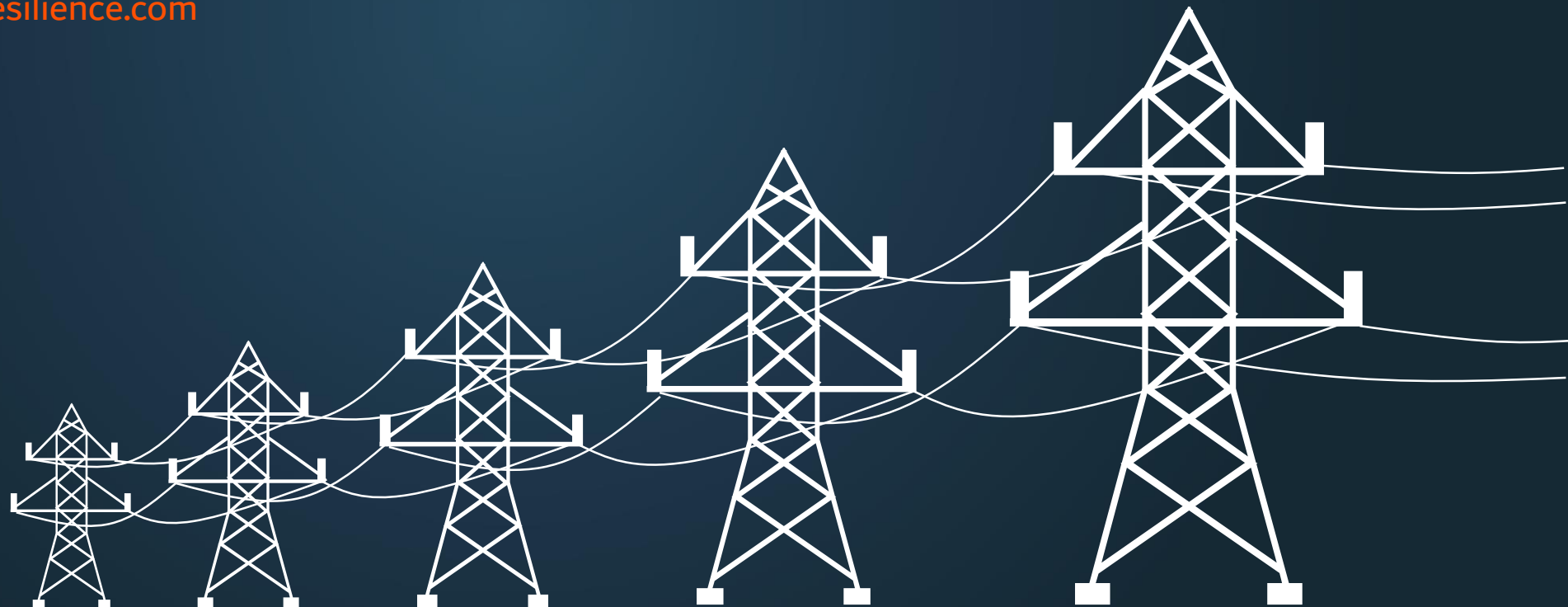
SMART GRID FORUMS

Smart Grid Cybersecurity 2020
7 October 2020 | Virtual Conference

SMART GRID FORUMS | IEC 61850 Global 2020
28 - 29 October 2020 | Virtual Conference

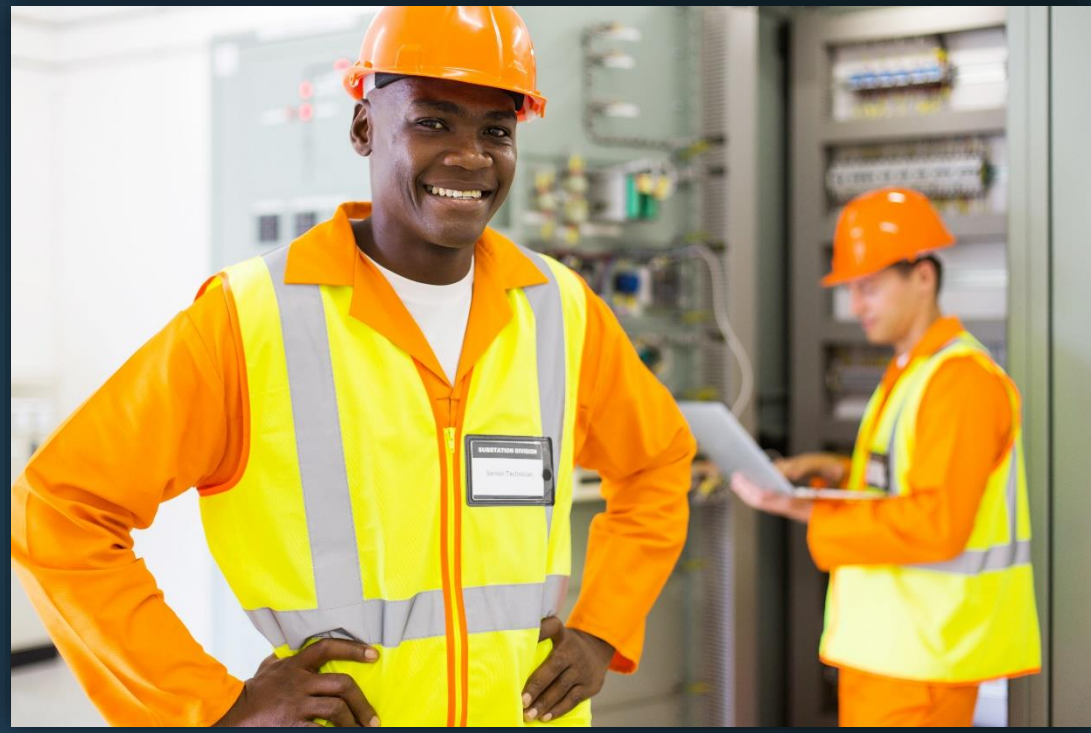
Secure Remote Access to IEC 61850-enabled Substations

Tahir Saleem - tsaleem@ICSresilience.com



Session Outline

1. Typical **use cases for remote access** to IEC 61850 substations.
2. **Why the traditional remote access model used in the industry in not adequate.**
3. **Quantifying risks** associated with remote access and engineering **mitigation** controls.



About Myself & Disclaimer

Over 12 years of experience in ICS/ SCADA/ OT cyber security: strategy, risk assessments, solution engineering, commissioning, operations and maintenance.

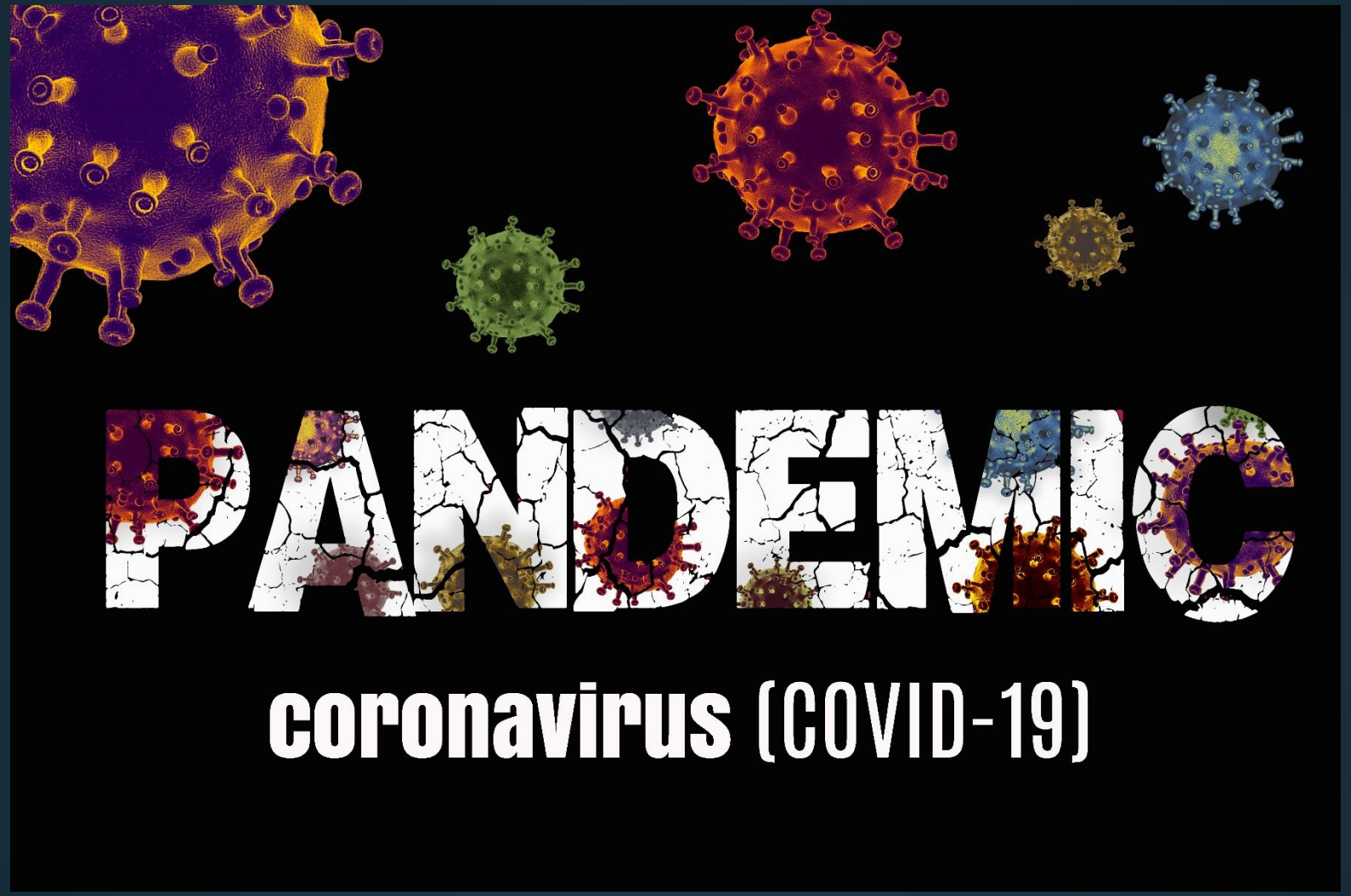
Recent relevant experience includes cyber security design, engineering & testing lead for:

- OT Security Operations Center (SOC) for Power Transmission Network; and
- one of the first 400kV switching station (IEC 61850) with integrated security encompassing SCS, bay control and protection functions per IEC 62443/ IEC 62351 requirements.

https://www.linkedin.com/in/**tahirsaleem/**

The opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect those of the presenter's employer. All content presented here is for education purposes only; the presenter bears no legal or financial consequences associated with utilizing this information.

Why Remote Access is in Demand Now?

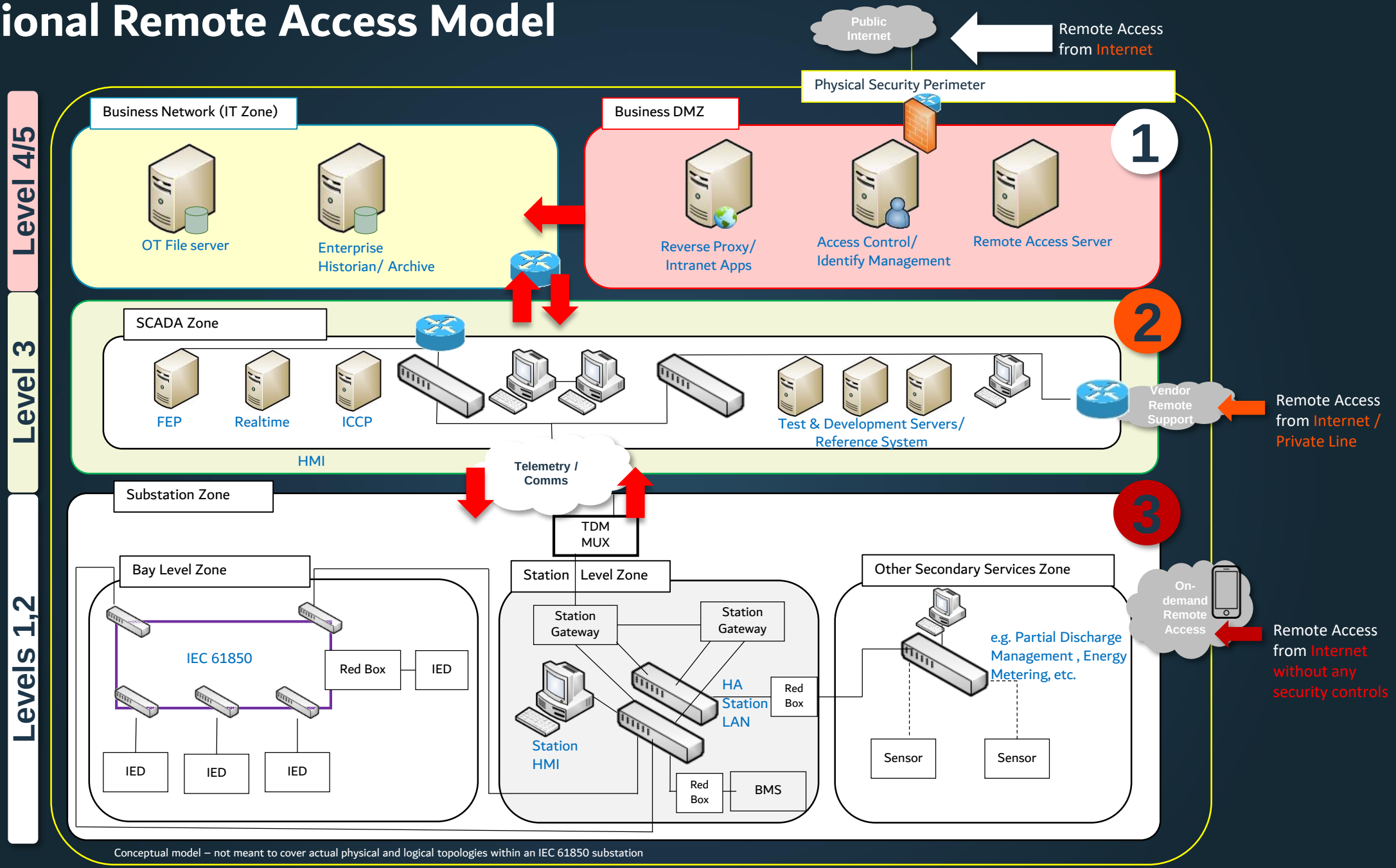


The key catalyst for transforming the risk appetite in power utilities for permitting interactive remote operations & maintenance from untrusted networks (aka the Internet).

Typical Use Cases for Remote Access Today

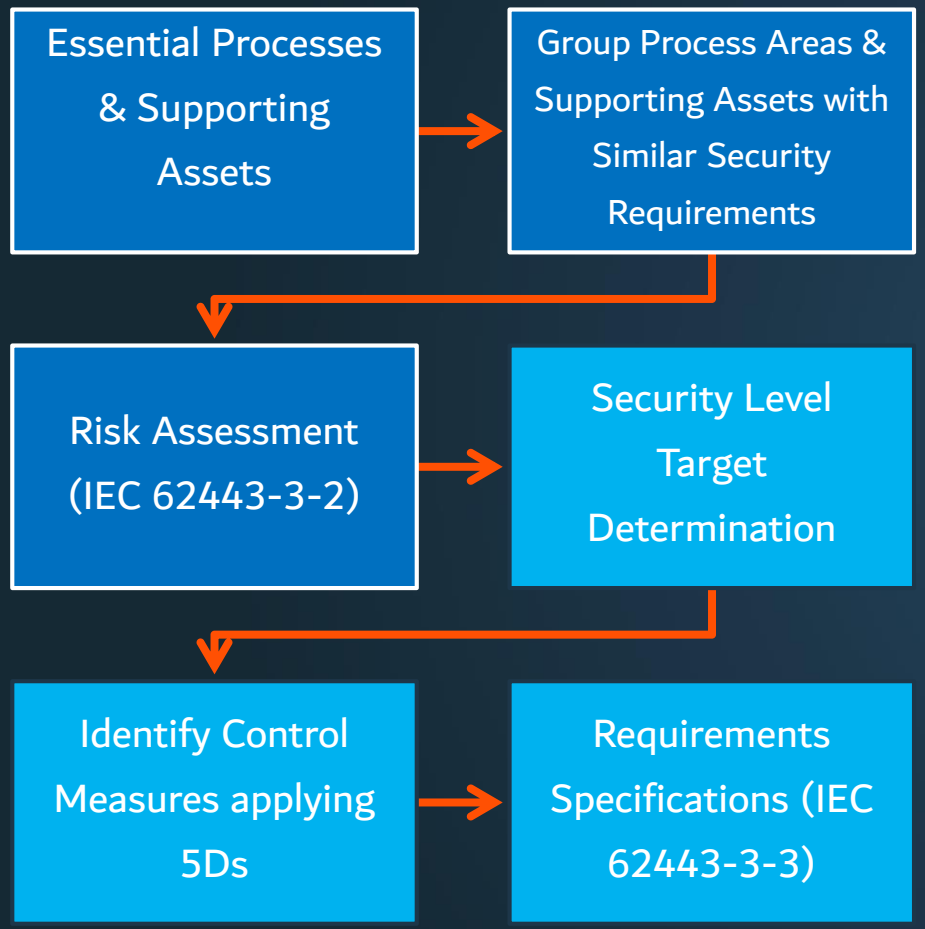
- **Asset Management**
  - Remote capability for multi-vendor IED monitoring, configuration/ settings management with version control. Data backup.
  - Cyber security objectives (e.g. IED firmware visibility utilizing IEC 61850 data model `LPHD.PhyNam`, event records, etc.)
- **Remote access to centralized disturbance records** upon trip signal or periodically or from local IED in proprietary or converted IEEE COMTRADE format. Remote disturbance analysis.
- **Remote SCS alarm investigations** to decipher grouped alarms and fault rectification.
- **Remote maintenance (vendor and internal staff),** e.g. IED parameterization support, data restoration, routine planned RCM activities, etc.
- **Systems commissioning** (e.g. point to point testing with SCADA/ control center).
- **Compliance reporting.**

Traditional Remote Access Model



Security Risk Assessment for Remote Access Requirements

IEC 62443 Risk Management Process

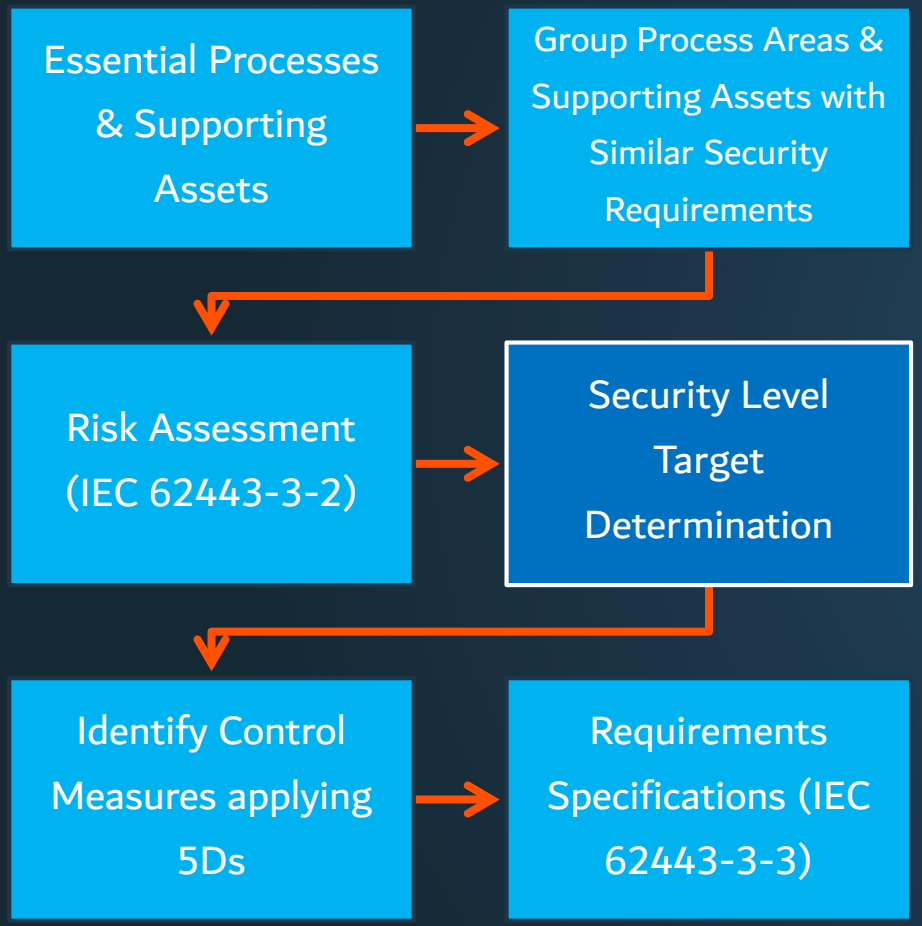


Risk Assessment (Example)

Threat	**System Under Consideration (SuC): Protection IEDs**					
Process / Threat	System Impact		Process Hazard Analysis (PHA)		Current Controls	**Risk Rating**
Remote Disturbance Records Acquisition	Major Consequence	Severity	Major Consequence	Severity	Hazard / Cyber (62443-3-3)	MAX(Cyber / PHA)
Unauthorized access to protection IEDs/ Station LAN.	Tampering protection settings impacting Network stability in the event of fault.	High (20)	Lost Time Injury. Substation offline; primary equipment damage.	Extreme (24)	Physical isolation. Locked cabinets. Protection check zone scheme.	Extreme (24)

Security Risk Assessment for Remote Access Requirements

IEC 62443 Risk Management Process



Example (cont.) – Risk Evaluation

Risk	CRRF	SL-T
1	0.25	0
2	0.50	0
3	1.00	0
…	…	…
24	6.00	3
25	6.25	3
26	6.50	3
27	6.75	3
28	7.00	4
29	7.25	4
30	7.50	4

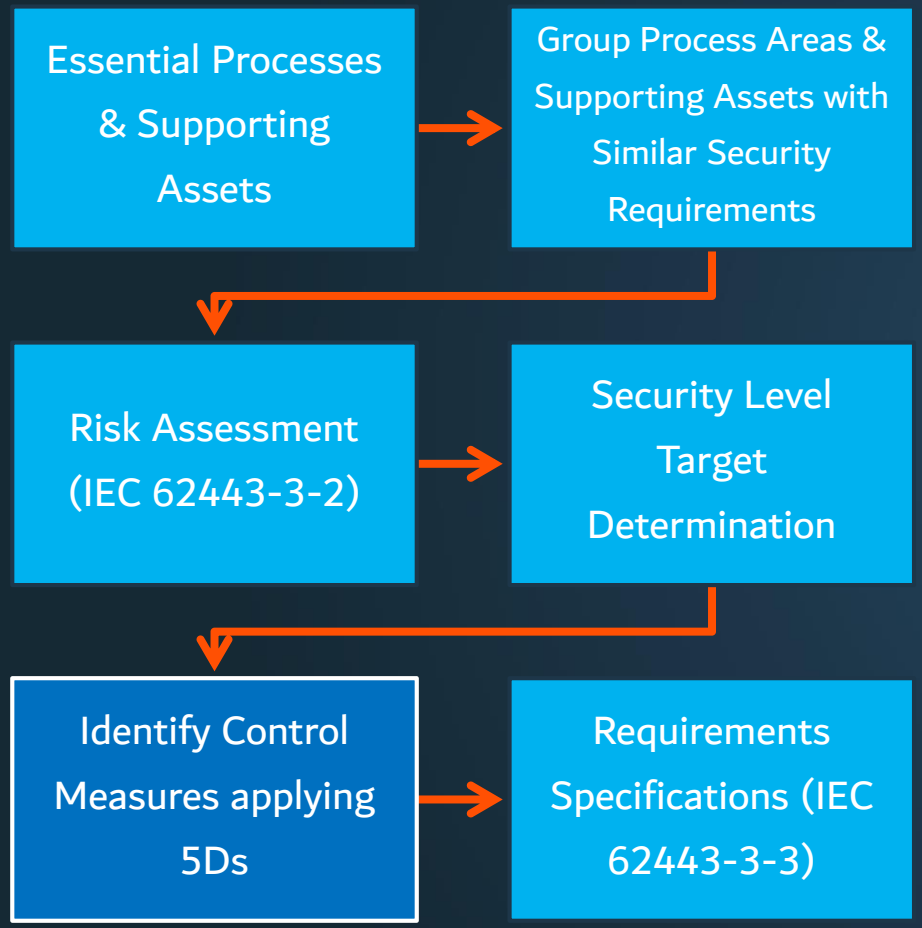
Given organization' tolerable risk score (Tolerable Risk) =< 4

Cyber Risk Reduction Factor (CRRF) = Identified Risk (Unmitigated) / Tolerable Risk.

24 / 4 = 6; corresponding **SL-T is 3**

Security Risk Assessment for Remote Access Requirements

IEC 62443 Risk Management Process

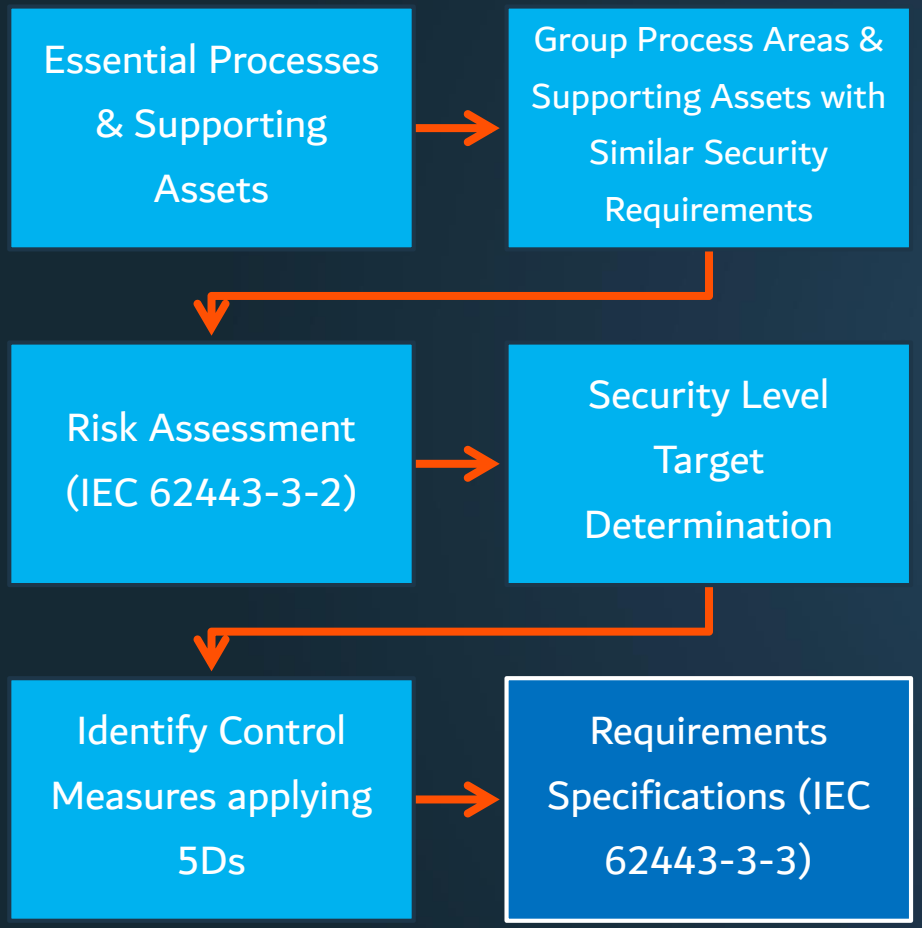


Example (cont.) – Risk Mitigation Identification – 5Ds

Risk	Potential Mitigation (IEC 62443-3-3 input)				
Process: Remote disturbance record acquisition & investigations	Deter	Detect	Delay	Deny	Defeat
Unauthorized access to protection IEDs leading to tampering protection settings impacting Network stability.	Policy. Security Awareness & Culture. Notices during remote logon.	Network/ Host Intrusion Detection System.	Removal of default password on IEDs and related software tools. Honeypot.	Prevent direct access to IEDs and instead utilize automated fault record collection system from IEDs and/or dedicated DFRs. Network segregation; controlled access points.	Remote access session monitoring. Cyber security vulnerability management.

Security Risk Assessment for Remote Access Requirements

IEC 62443 Risk Management Process



Example (cont.) – Requirements Specification

Security Service	Sub Function (Procurement Language Extracts)	Security Level Applicability	
		Level 1 Process Level	Level 2 Station Level
2.1 Network Segmentation & Segregation for Remote or Local Access	2.1.1 The proposed solution utilizing packet switched Local Area Networks (LANs) shall enforce segmentation and segregation of subnets based on the respective classification (see PL04). Access to a network segment with a higher level of trust shall not be accessible by a network segment of lower trust unless where explicitly permitted after fulfilling the requirements of the target network segment. SLT-4 - Point 4: Network segment traffic filtering shall be performed by means of an inline DPI-enabled firewalls that shall specifications provided in attachment FL01 (protocol decoder, message inspection, message value threshold control, etc.). SLT-4 - Point 5: Remote access for end-users shall not permit direct access to any of the IEDs; all such connections shall terminate in Level 2.5 (Station DMZ) only after successful two-factor authentication and/or digital relay contact closed by the Transmission Control Center via the SCADA after passing manual authentication mechanisms. Three failed logon attempts shall be recorded in SCADA as alarms relayed via the common station IED.	**SLT-4**	**SLT-4**
7.3 Authentication Credential Management	7.3.3 The proposed solution shall be dispatched to <acquirer> with all factory default credentials updated to match the required specifications in attachment DF01. The proposed solution shall further deliver the capability to change all set credentials upon installation/ commissioning of system components and during maintenance without any time or usage constraints. SLT-3: Point 2: Suppliers shall certify that no hardcoded or undocumented credentials exist within the supplied equipment/ systems. Where such credentials are identified later prior to asset decommissioning, the supplier shall be held accountable and shall be liable for defect rectification works as specified in attachment SL08.	**SLT-3**	**SLT-3**

Further Reference for Remote Access & Last Words

Standards & Regulations

- NERC CIP-005 R2
- IEC/ISA 62443
- ISO/IEC 27001:2013
- DESC ICS Standard v2
- IEC 62351 (access control and monitoring)

Guidance

- NIST SP 800-82
- NATF Vendor Remote Access Guidance (NERC compliance)
- DHS/CPNI Configuring & Managing Remote Access for ICS
- NIST SP800-46
- NSA Securing IPsec Virtual Private Networks

Technology Solutions (Reference only)

- BeyondTrust (Bomgar);
- TDi ConsoleWorks
- WALLIX
- Claroty SRA
- CyberArk

Technology alone is not the solution!

Strategy with defined processes for cyber operations and maintenance supported by trained staff are essential.

Technology will have vulnerabilities, e.g.:

- Secomea CVE-2020-14500
- Moxa CVE-2020-14511
- HMS eWon CVE-2020-14498

THANK YOU

https://www.linkedin.com/in/tahirsaleem

SMART GRID FORUMS

Smart Grid Cybersecurity 2020
7 October 2020 | Virtual Conference

SMART GRID FORUMS | IEC 61850 Global 2020
28 - 29 October 2020 | Virtual Conference