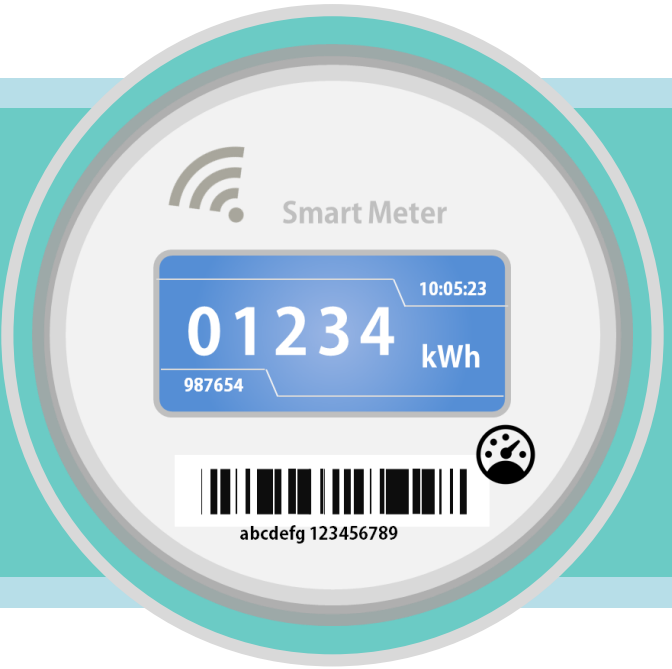
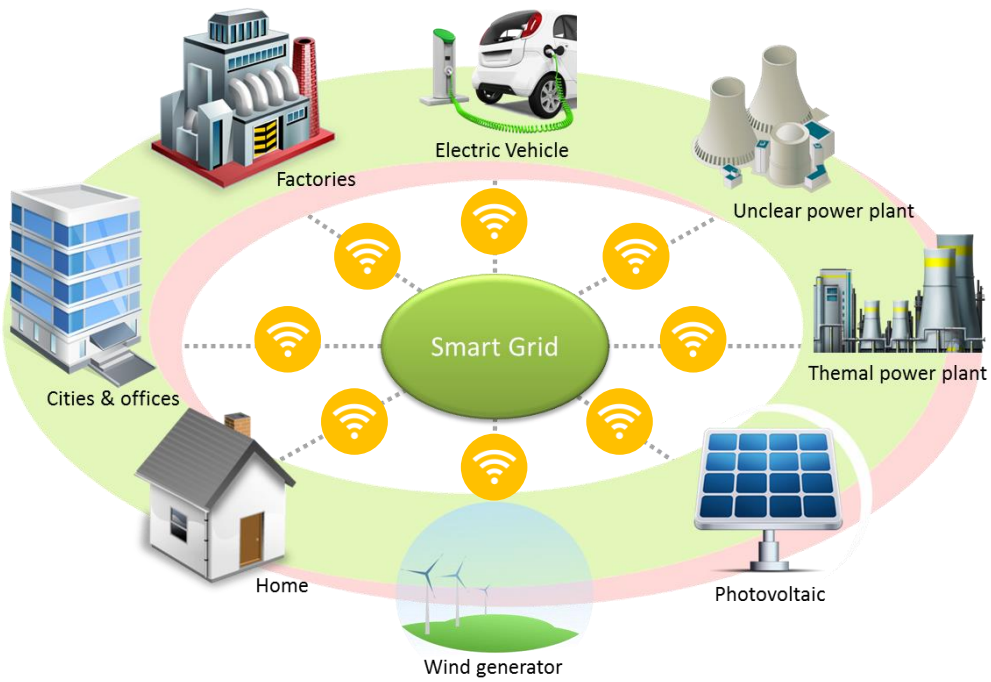


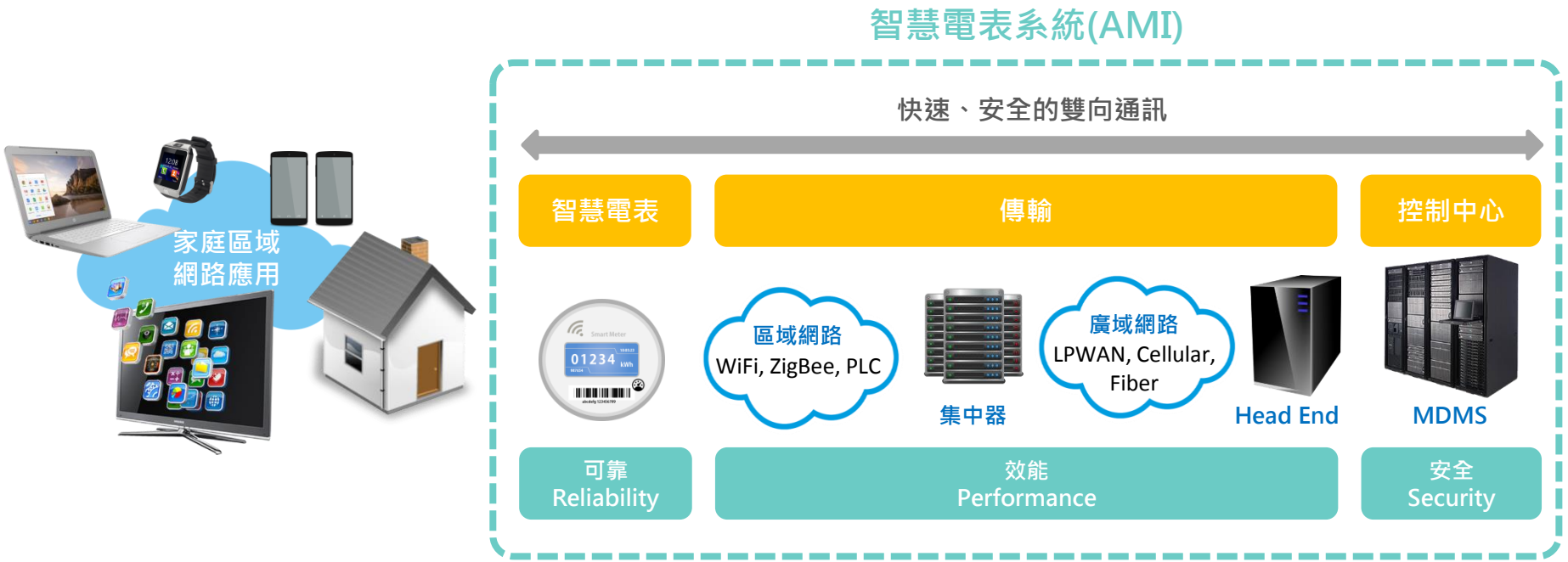
智慧電表通訊效能暨資訊安全驗證平台

智慧電表通訊效能與資訊安全驗證平台

- 為配合行政院「智慧電網總體規劃」確保穩定供電、促進節能減碳、提高綠能使用、引領低碳產業等目標，並達建立高品質、高效率和環境友善的智慧化電力網，促進低碳社會及永續發展的實現之願景。
- 智慧電網為我國重要關鍵基礎建設之一，可靠性的智慧電網必須倚賴高效能且安全的通訊系統。
- 本中心延續105年「我國智慧電網無線通訊品質及資通安全檢測方法之研究」之成果與發現，擬建置「智慧電表通訊效能與資訊安全驗證平台」，確保並驗證智慧電表使用高效能且安全的通訊系統，協助政府推動智慧電網之規劃，推動節能減碳之政策。



- 智慧電表系統通訊效能將直接影響讀表、自動需量反應或即時電價等智慧電網應用的效率，確保資訊安全則是智慧電網正常運作及發展的重要基礎。
- 「智慧電表通訊效能與資訊安全驗證平台」計畫係針對智慧電表系統通訊效能、可靠度、頻譜效率及資訊安全等技術進行研究、制定測試案例、評估指標與測試標準以協助台電於實際場域進行驗證。
- 本計畫也將評估智慧電表通訊系統整合水表及提供家庭區域網路(Home Area Network, HAN)服務的通訊效能及潛在資安問題，並協助台電建立智慧電表與配電系統資通訊系統整合及資安系統。



智慧電表通訊效能與資訊安全驗證平台

建置通訊效能測試驗證平台

- 通訊模組符合性驗證
- 系統層級效能驗證
- 智慧電表通訊系統加值服務評估
- 測試及驗證規範建立

建置資訊安全驗證平台

- 制定智慧電網資安規範指南
- 智慧電表通訊系統設備安全評估及驗證
- 建置智慧電網之安全與模擬試驗平台研究

智慧電表通訊效能與資訊安全驗證平台之計畫目標為確保並驗證智慧電網使用高效能且安全的通訊系統，以協助政府推動智慧電網之規劃，推動節能減碳之政策。

建置通訊效能測試驗證平台

- 開發智慧電表通訊效能(含頻譜效率)驗證技術並於試驗場域及現場進行實測與分析
- 建置智慧電表通訊效能(含頻譜效率)驗證平台並制定測試標準
- 智慧電表通訊系統加值服務評估
- 建置智慧電表整合智慧家庭應用通訊效能驗證平台
- 制定智慧電表通訊效能(含頻譜效率)優化程序規範
- 建置智慧電表通訊測試實驗室，提供標準化測試程序，輔導廠商提升資安與通訊效能可靠度
- 完成通訊效能可靠度改善技術並提出具體建議協助台電建立智慧電表與配電系統資通訊系統整合

建置資訊安全驗證平台

- 完成智慧電網資安規範指南制訂與風險評估、減輕與防護監控/AMI集中器設備安全性評估與驗證
- 完成AMI家用閘道器安全性評估、驗證及改善建議
- 完成智慧電表與配電系統資通訊系統整合
- 建置智慧電網之安全與模擬試驗平台
- 適用智慧電網資安衝擊對應處理及稽核程序
- 基於智慧電網之安全與模擬試驗平台，進行攻防情境演練，以供緊急應變、系統復原等演練
- 協助建立智慧電表與配電系統資通訊系統整合及符合我國環境之智慧電網資安系統

建置通訊效能測試驗證平台

智慧電表通訊效能測試驗證平台

1 通訊模組符合性驗證

免執照頻段及專用頻段驗證平台

- EIRP限制
- 跳頻特性
- 頻率穩定性
- 帶外輻射
- 電磁波密度
- 頻譜遮罩

研析及驗證

- 頻寬需求評估
- 帶外輻射
- PPDR保護頻寬
- 頻寬需求評估
- 抗干擾

2 系統層級效能驗證

無線通訊模組環境測試

- 耐候環境試驗
- 電磁相容試驗

通訊鏈路效能測試

- 射頻效能及頻寬需求驗證
- 涵蓋及服務品質驗證
- 頻譜使用率

通訊系統服務驗證

- 系統容量
- 系統參數優化
- 系統可接取性測試
- 服務情境可接取性
- 服務情境完整性

3 智慧電表通訊系統加值服務評估

加值服務評估

- 評估智慧電表通訊系統整合水表的可行性
- 評估智慧電表系統提供家庭區域網路(Home Area Network, HAN)服務的可行性

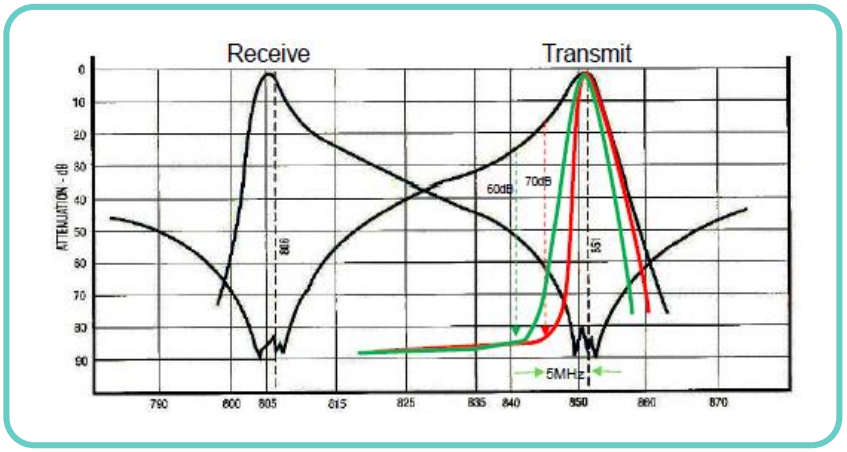
4 測試及驗證規範建立

測試及驗證規範建立

- 制定通訊模組符合性測試標準
- 情境化服務效能驗證案例開發
- 通訊系統應用開發驗證案例、優化及驗證標準

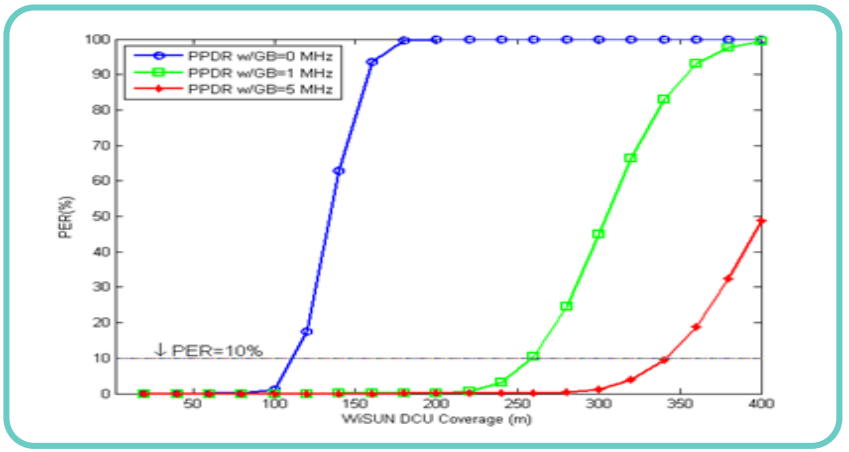
- 建置免執照頻段及專用頻段驗證平台，針對各種通訊設備的EIRP限制、跳頻特性、頻率穩定性、帶外輻射、電磁波密度及頻譜遮罩等國家法規項目進行測試。此外，也將針對頻寬需求評估、抗干擾及鄰近系統(如公共安全與救難應變, PPDR)間保護頻寬等相關研析及驗證，確保智慧電表通訊模組符合國家法規及實際運作時的效能要求。

智慧電表通訊模組頻譜遮罩



資料來源：Sensus

考慮PPDR存在GB下，
干擾對Wi-SUN DCU涵蓋距離之影響



資料來源：TTC,我國智慧電網無線通訊品質及資通安全檢測方法之研究期末成果報告

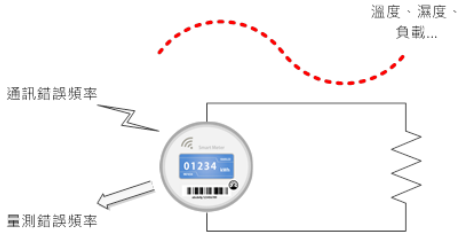
1. 無線通訊模組環境測試

2. 通訊鏈路效能測試

3. 通訊系統應用驗證

測試智慧電表在不同的環境因素下，各種通訊系統的通訊效能(如封包錯誤率)，並建立智慧電表通訊可靠度的測試與評估方法，用以評估電表實際佈建後的可用度與服務品質。

- 測試項目
  - 耐候環境試驗
  - 電磁相容試驗



- 測試方法：施行長時間的連續性測試，計算其發生錯誤的頻率，其可變之測試參數為負載、溫度、濕度、通訊之訊號強度與干擾等。
- 計算方法與指標

  $\lambda = 1/MTBF$ (錯誤率)，其中MTBF（Mean Time between Failure）為連續兩次發生錯誤間的平均時間

1. 無線通訊模組環境測試
NB-IOT、LoRa及Sensus FlexNet等

2. 通訊鏈路效能測試

3. 通訊系統應用驗證

射頻效能、頻寬需求驗證、通訊協定分析、涵蓋驗證、系統層級服務品質驗證、弱訊號環境效能測試等。

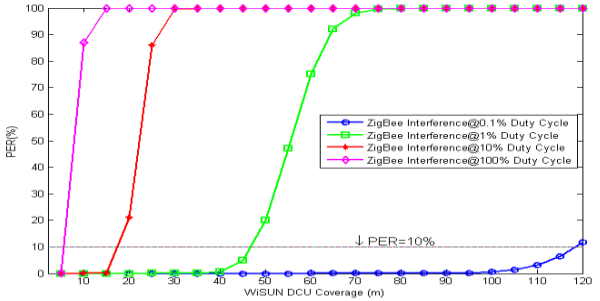
- 射頻效能及頻寬需求驗證

  EIRP測試、鄰頻系統保護頻寬驗證、同頻系統安全距離驗證、FDD系統上下行保護頻寬驗證與實際頻寬需求驗證。

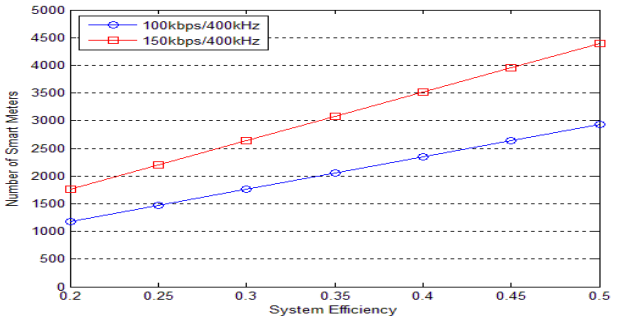
- 涵蓋及服務品質驗證

  室內/室外/地下室涵蓋驗證、干擾情境下涵蓋驗證（LTE 900MHz設備及免執照頻段設備為干擾源）、弱訊號及異常情境通訊協定驗證（Self-DDOS attacks）。

- 頻譜使用率：專用頻段頻譜使用率評估



考慮ZigBee於不同Duty Cycle干擾情況下Wi-SUN DCU涵蓋距離



400KHz通道頻寬可支援的電表數量

資料來源：TTC,我國智慧電網無線通訊品質及資通安全檢測方法之研究期末成果報告

1. 無線通訊模組環境測試
NB-IOT、LoRa及Sensus FlexNet等

2. 通訊鏈路效能測試

3. 通訊系統應用驗證

從系統可獲得性、接取性測試、服務情境(如讀表、升版、自動需量反應等)可接取性、完善性及可持續性驗證通訊系統網路服務效能。

網路可獲得性
Network Availability

第1層 智慧電表通訊模組可以擷取DCU(Data Collect Unit)或鄰近通訊模組訊號

網路可接取性
Network Accessibility

第2層 智慧電表通訊模組可在該網路完成驗證等註冊程序

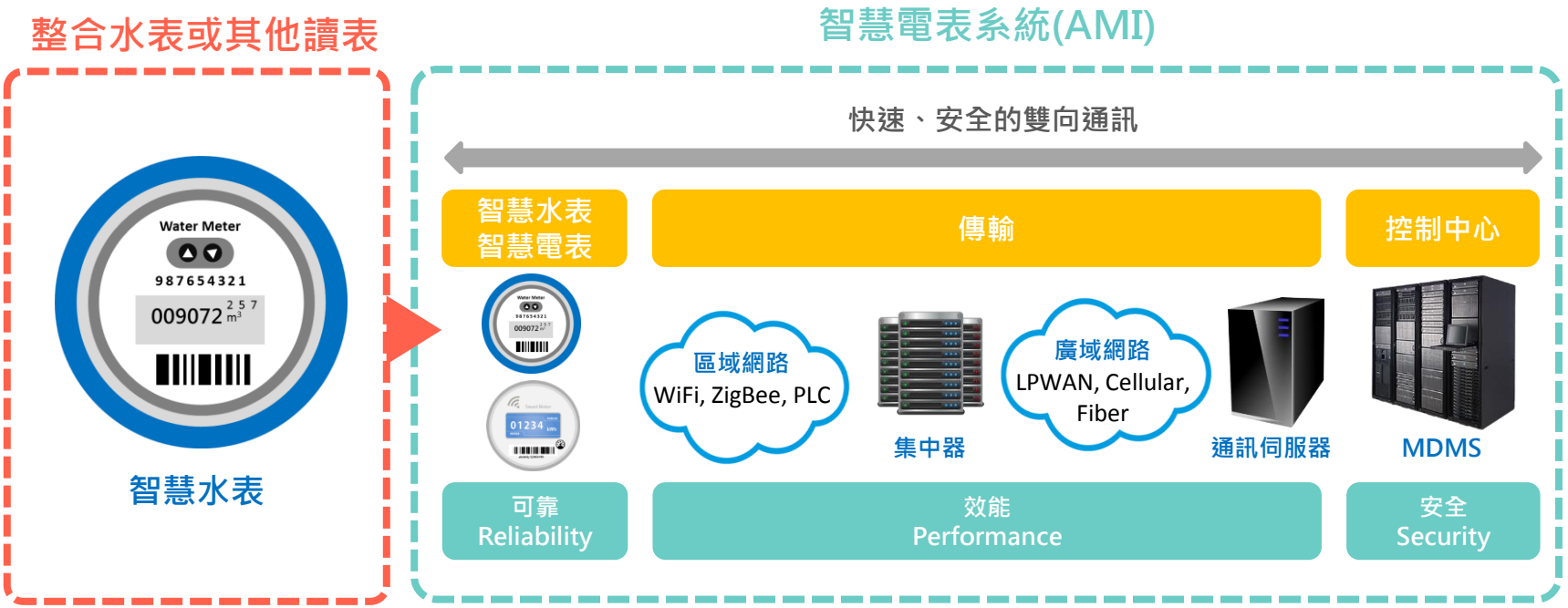
第3層

服務可接取性
Service Accessibility
智慧電表通訊系統成功接取某一應用服務，例如讀表、升版、需量反應...)

服務完善性
Service Integrity
智慧電表通訊系統使用某一服務過程中的品質，例如讀表、升版或需量反應時間超過預期

服務可持續性
Service Retainability
智慧電表通訊系統使用某一服務時是否發生中斷，例如讀表、升版或需量反應時間超過預期

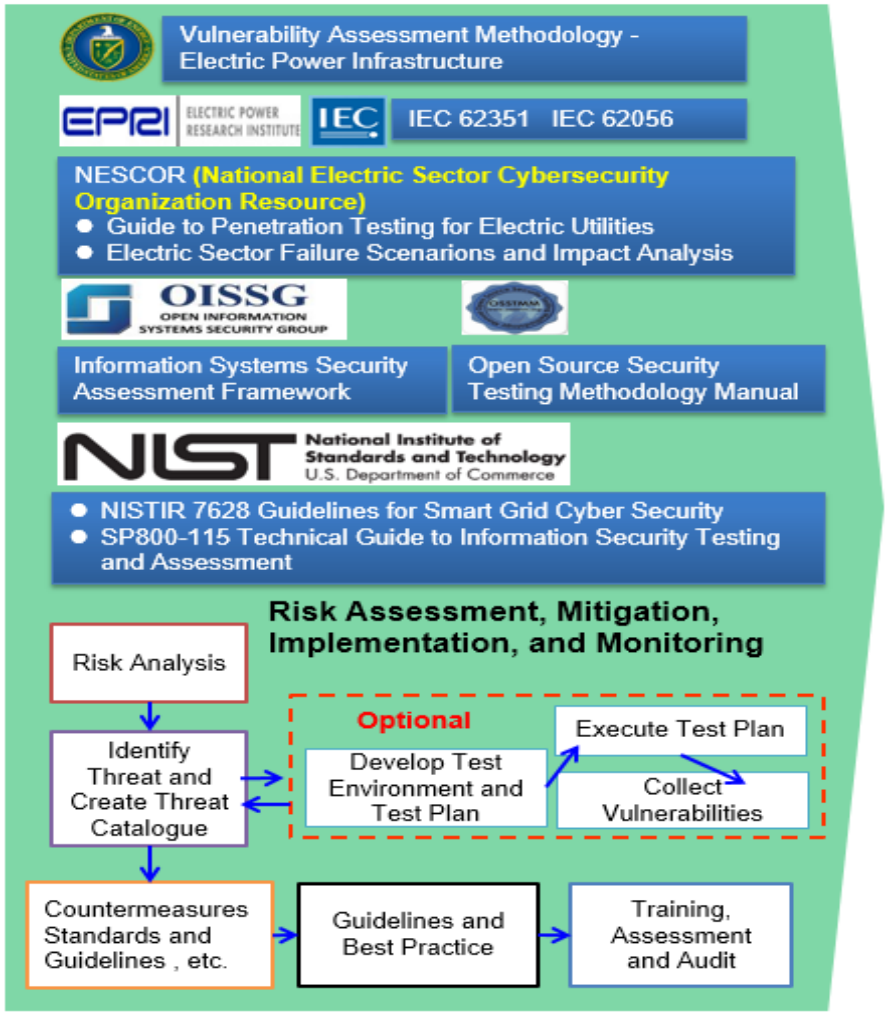
- 評估智慧電表通訊系統整合水表或其他讀表在容量、網路架構及資訊安全等議題
- 評估智慧電表通訊系統整合家庭區域網路(Home Area Network, HAN)各種應用的效能及資安議題



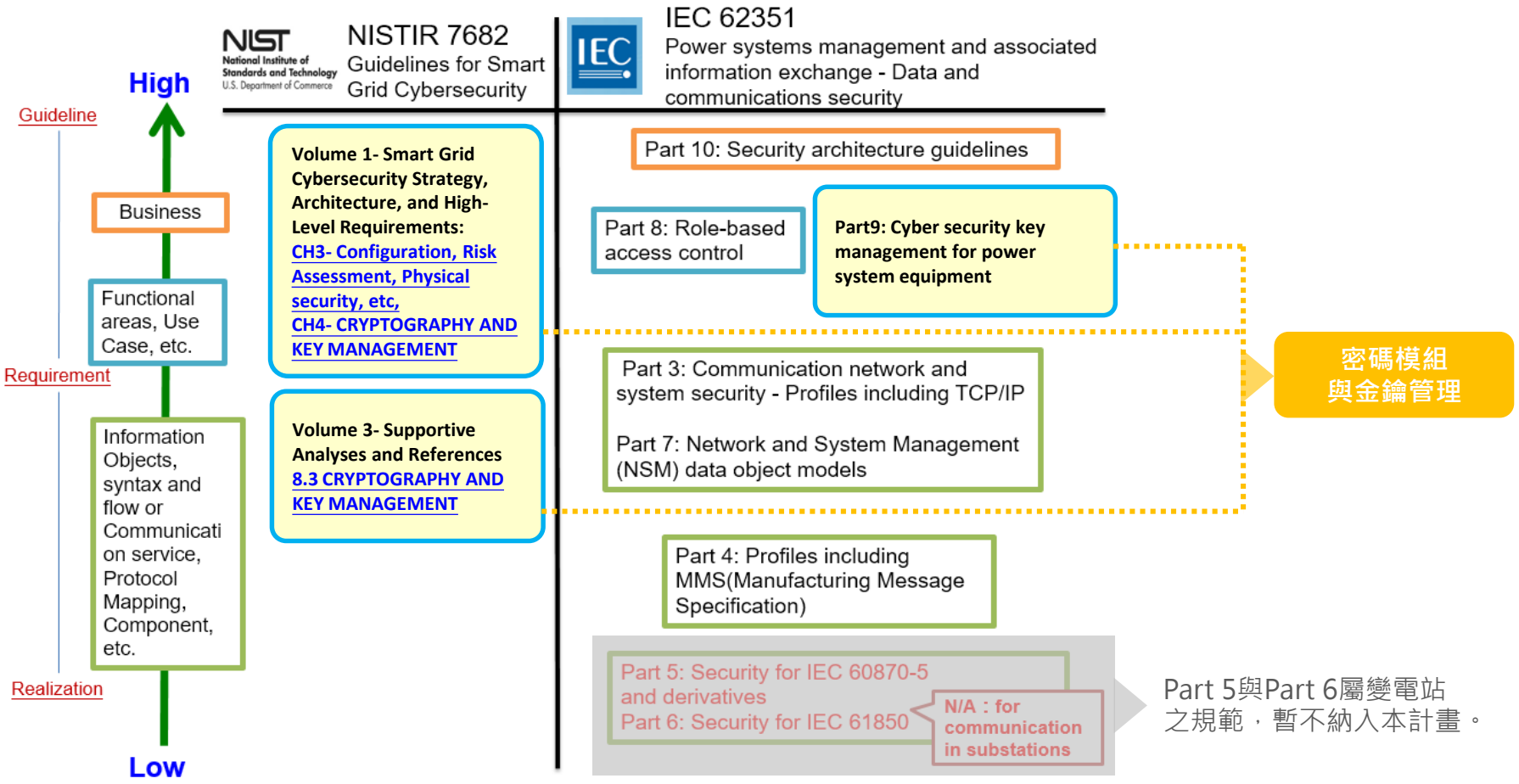
- 制定智慧電表通訊系統測試標準及驗證規範
  - 針對通訊模組符合性驗證、系統層級效能驗證及智慧電表通訊系統加值應用評估等工作項目，制定相關測試標準及驗證規範
- 智慧電表通訊系統效能優化程序
  - 依據上述測試結果，制定通訊系統效能制定優化程序

建置資訊安全驗證平台

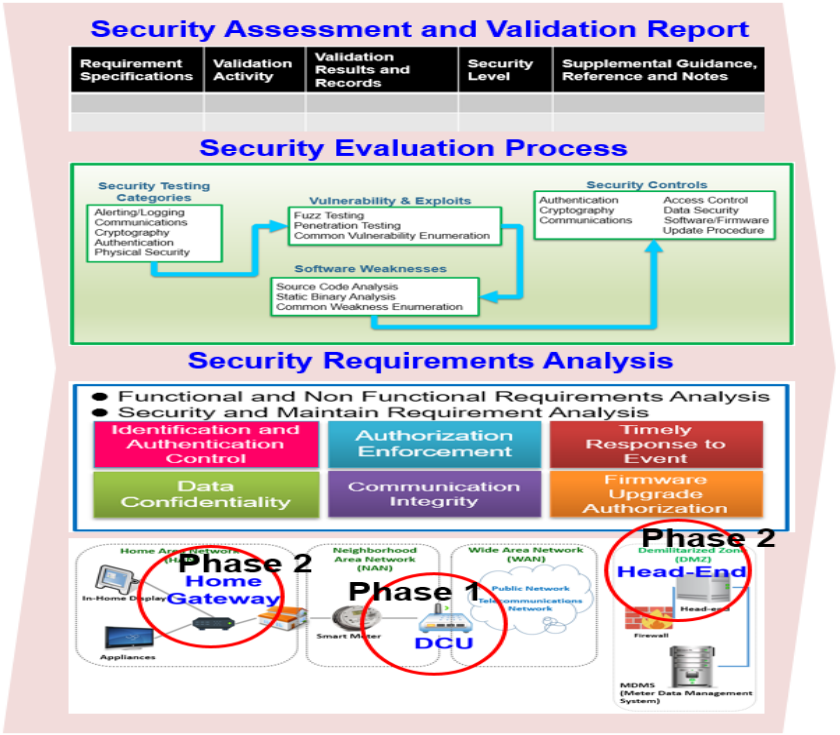
- 參考NISTIR 7628密碼模組與金鑰管理、美國能源部電力基礎設施之弱點評估方法論、IEC 62351資料與通訊相關之安全內容安全標準等，進行智慧電網風險分析、威脅識別、預防措施與對應其他國際安全標準，制定適合我國智慧電網資安相關規範指南。
- 107年完成智慧電網資安技術規範與指南/智慧電網風險評估、減輕與防護監控建議並逐年檢視與必要時之修正。

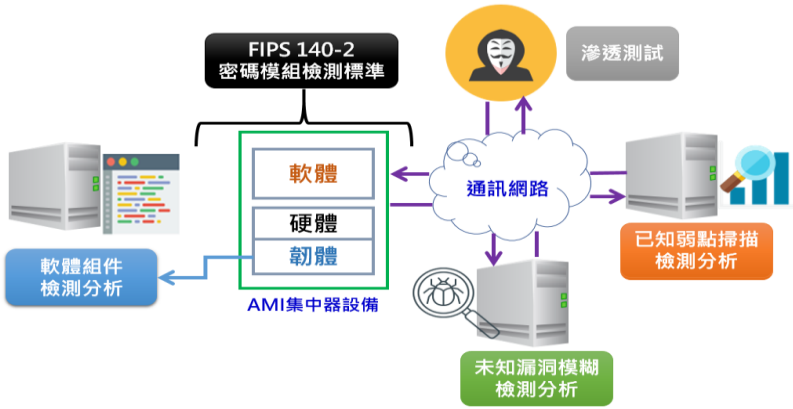


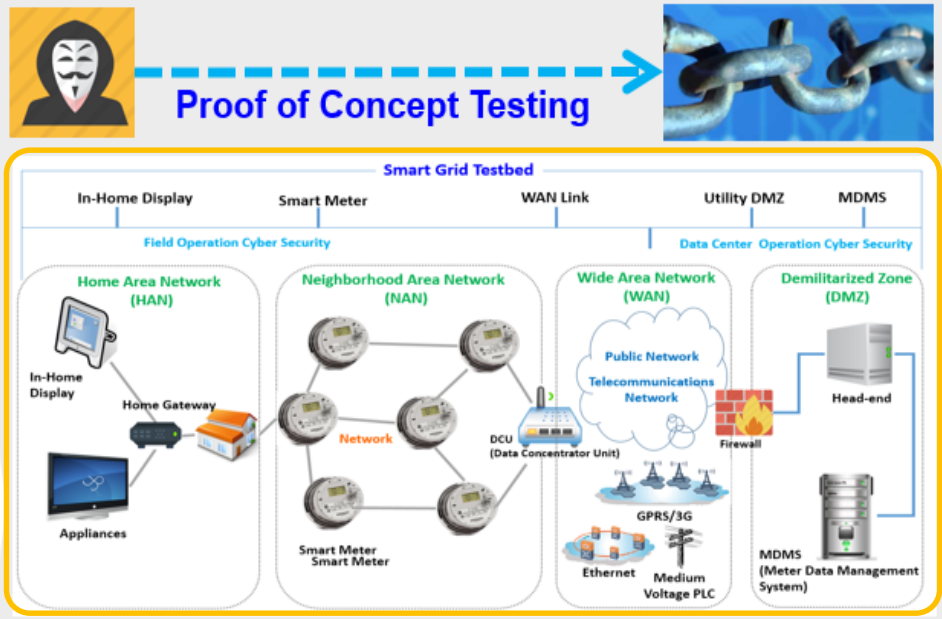
- 本計畫以NISTIR 7628以密碼模組與金鑰管理之內容為研析主軸；整合IEC 62351提取資料與通訊相關之安全內容，制定適合我國智慧電網資安相關規範指南。



- 進行智慧電網AMI及集中器設備的資安功能評估驗證，依據設備功能與角色安全確立必要之安全需求，規劃安全控制功能所需之測試案例，進行測試驗證。並從軟/韌體層面透過不同檢測工具進行弱點分析，提出必要之建議調整或修補建議報告。
  - 針對密碼模組以FIPS 140-2之標準進行評估
  - 研析AMI及其集中器設備管理機制與建議，在非安全管控範圍下，集中器實體防護安全是否應納入之設計。
  - 利用軟韌體分析與弱點掃描評估是否存有已知漏洞，並利用模糊測試技術探測是否有弱點瑕疵。
- 107年完成AMI及集中器設備安全性評估、驗證及改善建議報告並逐年延伸至HAN及HES (Head-End System)設備安全性評估、驗證及改善建議報告。







Embedded Device Penetration Testing

Dumping Data, Firmware Binary Analysis, etc.

Server Application Penetration Testing

Authorization & Authentication Testing, DoS Testing, Code Injection Testing, etc.

Network Communications Penetration Testing

Cryptanalysis, Network Protocol Fuzzing, etc.

Server OS Penetration Testing

DoS Testing, Vulnerability Scanning, etc.

- 參考日本Control System Security Center (CSSC)完成智慧電網之安全與模擬試驗平台，可應用於滲透測試與防禦技術之攻防情境演練，以供緊急應變、系統復原、協調控管等能力之演練強化等。

Defense in Depth Technology

Authentication, Firewall and White List, Intrusion Detection, Network Monitoring, Logging System and Analysis, etc.

計畫里程碑

107年

- 開發智慧電表通訊效能(含頻譜效率)驗證技術並於試驗場域及現場進行實測與分析
- 開發智慧電網資安技術規範與指南/智慧電網之弱點掃描與滲透測試技術
- 研究智慧電網資安及通訊效能可靠度改善技術並提出具體建議
- 協助台電建立智慧電表與配電系統資通訊系統整合及資安系統

108年

- 建置智慧電表通訊效能(含頻譜效率)驗證平台並制定測試標準
- 制定智慧電網資通安全檢測與資安風險評估與防護規範

109年

- 建置智慧電表整合智慧家庭應用通訊效能(含頻譜效率) 驗證平台
- 建置資安模擬測試平台強化AMI網路的安全性
- 協助台電完成智慧電表與配電系統資通訊系統整合及資安系統

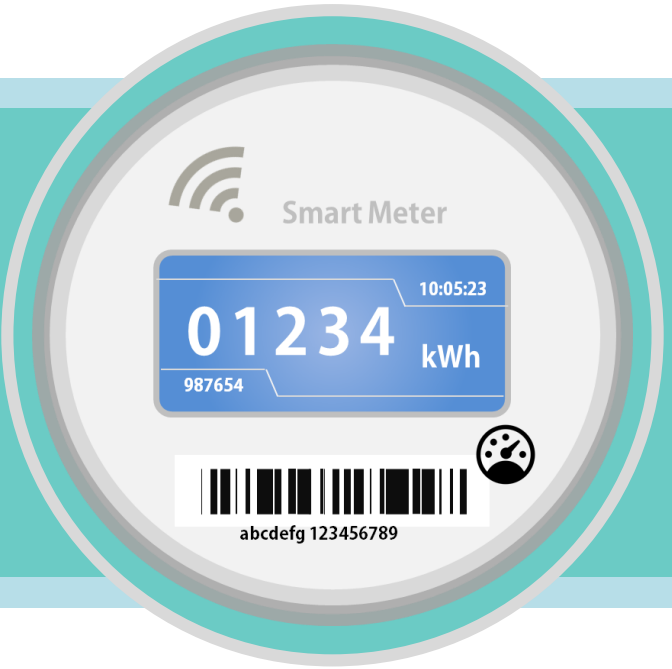
110年

- 制定智慧電表通訊效能(含頻譜效率)優化程序規範
- 適用智慧電網資安衝擊對應處理及稽核程序

111~115年

- 建置智慧電表通訊測試實驗室，提供標準化測試程序，輔導廠商提升資安與通訊效能可靠度
- 協助台電完成智慧電表與配電系統資通訊系統整合及符合我國環境之智慧電網資安系統
- **2024年協助完成300萬具低壓智慧電表佈建**

- 開發符合智慧電表通訊效能及可靠度測試方法與評估指標；透過弱點掃描與滲透測試，評估系統資安威脅，以發展符合我國環境之智慧電網資安規範指南規劃，確保智慧電表通訊系統效能與資訊安全防護。
- 整合資通訊軟硬體測試儀器，建構可複製或移轉智慧電表通訊效能與資通安全測試平台，評估專用頻段與ISM頻段效能差異及電磁波特性，協助民眾瞭解智慧電表運作時的安全性。
- 建置智慧電表通訊模組可靠度及效能測試平台，及智慧電表資通安全模擬試驗平台，提供我國智慧電網相關產業發展新技術研發測試驗證。



敬請指教，謝謝!