AMI-SEC Task Force

April 2008 Face-to-Face Meeting

→*System Security Requirements*
→*System Security Design*

Darren Reece Highfill, CISSP

EnerNex Corporation

darren@enernex.com

Agenda

0800-0900 Welcome and Orientation

0900-0945 System Security Requirements

- – Status update

1000-1100 Industry Perspectives

- – EdF
- – SDEX

1100-1130 Solving Complex Problems (SEI)

1130-1145 SSD Priming Discussion

1230-1345 System Security Design

1345-1400 Planning and Logistics

Definition

- Source: FERC Survey on DR

"AMI is defined as the communications hardware and software and associated system and data management software that creates a network between advanced meters and utility business systems and which allows collection and distribution of information to customers and other parties such as competitive retail providers, in addition to providing it to the utility itself."

Scope

For the purposes of the AMI-SEC TF, the scope of effort may be further defined as:

1. The hardware and software residing in, on, or closest to the customer premise for which the utility or its legal proxies are primarily responsible for proper operation.

2. The hardware and software owned and operated by the utility or its legal proxies which has as its primary purpose the facilitation of Advanced Metering.

Scope – Points of Interface

While many systems within the utility or customer premise may change or be impacted by the implementation of AMI, this Task Force shall limit the scope of its recommendations to the points of interface between the AMI and these affected systems. Informative-only special guidance may be provided relevant to affected systems if the Task Force deems the impact significant enough that such guidance is warranted.

System Development Life Cycle

- Initiation
- Development or Acquisition
- Implementation
- Operation and Maintenance
- Decommissioning

} **Current AMI-SEC Deliverables**

What should we provide for the other phases?

Roadmap Outline

1. Starting conditions and assumptions

2. Key project objectives

3. Description of long-term strategy, first-phase tactics, and reasoning for selection of each

4. Milestones, critical decision points, and associated decision-driving criteria

5. Important technological or business developments

6. Defined endpoint and success criteria

2008 Deliverables – Process Review
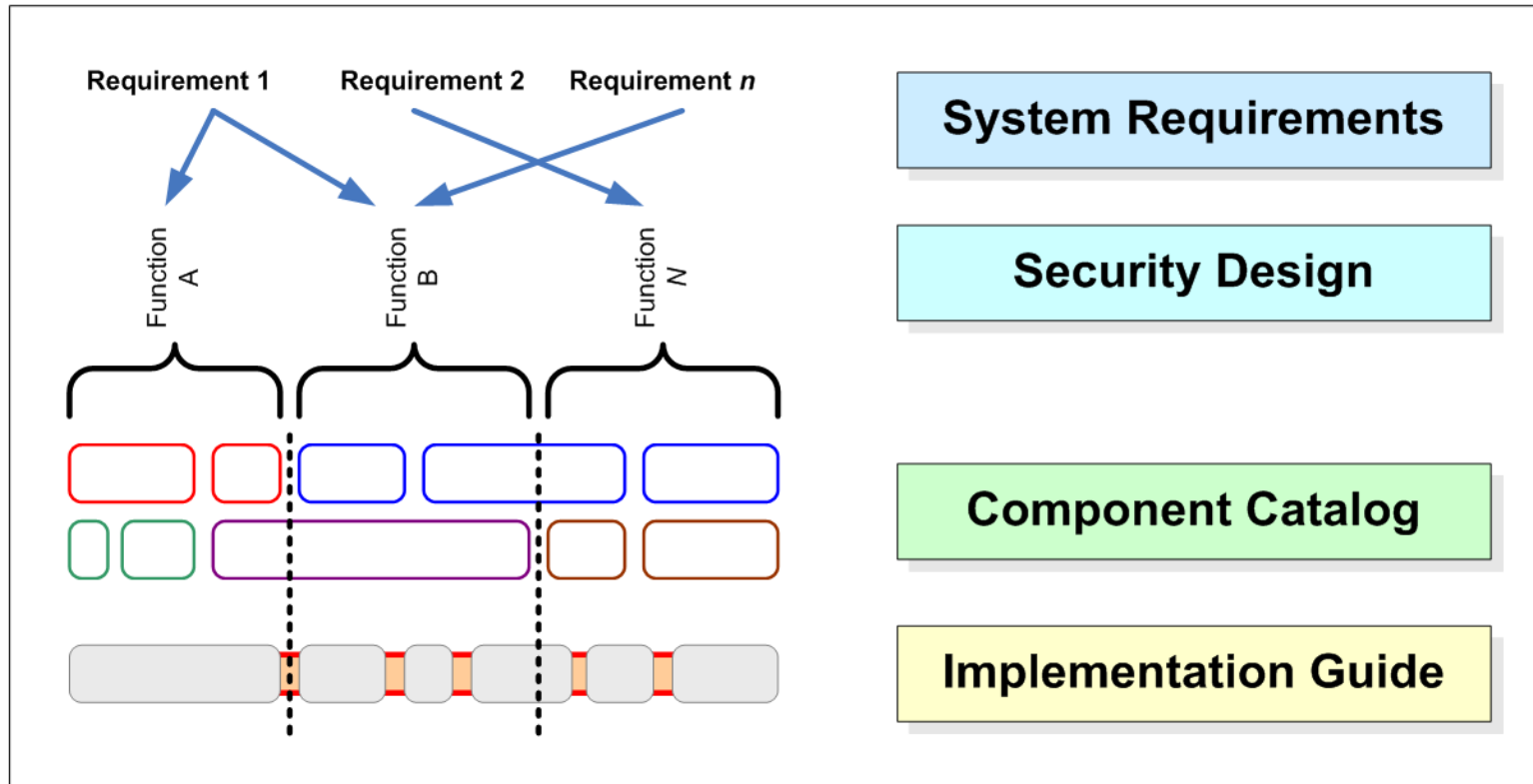
System Security Requirements

- System Security Requirements Document v0.3.doc
- AMI-SEC Requirements v0.1.xls

System Security Design

- Objectives and goals
  - Describe the abstract (logical, platform-agnostic) mitigation plan for addressing requirements identified in the Risk Assessment / System Requirements Document.

- Approach
  - Architectural Representation of Security Systems
  - Logical Function Descriptions
  - System, Subsystem, and Function Boundaries

- Reference: IEEE 1471-2000

Action Items

- Roadmap:
  - Contributions / Draft
- TF Scope:
  - Present to UtilityAMI?
- Requirements:
  - ASAP team augmenting
  - Review and comment
- System Security Design
  - Composition

- Next meeting dates
  - F2F
    - June 23-25
    - N'awlins (Entergy)
  - Teleconferences:
    - April 30th, 1-3pm EDT
    - May 14th, 1-3pm EDT
    - May 28th
    - June 11th

AMI Security Acceleration Project

- Collaborative opportunity open to utilities
  - Now supported by EPRI
    - POC: Erfan Ibrahim (eibrahim@epri.com)
  - DOE matching original private sector funds ($400K) 1 for 1
    - INL, ORNL, SEI

- AMI-SEC is key stakeholder
  - Can provide input through current meetings

- Deliverables provided back to AMI-SEC

ASAP Deliverables

- Produce content and drafts of AMI-SEC deliverables
  - Supplement SSR suitable for use in RFP

- Testing & Analysis
  - Analysis Roadmap: evaluation of AMI system / component security features
  - Technical Analysis of first-level reconnaissance
  - Documentation of AMI solutions testing at EPRI Living Lab
  - Metrics for evaluating solutions against Implementation Guide

- Recommendations
  - Enhancements to AMI security architecture
  - Survivability in the context of the SDLC