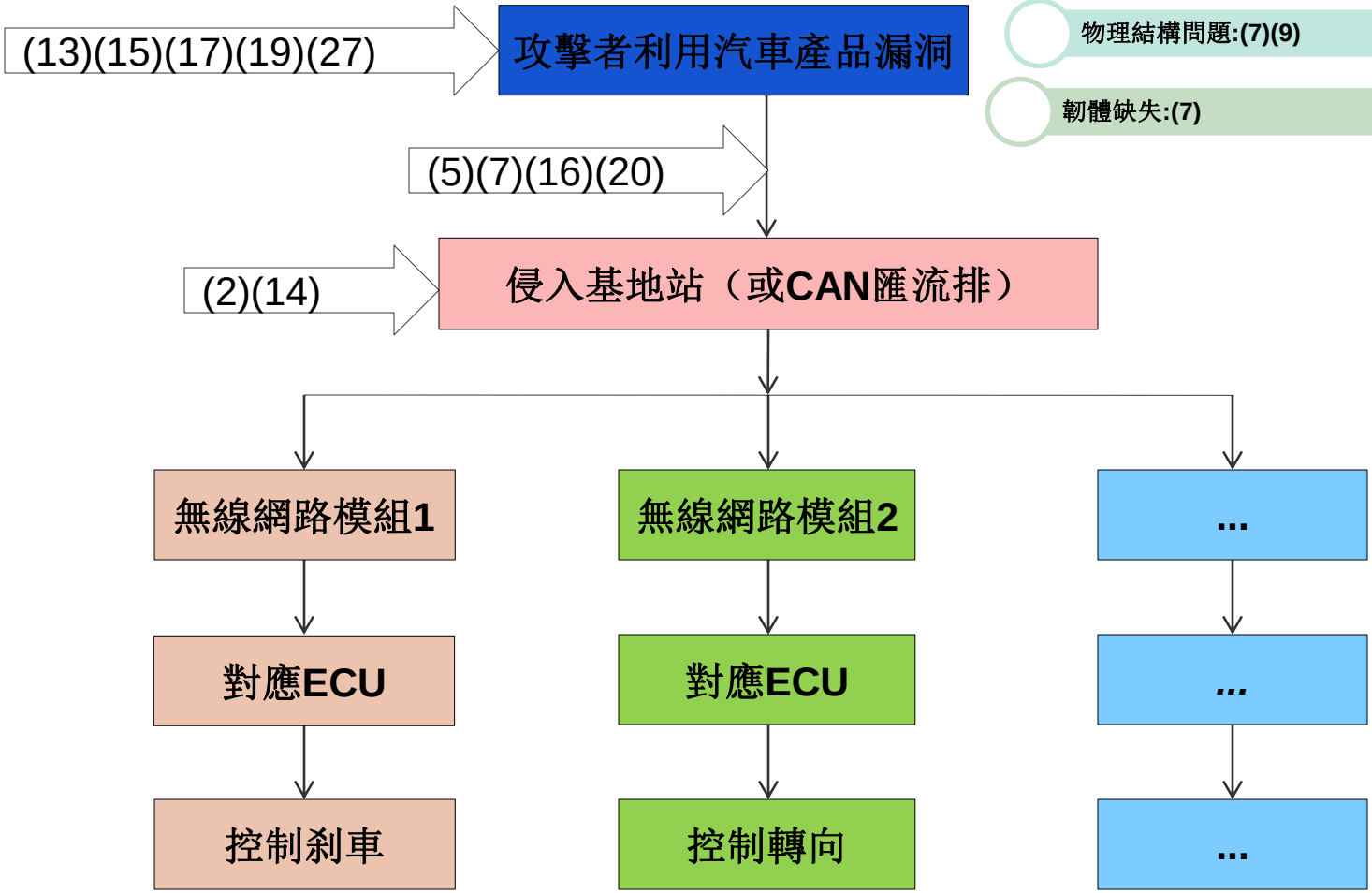
- (27) 雲安全認證
- (28) 雲安全諮詢
- (29) 建立ISO 27001資訊安全管理體制
- (30) 資訊安全性原則諮詢
- (31) 治理、風險與合規
- (32) 業務連續性管理(BCM)
- (33) 建立資訊安全意識
- (34) 外部資料隱私官
- (35) 建立資訊安全風險管理
- (36) 外部首席資訊安全官(Chief Information Security Officer)
- (37) 設置資料隱私管理
- (38) 企業資料保密性認證

我們的資訊安全服務

軟體設計漏洞:(1)(3)(7)(8)(18)(23)(24)(25)(26)

物理結構問題:(7)(9)

韌體缺失:(7)



用於改善整體管理的服務: (2) (3) (4) (5) (6) (8) (9) (10) (11) (12) (15) (16) (18) (20) (21) (22) (28) (29) (30) (31) (32) (33) (34) (35) (36) (37) (38)

車載信息安全性原則

1 資訊安全目標

2 管理與規劃

3 設計與設施

4 運行

5 審核

組織流程

- 建立資訊安全及安全管理機制ISMS
- 定義針對車載軟體資料安全目標
- 參照ISO 27001, IEC 62443以及ISO 26262規範汽車電子資訊安全設計要求
- 建立資料安全保護的開發流程
- 建立汽車運行中防攻擊及軟體安全性檢查流程

技術實施

- 安全防護實施機制定義
- 車載軟體安全性測試，包括韌體，通信協議
- 車-車間通信安全測試
- 車-後台通信安全測試

議程

1 案例分析

2 預見智慧交通系統安全要求

3 汽車資訊安全分析

4 SAE J3061

5 萊茵TÜV資訊安全服務

6 客戶及證書樣例

萊茵TÜV各領域資訊安全認證部分客戶名單

Finance

IKB Deutsche Industriebank
EOS
ING DiBa Die Bank und Du
HUK24 DIE ONLINE-VERSICHERUNG
GAD IT für Banken
Postbank
FIDUCIA Ihr IT-Partner
BUNDESDRUCKEREI
pbb DEUTSCHE PFANDBRIEFBANK
Frankfurter Volksbank

Healthcare

PVS holding GEMEINSAM BESSER.
HELIOS Kliniken Gruppe
ASKLEPIOS Gemeinsam für Gesundheit
Techniker Krankenkasse
DAK Unternehmen Leben
Malteser ...weil Nähe zählt.
BITMARCK®
OLYMPUS CONSILIO
KKH Allianz
BOSCH
GE Healthcare
ife Ihre freundlichen Experten.
HBSN AG Health Business Services Network

IT

BORnet Kommunikation
Computacenter Services & Solutions
smava Der erste Kreditmarktplatz
bank-verlag zahlungssysteme
GETYOURGUIDE Touren & Ausflüge online buchen
KID. Magdeburg
GLOBAL SWITCH
IT-Consult Halle GmbH
consint
BITMARCK®
INFO AG Ein Unternehmen der QSC AG
QVC Ideen für mich!
pco PERSONAL COMPUTER ORGANISATION
OEVERMANN® Networks GmbH
Herzlich Willkommen! Brandl
SYS
billiger.de
adlon Empowering Business with IT
icubic The solution®
on line
VIRTION
DATIS®
TAS

TÜVRheinland® Precisely Right.

萊茵TÜV各領域資訊安全認證部分客戶名單

Industrial

ThyssenKrupp Nirosta Präzisionsband
Edelstahl für Anspruchsvolle.

GEA

LANXESS
Energizing Chemistry

ifm

TAS

ThyssenKrupp VDM
Ein Unternehmen von ThyssenKrupp Stainless

ThyssenKrupp

enrichment technology
a joint venture between Urenco and Areva

OLYMPUS

fischerelektronik

Automotive

P+Z Engineering

delphi

LEAR CORPORATION

ZF

IAV GmbH
Ingenieurgesellschaft Auto und Verkehr

L'orange
YOUR POWERFUL INJECTION

BOSCH

VAPS | ACS

Audi
Vorsprung durch Technik

Others

Google Deutschland

vodafone

Lufthansa

Dumrath & Fassnacht
www.duf-online.de

GDF SUEZ
BY PEOPLE FOR PEOPLE

mediamonitoring

GREVEN'S
AdreßBuch-Verlag Köln GmbH & Co. KG

Deutsche Post

UNICEPTA
THE INFORMATION COMPANY

RTL

tipico

ERDGAS MÜNSTER
Partner für Deutsches Erdgas

HKR
Rechenzentrum GmbH

Telefónica

Lufthansa Cargo
Networking the world.

Deloitte.

VICTORGROUP

Tchibo

TÜVRheinland®
Precisely Right.

資訊安全證書範例

Certificate

Functional Safety Security

TÜVRheinland CERTIFIED

www.tuv.com
ID 0000000000

No.: 968/FSP 1104.00/15

Product tested	Safety-Related Programmable Electronic System (2oo3 with diagnostics (2oo3D) and 3-2-1-0 or 3-2-0 configurable mode of operation)	**Certificate holder**	Invensys Systems, Inc. - Triconex 26561 Rancho Parkway South Lake Forest, CA 92630 USA
Type designation	TRICON System, Details the actual "Revision List"		
Codes and standards	IEC 61508 Parts 1-7:2010 IEC 61511-1:2003 + Corr. 1:2004 ANSI/ISA -84.00.01-1:2004 EN 50156-1:2004 EN 298:2012 NFPA 85:2015 EN 54-2:1997 + AC:1999 + A1:2006 NFPA 72:2013		EN 50178:1997 IEC 61131-2:2007 IEC 61326-3-1:2008 EN 50130-4:1995 + A1:1998 + A2:2003 IEC/NP 62443-4-1:2013 IEC/NP 62443-4-2:2013 ISASecure EDSA 311:2010 ISASecure EDSA 312:2010
Intended application	Safety-Related Programmable Electronic System for process control, burner management systems (BMS), fire and gas, emergency shut down, where the safe state is the de-energized state, up to SIL 3. Applications, where the demand state is the de-energized or energized state, up to SIL 3. The system complies with the requirements of the relevant standards (SC 3 and SIL 3 acc. to IEC 61508 / IEC 61511) and can be used in safety-related applications up to SIL 3 acc. to IEC 61508, IEC 61511 and EN 50156-1. Furthermore the system complies with the embedded device requirements of the security relevant standards (Security Level 1 (SL 1) acc. to IEC/NP 62443-4-1, IEC/NP 62443-4-2, ISASecure EDSA-311 and EDSA-312). The Enhanced Safety Peer-To-Peer communication and the related Function Blocks (FBs) comply with the appropriate requirements of the relevant standards (SC 3 acc. to IEC 61508) and can be used in low/high demand applications up to SIL 3 according to IEC 61508, IEC 61511.		
Specific requirements	For the use of the system the safety and security considerations as documented in the product and user guides and the actual Revision List released by Invensys Systems, Inc. - Triconex and TÜV Rheinland must be considered.		

Valid until 2020-04-10

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1104.00/15 dated 2015-04-10.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2015-04-10 — Certification Body for FS-Products — Dipl.-Ing. Stephan Häb

ID No. 0000046188: salesforce.com, inc.

Certified Cloud Service

Certified Cloud Service

TÜVRheinland CERTIFIED

www.tuv.com
ID 0000046188

salesforce

Test Summary: | Certified Cloud Service

Information

Description:

The TÜV Rheinland i-sec GmbH certification body certifies that Salesforce has implemented effective processes and controls for achieving the following objectives for the cloud services branded as Sales Cloud, Services Cloud, Chatter, Analytics Cloud, Communities, Site.com, Database.com and Force.com.

- Effective implementation of the technical and organizational measures as required under Article 17 of the European Data Protection Directive 95/46/EC and Section 9 and the annex to Section 9 of the German Federal Data Protection Act, including
  - Physical Security : Securing data processing facilities against unauthorized access
  - Logical Security: Securing data processing systems against unauthorized access or use
  - Access Controls: Effective user authorization concept and user management – effective management of user permission profiles
  - Transmission Security: Secure data transmissions and data protection compliant transmission procedures
  - Logging: Auditability of data entries and modifications/deletions of data
  - Job Control: Securing of data protection throughout the entire supply chain
  - Desaster Recovery: Effective disaster recovery concept and architecture and processes to prevent destruction or loss of data
  - Logical segregation of individual cloud tenants and segregation of data processed for different purposes
- Conformance of Salesforce's data protection agreements with the German Federal Data Protection Act

Evidence was obtained by means of external and internal security analyses and an onsite audit of the technical, physical and organizational security measures and data protection-relevant business procedures. Test report 63006585-01 forms part of this certificate.

TÜV Rheinland i-sec GmbH conducts yearly follow-up audits of the assessed cloud services.

This certificate is valid until 31.08.2018.

TÜVRheinland®
Precisely Right.

Thank you !