Using Architecture to Guide Cybersecurity Improvements for the Smart Grid

Elizabeth Sisley, Ph.D.

Agenda

- Context
  - US Smart Grid
  - 7 Domains
  - Logical Reference Model
- Cybersecurity requirements
  - Confidentiality, Integrity, Availability (CIA)
  - Logical Interface Categories
- Risk-ranked User's Guide Process
  - Architecture's role

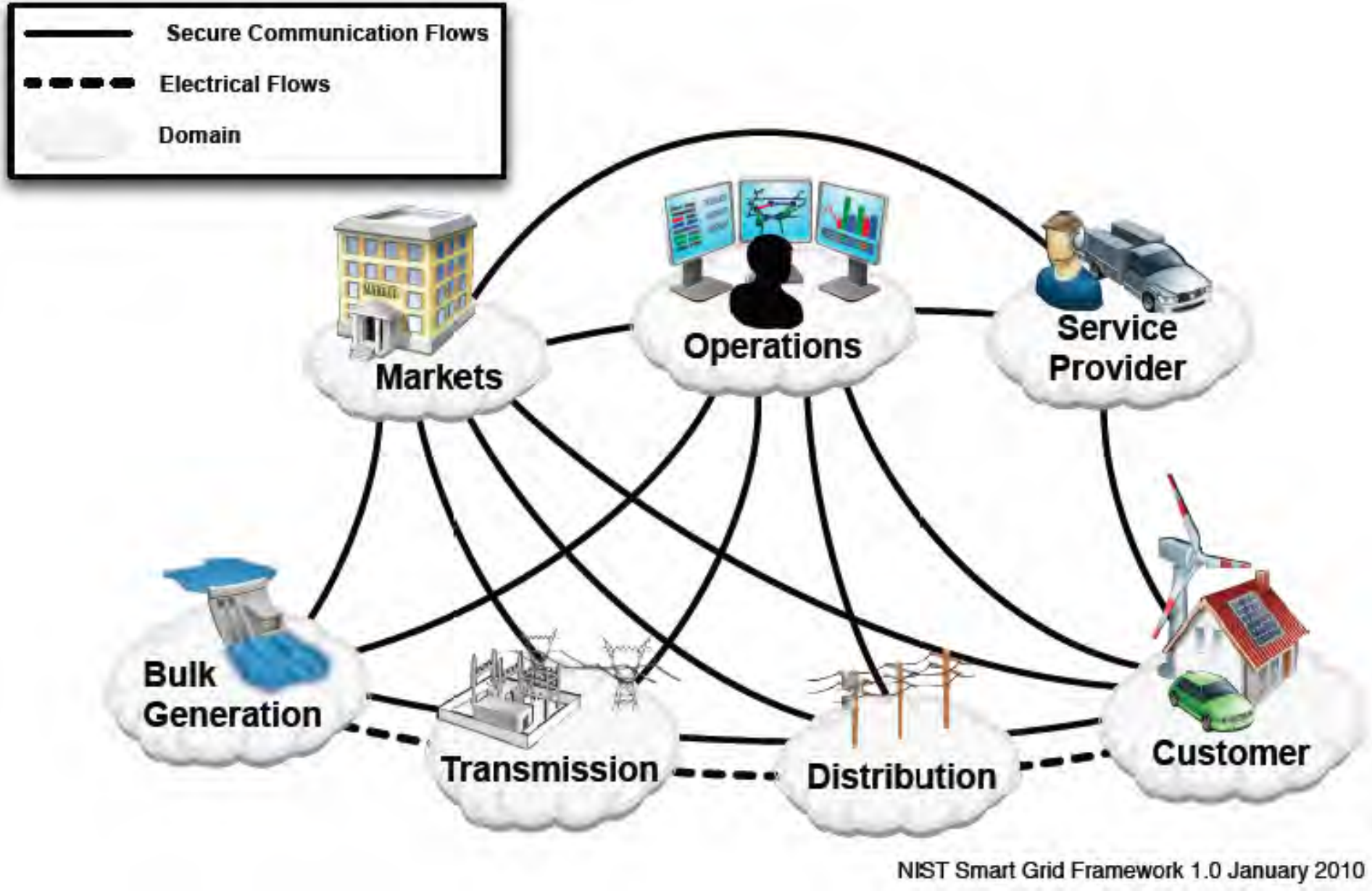
Hypothesis: Architecture-based cybersecurity improvement process can help in other industries, too.

Sources

- Smart Grid Cybersecurity Committee (formerly Cyber Security Working Group)
  - NISTIR 7628 *Guidelines for Smart Grid Cyber Security*, August 2010 (3 volumes)
    - *csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf*
  - Logical Reference Model
    - SGCC Architecture sub-team
  - *NISTIR 7628 User's Guide* (30+ pages)
    - SGCC User's Guide sub-team
    - **Draft:** *collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628UsersGuide*

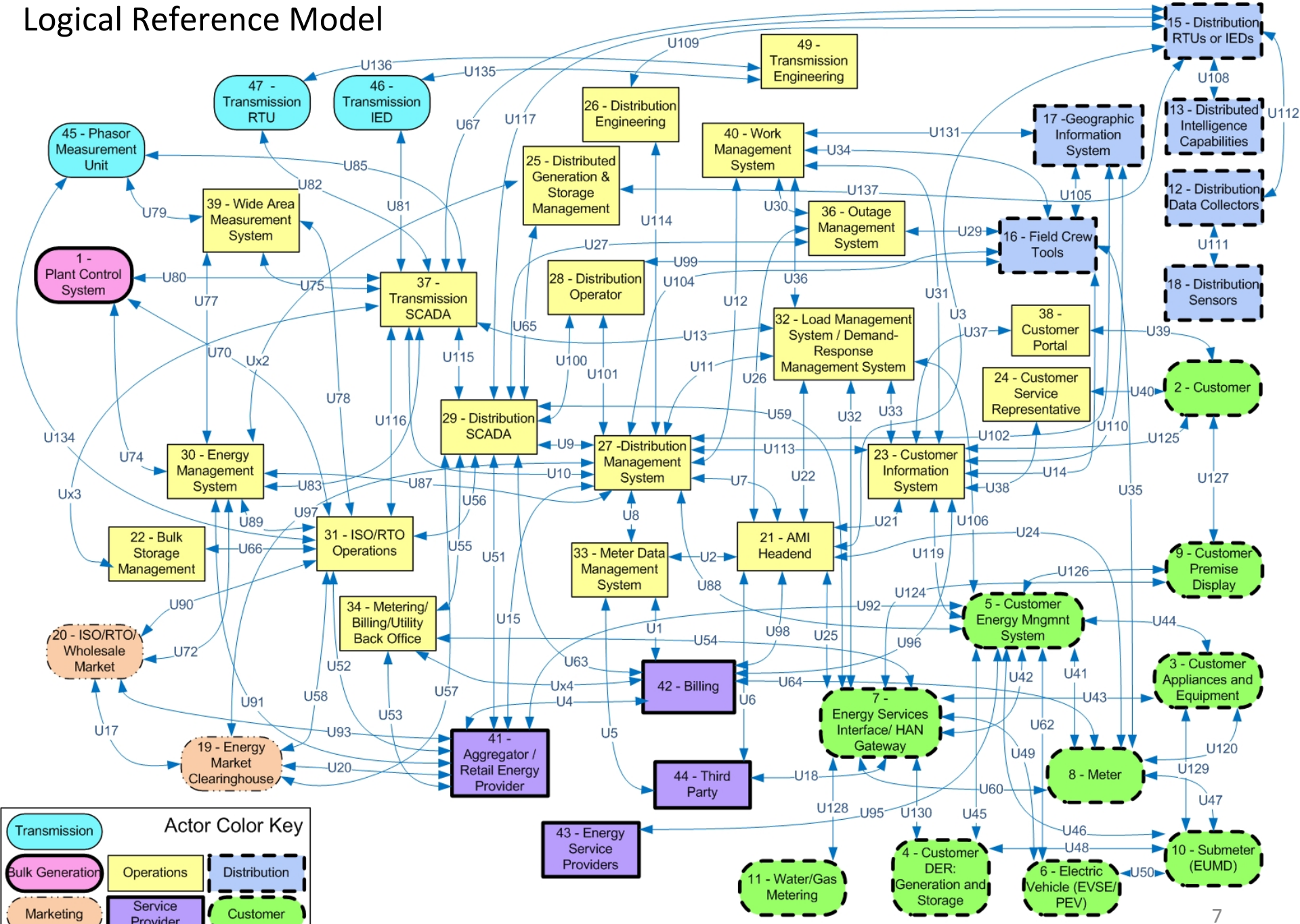
US Smart Grid

- A complex system-of-systems
  - Real-time control systems in power grid
    - Some mechanical automation, some computerized
  - Transforming into an advanced, digital infrastructure
    - Adding two-way capabilities for communicating information, controlling equipment, and distributing energy
  - This transformation adds Cybersecurity requirements



NIST Smart Grid Framework 1.0 January 2010

Logical Reference Model



Source: NISTIR 7628

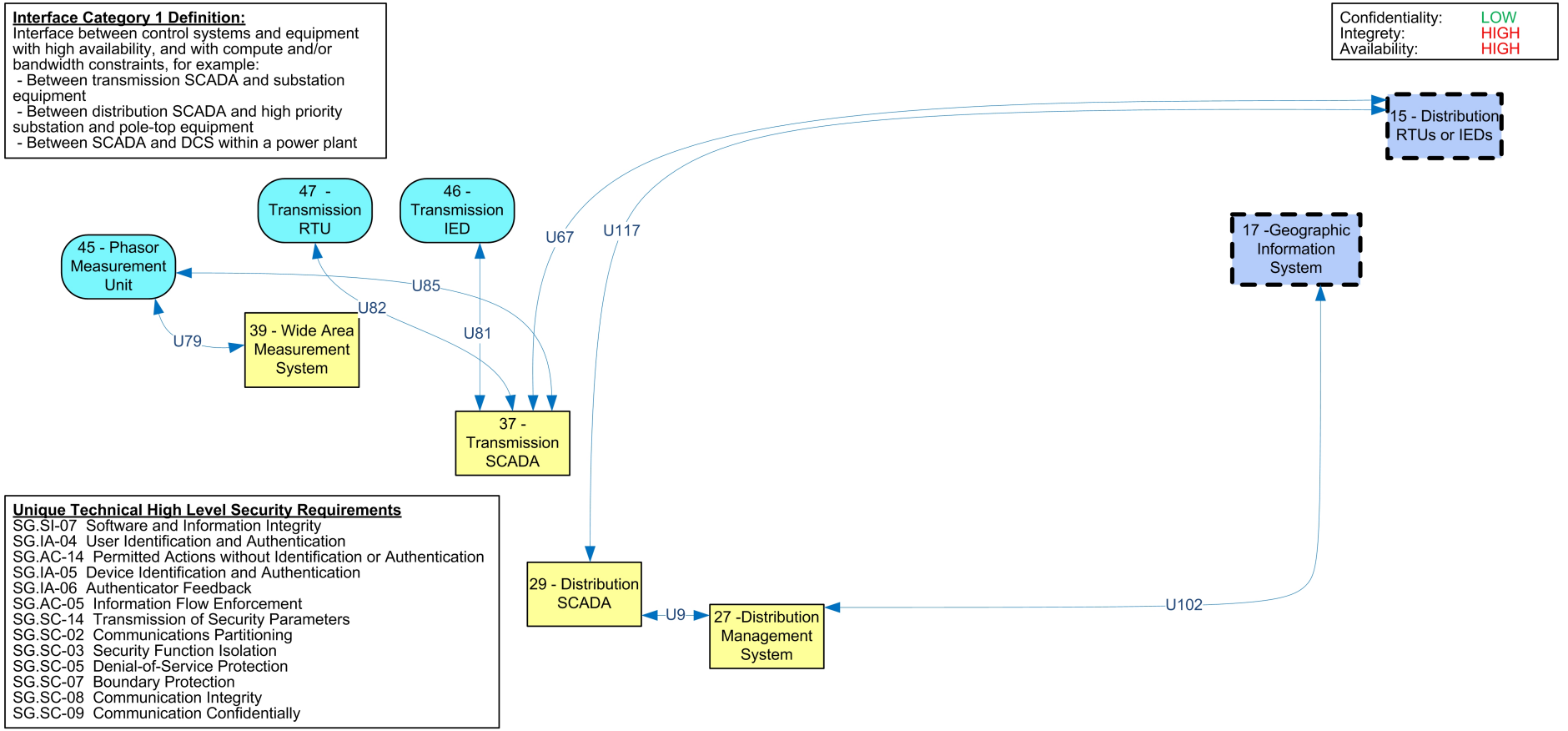
Cybersecurity Requirements

- Availability (most important)
  - Hard and soft real time
    - Wide-area situational awareness monitoring, etc.
- Integrity
  - Demand Response (DR) data used to drive energy generation
  - Stuxnet masked unauthorized operations from being detected by the operators
- Confidentiality
  - Privacy of customer information
  - Electric market information
  - General corporate information
    - Payroll, internal strategic planning, etc.

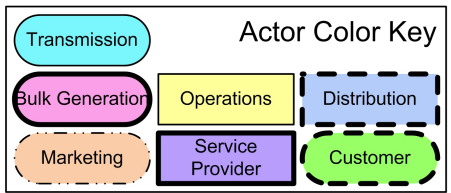
Security Requirements

- 19 Categories are documented
  - Each category has a number of specific requirements

IDs	Category
SG.AC-1, 21	Access Control
SG.AT-1, 7	Awareness and Training
SG.AU-1, 16	Audit and Accountability
…	
SG.IR-1, 11	Incident Response



Example of Actors, Interfaces, CIA, and HL Security Requirements: *LIC1 Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints*



Source: NISTIR 7628 **Figure 2-4 Logical Interface Category 1**

Logical Interface Categories

- NISTIR 7628 has 22 categories
  - For example: *Interface between control systems and equipment* has 4 categories:

	Computation and/or Bandwidth	
	Constrained	**Unconstrained**
High availability	LIC 1	LIC 3
Low availability	LIC 2	LIC 4

- Analyze interfaces to understand variations, categorize them

User's Guide Process

1. Identify Smart Grid Organizational Business Functions
2. Identify Smart Grid Mission and Business processes for the Prioritized Organizational Business Functions
3. Identify Systems and Assets that support the Mission and Business Processes
4. Map Systems to Logical Interface Categories
5. Identify High-Level Security Requirements
6. Perform a Smart Grid High-Level Security Requirement Gap Analysis
7. Create a Plan to Remediate the Gaps and Implement the Necessary High-Level Security Requirements
8. Monitor and maintain High-Level Security Requirements

Map Systems to Logical Interface Categories

- Actor refers to the Logical Reference Model systems, which needs to be validated for a specific organization
  - *"Are we missing something, do we do something differently? Why?"*
- Logical Interfaces also need to be validated
- Categories are then specified

Priority Business Function(s)	Business Processes	System Name(s)	Prioritization			Actor(s)	Logical Interfaces	Logical Interface Category(s)
			Impact (H, M, L)	Probability (H, M, L)	Risk Ranking			
Metering to Cash	d. Advanced Metering Infrastructure (AMI)	AMI Meters	High	High	High	8	U24 U64 U35 U41 U47 U80 U120	18 18 17 18 18 6 15
		AMI Head- End	High	Medium	High	21	U24	18
		MDMS	High	Medium	High	33	U2	7
		Billing Sys	High	Medium	High	42	U64	18

High-Level Security Requirements

- HL Security Requirements are mapped to LICs
  - Variation exists, so organizations still need to review and verify applicability
  - Requirements are evaluated as High, Medium, Low

Table 3-3 Allocation of Security Requirements to Logical Interface Catgories

Dark Gray = Unique Technical Requirement Light Gray = Common Technical Requirement
White = Common Governance, Risk and Compliance (GRC)

Smart Grid Requirement Number	Logical Interface Categories																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.AC-1	Applies at all impact levels																					
SG.AC-2	Applies at all impact levels																					
SG.AC-3	Applies at all impact levels																					
SG.AC-4	Applies at all impact levels																					
SG.AC-6	Applies at moderate and high impact levels																					
SG.AC-12							H	H									L				L	H
SG.AC-13																	M		M			
SG.AC-14	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H
SG.AC-15																				H	H	H

Identify HL Security Requirements

- For each prioritized system/asset:
  - Verify your organization's CIA levels from the NISTIR 7628
  - Document the security requirements

Table 7 System Inventory with CIA Impacts, Unique Technical Requirements, and Requirement Enhancements

System Name(s)	Risk Prioritization: Impact (H, M, L) C	I	A	Probability (H,M,L)	Risk Ranking (H,N,L)	Actor(s)	Logical Interfaces	Logical Interface Category(s)	NISTIR CIA Impact C	I	A	FINAL CIA C	I	A	GRC Req. for each system	Common Technical Req. for each system	Unique Technical Requirements for each Logical Interface Category	All Unique Technical Reqs for each system (including enhancements)[8]
AMI Meters	H	H	H	H	H	8	U24	18	L	H	L				SG.AC-1 SG.AC-2 SG.AC-3	SG.AC-6 SG.AC-7 SG.AC-8	SG.AC-14 SG.IA-4 SG.SC-3	SG.AC-12 SG.AC-13 SG.AC-14 (1)

Gap Analysis

- Verify that each system/asset's HLRs are addressed
  - Each Rating is either S=*Satisfied* or O=*Other*
  - Each Gap needs to be addressed by a Mitigation, such as *Audit Log* or *Penetration Test*

Table 8 System Inventory with Assessment Scores, Assessment Gaps, and Proposed Mitigations

System Name(s)		GRC Req. for each system	Common Technical Req. for each sys	Unique Technical Requirements for each Logical Interface Category	All Unique Technical Reqs for each system (including enhancements)	Assessment Ratings (S or O)	Assessment Gaps	Mitigations
AMI Meters	…	SG.AC-1 SG.AC-2 SG.AC-3 SG.AC-4 … … …	SG.AC-6 SG.AC-7 SG.AC-8 SG.AC-9 … … …	SG.AC-14 SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8	SG.AC-14 (1) SG.IA-4 SG.SC-3 SG.SC-5 SG.SC-6 SG.SC-7 SG.SC-8			

Applications in Other Industries

- The 7628 User's Guide documents an easy-to-understand process in 30+ pages
  - Your business processes will differ
  - Your systems and assets will differ
  - Your Interface Categories will differ
  - The process still works

Thanks and Contacts

Many thanks to the User's Guide sub-team!

Contacts:

- SGIP 2.0 website: sgip.org
- Marianne Swanson, NIST
  - SGIP *Smart Grid Cybersecurity Committee (SGCC)* Chair
- Mark Ellison, DTE Energy
  - *SGCC NISTIR 7628 User's Guide* sub-team lead
- Elizabeth Sisley
  - *SGCC Architecture* sub-team lead
  - sisley@cs.umn.edu