中原大學

國際智慧電網資通訊安全相關標準現況簡介

2014 智慧電網核心標準研討會

賴裕昆助理教授

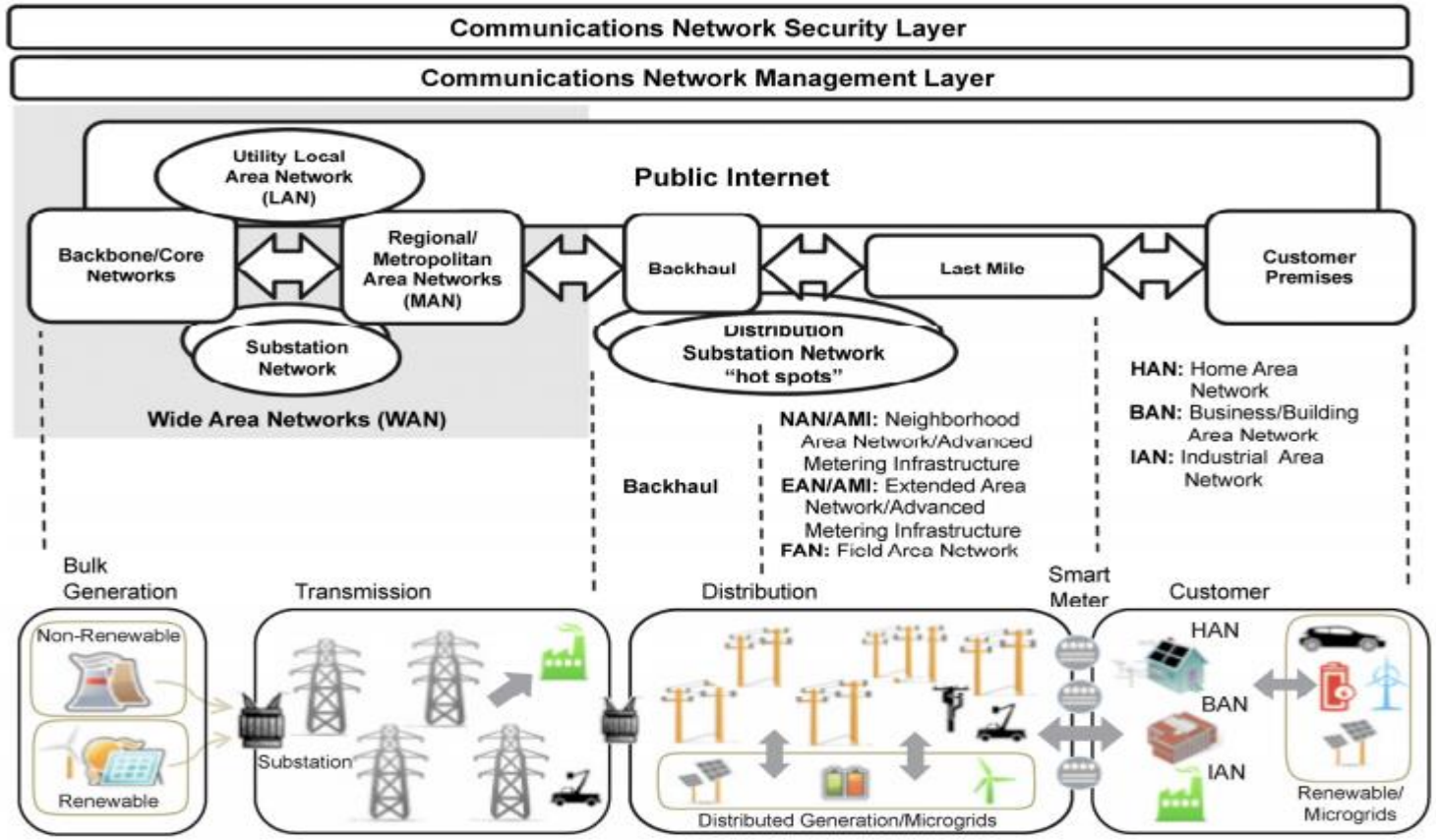
電機工程學系

大綱

- 前言
- 資通安全簡介
- 資通安全技術應用於智慧電網之挑戰
- 智慧電網資通安全標準發展現況
  - 標準規範制定機構
  - 智慧電網資通安全標準
    - ✓ NIST 7628
    - ✓ IETF RFC6272
    - ✓ NIST SP800-53
    - ✓ IEC 62351
- 展望與分析
- 結論

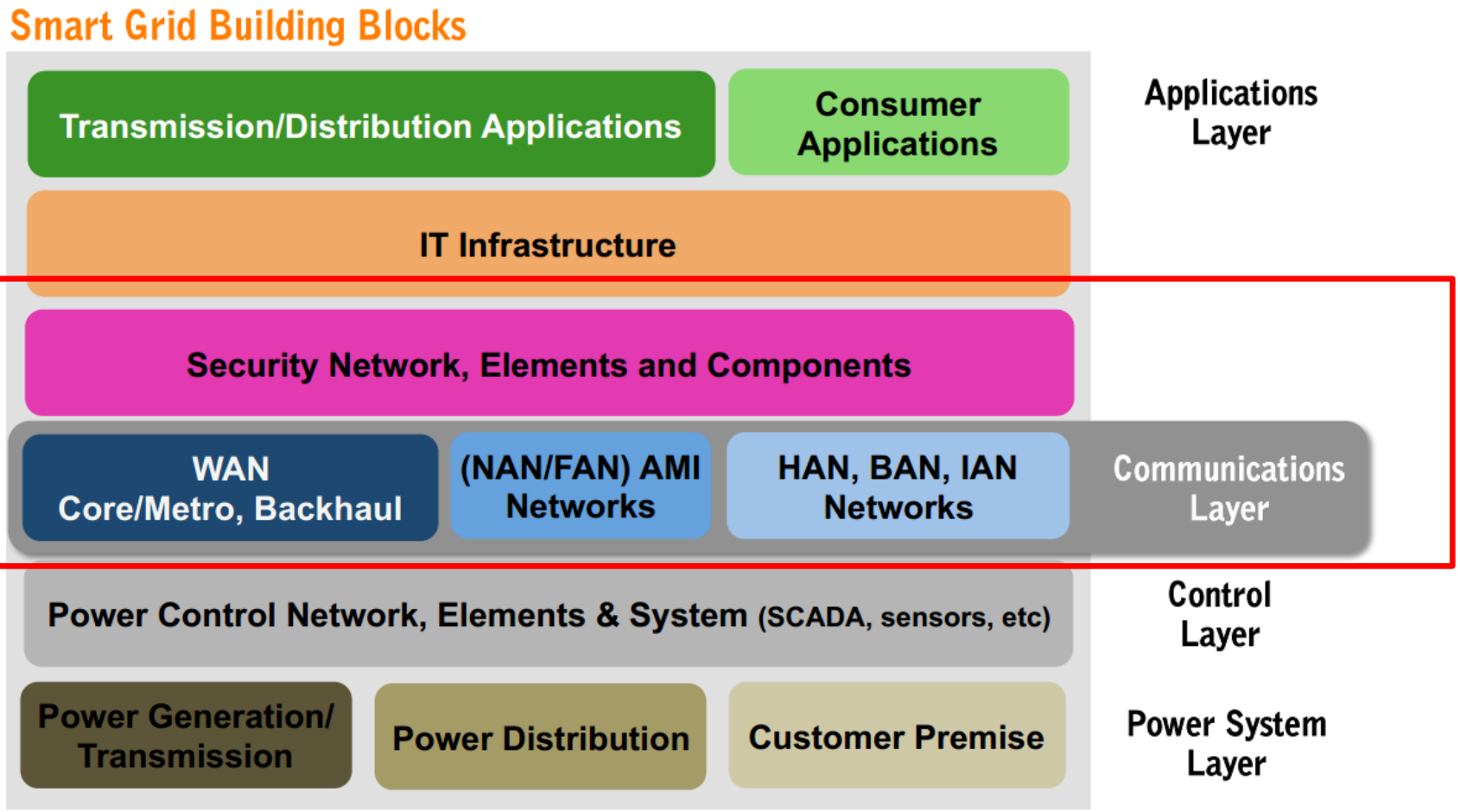
End-to-End Communication

- **The Key to Smart Grid Architecture**



Originated from IEEE 2030-2011

智慧 電網通訊 建構方塊


Smart Grid Building Blocks
Transmission/Distribution Applications
Consumer Applications
Applications Layer
IT Infrastructure
Security Network, Elements and Components
WAN Core/Metro, Backhaul
(NAN/FAN) AMI Networks
HAN, BAN, IAN Networks
Communications Layer
Power Control Network, Elements & System (SCADA, sensors, etc)
Control Layer
Power Generation/ Transmission
Power Distribution
Customer Premise
Power System Layer

資訊與網路安全

- 資安全必須確保

  保密性(Confidentiality)、

  完整性(Integrity) 、

  來源正確性/不可否認性

  (Authenticity/Non-repudiation)

  可用性(Availability)

- 於現有的通訊架構之下，已有諸多現行的標準與規範。

資訊與網路安全(2)

- **資通安全不僅需要解決蓄意攻擊，還要防範**
  - 來自心懷不滿的員工
  - 工業間諜活動
  - 恐怖分子
- **非故意的資訊基礎設施毀損**
  - 用戶不當操作使用之錯誤
  - 設備故障
  - 自然災害

資通安全技術相關規範

- 資通安全技術為智慧型電網建設重要的一環。
- 在智慧型電網互操作性標準計畫內之優先行動計劃中，被公認為極端重要的一個關鍵。
- 美國聯邦政府包括國土安全部(DHS)、能源部(DOE)和聯邦能源管制委員會都認為這些潛在智慧型電網中資通安全的弱點須要解決。

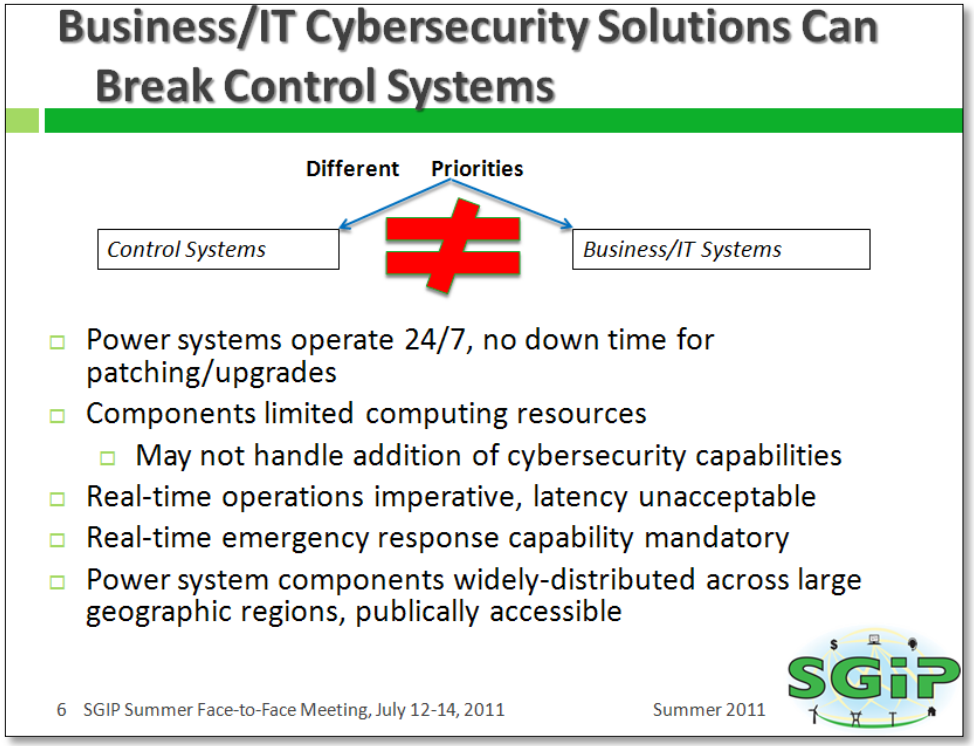
- 不要仰賴於私有協議來保護您的系統
- **"Do not rely on proprietary protocols to protect your system"**

"21 Steps to Improve Cyber Security of SCADA Network", U.S. Department of Energy

資通安全技術應用於智慧電網之挑戰

資訊安全於電力系統運作所面臨的挑戰

- **Threat of Denial-of-Service**
  - Dispatcher accessing power substation control
  - Customer accessing his bank account

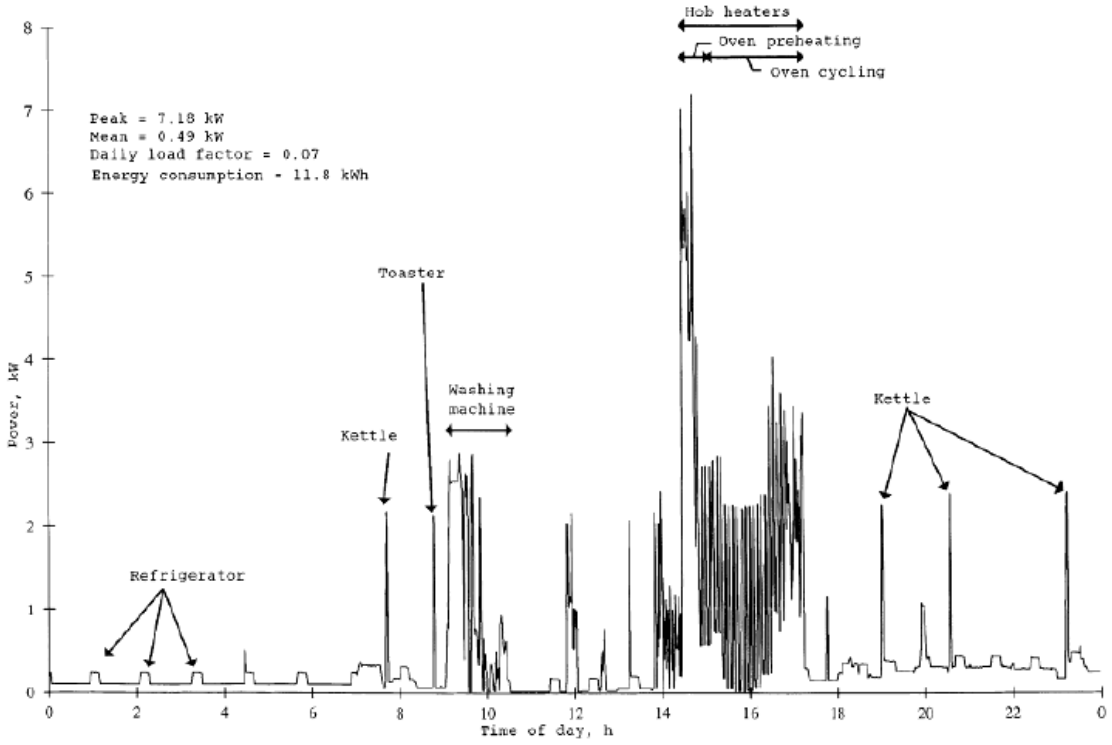


資訊安全於電力系統運作所面臨的挑戰

- **Limited Resources**
  - Narrowband communication
  - Not enough computation power
- **Geographical location**
  - Wide-spread, remote sites
  - Difficult to conduct /implement security measures
    - ✓Key managements, certificate revocation

隱私權的保障

- How often does a given customer eat microwave dinners as opposed to cooking three-pot meals?
- How many hours of TV does a resident watch? What kind of TV is it?
- When does a resident normally shower ?



Household Electricity Demand Profile Recorded on a One-minute Time Base[136]

資訊與網路安全技術應用於智慧電網之挑戰

- **智慧型電網**
  - 高複雜性
  - 眾多的利益相關者
  - 高時間敏感度和控制的需求。
- **資訊與網路安全管理之目標**
  - 已經有許多現有的、相關的安全標準、完善的評估程序以確定已知的系統脆弱性和漏洞
- **須依智慧型電網之特性**
  - 重新審視相關的安全標準
  - 並評估系統脆弱性和漏洞

智慧電網資通安全標準發展現況

智慧電網安全標準規範制定機構

- ANSI - American National Standards Institute
- CIGRE– International Council on Large Energy Systems
- FERC– Federal Energy Regulatory Commission
- IEEE– Institute of Electrical and Electronics Engineers
- IEC– International Electro-technical Commission
- IETF - Internet Engineering Task Force
- ISA – International Society of Automation
- ISO - International Organization for Standardization
- NERC - North American Electric Reliability Corporation
- NIST – National Institute of Standards and Technology
- PSRC–Power Systems Reliability Committee

國際電工委員會 IEC

- 國際電工委員會目前轄下共有175個技術委員會
- 技術委員會TC57，負責電力系統與其他相關系統資訊交換標準的發展

  包含有監控和資料擷取系統（Supervisor Control And Data Acquisition, SCADA）、

  能源管理系統、

  變電所自動化系統及遠端連線系統等。

- 技術委員會TC 57內部有多個工作小組，每個小組分別負責其領域的標準發展

組別	標準內容	標準制定
WG 3	遠端控制與連線安全標準	IEC 60870-5
WG 10	IED通訊與相關資料雛型	IEC 61850
WG 13	能源管理系統-應用服務介面	IEC 61970
WG 14	分散式管理系統-系統介面	IEC 61968
WG 15	資料交換與通訊安全標準	IEC 62351
WG 16	能源市場通訊相關標準	IEC 62325
WG 17	分散式能源來源的通訊系統	IEC 61850-7-420
WG 18	水力發電的通訊系統	IEC 61850-7-410
WG 19	長期TC 57之間標準的互通性	整合CIM 和 SCL的標準
WG 20	PLC系統規劃	IEC 60495, IEC 60663

美國國家技術標準局
National Institute of Standards and Technology (NIST)

- 美國能源獨立與安全法案的要求
- 為制定智慧型電網相關標準的主要協調機構
- **2009/4**

  公告與智慧型電網相關而待整合的16項技術標準

  確定若干的**資通安全**和**優先行動計劃**

  智慧型電網相關標準的三階段計畫
  - ✓ Phase 1 Roadmap and Smart Grid Release 1
  - ✓ Phase 2 Public-Private Partnership for Longer-Evolution
  - ✓ Phase 3 Testing and Certification Framework

  公開研討會(April, May, August)
  - ✓ 與廠商和利益團體、協調發展互操作性標準，並討論如何處理與標準相關的優先事項

現況

- 2014年4月 Open for Comments

  Draft 「 NIST Smart Grid Interoperability Standard Release 3.0」

  - ✓The number of implemented standards has increased from 37 to 74

- 2012年2月發佈智慧電網的互操作性標準「

  NIST Smart Grid Interoperability Standard Release 2.0」

  提出各項智慧電網基礎建設所必須依循的標準

  確定若干的資通安全和優先行動計劃

  智慧電網發展之依據及網路安全標準制定之準則

Critical Infrastructure

- SGIP Smart Grid Cybersecurity Committee
- 資通安全協調任務小組

  Cyber Security Coordination Task Group (CSCTG)

  整合並評估現有之資通安全規範

  隸屬美國國家技術標準局(NIST)

NIST
CYBER SECURITY WORKING GROUP

- **SMART GRID COLLABORATION WIKI**

資訊與網路安全相關規範

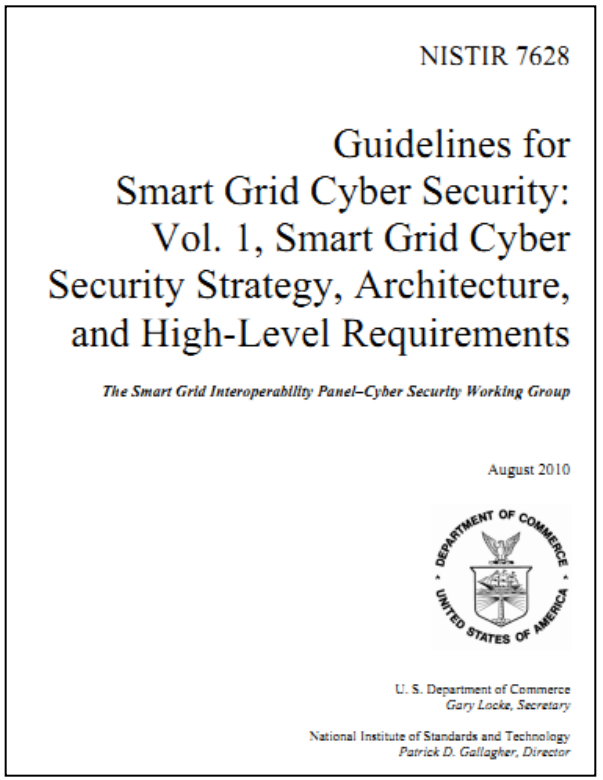
- Special Publication (SP) 800-39, DRAFT Managing Risk from Information Systems: An Organizational Perspective, NIST, April 2008;
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, NIST, March 2006;
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004;
- Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment, North American Electric Reliability Corporation (NERC), 2002;
- The National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency, Department of Homeland Security, 2009;
- The IT, Telecommunications, and Energy Sectors Sector-Specific Plans (SSPs), Initially Published in 2007 and Updated Annually;
- ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models, International Society of Automation (ISA), 2007
- ANSI/ISA-99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial an Industrial Automation and Control Systems Security Program
- **NISTIR 7628 Guidelines for Smart Grid Cyber Security**
- **IETF RFC 6272 Internet Protocols for the Smart Grid**

智慧電網資訊安全的必要條件

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Service Acquisition
- System and Communication Protection
- System and Information Integrity
- Program Management

NISTIR 7628

- NIST 制定了三大冊的規範
  - 第一冊
    - ✓驗證高層次的安全設備架構
    - ✓風險評估流程
    - ✓加密與金鑰管理技術
  - 第二冊
    - ✓用戶隱私問題
  - 第三冊
    - ✓自下而上進行安全性分析
    - ✓漏洞類別
    - ✓安全威脅
    - ✓互通性
    - ✓整體安全架構


NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

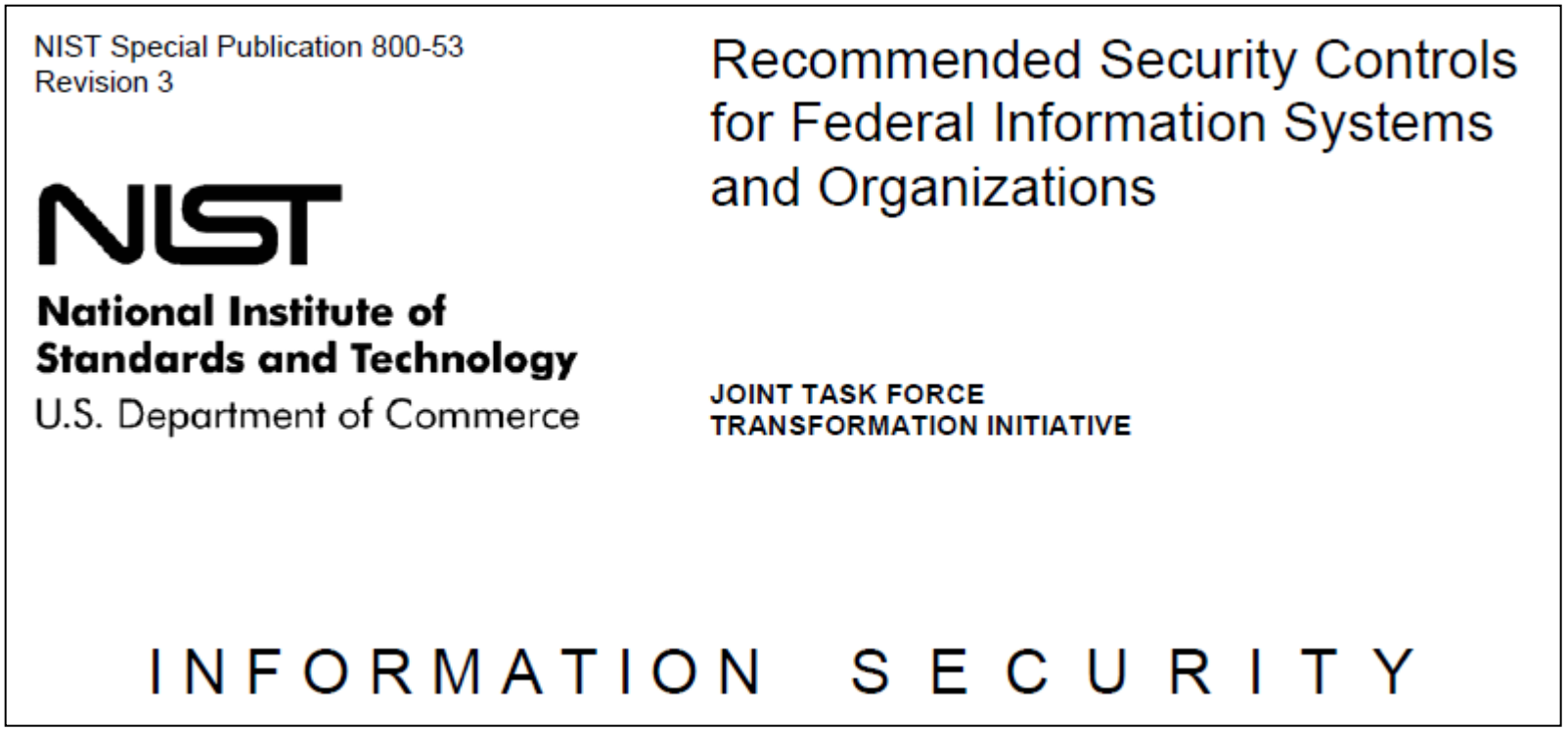
The Smart Grid Interoperability Panel–Cyber Security Working Group

August 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

NIST SP 800-53



NIST SP 800-53

- 用於發展電力系統時所參考的風險管理規範
- 美國聯邦資訊安全管理法案

(Federal Information Security Management Act, FISMA)

資訊系統風險管理評估流程

(Risk Management Framework)。

評估機制包含有六大步驟，藉由此機制，提高資訊系統的可靠度及安全性。

- ✓分類系統(Categorize)、安全控制選擇(Select)、
- ✓系統實現(Implement)、評估安全控制(Assess)、
- ✓授權資訊系統(Authorize)與監控系統(Monitor)，

RFC 6272

- **美國國家技術標準局**

  採用了網際網路協定(Internet Protocol Suite, IPS)為智慧電網眾多通訊協議中其中的一個規範

  - ✓唯一被廣範地運用於大規模網路架構中的標準

  RFC 6272已被智慧電網互操作性委員會納入25項標準之中

  組織並且匯集了

  - ✓相關徵求修正意見書(Request for Comments, RFC)
  - ✓適用於智慧電網的所有相關通訊協定
  - ✓並整合包括路由協定、網路安全以及智慧電網訊息交換行為等相關協定標準

IEC 61850

- **A popular standard for communication in Energy/Substation automation**
- **The successor of**
  - IEC60870-4-104
  - DNP3
- **Addressing**
  - Standardized data format/model
  - Interoperability of devices from different manufacturers

IEC 62351

- **智慧型電網倚賴資通訊技術**

  電力系統的管理、

  數據資料交換以及

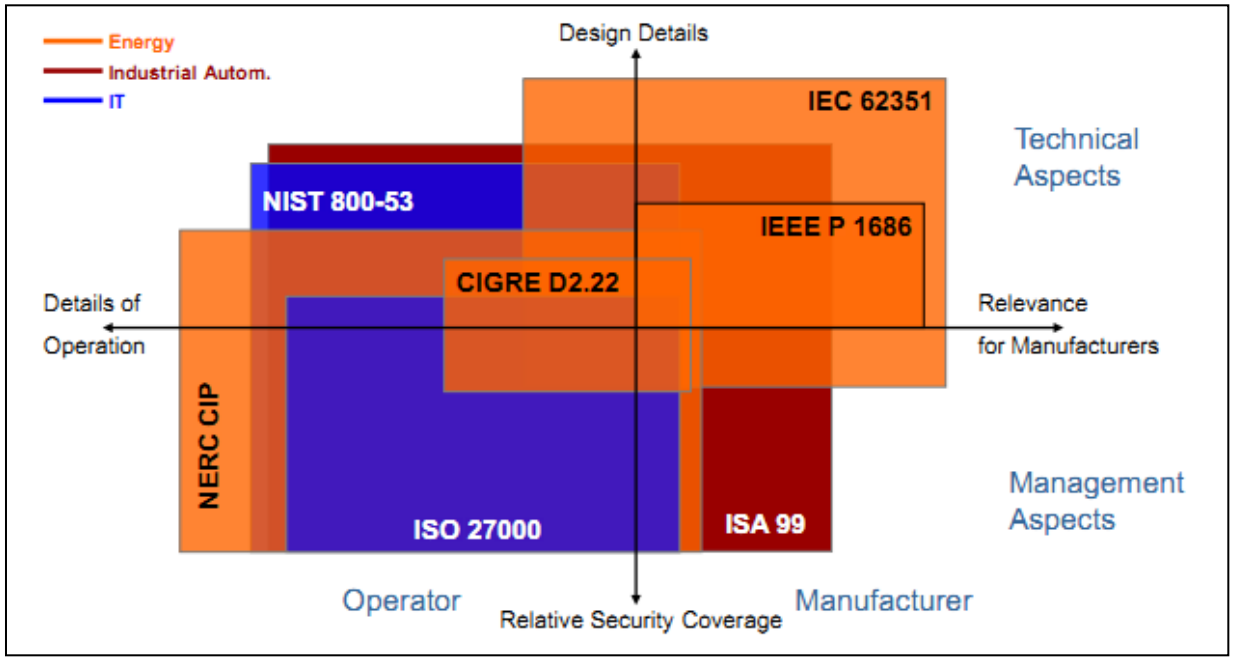
  通訊安全

- **IEC 62351主要是基於**

  IEC 61850、DNP3.0、IEC 60870-5、IEC 60870-6

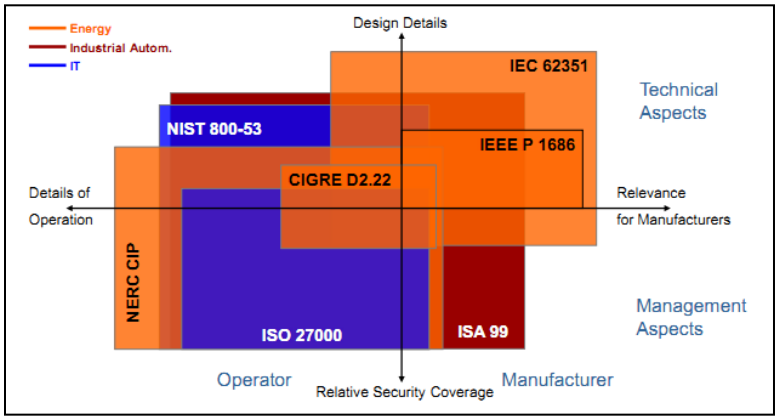
  四項通訊自動化標準所建立的**資通訊安全標準**。

分析與展望



- **IEC 62351**
  addresses the substation automation systems
- **ISA 99, IEEE P1686**
  directly address industrial automation systems.
- **NERC-CIP**
  generally for energy operators
- **ISO 27000, NIST 800-53**
  mainly targeted to IT environments
- **NIST SP800-82, NIST SP800-53**
  explicitly for industrial control systems

策略與風險評估



- **NIST 7628**

  資通訊安全策略評估流程圖

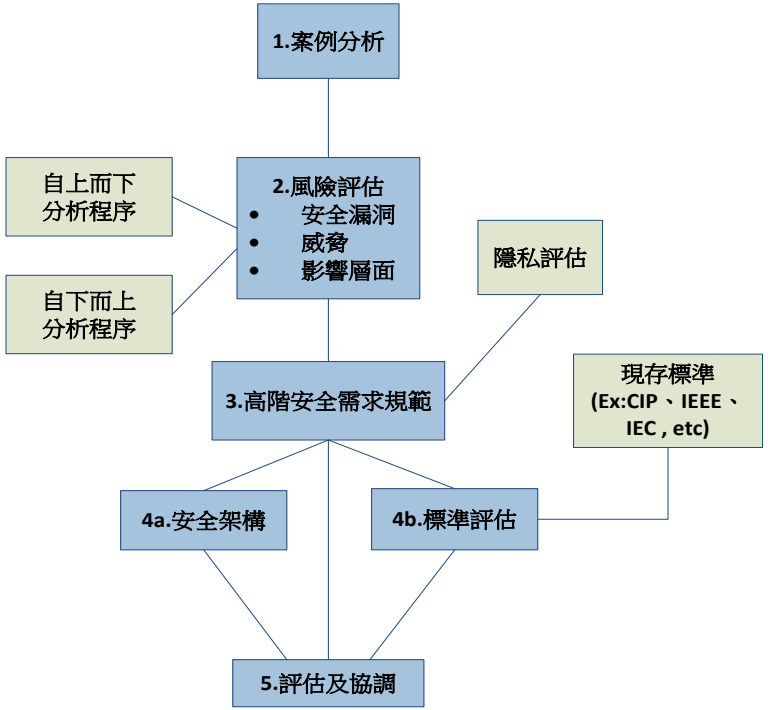
- **ISO-27001**

  明確的規範出必須要經由

  - ✓風險評估(Risk Assessment)、
  - ✓風險分析(Risk Analysis)，
  - ✓進而得知資訊功能的價值及其風險承受的脆弱度。

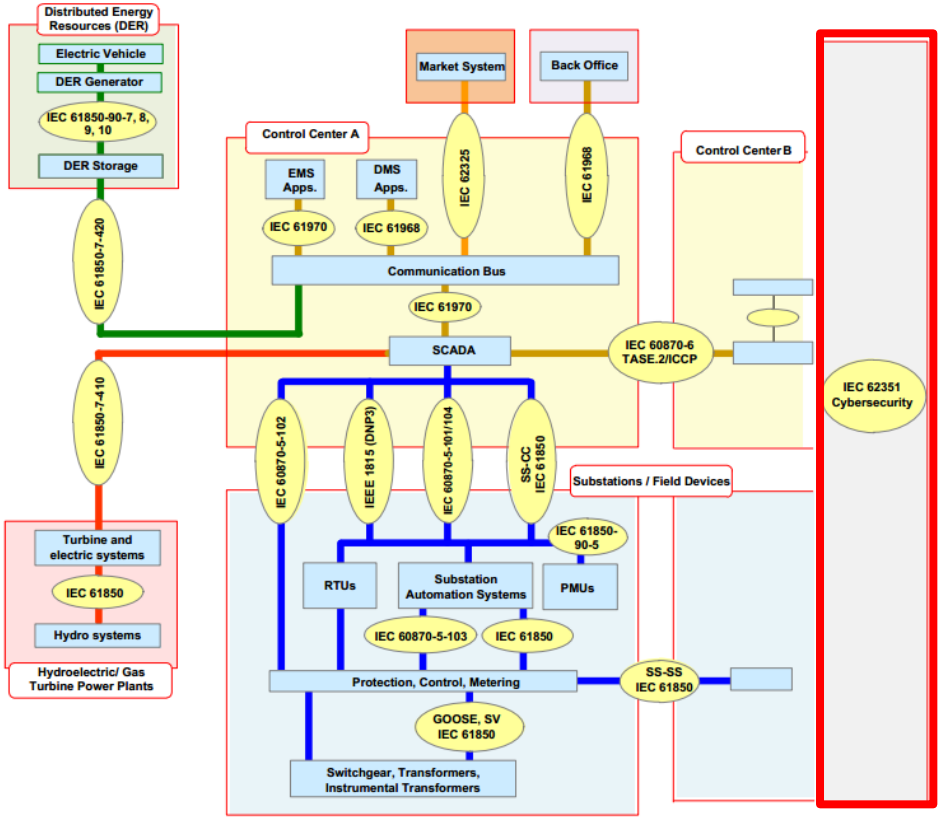
- **NERC CIP**

  高層次安全需求主要是依據北美電力可靠性公司的關鍵基礎設施保護標準

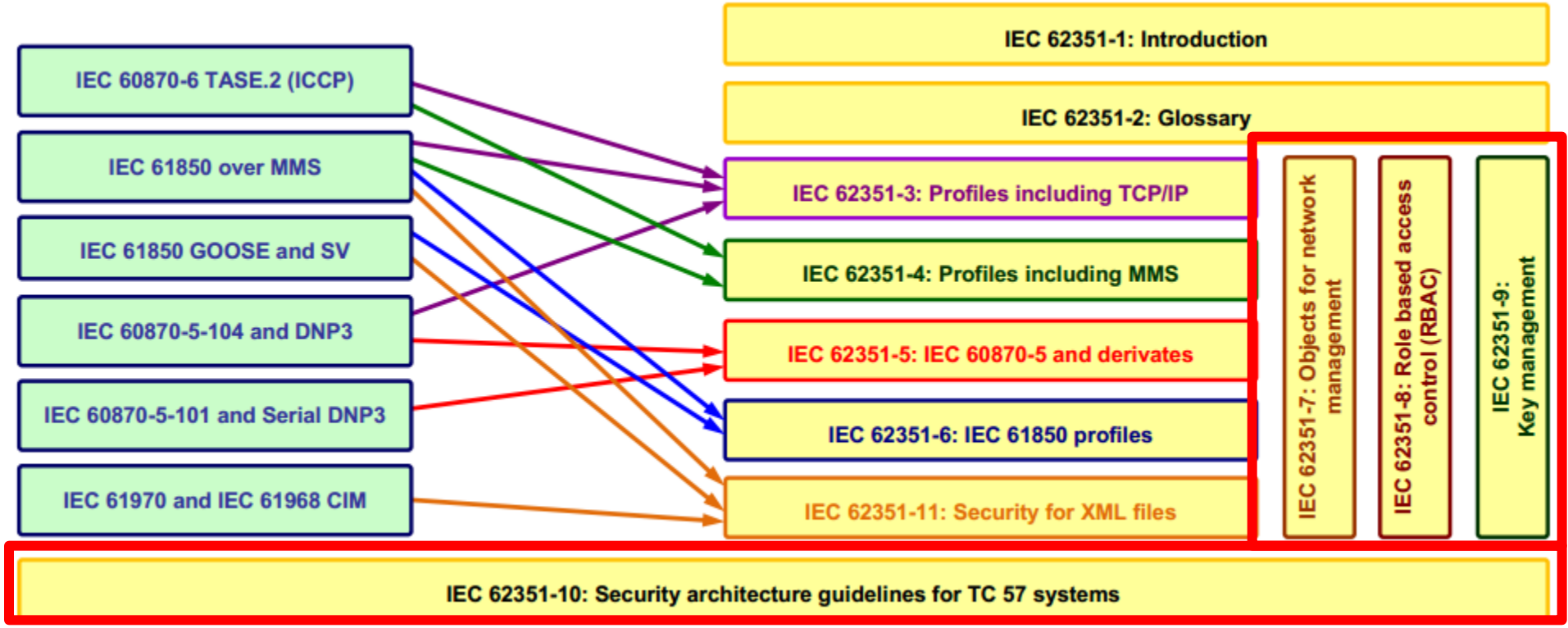


IEC 62351 Scope

- **Developed for different profiles of the three communication protocols:**
  - IEC 60870-6 (ICCP, TASE.2)
  - IEC 61850.
  - IEC 60870-5 and its derivatives
- **Security through network and system management**
- **One of the main focus areas of the IEC 62351 series is authentication**
- **The key to three of the four primary security threats: confidentiality, integrity, and non-repudiation.**



Mapping of IEC TC 57 Communication Standards to IEC 62351 Parts 7-11



Status of IEC 62351

(as of 2014-01-24)

IEC 62351 Part	Released	Activities (by November 2013)	Planned Release
IEC/TS 62351-1: Introduction to security issues	2007		
IEC/TS 62351-2: Glossary of terms	2008	Review Report pending	Pending
IEC/TS 62351-3: Security for profiles including TCP/IP	2007	Responses to Comments on CDV being developed	Submitted as CDV by Dec 2012, IS Ed. 2 by June 2014
IEC/TS 62351-4: Security for profiles including MMS	2007	Corrigenda submitted to IEC as an IEC Question to be sent to NCs	Resent Sept 2013 Waiting for response
IEC/TS 62351-5: Security for IEC 60870-5 and derivatives	2009	TS as Ed. 2	Released April 2013
IEC/TS 62351-6: Security for IEC 61850 profiles	2007	Updates underway, based on security requirements in IEC 61850-90-5	Update to Goose and SV as addendum by Dec 2013
IEC/TS 62351-7: Objects for Network Management	2010	An RR is being issued for developing Edition 2 as an IS	Wait for updates to be submitted to WG15
IEC/TS 62351-8: Role-Based Access Control	2011	Discussions on developing categories of roles	Planning IS in 2014/15
IEC/TS 62351-9: Key Management	Pending	CD issued August 2013; comments being reviewed	CDV in 2014 and IS in 2015
IEC/TR 62351-10: Security Architecture	2012	DTS sent to IEC	TR published Oct 2012
IEC/TS 62351-11: Security for XML Files	Pending	NWIP – initially rejected due to lack of sufficient NC support, but additional NCs have joined	CD 9/2013, CDV 3/2014, FDIS 3/2015, IS 7/2015
PWI: Resiliency and Security for DER	NWIP Pending		
PWI: Conformance Testing for IEC 62351	NWIP Pending		

IEC 62351-3
Profiles including TCP/IP

- **The purpose of IEC 62351-3 is to provide end-to-end transport security for the communications between software applications.**
- **Security profiles including TCP/IP on the following standards:**

  IEC 60870-6 (TASE.2 / ICCP)

  IEC 60870-5 Part 104

  IEEE 1815 (DNP 3) over TCP/IP

  IEC 61850 over TCP/IP

IEC 62351-3 Mandatory Requirements (excerpt)

- **5.1 Deprecation of non-encrypting cipher suites**

  Any cipher suite that specifies NULL for encryption shall not be used.

- **5.2 Negotiation of versions**

  Only TLS 1.0 corresponding to SSL version 3.1 (or higher) shall be allowable.

- **5.5.4.6 Key exchange**

  The key exchange algorithms shall support a maximum size of at least 1024 bits for the key.

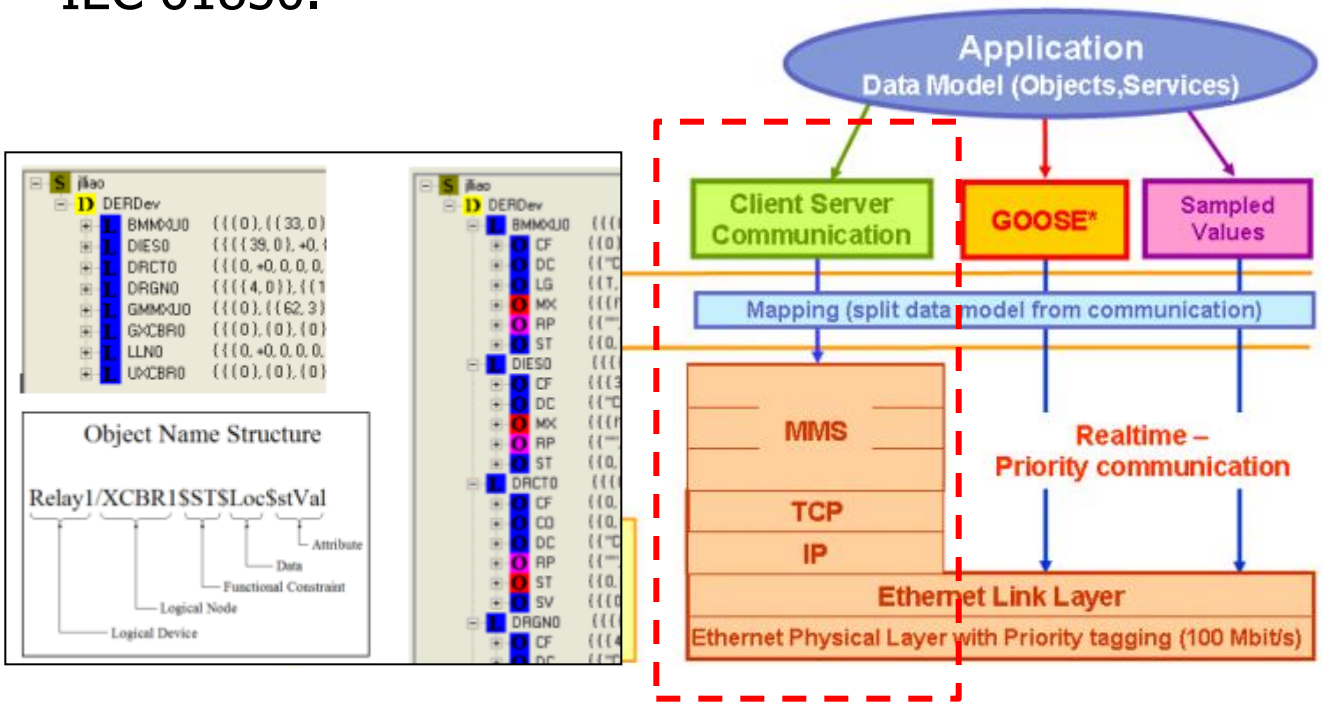
  Both RSA and Diffe-Hellman mechanisms shall be supported.

IEC-52351-4
Security for profiles that include MMS

- **Manufacturing Message Specification (MMS), including**

  IEC 60870-6 TASE.2 (ICCP) and

  IEC 61850.



IEC 62351-4 Mandatory Requirements (excerpt)

- 6 T-Profile security
- 6.1.6.5 Mandatory and recommended cipher suites

  All implementations that claim conformance to this specification shall support **TLS_DH_DSS_WITH_AES_256_SHA** at a minimum.

Key Exchange		Encryption	Hash	Support		
Algorithm	Signature			Interoperable	Export restriction	Supported
TLS_RSA_		WITH_RC4_128_	SHA	o	C1	
TLS_RSA_		WITH_3DES_EDE_CBC_	SHA	o	C1	
TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA	o	C1	
TLS_DH_	RSA_	WITH_3DES_EDE_CBC_	SHA	o	C1	
TLS_DHE_	DSS_	WITH_3DES_EDE_CBC_	SHA	o	C1	
TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA	o	C1	
TLS_DH_	DSS_	WITH_AES_128_	SHA	o	C1	
TLS_DH_	DSS_	WITH_AES_256_	SHA	o	C1	
TLS_DH_		WITH_AES_128_	SHA	o	C1	
TLS_DH_		WITH_AES_256_	SHA	m	C1,C2	

IEC-52351-5
Core Technical Specifications

- **The serial version**
  - only support low bit rates or
  - field equipment that is compute-constrained
- **Simple authentication mechanisms**
- **The authentication mechanism is based on two concepts:**
  - a challenge and response protocol
  - the concept of a keyed-hash message authentication code (HMAC)
- **This challenge-reply mechanism using an HMAC is a "unilateral, two-pass authentication" mechanism as described in ISO/IEC 9798-4.**

IEC 62351-6

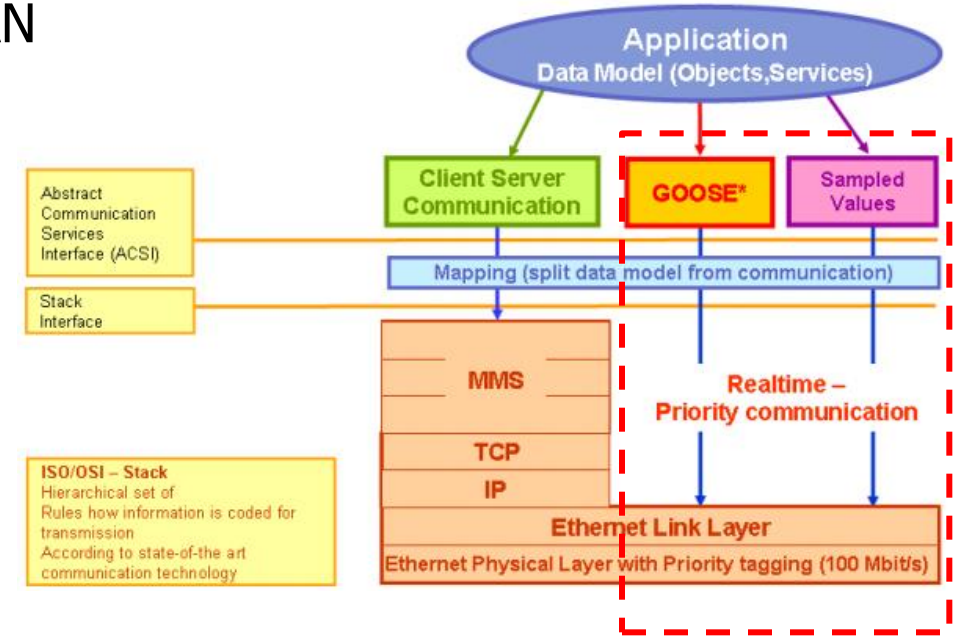
Security for IEC 61850 Peer-to-Peer Profiles

- **Sample Values & GOOSE**
- **Protocols**

  peer-to-peer multicast datagrams

  on a substation LAN

  none routable



IEC 62351-8 Role-Based Access Control for Power System Management

- **The access control of users and automated agents to data object in power systems**

  by means of role-based access control (RBAC).

- **RBAC enables an organization to separate super-user capabilities**
- **Package them into special user accounts termed roles**
- **Assign to specific individuals according to their job needs.**

傳輸層安全（TLS）

- 在各標準中被廣泛地提及，藉由傳輸層安全來讓通訊雙方相互認證，並以數位簽章和加密系統來提供通訊雙方能夠互相認證的安全機制。
- 在通訊雙方通過身分認證後，雙方會協商要採用的
  - 簽章方式、
  - 加密方式以及
  - 雜湊演算法和
  - 對稱金鑰
- 在協商後傳送端便開始將訊息分段，再以雙方協商的加密演算法、雜湊檢查碼進行處理後將訊息送出，
- 接收端再收到訊息後，便開始將訊息解密、驗證、以及訊息重組，提供訊息完整性與保密性的安全要求。

IEC 62351-9
Key Management

- **Specifies how to**
  - Generate
  - Distribute
  - Revoke and handle
    - ✓ digital certificates
    - ✓ cryptographic keys
- **Handling of**
  - asymmetric keys (private keys and X.509 certificates)
  - symmetric keys (pre-shared keys and session keys)

公開金鑰基礎建設

- 實現具有成本效益與安全性的智慧電網
- 使用PKI技術，可以讓分散在各地不同區域數以百萬計以上的電力設備與安全連線，減少對稱密鑰的數量
- 以更有效率的方式來進行

  跨域憑證更新、撤銷、新增密鑰等管理

公開金鑰基礎建設 (2)

- **NISTIR 7628 提出了使用公開金鑰基礎建設密鑰管理的議題與相關注意要點**

  設備的計算能力、傳輸頻寬、加密演算法等考量與限制。

- **在實現準則方面包含**

  信託管理，憑證策略定義、憑證是否撤銷、有效期限及憑證狀態資訊。

  並保證憑證的互通性，使其可被不同的機構所使用。

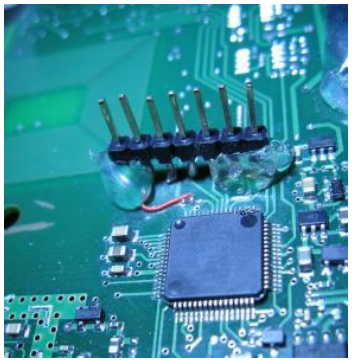
智慧電網系統對於PKI的獨特需求

- 安全性(Safety)
- 高可用性(High Availability)
- 即時處理(Real-Time Operation)
- 向下相容(Legacy Support)
- 可擴充性(Scalability)
- 可升級性(Upgradeability)
- 政策強制執行(Policy Enforcement)
- 靈活性(Flexibility)
- 互操作性(Interoperability)
- 可整合現有架構(Existing Structure Integration)
- 虛擬邊界(Virtual Borders)
- 有規律的命名規則(Naming Convention)
- 支援外部設備(External Equipment)

•Todd Baumeister, Adapting PKI for the Smart Grid, Cyber and Physical Security and Privacy (IEEE SmartGridComm) 2011

Conclusions

- Many Existing Proposals & Solutions
- Many Challenges
- How can we make sure it's safe & secure?



rdist.root.org/category/hardware/

Researchers discover flaws in smart meters

Hackers could turn a person's power on or off, jack up their bills

JORDAN ROBERTSON, Associated Press
Posted March 31, 2010 at midnight

Q & A