F2F SF 3.8.11 Session 1

Agenda:

1. Tuesday:
   a. IEC TC57 WG 15
   b. Usability Analysis TF
   c. SG Sec/Net Joint Session
2. Wednesday:
   a. CyberSec Interop
   b. ASAP SG- WAMPAC SP
   c. Embedded Systems Security TF
   d. SG Sec/Open ADR Joint Session
   e. Planning and Prioritzation

Updates:

3. New task force created - Embedded Systems Security TF, Rohit
   a. Issue surrounding intellectual property rights
      i. Detailed technology specifications
      ii. Following IEEE / IETF process
   b. 42 members in the group
4. External Coordination
   a. NIST AMI SEC
      i. Co chairs DH and Eberoset, Secretary B. Monkman
      ii. Objective: facilitate the implementation of sec requirements for AMI by a recognized Standards Development Organization
      iii. SG Security AMI SEC TF is on stand-down due to the work of this group
      iv. Setup specifically as coordination between sg security and nist cswg
      v. Work with MIST Testing & Certification group to ensure the specs/requirements are testable
      vi. Twiki site: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGAMI; contact tanya.brewer@nist.gov
      vii. Update: Wendy from CA PUC - Direction from M. Swanson is to produce a document for AMI requirements. One document is use cases. Has worked been already done by SG Security? Request for Utility participation since this group will produce actionable security requirements.

Conversations:

Resources:

The group is need of resources and people willing to take on leadership of sub-teams with specific tasks. There needs to be more subject matter experts to help drill down into the use cases.

Use Cases:

What is an authoritative source for use cases? There is no authority.

Darren Highfill noted that context for the use cases is important to understand

SG Security developed use cases for AMI in a security context

Southern California Edison developed use cases in context of smart grid functionality and has since expanded on them
Consumers Energy further expanded SCE's use cases
NISTIR 7628 has 8-9 use cases that are under consideration by NIST AMI Security Subgroup
Sources for Use Cases:
www.Smargridipedia.org
http://www.sce.com/CustomerService/smartconnect/industry-resource-center/use-cases.htm

Use Case Testing:
What is an authoritative source that decides what the use cases needs to be tested against? This has no answer.
State of CA PUC has authority. FERC has authority. NIST SGIP cannot dictate to FERC. International Standards Organizations do not recognize NIST. UCA does not have organizational commitments to obey NIST. And so on. Context is important here as well - functional or threat use cases. SG Security will not be the authority for a set of use cases.

Good work bubbles up and the information converges. Look for opportunities to share good work with amongst groups

Gas and Water Meters:
NIST does not have authority over this sector and therefore out of scope. Issued already discussed and settled in earlier meetings of the group. However, requirements need to be designed not to preclude these meters.

5. ICSJWG Vendor Subgroup
   a. Coordinating activities with other groups
   b. Interest in working with SG Security

Action Item: Conference call with between this group, DHS, and SG Security

6. DOE-NIST-FERC-NERC Activity on Risk Management Framework - Bill Hunterman, DOE
   a. Provide practical guidance and converged/consistent way to manage risk for companies in the Electric Power Industry
   b. Many diverse ways to manage risk in this sector
   c. Chris with CA PUC - monitoring this activity

Suggestions:
Coordinate activity with NIST CSWG Design and Principles group - work being done on key management

Response: Ther:e is active coordination - DH has weekly calls with M. Swanson at NIST to ensure coordination
Response: Overlap with NIST CSWG AMI SEC group at the technical level - more talks required at this deeper level

Action Item: Darren Highfill to coordinate work with all groups in common with this effort

WASHINGTON, DC - The Department of Energy is launching an initiative to enhance cyber security on the electric grid. The initiative, led by the Department's Office of Electricity Delivery and Energy Reliability (OE), the National Institute of Standards and Technology, and the North American Electric Reliability Corporation, will be an open collaboration with representatives from across the public and private sectors to develop a cyber security risk management process guideline for the electric sector..
For more information or assistance, please contact Kimberly Mielcarek or at (202) 383-2622.
North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

7. Cyber Attack Task Force - NERC/DOD(?)

Action Item: Follow-up with S. Bacik for the NERC angle
Action Item: Include as an item on the Agenda for SG Security Meetings
Action Item: Darren Highfill to reach out to the group

WASHINGTON, DC – As part of its Coordinated Action Plan, the North American Electric Reliability Corporation (NERC) announced that it has formed the Cyber Attack Task Force. The task force will consider the impacts of a coordinated cyber attack on the reliability of the bulk power system.
For more information or assistance, please contact Kimberly Mielcarek or at (202) 383-2622.
North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

8. Interest Groups / topics of discussion
    a. Vulnerability Handling
        i. J Wright, InGuardians, D Weber continue work in this area
        ii. Information Sharing

9. ASAP SG - WAMPAC (synchrophasors) Security Profile
    a. Started with AMI Security Profile; and now has created DMS Security Profile, 3rd Part Data Access Security Profile
    b. Working on WAMPAC Security Profile
    c. Dedicated resources required to get these security profiles created
    d. Need Utility sponsorship - urgently
        i. ~100K per year required from Utility
        ii. Get named explicitly in federal level reports issued by DOE
    e. Huge priority for DOE - win/win with private/public collaboration

10. IEC TC57 WG 15
    a. There is a relationship between UCA and IEC TC 57

b. Undertake develop of standards for security of communication protocols defined by iec tc 57
    i. IEC 60870-5, 6 (control center to control center) ; 61850, [61970, and 61960 CIM for transmission and distribution)]
c. Undertake the development of standards or technical reports on end to end security issues
d. Slide on mapping of IEC 62351 to the above IEC Standards

    Question: How does this work with 62351 and the IECs above?
    Response: There are internal processes with IEC. Each part of these are standards. Which bytes go where on what wire. Security to be handled by 62351 for these other protocols - but not entirely consistent. Security for synchrohpasors being added to 61850 spec. could be rolled out and into 62351

    Question: Can SG Security feed information to IEC?
    Response: Yes. These issues can and should be passed onto IEC

    Question: Does SG Security have access to the standards?
    Response: No. SG Security should review what NIST CSWG has put out on the review of 62351. Darren Highfill working on getting access to drafts on wg 15 for sg security members. If you are a member of IEEE, then can leverage that to gain access to IEC standards.

11. NERC CIP v4
    a. Here is the list of things that qualify as critical assets:
    b. Provides bright lines;
        i. generation over 1500 mw
        ii. Substations greater than 500kv
        iii. Control centers for rc/ba/top functions or > 1500mw
        iv. 300 mw automatic load shed criteria - AMI??
    c. FERC directives have not yet been addressed

F2F SF 3.8.11 Session 2

Tuesday, March 08, 2011
3:48 PM

Joint Session with SG Network

1. Show collaboration work between sg security and sg network
2. Payloads in communications
   a. LIC - joint work with NIST CSWG
   b. CIA ratings developed by NIST CSWG, SG Security, SG Network
3. Make awareness of the information
4. Big kudos to S. Bacik for support on LICs
5. Background
6. SG Network Requirements Table:
   a. Determine LIC values from NISTIR 7628
   b. Populate a CIA Risk Level for the payloads
   c. Assessment based off payload insteand of all 1400 separate transactions - way too much effort
      i. Reduced to 180 payloads - data that is sent - "Read Meter"
   d. Produced CIA ratings at the business level -
      i. Question: What was the H-M-L based on? Response: Same scale that was in the NISTIR 7628

Question: SG Network has work to complete on descriptions and red text. What is the long term use of this document
Response: Working archive, Usable version - gray columns - will be entered in requirements database, included as appendix in systems requirements specification document.

Question: Does the "clean" version make it to NIST CSWG or other organization
Response: Yes. Targeted audience is utilities, vendors, and regulator
Response: This is a set of requirements and does a product meet all of these?
Shows implications of the payloads but does not specify security controls
Specification of sensitivities and priorities of what needs to be protected but not how to protect it

Question: What about replay attacks? Not directly addressed. And did not get down to that level of detail
Control system so this should be critical
Developed being technology agnostic
SG Security Embedded Systems work will provide for replay protection - is in scope for that TF
SG Network table does not threats into account; not a risk management/assessment tool or security analysis tool. Can take this document and perform those analyses to determine what measures are needed to protect against threat

Question: Taking this work and put it through a threat model or threat modeling?
Makes sense but challenge is the rate which the threat landscape changes. Idaho National labs say there is no way to determine the odds of an attack occurring - threat level of 1. Odds of predicting a specific fantastic event is nearly 0.

But good at predicting low level events but society/industry has done a poor job of documenting/disclosing those occurrences (how often and what type of attack occurs - info sharing issue); threat assessment started by AMI Sec 4 years ago and got to 80 percent.

Can it be easier to look at threat assessment from this work? Yes - makes it easier and this work is very valuable - inventory and impact identified. Have 2 of three components of the equation - need the vulnerability for the payload under discussion.

More vendors being transparent once in an arrangement with a customer and the customer only
Who would do the 3rd step and when? Burden on Assets Owners to ask the vendors for this information

Question: How many payloads are related to different domains - AMI? 30-40 for ami, DMS, DA, Dstorage, Evs, etc.

Information is available for NIST CSWG AMI Sec group
Should become a published product and revise as needed. This should be considered v1.0
This was work directed by PAP 02 - will be part of PAP 02 deliverables

Difference between NISTIR 7628 and this work - this work is 2 or 3 levels deeper than the work done in NISTIR 7628

Question: How does this live on - comments, revisions, etc?

Response: There is no defined process for maintenance of this document.
Response: Is there a formal review, comment, or voting on changes? No process has been defined.

Use of xtalk listerv and joint SG sessions

Question: How does this related back to business processes?
Column F denotes a reference to a use case but there is no correlation back to the source use case. Can this be done? Herculean effort given the granularity of these payloads. The use cases are at a higher level and do not talk about payloads or payload failures. Some of the use cases are copyrighted and not in the public domain (Intelligrid, SCE EVs, fo example)

Question: How can these be used to determine if security has been applied? PUC or regulator could hand this over to a utility and ask how the utility complies?

Question: How do protocols fit into this? IPSEC gives C and I on all; DNP3 gives I but not C. There needs to be analysis around what protocols should be used. This work is starter for those conversations. There needs to be a technology mapping for existing solutions.

Action Item: Revisit the request for SG Security to take this work to the next step - risk mitigations/threat identification/??

Take this work and draw an architecture without security and assess vulnerabilities, and then discuss solutions (pros and cons)

Need a reference architecture - take the existing SG Net diagram and drill it down to the technical solutions but remains vendor agnostic

How are legacy systems and devices accounted for? Yes, they are part of this analysis at the payload level but not at the technical level

To answer the security question, each legacy device and path needs to be looked at - scaling issue

Issue: No clear guidance on how to encrypt various payloads - when is transport security sufficient? When is transport and application security required?
Look to NISTIR or FIPS but those do it at high level. There is a difference between a control command payload and a ping message. There are costs - financial and performance for using TLS everywhere.

Question: Is financial impact considered in the CIAs in the NISTIR? No.

Question: CA PUC is concerned about safety and cyber security is high on the list as well. There are public goals that are important and how are these accounted for?
Response: The rational in the document does take into account general public safety and grid reliability. Each payload does not have impact to each criteria.

Comment: talk with the new EIM group and see how these groups can work together or leverage work already done

Follow-ups:
Request access to document - Matt Gilmore
More eyes and ears on this work makes it even better
One more email to all groups and ask for one more round of comments with a due date

Driver is SGIP meeting in Nashville 3/29-3/31 - work from that date back for comments, comment resolution, revision
Comments/Review due by 3/22
Communication should include a targeted example where feedback is required

F2F SF 3.9.11 Session 3

Wednesday, March 09, 2011
7:53 AM

1. Cyber Sec Interoperability (D. Teunim, Chair)
    a. Created May 2010
    b. Spinoff from the DOE National SCADA Test Bed Lemnos Project
    c. Develops interoperable configuration profiles for widely accepted Internet Protocols
    d. These ICPs then become SG Security documents
2. Updates since last Face to Face Meeting
    a. Issued IPSec ICP as a draft document
    b. Issued proposed Syslog Message Woring to Lemnos Team and this TF
    c. Issued Lemnos draft ICP for Secure Shell to TF
    d. Lemnos timeline extend to 1.31.2012
3. Work In Progress
    a. Work on Standardized Syslog White Paper with End-Users
        i. Stress importance of standardization to ease NERC CIP Compliance
    b. Compose ICP for LDAP
        i. Need LDAP experts
    c. Finalize SSH ICP
    d. Arrange two Lemnos "plugfests" demos at EPRI in Knoxville (June and August)
        i. Preliminary practice June 1st and 2nd
            1. New Vendors to make IPSec connections
            2. work on new protocols - LDAP, SSH, and SYSLOG
        ii. Main Demo During week of August 8th
            1. Demo Existing and New Lemnos protocols
            2. Open demo for Open SG and EPRI Utilities to observer
            3. Discuss industry participation to continue the work - DOE funding will expire.
        iii. 7 vendors participating
4. New SSH draft ICP
    a. TCP SSH Mode provides SSHv2 client and server connectivity processes
    b. Standards: RFC 4250, 4251, 4252, 4253, 4254
    c. Inputs
        i. SSH Related Settings
            1. DirectionIndication -
            2. connectionHostkeys
            3. AuthenticationContains
    d. Processing
        i. Must conform to all requirements in the RFCs
    e. What does interoperable testing mean?
        i. NIST just used the "musts" from the RFC Standards
        ii. Industry/Vendors tests all relevant parts of the RFC Standards

            <u>Conversation:</u>
            Use of ICPs:
            In order to test ICPs, interoperability issues already have had to be resolved to test the ICPs.
            Can these ICPs be taken into consideration by the NIST Testing & Cert group?

NIST Testing & Cert is a framework and to be certifited must follow ISO standards

Plugfests lead to vendor techies fixing products on the fly in a rushed setting - it is not a interoperability test

Difference between certification and interoperability testing

ICPs prime the pump to have conversations and come to an agreement on configurations for interoperability

Handoff to the NIST Testing & Certification to determine process for testing and certification; all the players are not coming into the NIST testing cold - they already had input into the ICPs

The ICP becomes accepted through OpenSG/UCA - there is behind scenes of forming a UCA "Interoperability Testing"

f. Resources Needed
   i. LDAP ICP writeup assistance
   ii. SSH draft ICP comment
   iii. SYSLOG White Paper
   iv. IPSEC OpenSG ICP tune-up

5. ASAP-SG WAMPAC - Wide Area Monitoring, Protection and Control (Synchrophasors)
   a. Synchrophasors are in the Transmission Domain;
      i. ASAP-SG has focused on Distribution and Customer Domains
   b. Transmission moves electricity across the grid
      i. 3 interconnects - Eastern, Western, and Texas
      ii. Highly meshed network; bulk generation is moved to Transmission and then finds it way out to Distribution domain on its own
      iii. Not easy to control how electricity moves in the transmission domain
      iv. System does some balancing/control of flow but can't optimize the paths
   c. Method for Monitoring Today: State Estimation - SCADA measurements - voltage and current measurements across the grid taken at 2-4 second intervals; fed into a black box and runs mathematics and provides an educated guess at the state of the system
   d. Synchrophasor
      i. Sin waves
      ii. 2 measurements - two parts of a vector that represent an angle and a magnitude.
      iii. Phase angle represents the phase difference by which the voltage leads or lags the current in the AC circuit
      iv. Place phasor measurement units at critical points on the grid and associate with GPS for timestamp to figure out the health of the system
      v. If this existed in the blackout of 8.14.2003 - would have had 4 hours of warning of the event
         1. Blackout is never caused by a single circumstance but by inadvertently operating system at its limits
   e. DOE and NERC working with Industry to enable wide area time-synchronized measurements
   f. 300 PMUs on the grid today; at the end of the project, ~800 PMUs deployed
      i. Beginnings of new way to operate and monitor the grid
   g. 61850-90-5 Synchrophasor Communications
      i. Work actually taking place in WG 10
         1. Power system IED comms and associated data models
         2. Security work on 90-5 coordinated with WG 15

3. Produce single Technical Report to accelerate process

ii. Issues on Devices
    1. Resource constraints
    2. Very low latency
    3. Continuous service
    4. No error correction built-in - continuous flow of discrete data - wait for the next data set

iii. Solution Path
    1. Signature on all messages
    2. Option for encryption
    3. Use public-private keys to negotiate a temporal symmetric key
    4. NASPI has 5 data classifications for synchrophasor data: A through E.
        a. Class E is purely for research.
        b. Class D is post event analysis in the Utility
        c. Class C is visualization; state of the system in a control room; separate display from SCADA
        d. Class B is feed-forward - being used by state estimator along with SCADA data
        e. Class A is closed-loop control - wide area protection system plugged in and can trip a breaker

h. Security Concepts
    i. Need to support UPD unicast and multicast (preferred)
    ii. Need perfect forward security mechanism
        1. Cant disrupt data flow with key changes
        2. Impacts protocol and key distribution center (KDC) function
        3. Starts in the protocol
    iii. KDC must provide key management capability based upon individual stream definitions
    iv. Evaluated existing KDC technologies - gsakmp, gdoi, mikey rsa-r
        1. Chose GDOI, RFC 3547
            a. Provided additional functionality for other parts of the smart grid
            b. GDOI is clear of licensing/copyrights/etc.

i. ASAP-SG Work on WAMPAC
    i. Started nov 2010
    ii. April 2011 draft expected
    iii. Scope
        1. Time-synched, moderate resolution, power related waveform data
            a. Phasor measurements leaving the substation
            b. transport, delivery, and integrity of processes
            c. Data classes A-D
            d. Does not address sample values or business/system protection logic
    iv. Developed a functions and logical Architecture
    v. WAMPAC Use Cases
        1. 16 use cases identified
        2. Failure analysis and control derivation completed
            a. Developing specific controls if needed for phasor data

j. ASAP - SG Proifle Development Process
    i. Now includes steps to map to the NISTIR 7628 for each part of the process

F2F SF 3.9.11 Session 4

Wednesday, March 09, 2011
1:31 PM

Embedded Systems Update, Rohit Khera

1. Up and running for 2 months
    a. 45 members
    b. Utility membership is light

2. Update on Secure Device Profile Components
    a. Profiles for HAN, Substation/Wide Area, Distribution Automation, AMI
    b. CIA requirements from NISTIR, AMI-Sec
    c. Crypto requirements and cost-be based factors
    d. Hardware - secure microprocessors
    e. Memory - no data stored in clear text in the memory on the device
    f. Cipher Stack - parts of the stack can be implemented with firmware/software or hardware
    g. Side Channel Protection across all areas of the device
        i. Observing timing related parameters - i.e. execution time of encryption :: put in buffers
        ii. Observing the power analysis of the core - i.e. how much power is consumed
    h. Operating System is out of scope but does address Crypto APIs to interact with Cipher Stack
    i. Network Stack
        i. Cipher suites - combination of crypto primitives to form suite to provide CIA
        ii. Secure Transport Protocols
        iii. AAA Protocols
    j. Management Stack -
        i. configuration management,
        ii. secure updates,
        iii. MIB/Sec Taxonomy
        iv. Newly added for the original device profile

    Question: Any consideration of hardening the OS?
    Response: Not in scope but a legitimate concern
        Additional discussion to determine to bring into scope
        There exists specifications on hardening OS - these can be reviewed and determine if applicable, and then reference it.

    Comment: Requirements need to applied based on the environment that device is in - Recloser in the field vs. Device in Substation
    Comment: Formal threat modeling is outside the scope
    Comment: People should not be afraid of the deep dive into this area. There is opportunity to participate and gain understanding.

    Question: Could this have discovered or prevented Stuxnet?
    Response: Nothing could have stopped or prevented Stuxnet - very complex, 4 Zero Days, and a Socail Engineering component. This device profile raises the bar for security.

    Question: Is any of the device profile aimed at physical protection?

Response: Tamper-proofing is incorporated into hardware

3. Deliverables and & Progress
    a. Crypto Hardware requirements first draft submitted
    b. Ciphers - work is underway but NISTIR has Crypto information but if references NISTIR becomes a requirement
    c. Key players identified for these sections - Random Number Generator, Device Robustness & Resilience, Key Management, Device Management,
    d. Key players needed for Device Authentication & Access Control, Secure Protocols

    Question: Does key management include a policy around handling keys?
    Response: Yes - key rotation, key initiation, etc. is in scope

4. Some Questions Around Hardware
    a. Monolithic/Single Die - smart cards - data never leaves the chip
        i. Self contained
        ii. But limited functionality due to size (16 bit)
    b. Co-processor
        i. Augment security features
        ii. But clear text traverses bus to general purpose MCU?

5. Intellectual Property Rights Considerations
    a. All contributions need to contain a statement regarding intellectual property
    b. Default assumption is that contributions do contain intellectual property
    c. UCA is working on a policy for intellectual property rights - 15 points in the policy
        i. To be reviewed by a lawyer and rewritten in policy format
        ii. Pressure to get it done ASAP - concern with exposure on existing material in the UCA domain

6. Constraint Characterization
    a. Robust crypto can is possible on constrained systems
    b. Goal is to point out the options that are available
    c. Performance numbers displayed need context - max, optimized, or a group comes to this TF with speed requirements

7. Organization and Contact Info
    a. Chairs: Rohit Khera – rxkw@pge.com; Daniel Thanos - Daniel.Thanos@ge.com
    b. Sharepoint: http://osgug.ucaiug.org/utilisec/embedded/default.aspx
    c. Email Reflector – 'OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG'
    d. Bi-Weekly Co-ordination and status calls

F2F SF 3.9.11 Session 5

Wednesday, March 09, 2011
3:51 PM

Joint Session SG Security and SG OpenADR

1. SG OpenDR is focused on the exchange of information between entities
   a. DR - demand response: changes the behavior of customer intentionally by Utility/Load Service Entity
   b. Information models
   c. Types of information that needs to be exchanged
   d. Event Messages involve multiple 3rd Parties
      i. DR Event Request
      ii. DR Event
      iii. DR Acknowledgement

Conversation:

Are there agreements between Utility, 3rd Party, and Customer for exchange of data?
Can any party decide what path or how messages are sent and received?
How does a customer know to trust the demand response signal from a 3rd party that is in between Utility and Customer?

Assumed that there is a business relationship in place amongst the parties; there is no interface or actions for these relationships

What are the technical means used for the communications for messages are following the established business relationship?

There needs to be some kind of exchange of credentials between the parties with the business relationship

Assumption of the working model is that the credentials are part of the setup of the system/communications between the parties and it has followed a standard/secure method

How does customer tell its widget on the wall to only respond to QueItComm and not HacksAlot?

Need to identify source, authenticate the source, and respond to source. Are there mechanisms in place for this?

Not identifying these issues at this lower level - like identifying a version of TLS

Is there a difference in security requirements for a single DR Message that says [100 MW] versus 100 DR Messages that says [1 MW]?
Overlap with SG OpenADE and Third Party Data Access Security Profile

2. Path Forward
   a. Look at use cases in Third Party Data Security Profile
   b. Codify what needs to be accomplished and vet it in the community
      i. Scope limited to cyber security; physical security is out of scope
      ii. Define cyber security
      iii. Data needs to be accessed at rest, in transit, and in processing
   c. What is sensitive about ADR systems?
      i. Load information

ii. Privacy concerns

d. Look at e-Commerce security mechanisms [minus the payment stream]
   i. Take the good that is applicable
   ii. Money is not exchanging hands in OpenADR messages/events
e. Suggestion: Form a joint team to work through a draft document of objectives of OpenADR for security needs
f. For OpenADR:
   i. Action Item: Can the story of OpenADR be told through the 3 actors in the Third Party Data Access Security Profile?
   ii. Action Item: Can the use cases in the Third Party Data Access Security Profile be used with simple word substitution?
   iii. Action Item: Does this work now cover all of the OpenADR use cases already identified?
   iv. Communication in both forums for interest in joining a joint team to address the action items
      1. Potentially create a new xtalk listserver for this purpose

F2F SF 3.9.11 Session 6

Wednesday, March 09, 2011
5:46 PM

SG Security

1. Usability Analysis TF Update
   a. Meet every two weeks; Next Meeting 3/14/2011 at 10 AM Pacific
   b. Completed Activities:
      i. Charter has been finalized including evaluation criteria
      ii. Third Party Data Access (3PDA) Security Profile
      iii. Analysis Report has been completed

      Action Items:
      Send Analysis Report to Utilisec-Announce
      Send Comment Resolution Sheet to Utilisec-Announce
      Post Updated version of 3PDA Security Profile
      Communicate Review Period of 3PDA Security Profile - 1 week period
      Communicate Voting Period (and Instructions) on 3PDA Security Profile - 1 week period
      Update link to the 3PDA Security Profile on SG Security SharePoint homepage

   c. Distribution Management Security Profile
      i. Comment period closed
      ii. Comment resolution completed
      iii. Document updated based on comments
      iv. Drafting analysis report
      v. VPN over Public Network
         1. Discouraged in the profile
         2. Need verification that text is correct or is more explanation required
            a. Rational from ASAP-SG: Public Network does not provide QoS or Availability of Delivery for Control Messages
            b. Does a contractual arrangement mitigate these concerns?
            c. What about Carrier Networks that are dedicated to a Utility?
            d. How much control is in the system? Whole substation and its feeders? Last few mile to a feeder? It is a difficult threshold to define.
            e. What about Satellites? Geographically dispersed territories - feasiblity of having a private Utility network built

      Action Item: Flag the section in the document for further discussion and elaboration and hand off to SG Security

   f. Use Case 13 updated/corrected to kick off Use Case 2 instead of Use Case 5 in Field Application Swim Lane