

SG Security Working Group Charter and Scope

Abstract

The SG Security Working Group has been formed by the UCAIug OpenSG Technical Committee (TC). This document defines the charter, scope of work, and process for this Working Group.

SG Security Working Group Charter

Table of Contents

CHAPTER 1: DOCUMENT CONTROL	3
1.4 Change Record	3
CHAPTER 2: SG SECURITY WORKING GROUP CHARTER AND SCOPE	4
2.1 Charter	4
2.2 Scope	4
2.3 Mission	4
2.4 Guiding Principles.....	5
CHAPTER 3: TASK FORCES AND THEIR RESPONSIBILITIES	6
3.1 Current Task Forces.....	6
3.1.1 <i>AMI-Sec Task Force</i>	6
3.2 Task Force responsibilities	6
CHAPTER 4: PROCESS	7
4.1 Participation.....	7
4.1.1 <i>ListServes</i>	7
4.2 Voting	7
4.2.1 <i>Voting Eligibility</i>	8
4.3 Organization	8
4.4 Documents	8
4.4.1 <i>Document Access</i>	8
4.4.2 <i>Revision control</i>	8
4.5 Meetings.....	8

Chapter 1: Document Control

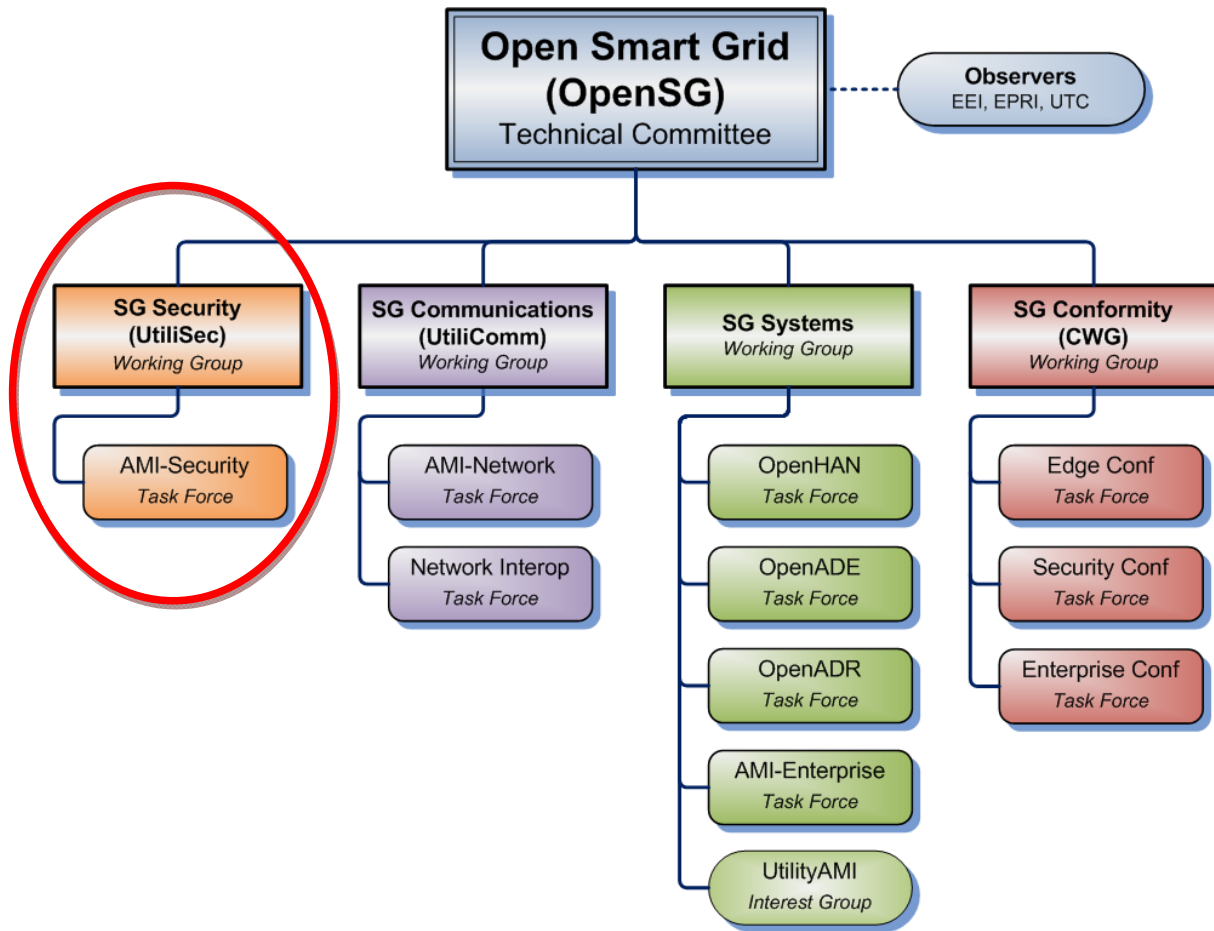
1.4 Change Record

<i>Date</i>	<i>Author</i>	<i>Version</i>	<i>Change Reference</i>
12/16/09	SG Security Charter Team	0.1	Initial draft of SG Security WG charter. Started with "OpenHAN TF Charter v0.2.doc" as template
12/17/09	SG Security Charter Team	0.2	Miscellaneous changes
12/21/09	SG Security Charter Team	0.3	Miscellaneous changes
01/26/10	SG Security Charter Team	0.9	Final draft for vote. Encorporated comments returned in Chapter 4

Chapter 2: SG Security Working Group Charter and Scope

2.1 Charter

The SG Security Working Group (SG Security WG) was formed by the UCAIug Open Smart Grid (OpenSG) Technical Committee.



2.2 Scope

The scope of the SG Security WG is to develop detailed security and assurance requirements and security best practice guidance for organizations throughout the lifecycle of smart grid technology.

2.3 Mission

The primary mission of the SG Security WG is to influence development of a higher level of cyber security and governance tied to mission reliability than is required for traditional IT applications. To support this mission, the SG Security WG will:

SG Security Working Group Charter

- Provide guidance to support a smart grid security program
- Collaborate with other working groups to ensure security is designed into smart grid solutions rather than added onto.
- Maintain technical alignment with other OpenSG Working Groups
- Feed and accelerate SDO and other external work (NIST, IEC, IEEE, etc.) by identifying gaps in current standards and technologies
- Feed and accelerate research efforts by providing guidance and prioritization
- Apply security best practices to operational context
- Adapt traditional IT and traditional control systems security guidance to operational context
- Coordinate with appropriate groups and provide guidance on security testing and conformity

2.4 Guiding Principles

Guiding principles are the philosophies which shall guide the SG Security WG in its mission. These capture the values and priorities of the WG and are summarized as follows:

- Provide technology-specific, but vendor-agnostic guidance
- Leverage existing industry body of knowledge where applicable
 - Security Standards and Practices
 - Power reliability engineering including control and automation systems
 - Technical solutions
 - Research
- Identify and provide guidance on cyber security metrics and criteria for testing and validation
- Provide cyber security measures that enhance reliability rather than degrading it
- Contribute to making security technology and processes more efficient and cost effective
- Provide guidance on security solutions relative to balancing reliability, business needs, and risk
- Provide domain specific guidance

Chapter 3: Task Forces and their Responsibilities

The SG Security WG may form task forces from time to time to work on a specific deliverable.

3.1 Current Task Forces

The SG Security WG currently has instantiated the following Task Forces. As a general guideline, each Task Force shall be co-chaired by one utility representative and one non-utility representative. Each Task Force chair may also choose to elect secretary, technical editors, and other focus groups as needed. The detailed tasks will be tracked by the Task Force and reported to the working group periodically.

3.1.1 AMI-Sec Task Force

AMI-SEC will produce technical specifications, best practices, and guidance that can be used by utilities to assess, procure, and implement security related functionality for Advanced Metering Infrastructure. In addition to utility use, this specification may also be used by the OpenAMI task force as part of their AMI/DR Reference Design specification, and by vendors to produce compliant and compatible security technologies. Specifications will be prescriptive in nature, such that compliant products will have known functionality and robustness. The specific intent of AMI-SEC is to provide the means by which to achieve additional security-related assurances not previously available within the utility industry. AMI-SEC will also work with standards development organizations such as the International Electrotechnical Commission (IEC) to feed the standards development process where appropriate.

3.2 Task Force responsibilities

Each Task Force shall develop and deliver a scope and charter document to the SG Security WG for approval. Additionally, all Task Forces will create, distribute and maintain a schedule and roadmap detailing the tasks and milestones that comprise the group's work.

All Task Force work products are subject to the SG Security WG and OpenSG TC approval.

SG Security Working Group Charter

Chapter 4: Process

The SG Security WG follows the Operating Procedures for OpenSG Technical Committee (<http://osqug.ucaiug.org/default.aspx>). Where there is a conflict between this charter and the version of the Operating Procedures for OpenSG Technical Committee in effect, the Operating Procedures will take precedence.

4.1 Participation

The SG Security WG holds open meetings and all interested parties are encouraged to participate by joining the meetings and providing comments on documents in progress. The main SG Security WG SharePoint page can be found at the following url: (<http://osqug.ucaiug.org/sqsystems/utilisec/default.aspx>).

4.1.1 ListServes

Interested parties may join one or more of the SG Security ListServes to receive meeting notices and SG Security related email communication. Subscription to these lists can be found on the main SG Security SharePoint page. The current ListServes for the SG Security WG are:

- UtiliSec Announce – Used for meeting notices and general SG Security WG announcements.
- UtiliSec Technical – Used for detailed technical discussions and debate.
- Usability Analysis – Used to review the effectiveness of work products produced by the SG Security WG and their ability to be applied to the problem space.

4.2 Voting

SG Security WG participants are granted voting rights in accordance with the rules set forth in the Operating Procedures for OpenSG Technical Committee Section 9.2 Working Group and Task Force Voting (<http://osqug.ucaiug.org/default.aspx>). Voting privileges are contingent upon membership in UCAIug (<http://www.ucaiug.org/Pages/join.aspx>) and meeting the attendance requirements. The SG Security WG officers will track attendance in group meetings in order to establish a member's voting rights. Only one vote may be cast per entity. Valid votes are as follows:

- YES
- YES with comments
- NO with comments
- ABSTAIN

The work product vote must achieve a quorum (50% of eligible voters casting votes) with a 2/3 majority of cast votes in favor to pass. ABSTAIN votes will not count toward the 2/3 majority calculation.

If the vote passes, comments received with YES votes shall be resolved prior to publication of the work product if and only if they are strictly editorial in nature. All comments received in the voting process with substantive technical impact shall be

SG Security Working Group Charter

noted, retained in a separate document, and handled in a future revision of the work product. Approved versions of work products shall contain no comments or mark-up.

4.2.1 Voting Eligibility

To qualify to vote, an entity must be a member in good standing in the UCA International Users Group as of the call for vote and must have representation at 3 of the previous 5 Task Force meetings.

4.3 Organization

The SG Security WG will have a chair, one or more vice-chairs, and a secretary. The chair will be the entity designated representative and report status to OpenSG Technical Committee. The vice-chair(s) will carry out the chair's duties if the chair is temporarily unable to do so. The secretary will schedule meeting, record and publish meeting minutes, record member attendance for voting rights, maintain list of unresolved issues, action items, and assignments.

4.4 Documents

Approved content and content released for review may also be posted on SmartGridiPedia.org (<http://www.smartgridipedia.org>), and is subject to the terms and conditions of the Creative Commons license. The details of this license can be found at (<http://creativecommons.org/licenses/by/3.0/us/>).

4.4.1 Document Access

Historical and current working documents will be located on the UCAIug OpenSG website (<http://osgug.ucaiug.org/sgsystems/utilisec/default.aspx>). Generally, no account is necessary to download documents from the SG Security WG SharePoint. An account may be required for document upload.

4.4.2 Revision control

The SG Security WG shall be responsible for ensuring accurate revision control and traceability of working documents.

4.5 Meetings

The SG Security WG holds open meetings and all interested parties are encouraged to participate by joining the meetings and providing comments on documents in progress. The SG Security WG will schedule regular teleconference / web meetings and notify participants through the UtiliSec Announce ListServ.

Face to face meetings will be held at the quarterly OpenSG meetings, which will be announced no less than 14 days in advance.