IEEE PSCC S11 TF

Chair – Theo Laughner

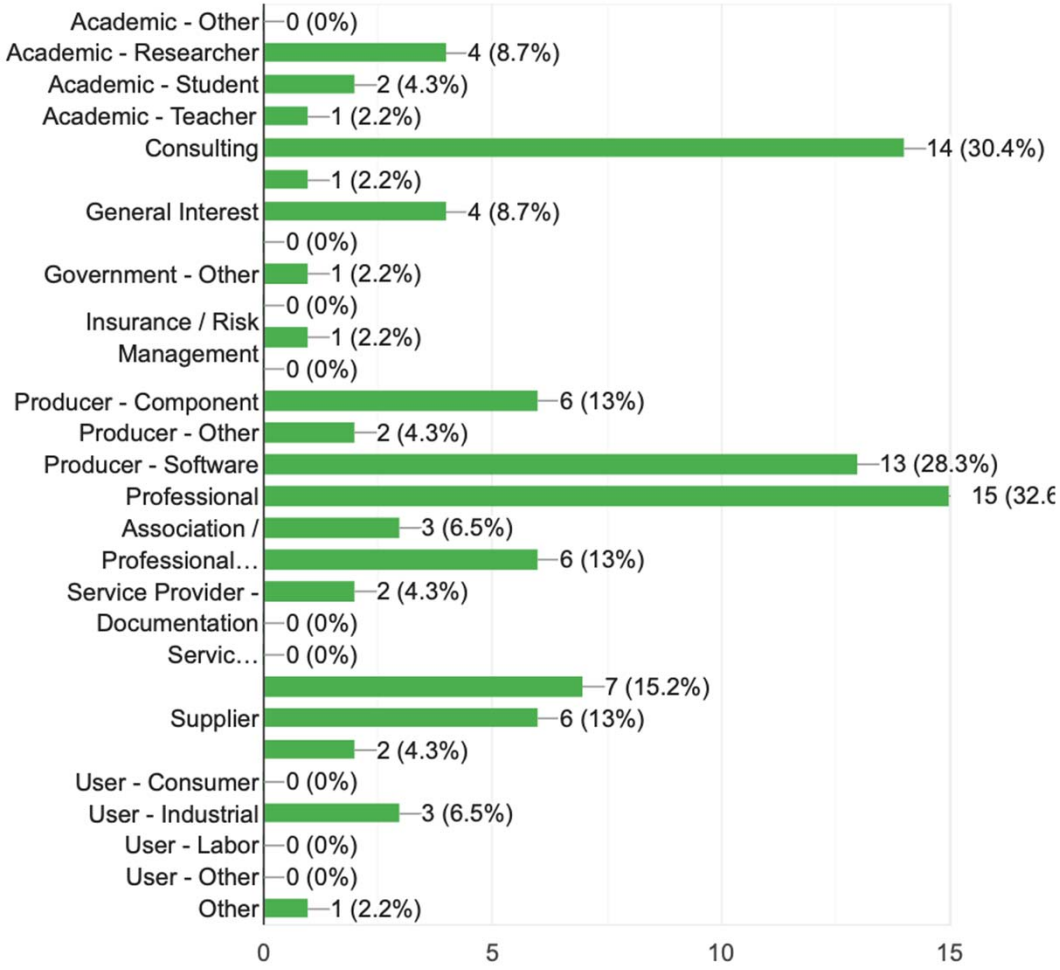
Vice Chair – Ralph Mackiewicz

Purpose of S11 TF

From S0 Minutes - New Study Group to explore: standardization of MIBS, (snmp, syslog, etc) prioritize what to look at: task force S11 (steering committee) to look at prioritizing profiles to support cyber related services and cyber security controls to be completed one year of assignment.

In Practice - Develop a **roadmap** for activities that S Subcommittee should undertake related to communication security issues.

Survey Results - Link

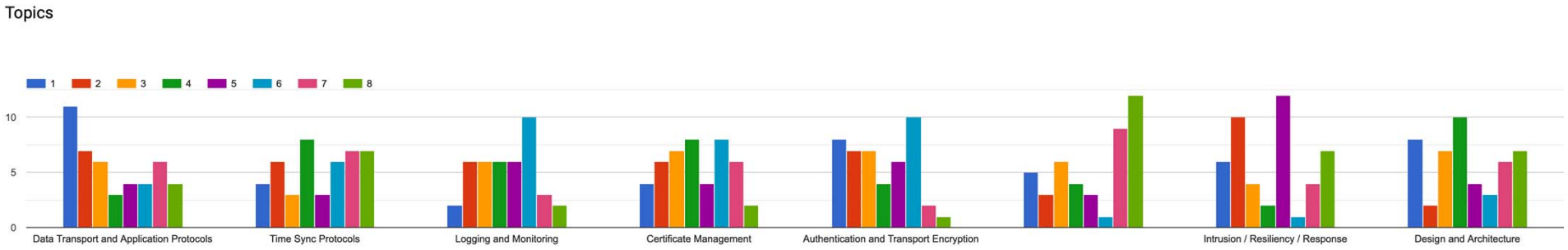


50 Responses!

IEEE PES Power & Energy Society®

IEEE

Topics



	Data Transport and Application Protocols	Time Sync Protocols	Logging and Monitoring	Certificate Management	Authentication and Transport Encryption	Use of wireless in substation or at the edge in operational systems	Intrusion / Resiliency / Response	Design and Architecture
median	3	5	5	4	4	6	5	4
mode	1	4	6	6	6	8	5	4
count < 4	24	13	14	17	22	14	20	17
Priority	H	L	L	M	H	L	H	M

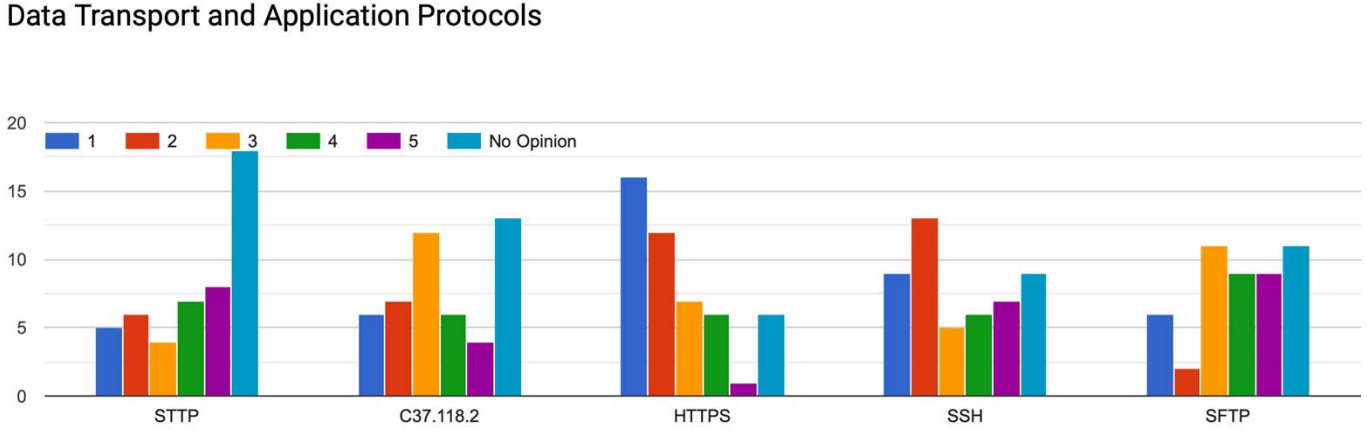
Topics Comments

Are there any other overarching concepts that need to be considered? (Please be specific)

10 responses

No
DER Security
Data transfer speed (for protection) and dependability of such data.
DER Integration
Reference substation network architecture for improved security
1. I believe an authorization mechanism for managing relationships between OT systems and devices (e.g. master station to substation) is a very effective complement to authentication for security. 2. We need a comprehensive standardized approach or at least a recommended practice for operational (OT) cyber security that is actively maintained and updated in response to industry needs. 3. I recommend the IEEE and the DNP Users Group work closely together to develop and standardize this.
Identity and mutual Authentication
Cyber metrics and measurements
Supply chain collaboration Secure product development lifecycle

Data Transport and Application Protocols



	STTP	C37.118.2	HTTPS	SSH	SFTP
median	3.5	3	2	2	3
mode	5	3	1	2	3
count < 3	11	13	28	22	8
Priority	L	M	H	M	L

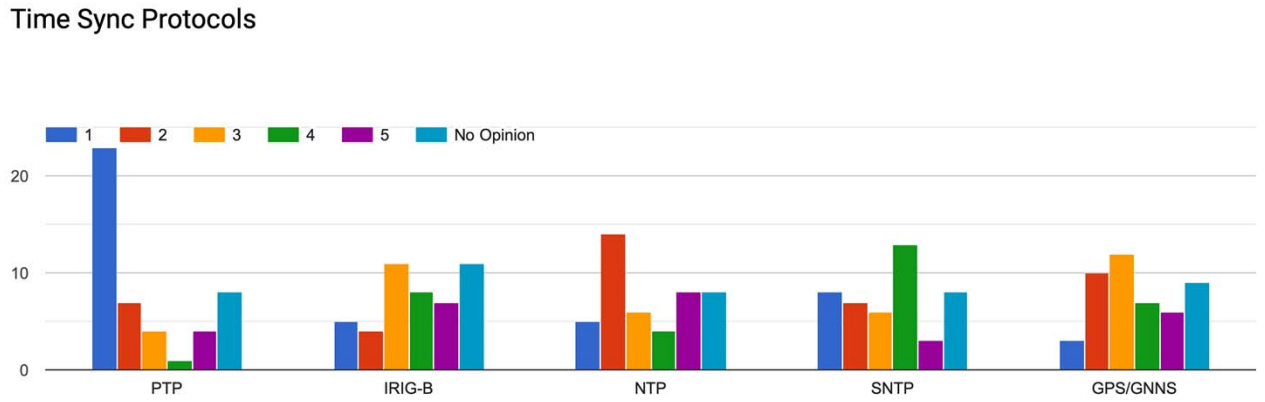
Other Protocols

Other Data Transport and Application Protocols

7 responses

For smart energy, these are not the right protocols. Focus should be on TLS 1.3 to avoid having to do encryption
Modbus, 61850, DNP3, T104
The security for protocols IEC 60870-5-104, DNP3i, and IEC 61850 MMS is already addressed in the IEC 62351 standard for data and communication security for power systems.
DNP3, MQ
IEEE 1815 (DNP3)
VPN, WireGuard
No

Time Sync Protocols

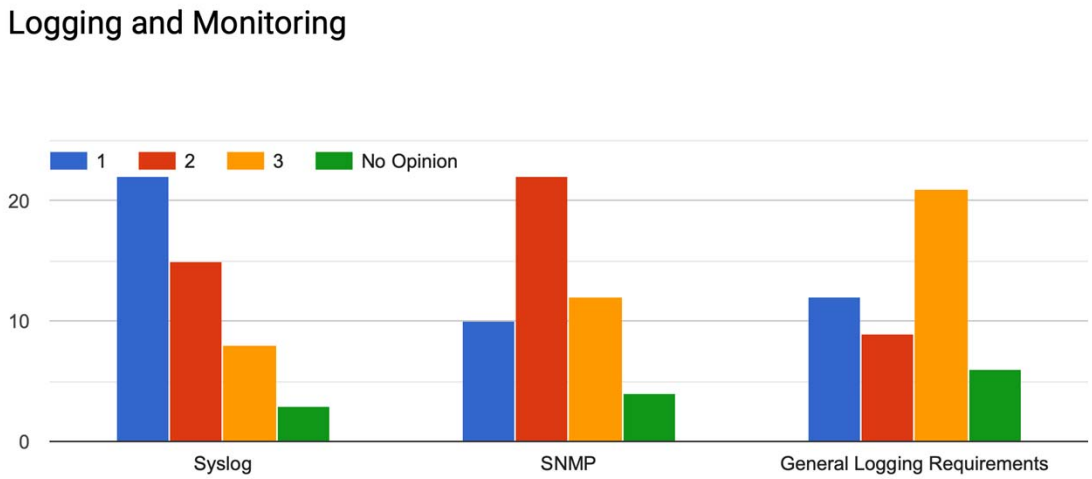


	PTP	IRIG-B	NTP	SNTP	GPS/GNNS
median	1	3	2	3	3
mode	1	3	2	4	3
count < 3	30	20	25	21	25
Priority	H	L	M	L	M

Other Time Protocols

did mean GPS/GNSS?
Protocol Time sync command (DNP)
No

Logging and Monitoring

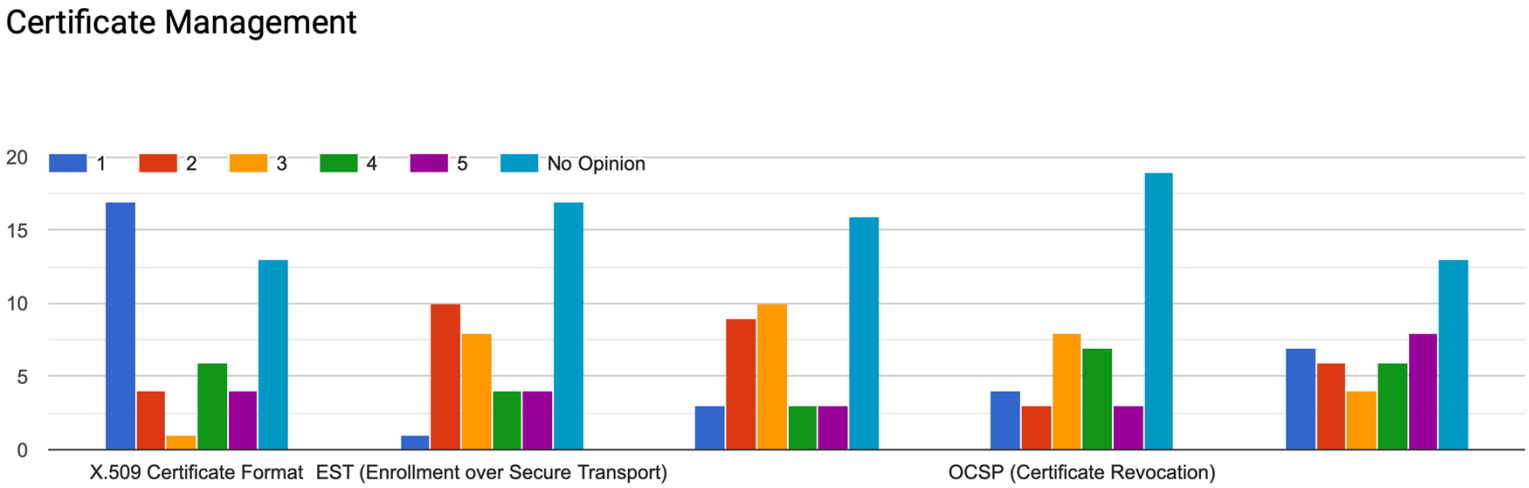


	Syslog	SNMP	General Logging Requirements
median	2	2	2.5
mode	1	2	3
count < 3	22	10	12
Priority	H	M	L

Logging Comments

IEC 62351-14 covers Shelly for 62351
Syslog based security monitoring is already being addressed in IEC 62351-14. SNMPv3 based security monitoring is yet to be standardized with a MIB, hence priority 1.
What's needed for compliance audit
No

Certificate Management

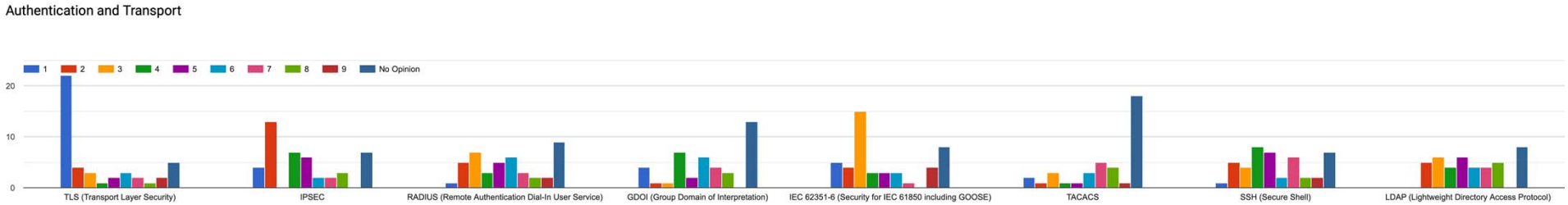


	X.509 Certificate Format	EST (Enrollment over Secure Transport)	SCEP (Simple Certificate Enrollment Protocol)	OCSP (Certificate Revocation)	DKMP (DNP Key Management Protocol)
median	1	3	3	3	3
mode	1	2	3	3	5
count < 3	17	1	3	4	7
Priority	H	L	L	L	M

Cert Mgt Comments

Software validation
X.509 based certificate management for power systems together with EST, SCEP and OCSP are alread addressed in IEC 62351-9.
Only few users may know where these different certificate management protocols are used. Would have been better to describe the application where they are used.
DKMP is being renamed to AMP
DKMP is being replaced by AMP, AMP could apply to other apps, makes use of X.509
No

Authentication and Transport



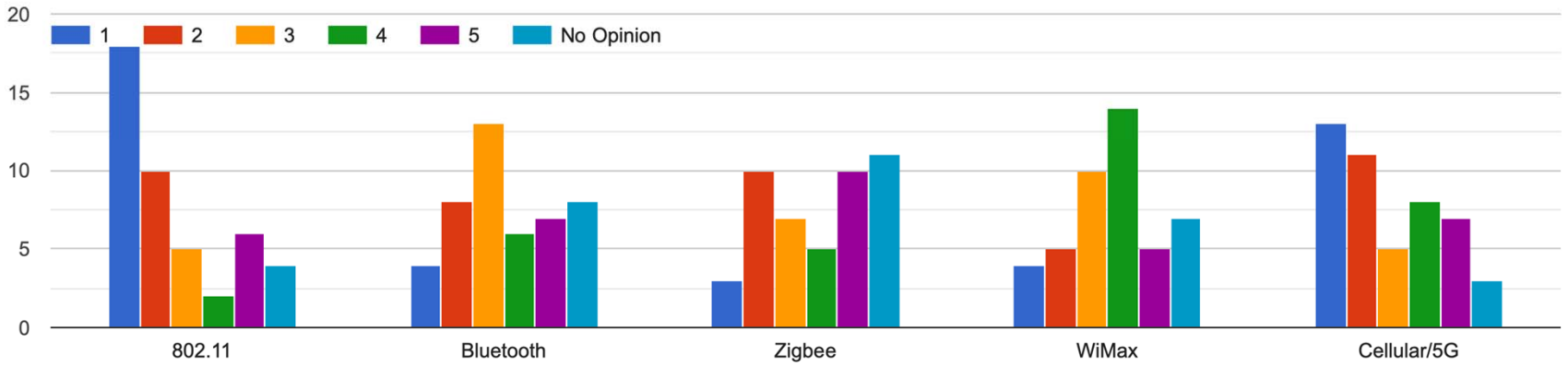
	TLS (Transport Layer Security)	IPSEC	RADIUS (Remote Authentication Dial-In User Service)	GDOI (Group Domain of Interpretation)	IEC 62351-6 (Security for IEC 61850 including GOOSE)	TACACS	SSH (Secure Shell)	LDAP (Lightweight Directory Access Protocol)
median	1	4	5	5	3	6	5	5
mode	1	2	3	4	3	7	4	3
count < 4	29	17	13	6	24	6	10	11
Priority	H	M	M	L	H	L	M	M

Auth & Transport Comments

IEEE shouldn't address 62351-6
OpenID or other JSON token related
All the aforementioned protocols except SSH, TACACS and IPSec are addressed in IEC 62351-3, -8, and related IEC 62351 parts.
DNP3 SAv6 (making it available as a protocol-agnostic standard)
IEEE 1815 Secure Authentication - Version 5/6
No

Wireless

Use of wireless in substation or at the edge in operational systems

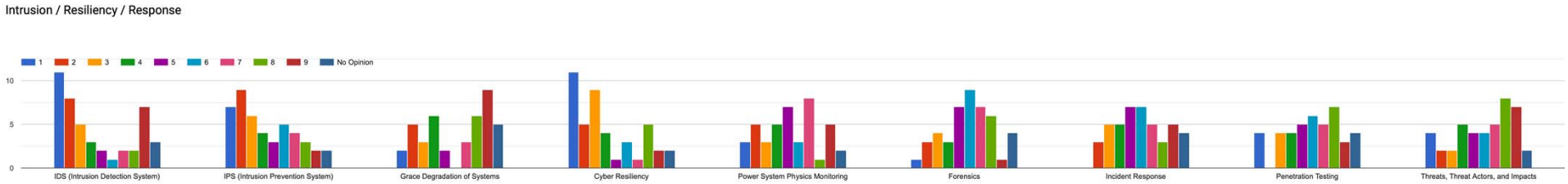


	802.11	Bluetooth	Zigbee	WiMax	Cellular/5G
median	2	3	3	3.5	2
mode	1	3	5	4	1
count < 4	18	4	3	4	13
Priority	H	L	L	L	M

Wireless Comments

AMI wireless systems
As of now, we consider wireless communication in substations to be not apoplicable / preferable.
6LoWPAN
No

Intrusion / Resiliency / Response

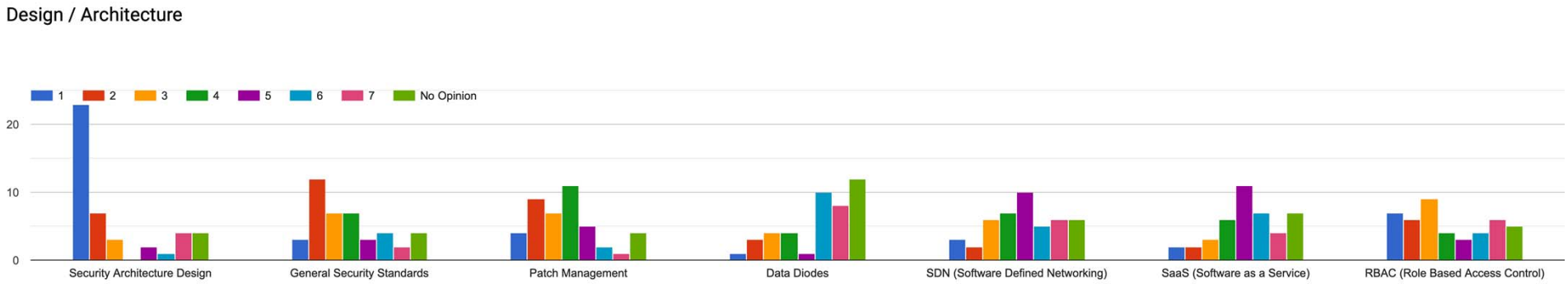


	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)	Grace Degradation of Systems	Cyber Resiliency	Power System Physics Monitoring	Forensics	Incident Response	Penetration Testing	Threats, Threat Actors, and Impacts
median	3	3	6	3	5	6	5.5	6	6
mode	1	2	9	1	7	6	6	8	8
count < 4	24	22	10	25	11	8	8	8	8
Priority	H	H	M	H	M	L	L	L	L

Other Resiliency

I assume that's "Graceful degradation"
No

Design / Architecture



	Security Architecture Design	General Security Standards	Patch Management	Data Diodes	SDN (Software Defined Networking)	SaaS (Software as a Service)	RBAC (Role Based Access Control)
median	1	3	3	6	5	5	3
mode	1	2	4	6	5	5	3
count < 4	30	15	13	4	5	4	13
Priority	H	M	M	L	L	L	M

IEEE PES Power & Energy Society®

IEEE

Design Comments

Security Architecture & Design has already been abundantly covered in existing security standards such as IEC 62443 and IEC 62351.
No

Other Topics/Themes

More focusing on security processes than technologies
As mentioned above, an authorization management mechanism.
DER Security
No

Road Map Document

Category	Topic	Description	Recommended Activity	Priority (H/M/L)
Data Transport and Application Protocol (HIGH 24)	STTP			LOW
	C37.118.2	IEEE Synchrophasor Protocol		MED
	HTTPS	Secure HTTP		HIGH
	SFTP	Secure FTP		LOW
	SSH	Secure Shell (SSH)		MED
Time Sync Protocols (LOW 13)	PTP	Precision Time Protocol		HIGH
	IRIG B	Serial Time synchronization		LOW
	NTP	Network Time Protocol		MED
	SNTP	Simple Network Time Protocol		LOW
	GPS/GNNS	Using GPS for time synchronization		MED

Adjourn

Thank you for coming/participating!