Applying Model Based Systems Engineering approach to Smart Grid Software Systems Security Requirements

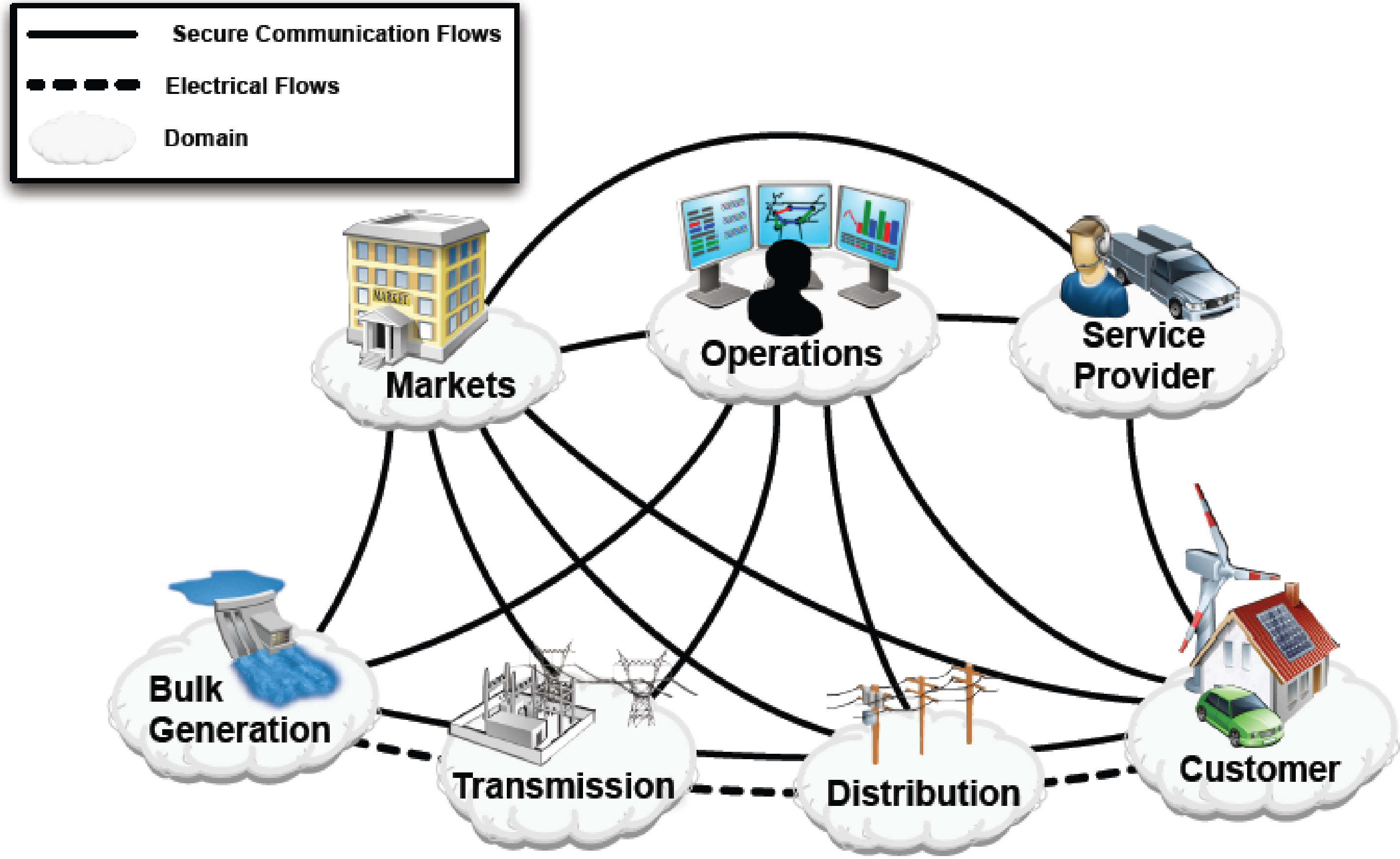
Authors: Sitaraman Lakshminarayanan
& Manyphay Souvannarnarth

Presented by: Kristin Kelly
July 9, 2012

Overview

- Smart Grid overview
- Smart Grid Systems & Security
- Smart Grid logical interfaces from NIST IR 7628
- System Analysis
- Incorporating Security Analysis with Systems Engineering process
- Summary

Smart Grid Overview

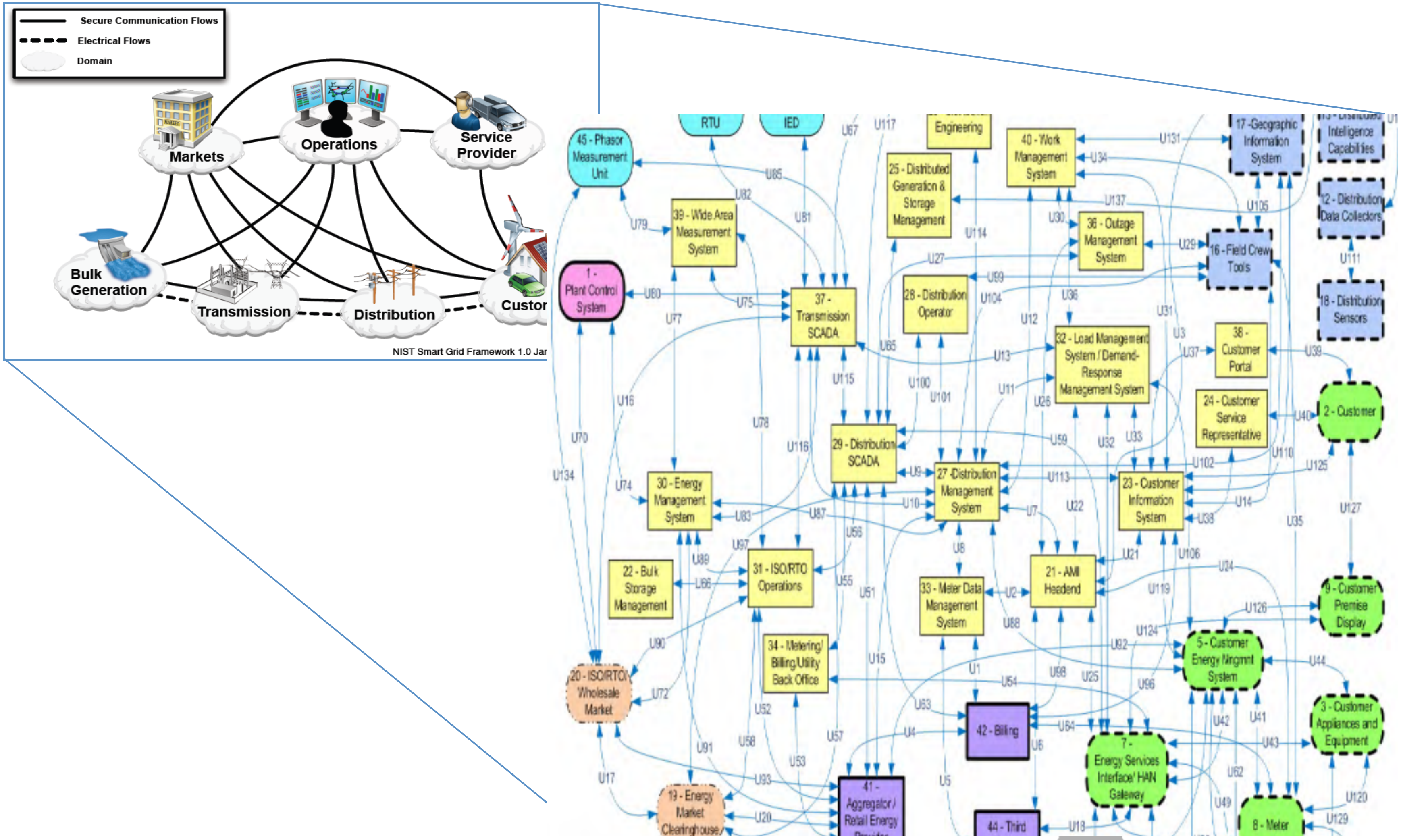


NIST Smart Grid Framework 1.0 January 2010

Smart Grid Systems & Security

- Conceptually Security is Simple.
  - Confidentiality , Integrity, Availability
    - Authentication, Authorization, Encryption, Digital Signature, etc.
- Smart Grid System comprises of
  - Sub systems that interfaces across Various logical and physical boundaries
  - Sub Systems & Components deployed in the field, customer premise, control center, etc.
  - Various vendors involved for any given Sub System or System (HW, SW, Communication network, etc.)

Logical Interfaces from NIST IR 7628


Secure Communication Flows
Electrical Flows
Domain
Markets
Operations
Service Provider
Bulk Generation
Transmission
Distribution
Custor
NIST Smart Grid Framework 1.0 Jar
RTU
IED
Engineering
45 - Phasor Measurement Unit
39 - Wide Area Measurement System
25 - Distributed Generation & Storage Management
40 - Work Management System
17 - Geographic Information System
Intelligence Capabilities
12 - Distribution Data Collectors
36 - Outage Management System
16 - Field Crew Tools
18 - Distribution Sensors
1 - Plant Control System
37 - Transmission SCADA
28 - Distribution Operator
32 - Load Management System / Demand-Response Management System
38 - Customer Portal
24 - Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 - Distribution Management System
23 - Customer Information System
30 - Energy Management System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
9 - Customer Premise Display
34 - Metering/ Billing/Utility Back Office
5 - Customer Energy Mngmt System
20 - ISO/RTO Wholesale Market
42 - Billing
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
19 - Energy Market Clearinghouse
41 - Aggregator / Retail Energy Provider
44 - Third
8 - Meter

Security Overview

Challenges

- As seen on logical interface diagram, almost every component or sub system is integrated with another.
- Security vulnerability/weakness in one part of the system could cause potential damage to Grid reliability.
- Various Industry & Regulatory Standards (NIST, IEC, ISA, NERC, etc.)
  - Not enough technical details to facilitate Implementations across components, Sub Systems and Interfaces.

Impacts

- Outages = unhappy customers/Consumers
- Reliability = additional fees for Utilities

Model Based Systems Engineering Approach to Security Engineering

- Provides a method for tracing security standards to system requirements
- First level of filter to extract applicable standard needs
- Security requirements can be decomposed to various level of detail for multiple iteration systems engineering
- Security requirement objects are reusable for similar projects in the same industry and security class

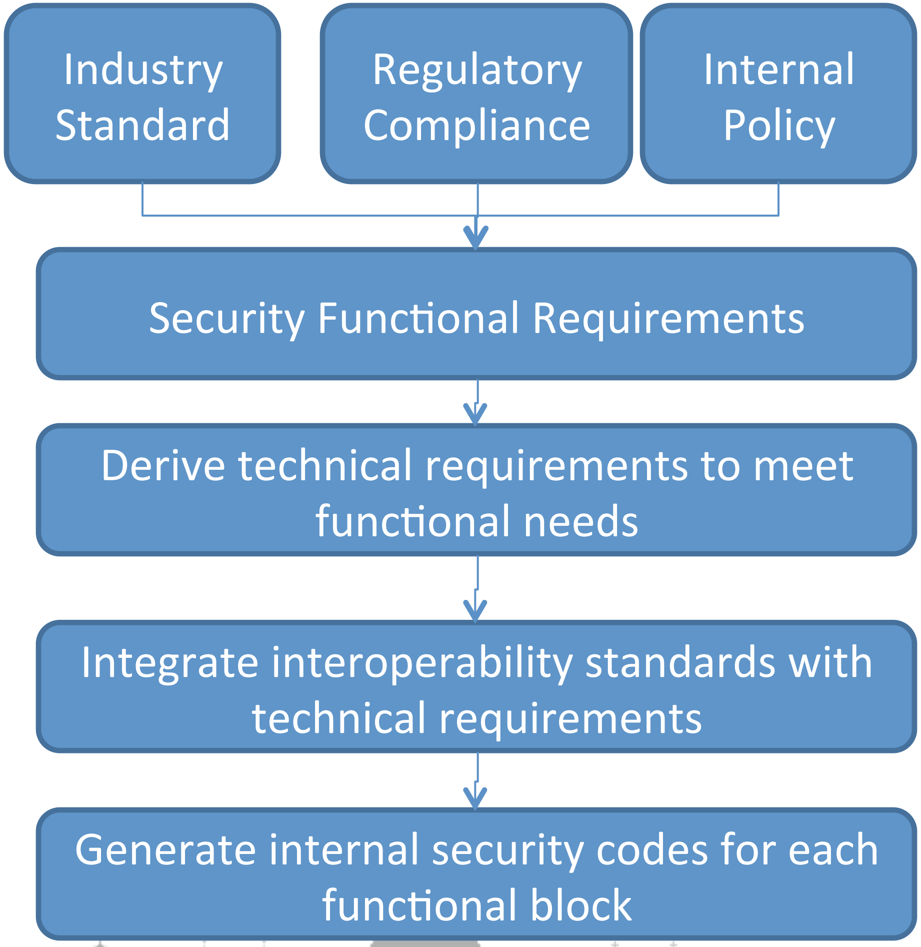
Process

1. Build out the Security Functional Requirements
2. Classify Security Requirements into classes (Authentication, Authorization, Encryption, Digital Signature, etc.)
3. During project Functional Analysis, associate Security Requirement class objects with System Functions
4. Query the model to extract all Security Requirements as needed

Step 1. Build out of Security Functional Requirements

- Security requirements come from multiple sources (Industry Standards, Regulatory Agencies, Internal Corporate Standards)
- Derive security requirements to fill gaps
- Derive interoperability security requirements

Security Code Analysis:



Industry Standard

Regulatory Compliance

Internal Policy

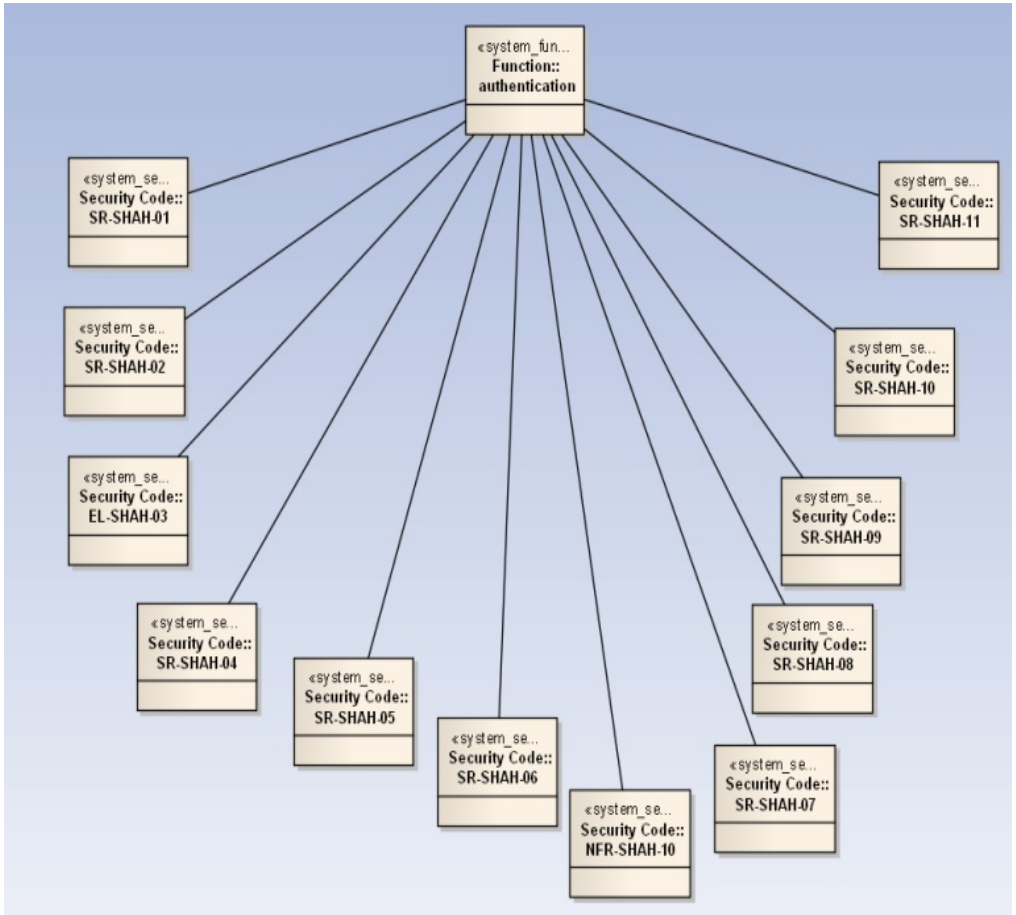
Security Functional Requirements

Derive technical requirements to meet functional needs

Integrate interoperability standards with technical requirements

Generate internal security codes for each functional block

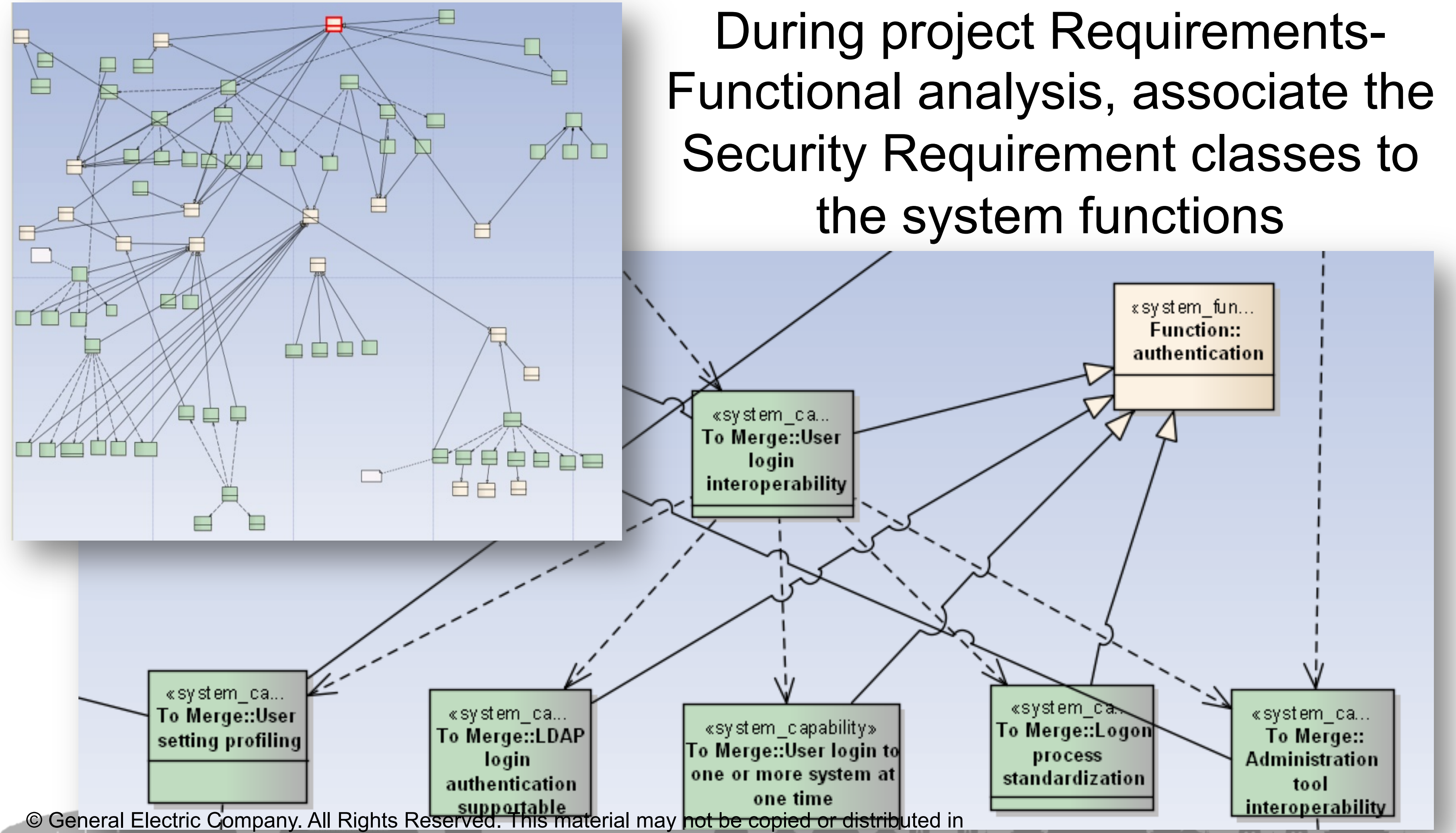
Step 2. Classify Security Requirements into classes



- Create high level security classes
- Associate appropriate Security Requirements to the classes
- Continue to build out and draw associations as new security requirements as added to model

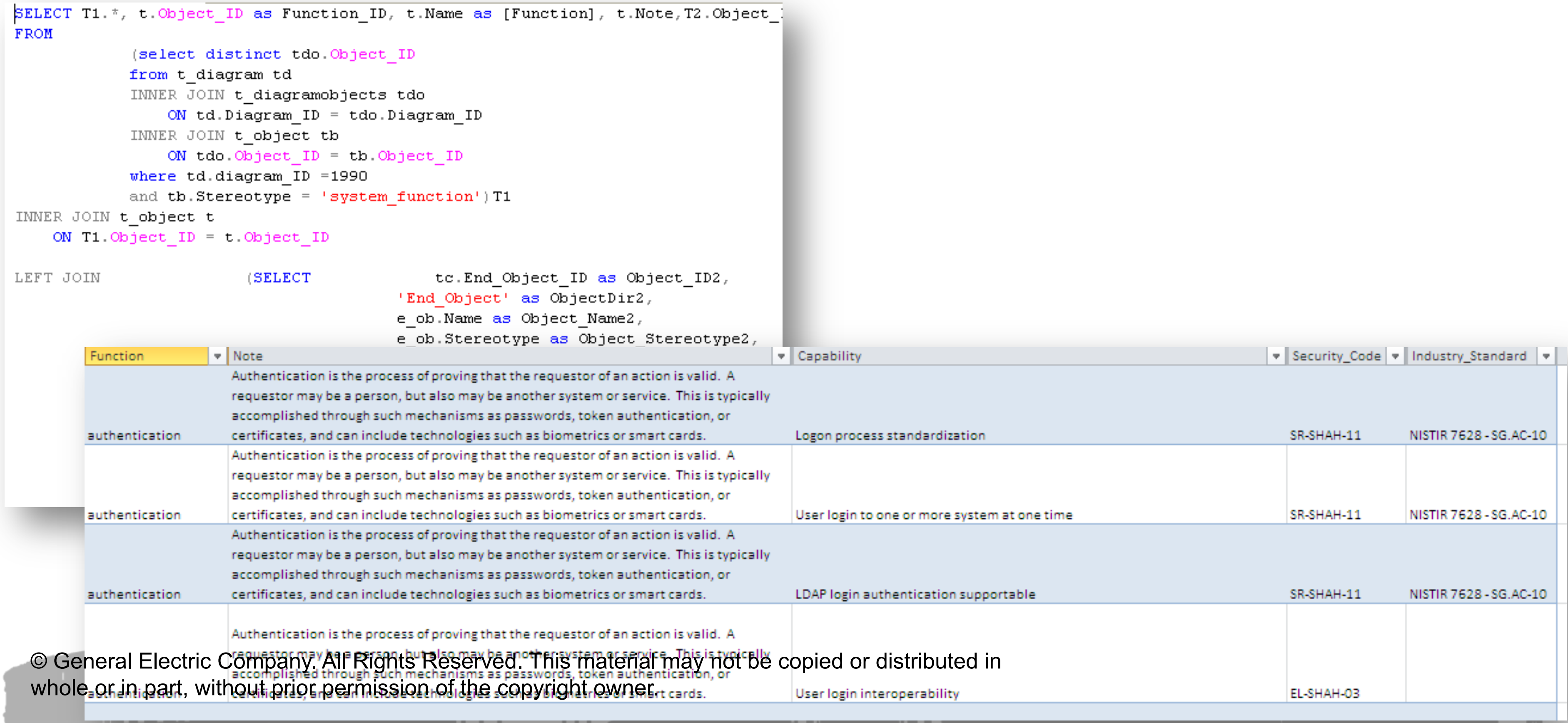
Step 3. Associate Security Requirement class objects with System Functions

During project Requirements-Functional analysis, associate the Security Requirement classes to the system functions



Step 4. Query the model

- Database modeling systems allow for custom queries
- Query all applicable Security Requirements by Function, Security Class, Project, etc.



```
SELECT T1.*, t.Object_ID as Function_ID, t.Name as [Function], t.Note,T2.Object_
FROM
            (select distinct tdo.Object_ID
            from t_diagram td
            INNER JOIN t_diagramobjects tdo
                ON td.Diagram_ID = tdo.Diagram_ID
            INNER JOIN t_object tb
                ON tdo.Object_ID = tb.Object_ID
            where td.diagram_ID =1990
            and tb.Stereotype = 'system_function')T1
INNER JOIN t_object t
    ON T1.Object_ID = t.Object_ID

LEFT JOIN                (SELECT             tc.End_Object_ID as Object_ID2,
                                         'End_Object' as ObjectDir2,
                                         e_ob.Name as Object_Name2,
                                         e_ob.Stereotype as Object_Stereotype2,
```

Function	Note	Capability	Security_Code	Industry_Standard
authentication	Authentication is the process of proving that the requestor of an action is valid. A requestor may be a person, but also may be another system or service. This is typically accomplished through such mechanisms as passwords, token authentication, or certificates, and can include technologies such as biometrics or smart cards.	Logon process standardization	SR-SHAH-11	NISTIR 7628 - SG.AC-10
authentication	Authentication is the process of proving that the requestor of an action is valid. A requestor may be a person, but also may be another system or service. This is typically accomplished through such mechanisms as passwords, token authentication, or certificates, and can include technologies such as biometrics or smart cards.	User login to one or more system at one time	SR-SHAH-11	NISTIR 7628 - SG.AC-10
authentication	Authentication is the process of proving that the requestor of an action is valid. A requestor may be a person, but also may be another system or service. This is typically accomplished through such mechanisms as passwords, token authentication, or certificates, and can include technologies such as biometrics or smart cards.	LDAP login authentication supportable	SR-SHAH-11	NISTIR 7628 - SG.AC-10
authentication	Authentication is the process of proving that the requestor of an action is valid. A requestor may be a person, but also may be another system or service. This is typically accomplished through such mechanisms as passwords, token authentication, or certificates, and can include technologies such as biometrics or smart cards.	User login interoperability	EL-SHAH-03	

Conclusions

- Construction of a security model – incorporate standards, regulation and policy
- Incorporate the security model with project model of interest
- Traceability enable searchable platform to identify project requirements to industry standards to security requirements

Questions

Sitaraman Lakshminarayanan

- Security Architect, Systems Engineering, GE Energy, Atlanta, GA
- Email: S.Lakshminarayanan@ge.com

Manyphay Souvannarnarth

- Senior Systems Engineer, Systems Engineering, GE Energy, Atlanta, GA
- Email: Manyphay.Souvannarath@ge.com