OT 網路資安規範趨勢與設備供應商之因應

黃凱偵 (Kai Chen Huang)

Lead SW Engineer, R&D Center

2024/05/16

MOXA®

Reliable Networks ▲ Sincere Service

黃凱偵 (Kai chen Huang) aka Kevin KC Huang

kevin.huang@moxa.com

- 軟體研發部 R&D (2008~)
- ISA/IEC 62443 Expert (2023~)

- **經歷**
  - 工業網路安全路由器 Secure Router 研發
  - IEC 61162-460(Ed.2, 2018)產品認證
  - IEC 62443-4-2 SL2產品認證
  - UR E27(Rev.1, 2023)船籍社SL2/SP2產品型式認可執行
  - IEC 62443-3-3研究小組
  - UR E26/E27研究小組

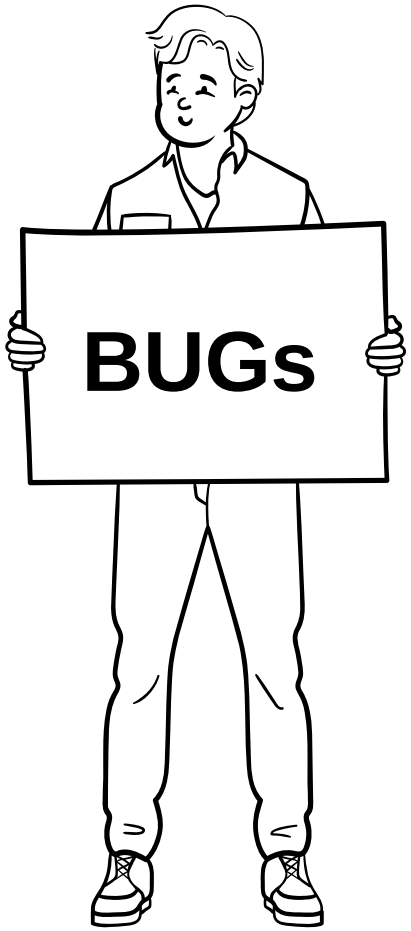
Scan to validate

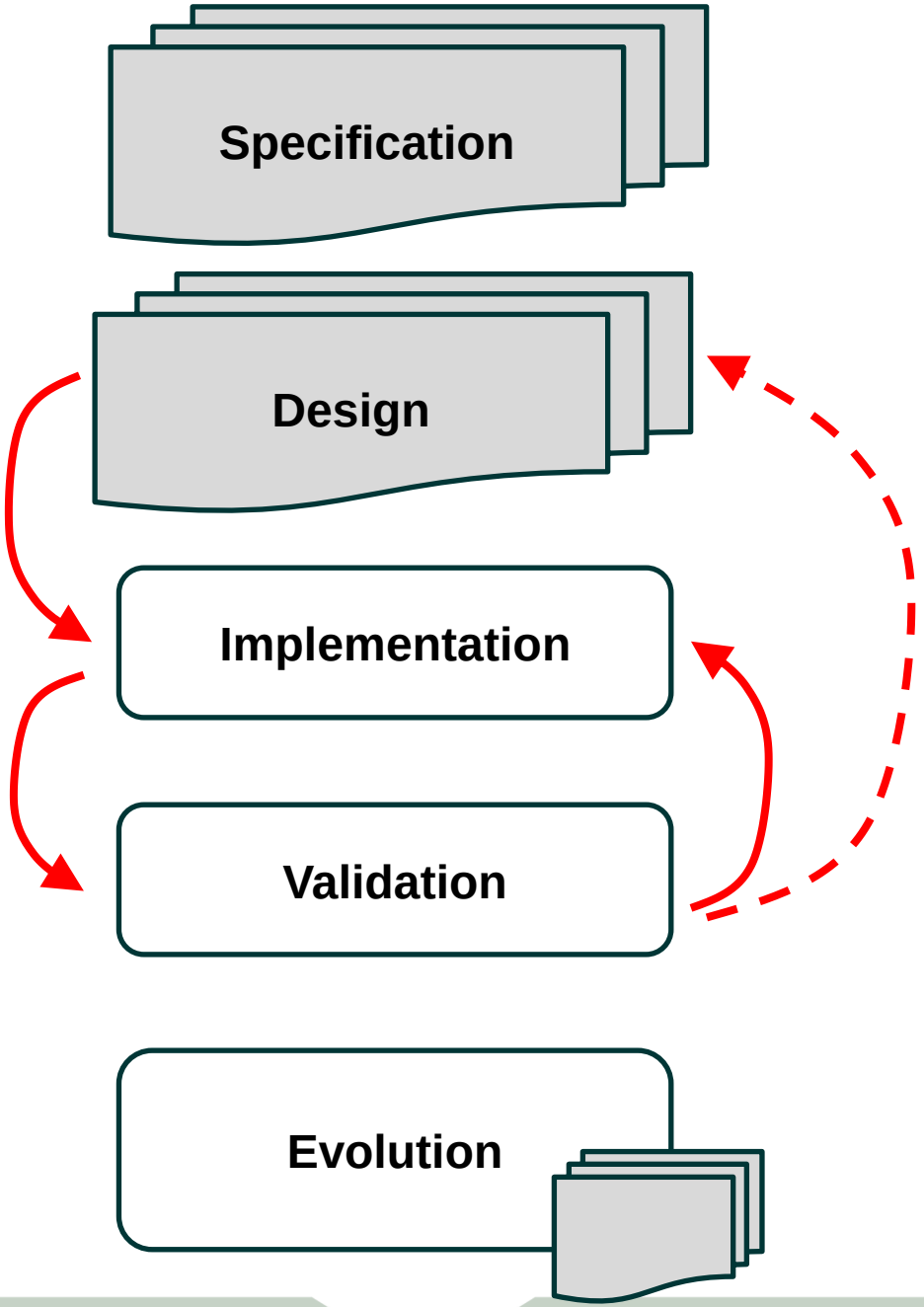
ISA/IEC 62443 Badge

Agenda

- 62443-4-2產品開發經驗與發現
- 以UR E27為例 – 62443與規範間的差異
- Summary - R&D心得

R&D開發-4-2產品經驗 (62443-4-1)



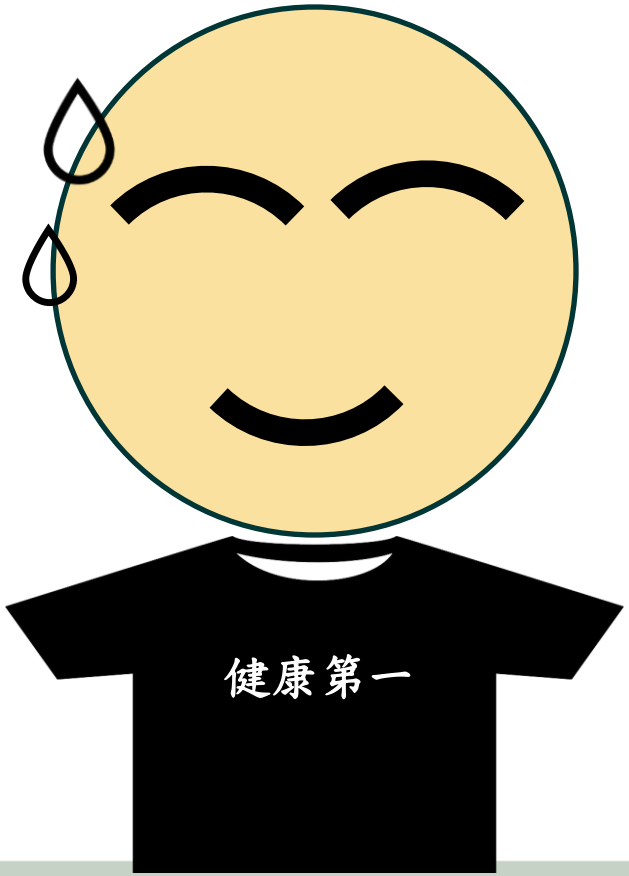


62443-4-2取證後

YA，終於拿到62443-4-2產品認證，來爽慶祝一波。

R&D

我很有興趣。想多瞭解62443-4-2產品怎麼應用到**系統**



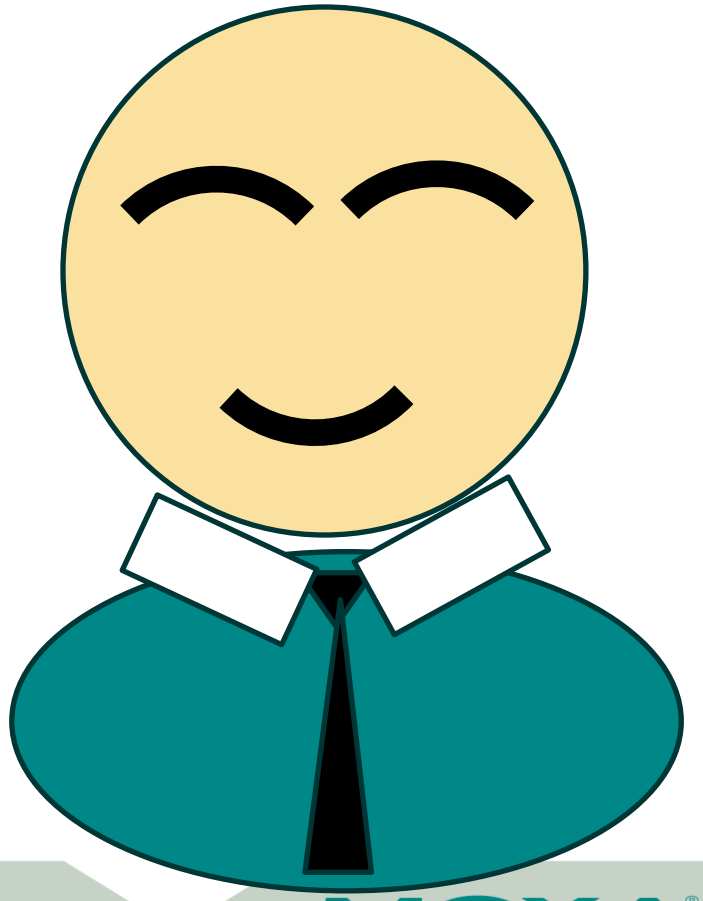
62443-4-2有對應62443-3-3

我要符合XXX資安規範。

我家顧問說: 規範參考62443-3-3。使用62443-4-2產品比較容易，是嗎?

難道不是嗎???

客戶

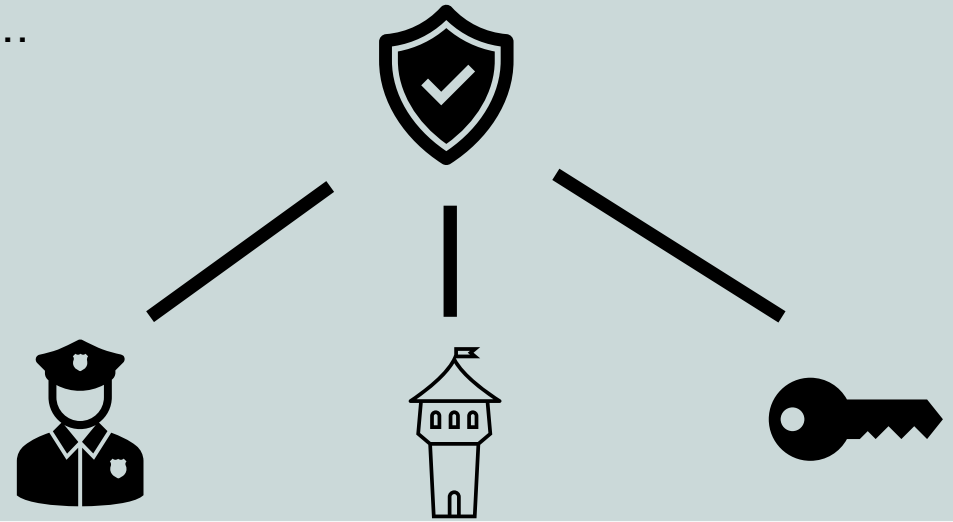


引用到62443-3-3的例子

應用	Regulation / Standard / Guideline
Marine	UR E27
Rail	CLC/TS 50701:2023
EV charging infrastructure	EV-211-2022, ENCS
電動車供電	電動車供電設備資訊安全檢測技術規範
⋮	⋮

Requirement更明確

- **Authenticator管理**

IEC 62443-3-3	Others Regulation / Standard / Guideline
• 保護所有authenticator 	• 用A方法保護 • 用B方法保護 • 用C方法保護 • …. 

System v.s. Component

Source	Description
62443-4-2	來自或經由不可信網路 + 存取**設備** -> 監控
62443-3-3	來自或經由不可信網路 + 存取**系統** -> 監控

	Switch	Firewall
62443-4-2	• Trusted Access List	• Trusted Access List
62443-3-3	• **N/A (Protected by Firewall)**	• Trusted Access List • **Firewall Policy**

注意: **不能影響Essential Function**

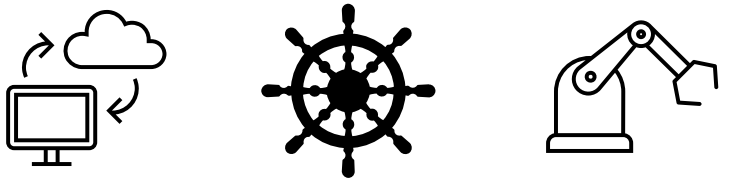
以UR E27為例

62443與規範間

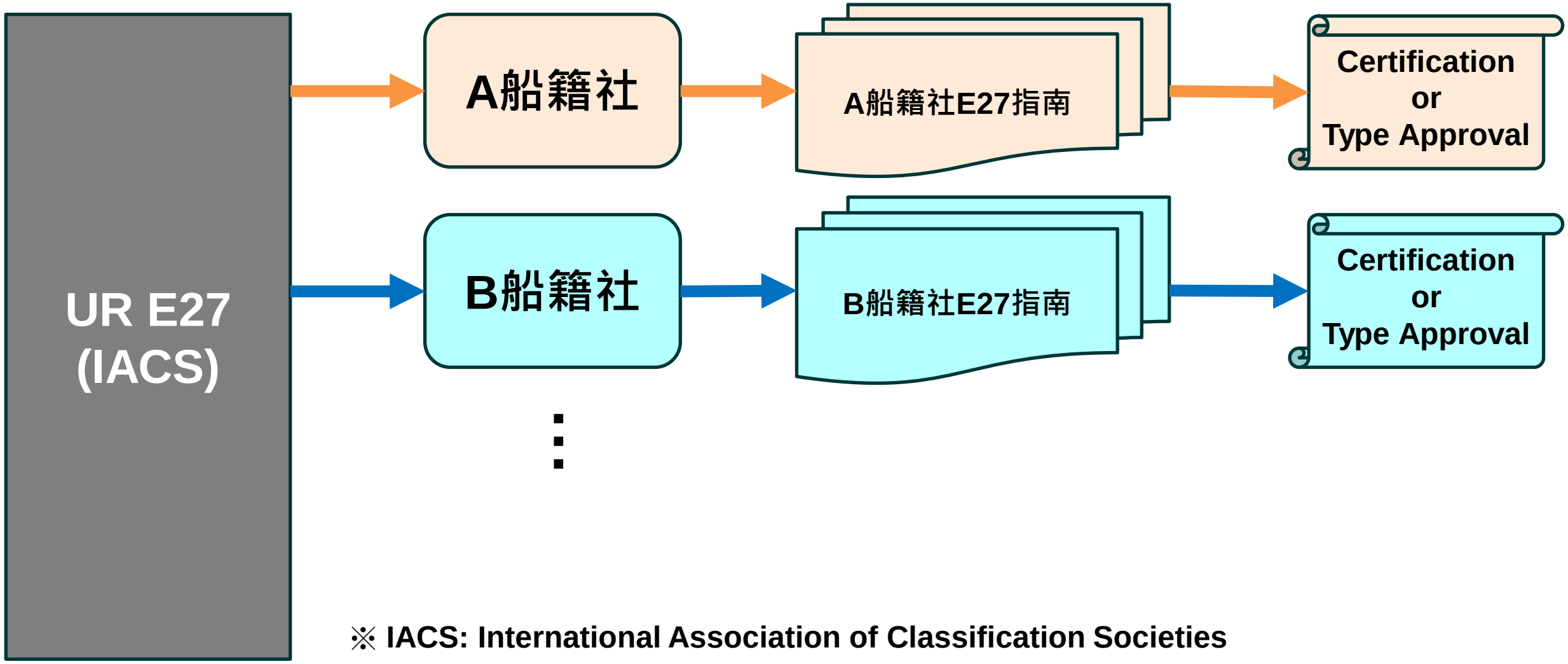
簡介UR E26/E27 UR: United Requirement

E26: 船舶管理及相關需求

E27: 船舶網路系統和設備韌性的相關安全功能需求



UR E27 and 船籍社(Classification Society)



※ IACS: International Association of Classification Societies

內容差異 (1/2)

Source	Description
62443-4-2	來自或經由不可信網路 + 存取設備 -> 監控
62443-3-3	來自或經由不可信網路 + 存取系統 -> 監控
UR E27	來自或經由不可信網路 + 存取CBS -> 監控
A船籍社	經由不可信網路 + 存取CBS -> 監控
B船籍社	來自或經由不可信網路 + 存取設備 -> 監(log、…)控(限制、...)

※ CBS: Computer Based System

	Switch	Firewall
62443-4-2	• Trusted Access List	• Trusted Access List
UR E27	• N/A (Protected by Firewall)	• Trusted Access List • Firewall Policy • Log…etc Capability (by B船籍社)

內容差異 (2/2)

Source	Log Category
62443-3-3	1. xxxx **2. YYYY** 3. xxxx 4. xxxx 5. xxxx 6. xxxx **7. DDDD** **8. BBBBB**
62443-4-2	1. xxxx **2. YYYY** 3. xxxx 4. xxxx 5. xxxx **6. BBBBB**
UR E27	1. xxxx 2. xxxx 3. xxxx 4. xxxx **5. SSSSSS**

Source	Log Category
A船籍社	1. xxxx 2. xxxx 3. xxxx 4. xxxx **5. SSSSSS**
B船籍社	1. xxxx **2. YYYY** 3. xxxx 4. xxxx 5. xxxx 6. xxxx **7. DDDD** **8. BBB**

Security Level

Source	Security Level	Description
62443-3-3	3	人類使用者 + 來自或經由不可信網路 + 存取System -> MFA
62443-4-2	3	人類使用者 + 來自或經由不可信網路 + 存取System -> MFA
UR E27	--	人類使用者 + 來自或經由不可信網路 + 存取CBS -> MFA
A船籍社	0	人類使用者 + 經由不可信網路 + 存取CBS -> MFA
B船籍社	1	人類使用者 + 來自或經由不可信網路 + 存取CBS -> MFA

額外需求

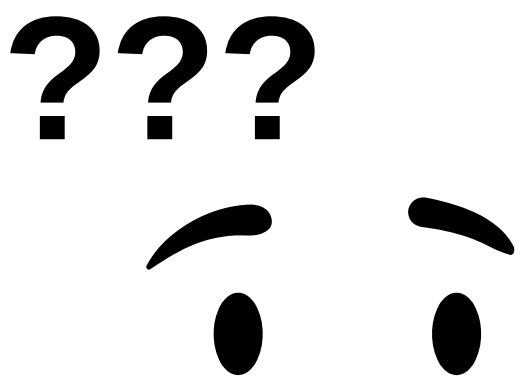
Source	Description
B船籍社	DoS防護。(See IEC-62443-3-3 SR-XXX) Amendments: 參考B船籍社另一份文件ABC

Source	Description
62443-3-3	• DoS防護
B船籍社 - 文件ABC	• 應防範過量的Network Traffic。 • 偵測到異常後及時通知。

Summary

R&D心得

參考哪些Regulation?



Which one?

- 法規強制力
- 客人需求
- 產品加分

Summary

- **發現Regulations/Standards/Guideline間的落差**
  - **優點**
    - 以**系統**層面思考**產品**功能
    - 多面相理解/比較條文需求，寫出更精準的statement (有些寫得模稜兩可) -> Spec.
    - (optional) 善用顧問
    - **前期確認完要過的目標規範後才訂Spec.，避免二次開發**
  - **缺點**
    - 選定目標不易
    - 花費比較多的時間理解條文

Takeaway (產品合規)

- **化繁為簡 (多個版本的firmware，No!!!)**
- **化簡為繁 (設計時有意義地參考多份Regulation/Standard/Reference，Yes!!!)**

謝謝