PSCC S16 SG Meeting Notes

Designation:	Name:
S16	Application of IDS and IPS to Electric Power Systems

Meeting Location:	Meeting Time:	Meeting Date:	Minutes Revised:	Minutes Approved:
Webex	8:00AM CST	2021/05/04	2021/09/21	2021/09/21

PAR Output:	PAR Output:	PAR Approval Date:	PAR Expiration Date:	Target Sponsor Ballot Date:	Target Completion Date:
N/A		N/A	N/A	N/A	N/A

Presiding Officer:	Recorded by:	Draft Number:
Eugenio Carvalheira, Chair	Eric Thibodeau	

Attendance:

Name	Affiliation	Attending via Phone (P) / Web (W) or Local (L)	M/CM/G
Jason Lombardo	S&C	W	M
Mickey Schultz	Black and Veatch	W	M
Nathan Wallace	Cybirical	W	M
James Formea	Eaton	W	M
Sakis Meliopoulos	GA Tech	W	M
Deryk Yuill	iS5	W	M
Priyanka Nadkar	SEL	W	M
Gayle Nelms	SEL	W	M
Wayne Stec	Distregen	W	M
James Bougie	Global Power Technologies	W	M
Luke Hebert		W	M
Eugenio Carvalheira	OMICRON	W	M
Shane Haveron	Ametek	W	M
Colin Gordon	SEL	W	M
Steel McCreery	OMICRON	W	M
Scott Mix	PNNL	W	M

M:Member
CM: Corresponding Member
G: Guest

Item no.	Notes	Action by
CALL TO ORDER	Called to order at 8:02AM CST by Eugenio Carvalheira.	
INTRODUCTIONS AND QUORUM	17 attendees to the meeting, all members for study group purposes. Quorum was met.	
CALL FOR PATENTS	Pre-PAR slides were shown	
COPYRIGHT SLIDES	Copyright slides were shown	
CHAIR'S REMARKS	No remarks	

Item no.	Notes	Action by
AGENDA APPROVAL	Motion to approve agenda by Nathan Wallace, Scott Mix seconds. Agenda approved.	
APPROVAL OF PREVIOUS MINUTES	First meeting, no previous minutes to approve	
BRIEF HISTORY	Eugenio presents the background of the group. S11 performed a survey of security topics that should be addressed. IDS/IPS were identified in this effort. The goal of this group is to determine whether there is room for an IEEE Standard, and determine if we first want to draft a report, a guide, a recommended practice, or a standard.	

Item no.	Notes	Action by
DISCUSSIONS ABOUT THE NEED FOR A STANDARD	Eugenio presents the NIST Security Framework and a diagram about IDS/IPS in substations. Eric talks about the need for the document to provide a good picture of OT needs regarding IDS/IPS, as these needs are not well understood by IT often. Since IDS/IPS are mostly IT-driven solutions, this document could prove a good tool to help IT understand OT use cases. Mickey Schultz shares an experience using transparent firewalls, which allows shutting down traffic. Shows to be a very cost-effective solution. This experience required an elaborate collaboration between IT and OT sides of business. Nathan talks about risks of using IPS in the EPS especially when controls must be sent to a system. There is a need for such a work, but the scope is still very blurry. Do we want to cover only monitoring, or also blocking? Do we want to even cover physical security? Depends on the scenario we are facing. Shane Haveron reminds us that IDS/IPS goes much more in depth than only allowing/blocking data flows. It also does inspection of payloads. Scott Mix asks what is our audience? This will impact the contents of our document. He feels we are not close to a standard yet, and probably more along the lines of a technical report and or a guide. Eric and Colin agree that a technical report should be our first target. Colin thinks the target audience should be IT-oriented technical experts, and the goal of the report could be to inform them of the OT perspective and utility-specific considerations and requirements How to scope the effort? Are the alarms reported by an IED, as required by IEEE 1686, can be used by an IDS? Mickey Schultz puts forward that does not fall under the classic definition of IDS, but it is rather a security monitoring solution. Eric feels this is very well covered in 1686 and 37.240, but also in 62351-14. The audience feels that the report should be more like a tutorial report than a technical report. Like an academic survey of what exists. Consensus goes towards a Task Force that will output a report. Nathan suggests proposed title for the new group could be “Systems for detecting and preventing intrusions in Electric Power Systems”. This will enlarge the scope of the group and will cover all forms aspects in connection with the OT. The group will use the time until the September meeting to draft a scope. This will be discussed as a Study Group next September. We might need a meeting in between around June.	
TIME OF FINAL ADJOURNMENT	Scott Mix motions, Nathan Wallace seconds, meeting is adjourned at 8:59AM CST.	
NEXT FACE TO FACE MEETINGS	September, TBD	

Item no.	Notes	Action by
FUTURE MEETING ROOM REQUIREMENTS		