Improving Cybersecurity Through a Centralized Password Management System

Ammad Ali and Husam Ahmed
Schweitzer Engineering Laboratories, Inc.

Original edition released October 2019

IMPROVING CYBERSECURITY THROUGH A CENTRALIZED PASSWORD MANAGEMENT SYSTEM

Ammad Ali* and Husam Ahmed
Schweitzer Engineering Laboratories, Inc.

USA

***Summary*—With the expansion of power system communications networks worldwide, the growing number of digital devices, and the reliance on Ethernet-based protocols, there is a temptation to design a substation automation system that can be accessed remotely for efficient monitoring and control. However, this creates security challenges that go beyond physical security.**

The main challenge for any power system owner is choosing the most secure principle for the customized network infrastructure from a range of security standards, such as NERC CIP, NIST, and IEC 62351. The principle should dictate the methodologies and processes that will ensure secure access, authentication, and auditing for each electronic security perimeter and that will protect critical and noncritical assets from being compromised via internal or external Ethernet access points.

Substation field devices, such as intelligent electronic devices (IEDs) that are designed with a focus on power system availability and reliability, have fundamental security features. In addition, they are usually distributed across remote locations. Consequently, considerable cost, effort, and stringent procedures are required for personnel to manually control and manage password changes and user access levels for those IEDs.

For example, enhancing accountability by cross-referencing physical security event logs with the IED information from a settings change is just one of the many challenges that the system owner has to undergo in the case of an unwanted event. Most higher-level communications media have hardware and software features that protect themselves and their peer devices and which consider multilayer security. Unfortunately, the security of bay-level devices is often undermined by the lack of proper access management systems.

Therefore, some users have begun identifying secure, convenient, and modern mechanisms to automate access levels and IED password management for their power facilities. Whether these facilities comprise decentralized substation systems or centralized architectures, a system can be designed to achieve the centralized user access control and IED password management.

This paper discusses ways to implement such a centralized user and password management system to enhance the security of secondary system infrastructure. It also discusses the encryption for security certificates, user authentication, complex password management for IEDs, and automatic auditing of the whole process. Finally, the paper discusses how this system can enhance any existing commissioned substation infrastructure without interrupting its operations.

***Keywords*—Centralized user management in power systems–Cybersecurity proxy services and password management system–Monitoring and controlling IEDs remotely–Secure engineering access.**

I. INTRODUCTION

Power system communications networks are growing, and they facilitate many critical operations in transmission grids and power plants. In the industry, these networks are referred to as operational technology (OT), and they usually handle critical assets. Hence, protecting them from internal and external cybersecurity threats is paramount. Power system operators are always looking for ways to enhance and secure these networks and minimize risks. Vulnerabilities in an OT network can lead to devastating attacks. The efforts to protect these critical assets pale in comparison to the amount of work needed to secure a system once an attack has occurred.

*Schweitzer Engineering Laboratories, Inc., 2350 NE Hopkins Court, Pullman, WA 99163 USA • papers@selinc.com

The introduction of strict policies and methodologies that incorporate multiple security standards is pivotal to providing the required security for power system infrastructure. Part of the larger security scheme includes the centralized access control and automatic password management (APM) system, which is discussed in this paper. The paper details how this security scheme can be smoothly implemented on either a live substation or a system under design.

Usually, SCADA and metering applications are the backbone of the daily operations of the electric power industry. The main purpose of such systems is to collect data from remote intelligent electronic devices (IEDs) and send them to a control center where an operator can act on them. A visual representation of the system gives human operators a view of the current substation statuses. Metering and data gathering applications are often limited to gathering very accurate power usage measurements or system statuses for the purposes of power management and visualization.

The amount of security applied to infrastructure should reflect the importance of the operations it provides and should mitigate any risks from unauthorized access. Effective security measures on each electronic security perimeter (ESP) [1] are more vital in a traditional SCADA system because of the added control capability and the importance of the SCADA function.

The APM system is one of those measures that strengthen the security of critical and noncritical assets in substations and ensure expected operations. APM uses embedded devices, which are substation-hardened access control peripherals that provide authentication, authorization, and accounting (AAA) proxy services for relays, IEDs, and other system-critical devices on Ethernet and/or serial networks. These devices provide an ideal access point to the ESPs for sites that fall under NERC CIP [2], NIST [3], and other regulations required by power utility and industrial specifications. The hardware uses a secure mechanism to configure, integrate, and commission even large and complex systems without any interruption.

II. Background

A growing number of sophisticated and complex IEDs are finding their way into substations. These computerized devices, such as digital processing devices, programmable logic controllers, equipment monitoring devices, digital protective relays, power quality meters, and metering devices, come with new challenges. The presence of these devices should change the way substation security is handled. In the past, security in a substation was limited to physical security. With the introduction of these modern technologies, securing assets has become more challenging and is not just limited to physical security.

NERC CIP requires entities to detect and mitigate malware threats and to maintain the most recent signature-based detection methods. NERC CIP standards also require a defense-in-depth posture [4], different protection layers, and certain types of controls on multiple access levels. Defense-in-depth is not one thing, but rather a combination of people, technology, operations, and adversary awareness. Proper analysis of system assets helps users to think about the right problems, and technology solves those problems by providing a set of tools that reduce risk. Organizations must constantly adjust and refine security countermeasures to protect against known and emerging threats. Systems should support preventative measures to block unauthorized access to critical assets and provide timely notifications to a centralized location. The systems should also perform detective measures to automatically log all the activities performed by authorized personnel [5].

Cyber assets, such as control and protection IEDs, must be assessed to determine if they support reliable operation of the bulk electric system (BES), i.e., whether their impact plays a significant enough role to be covered by NERC CIP [6]. The impact analysis looks at both time-based impacts and magnitude-based impacts, and the analysis is heavily dependent on how a particular cyber asset is used at a specific utility. For example, a market operations system at one utility may not play a reliability role, while at another it is tightly integrated into BES operational specifications [6].

NERC CIP requires the owners of high- or medium-impact BES cyber assets (embedded devices) to record and deploy procedures to protect against all kinds of malware, commonly referred as malicious code. The standards require utilities to randomly generate complex passwords and systematically deploy them at critical cyber assets, where possible [5]. The solution providers must determine, based on a BES cyber system's nature, which cyber assets are susceptible to intrusion and deploy proper plans and processes to mitigate the risks. There are numerous options available, including traditional antivirus solutions for common operating systems, whitelisting solutions, network isolation techniques, intrusion detection and prevention solutions, and so on. But, those options might not be applicable to IEDs that have closed, embedded operating systems [5]. Those IEDs have no updateable software, and their executing code cannot be altered, so they are considered to have an internal method of deterring malicious code. IED manufacturers should continuously recognize the need to protect their embedded devices.

The design of these embedded devices should include strong whitelist protection that does not allow additional software to be installed. The devices should also have digitally signed firmware and mandatory access controls. They should compartmentalize each

application process and only allow access to the memory a process needs to accomplish the task it is responsible for. The embedded devices should include self-testing that continually checks running code against a known good baseline version of code in nonvolatile memory, and they should remain malware-free because they do not accept, store, or execute third-party programs. They should only accept manufacturer-generated firmware and only run this firmware after it passes verification (e.g., hash key checksums) [7]. With all of these protections on the relays, they can only be manipulated if their passwords are known.

Most IEDs provide two types of connections. The first is the device maintenance serial port. This port is designed to allow configuration, setup, settings retrieval, harmonics readings, waveform data collection, and so on. Access is usually accomplished using a laptop locally. The second type of IED connection is an Ethernet port, which supplies data from the network and SCADA through a direct connection or from a centralized system that performs remote engineering access or other operations and functions.

Most substation gateways have a pass-through capability to provide remote IED access. However, this option has proven to be not very secure. As the use of IED Ethernet capabilities in substations becomes more prevalent and required, the security risk compounds for mission-critical data and information. Hence, the need for more secure device access (local and remote) becomes paramount. Accessing protective relays remotely is very tempting and is, in some cases, necessary. But, not having proper security measures in place, such as password protection and an authorization system, can widen the attack surface for threat actors.

III. Typical Control System Architecture

A telecommunications network can be as simple as two devices linked together for information sharing or as complex as the internet, involving many devices serving a multitude of purposes. Network devices need a common model for interconnectivity across various communications media, manufacturer equipment, protocols, and applications. Connecting integrated IEDs creates a trusted, physically distinct local-area network (LAN). LANs can be created from using EIA-232, EIA-485, Ethernet, and/or other connections. They may support one or more communications protocols [8]. Information moves within the LAN via SCADA and engineering access.

SCADA conversations involve constant messaging between a control center and IEDs across the LAN to acquire present values for predefined data points and to perform control operations. Engineering access conversations involve on-demand data acquisition between a user or automated process and a LAN device to support virtual terminal connections and file transfers [8].

Typical SCADA applications include the following:

- Centralized APM systems.
- Substation gateways and data concentrators.
- Human-machine interfaces (HMIs) at the substation level and at the control center level. At the substation level, the HMI provides full monitoring and control as well as monitoring of other substations. The control center HMI provides full monitoring for all of the substations, depending on the role-based user account access.
- Engineering access from a designated engineering workstation to a particular IED at a substation to enable relay setting configuration.
- Disturbance fault recording, event reporting, and analysis.
- Alarm logging, management, auditing, and reporting.
- Data management, trending, and historian.
- Secure time synchronization.
- Integration of substation IEDs, via IEC 61850, with other systems, such as partial discharge systems, uninterruptible power supplies, and dc systems.
- IEDs interfacing with higher-level systems through various secure industrial protocols.
- Power management and load-shedding systems.
- Localized authentication servers using Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-In User Service (RADIUS) protocol.
- System logic processors.

The network design shown in Fig. 1 uses a double-contingency, substation-hardened switching communications architecture configured with failover Ethernet. The figure shows how APM devices are deployed in a typical power system network. This arrangement creates a system in which a minimum of two separate hardware or cabling failures must occur before communication are lost to any substation.

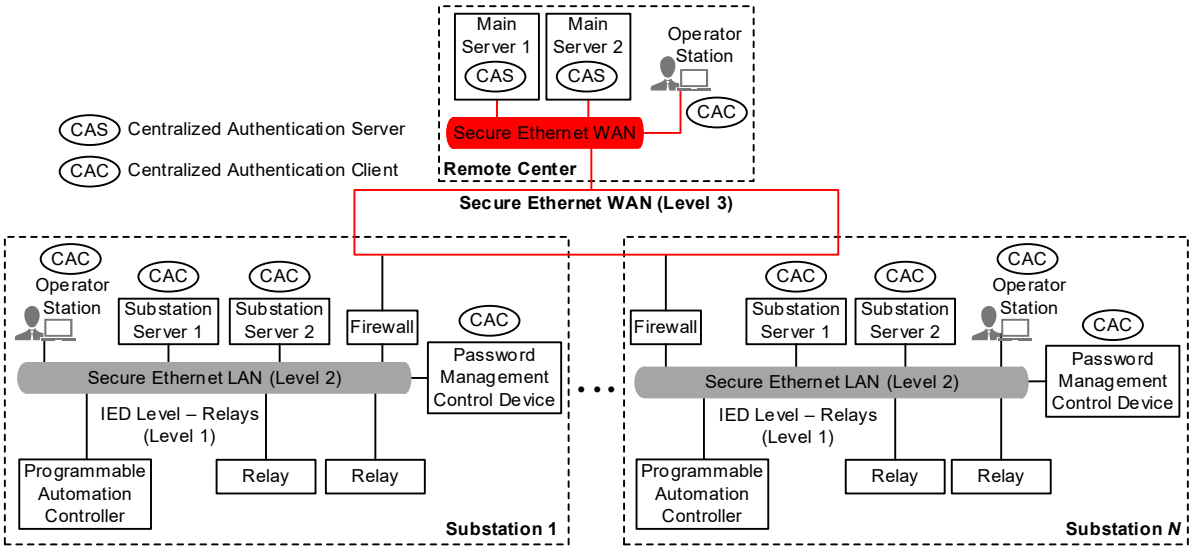

Fig. 1. Typical power network architecture with sample APM system.

The levels of a typical architecture are described as follows:

- The Level 1 network is within the switchgear. It comprises networked IEDs with a common redundant interface to the Level 2 network. It also includes their interconnecting cables. This level includes IEDs whose credentials are controlled by the APM system.
- The Level 2 network is within an individual substation. Level 2 components include substation automation panels and APM control devices. This level includes the proxy access devices as centralized authentication clients (see Fig. 1). The operator workstations can provide secure engineering access to the IEDs after going through an AAA process.
- The Level 3 networks interconnect the individual substation automation systems and the centralized control center system with a ring architecture. This level includes centralized authentication servers that provide secure authentication of user access to multiple centralized authentication clients at the substation level, as shown in Fig. 1.

Embedded and secure satellite-synchronized clocks at the substation level provide IRIG-B time outputs to synchronize all IEDs to within 1 µs, complying with IEEE and IEC relay standards. All the station-level devices are also synchronized with these high-accuracy time sources; it is vital to record security logs with accurate time stamps.

IV. The Need For Centralized APM Systems

A. The Importance of Strong Passwords

There is a lot of pressure for utilities to improve the security posture of their networks. While it is good that the industry is moving toward more security in their infrastructure, utilities need to accomplish this change without affecting the availability of their systems. In other words, they should move forward at a pace that maximizes reliability rather than changing procedures and security architectures all at once.

In energized systems, it is always a challenge for power utilities to deploy a large-scale access control system. Products, principles, procedures, and standards need to be meticulously considered to make sure that the most reliable and secure solution is deployed without interrupting critical operations. However, it is equally demanding to adapt access control standards and principles during the design stage of a project, well before deployment.

The security shortcomings of default and static passwords are well known. Default passwords and other generic accounts are often left in place even at commissioned systems where the cyber assets are in use. However, these default credentials are commonly published in manufacturers' documentation and are readily available on their websites.

Systems that must protect information and services, or allow only certain people or systems access to information and services, require access control capabilities configured in compliance with the principle of least privilege.

"To prevent attackers from predicting users' text-based passwords, and hence impersonating users, system administrators typically require that users select passwords according to a password-composition policy designed to make users' passwords harder to predict. Such a policy may require, for example, that passwords exceed a minimum length, that they contain uppercase letters and symbols, and that they do not contain dictionary words … The intention is that the end user will change the default password to something unique and strong, but many end users, for ease of use, leave the password as the default," [9].

Similarly, when selecting passwords at IED level or user access level, avoiding common words or number sets is essential. "Humans … have only a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed," [3]. To address these kinds of security concerns, the APM system has eliminated the need to increase the complexity of these memorized secrets at the IED level.

"The most notable form of these is composition rules, which require the user to choose passwords constructed using a mix of character types, such as at least one digit, uppercase letter, and symbol. However, analyses of breached password databases reveal that the benefit of such rules is not nearly as significant as initially thought, although the impact on usability and memorability is severe…Password length has been found to be a primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords," [3].

"There is a list that comes out each year, covering the top 25 most popular passwords. Repeatedly, year after year, passwords like '123456,' 'password,' 'qwerty,' 'baseball,' 'football,' 'Yankees,' 'Steelers,' and 'Lakers,' are found on the top of that list. Common numbers or words are not cryptographically secure. Passphrases, substitution, and slang are all better ideas for creating stronger passwords," [9]. For example, a phrase like 'Fahad And Sehrish Like To Have Hummus and Bread For Dinner!' becomes 'F&SL2HH&B4D!'. This is not a dictionary word; contains letters, numbers, and symbols; and is long yet memorable [9].

With an APM system, the assignment of complex passwords to IEDs is handled by proxy devices while users generate and remember their own sign-on passwords to access the centralized accounts. Keep the information in this subsection in mind when defining user sign-on credentials.

As simple as not using default passwords may seem, the practice is sometimes overlooked, usually because of asset management challenges. One prominent manufacturer of controllers for critical infrastructure had their default credentials leaked to the internet [10], where they circulated for years. Stuxnet malware [11] took advantage of default passwords, allowing access and control of the targeted SCADA system. Keeping default passwords in any SCADA equipment poses a significant risk of unauthorized access. Using strong passwords is necessary for a defense-in-depth strategy.

B. The Need to Change Passwords at Regular Intervals

A complex password not only protects a specific device against unauthorized access but also safeguards the integrated system and helps ensure the reliable operation of a substation or SCADA system. However, if a password is disabled, easily predicted, or at default, systems are at risk. Intruders can use the system susceptibilities to distribute false data and disrupt related systems in the control systems. Strong passwords are virtually impossible to guess and may take hundreds of thousands of hours to crack. Easy passwords can be guessed or cracked in minutes. Hence, it is extremely important to maintain the security of the system by having centralized user accounts and using strong passwords in communications processors, IEDs, and access point devices, and to frequently change them using automated encrypted proxy channels [10].

C. IED Password Management Capabilities

Substation field devices, such as IEDs designed with a focus on power system availability and reliability, have built-in security features. Such IEDs should support complex passwords, long passwords (i.e., 12 characters or more), multilevel and multidiscipline discrimination access control, access alerts, failed access attempt alerts and pushback, inactivity timeouts, and blocking of unused serial and Ethernet ports to implement a defense-in-depth strategy [4].

Implementing manual password management on a large scale while enhancing the control, security, and situational awareness requires considerable cost and effort. Stringent procedures are needed for personnel to physically control and manage password change processes and user access for those IEDs. For more convenient, better controlled, and enhanced access control, a centralized and automated mechanism should be used.

D. Central Management of Passwords

Every power system owner has unique requirements for implementing network security, asset management, access control, and auditing and monitoring systems. The wide range of requirements, including those from carefully selected standards organizations (IEC, IEEE, NIST, NERC CIP, and others), force manufacturers to impose a centralized system for digital access control and device management. The requirements also call for AAA for the whole infrastructure as a baseline. Without an automated, digitally encrypted system in place, manually managing the assets in each substation would be a lengthy, costly, nonsecure, and inefficient process.

A centralized APM solution can fulfill these requirements, provide flexibility, and fit the existing system for easy migration, even in energized systems.

V. Access Control in Password Management Systems for Secure Engineering Access

Access control and user management are usually attained using proxy services. The idea behind proxy services is that they convert locally shared credentials with limited logging into user-based, centralized access with full-user activity logging. The proxy consists of security access points that allow specific users access to authorized devices without those users having to know the actual IED passwords. However, they are required

to know their own user credentials. This greatly simplifies password management and supports swift, system-wide password changes and secure engineering access when required. It also simplifies the removal of a user or group from the system.

Proxy services also provide a method of tracking specific user activities over the whole system. The access point device logs all activities, records individual commands sent to every device it manages, and generates reports to create auditable user activity trails. The system performs the following actions at a minimum:

- Authenticates users with local or centralized user accounts.
- Authorizes which users can access what devices and at what access levels.
- Provides accountability by recording the commands sent to all managed devices.

Centralized authentication eases management concerns by allowing the control and configuration of user access from a single point: the centralized authentication server. In a centralized authentication system, a device using centralized authentication does not authenticate an accessing user. Instead, it passes the credentials back to the authentication server, which, in turn, performs the authentication function (see Fig. 2). The LDAP or RADIUS client only allows the user access if the server reports that the provided credentials are valid. Adding or revoking access is simplified because all credentials are managed at the server instead of at every client. Revoking a user's access to an entire system is now one simple operation on the authentication server.

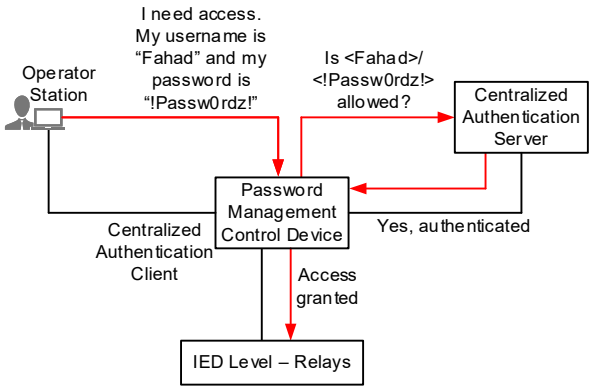

Fig. 2. Access control authentication flow.

The whole transaction uses several mechanisms, like public key infrastructure (PKI) deployment [12], TLS for encrypting and authenticating, and X.509 certificates and digital signatures to ensure data confidentiality, integrity, and availability.

The certificate chain, also known as the certification path, is a list of certificates used to authenticate the LDAP/RADIUS server. The chain begins with the certificate of the LDAP/RADIUS server, and each certificate in the chain is signed by the Certificate Authority (CA) identified by the next certificate in the chain. The chain terminates with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in the chain are verified by the proxy clients until the root CA certificate is reached. The certificate chain and binding ensure that unauthorized personnel and devices are not able to spoof the active sessions.

A digital signature, which is part of the process, is created by computing a hash of the certificate and encrypting that hash with the issuer's private key. This signature is then attached to the certificate. To verify the authenticity of the certificate, the certificate and signature are first separated. A hash of the certificate is computed, and the signature is decrypted using the issuer's public key. These two results are compared, and if they match, the system knows that the certificate is authentic.

Fig. 3 shows an example of a server-client transaction procedure over TLS.

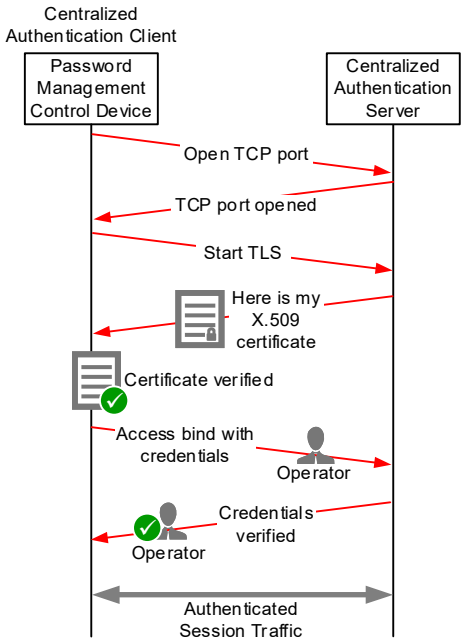

Fig. 3. Client-server authentication and authorization session over TLS.

The system imposes user-based access controls before allowing communication to IEDs. When a user logs in to the proxy client, the user is authenticated using a centralized authentication server via secured Transport Layer Security/Secure Shell (TLS/SSH), LDAP, or RADIUS. The access point clients receive user authorization directly from the centralized authentication server and then manage the entry of the passwords of specific IEDs so that the user never needs to know them. The proxy devices do not pass user-initiated commands directly to the devices to which they are connected. Instead, the proxy devices record the command and check it for predefined scripts that interact with the end-managed IED. If a command

matches a script (e.g., “read only access” to an IED), then a script is invoked for the destination device. In effect, the entry of a command becomes the execution of a script by the proxy device. The results returned by the device, as the script, are passed back to the person or computer process that initiated the exchange.

An integral part of the system enforces automatic session termination when there is no activity on the secured engineering access. As observed in control systems around the globe, serious security lapses have occurred when a lack of remote session termination led to the creation or unintentional support of hidden channels and denial-of-service situations. Regardless of the method used for remote engineering, active channels need to be configured to terminate under certain conditions.

VI. IED Credential Control in an APM System

Automated IED password management swiftly ensures that passwords are changed regularly without any interruption to IED operations and that passwords conform to complexity rules for stronger security. Enforcing strong passwords on IEDs and having the passwords automatically changed on a configurable schedule satisfies regulatory password requirements and ensures that no weak or default passwords are in use on critical assets.

The concurrence of multilayer proxy and APM systems provides security against unauthorized access at each ESP. The system can give personnel access only to those functions they require. Though many different levels of access are used to differentiate users and processes, the most essential levels are as follows [8]:

- Connect Only is the lowest access level. It provides only IED identification. For example, this could be used if the operator only needs to view the current status.
- Read Only is one level higher than Connect Only. It allows viewing of IED parameters and information. For example, this could be used if the technician needs to view and download relay settings.
- Elevated Access is any level higher than Read Only. For example, this could be used if the engineer needs to view, download, and change relay settings.

These categories of access levels provide various combinations of control abilities, extended data acquisition, data clearing and/or entry, and configuration manipulation. The management of the global accounts in IEDs behind the proxy includes the ability to rotate passwords on a scheduled or triggered basis, ensure that the randomly generated passwords are complex enough to meet or exceed NIST standards, and remove the need for the end user to know the global account password. The global password switches from an authentication role to an authorization role. The system manages IED passwords by using information sent by a predefined database at the time of initial commissioning. The system always separates out the steps for generating new IED passwords and applying them and for reverting the IED passwords to a default state in extenuating circumstances. This makes the system more unique for maintenance purposes and for keeping long-term audits for the company’s use.

VII. Security Situational Awareness Enhancement Using User Access Activity Monitoring

The APM access proxy solution takes system situational awareness to another level. User activity is completely monitored. Full commands and attempts are logged with time-stamped information about action as well as user and connection details, such as the source IP address. Audit reports from various proxies can be automatically collected and stored, as shown in Fig. 4.

In addition, information regarding access to the proxy and its status is logged and can be sent using Syslog Protocol to security monitoring system servers.

Commands and Devices Created on 26/10/2015 by Ammad
Dates Covered: 2015-10-15 to 2015-10-26

User	Command	User's Address	Timestamp
Alex	sta	192.168.2.24	25/10/2015 16:00:07 UTC
Alex	quit	192.168.2.24	25/10/2015 16:00:04 UTC
Alex	2ac	192.168.2.24	25/10/2015 15:59:58 UTC
Alex	acc	192.168.2.24	25/10/2015 15:59:51 UTC

Fig. 4. Sample audit report.

VIII. Conclusion

The overall system after deploying APM has a stronger security posture than one that uses traditional global accounts. The system greatly enhances the capabilities of operators to securely manage and operate power system functions with secured, centralized access control. The system adds value by compiling and exceeding the security standards that industry practices call for. Traditional methods with manual accounts have inherent vulnerabilities because everyone who uses a mechanism can threaten the critical infrastructure.

With user-based accounts and an APM system, all assets are secured in a seamless, systematic way that keeps critical operations readily available, reliable, and more secure than ever. The single sign-on capabilities of the proxy services require a device to be aware of the passwords of all the protected devices behind it. The combination of the internal script engine and the password knowledge gives the device the ability to manage the passwords of all managed devices, enforce strong passwords, and provide audit reports of all password changes.

When password changes are required, either because of routine maintenance or regulatory requirements, users are not required to remember new complex passwords for IEDs; they only need to remember their own personal password. This increases security by reducing the need to write passwords down and by mitigating the chance that an active password will be leaked.

Moreover, the system delivers a unified, purpose-driven functionality that exceeds AAA requirements for secure engineering access activities like settings retrieval or updates, event retrieval, and so on. Auditing capabilities (like granular Syslog collection, audit reports, and other security reporting mechanisms for tracing ports, devices, or user-based activities) make power monitoring and control operations smoother and more secure and also help system owners allocate resources efficiently and manage wide-area assets optimally.

IX. Acknowledgment

The authors gratefully acknowledge Colin Gordon, Amandeep Kalra, and Jason Dearien for reviewing this paper. They also offer a special thanks to Zafer Korkmaz and Swaminathan Rajkumar for their reviews, support, and motivation throughout the process.

X. References

[1] North American Electric Reliability Corporation, "Glossary of Terms Used in NERC Reliability Standards," *Reliability Standards for the Bulk Electric Systems of North America*, April 2010. Available: https://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf.

[2] North American Electric Reliability Corporation, "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets," June 2010. Available: https://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Critcal_Cyber_Asset_ID_V1_Final.pdf.

[3] National Institute of Standards and Technology, "NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management," June 2017. Available: https://pages.nist.gov/800-63-3/sp800-63b.html.

[4] C. Ewing, "Engineering Defense-in-Depth Cybersecurity for the Modern Substation," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[5] NERC Standard CIP-007-5 – Cyber Security — Systems Security Management. Available: https://www.nerc.com.

[6] NERC Standard CIP-002-5.1 – Cyber Security — BES Cyber System Categorization. Available: https://www.nerc.com.

[7] Schweitzer Engineering Laboratories, Inc., "The SEL Process for Mitigating Malware Risk to Embedded Devices," September 2015. Available: https://selinc.com.

[8] D. Dolezilek, "Methods for Securing Substation LAN Communications," proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2003.

[9] J. Smith, J. Pereyda, and D. Gammel, "Cybersecurity Best Practices for Creating Resilient Control Systems," proceedings of Resilience Week 2016, Chicago IL, August 2016.

[10] U.S. Department of Homeland Security, "ICS-ALERT-11-186-01: Siemens SIMATIC Controllers Password Protection Vulnerability," ICS-CERT, July 2011. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-186-01.

[11] D. Kushner, "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware That Stymied Iran's Nuclear-Fuel Enrichment Program," February 2013. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[12] D. Wood, "PKI, The What, The Why, and The How," *SANS Institute InfoSec Reading Room*, 2002. Available: https://www.sans.org/reading-room/whitepapers/vpns/pki-what-why-764.

XI. Biographies

Ammad Ali is an Application Engineer III with Schweitzer Engineering Laboratories, Inc. (SEL), Middle East. He earned his bachelor's degree in electronics engineering from the GIK Institute of Engineering Sciences and Technology in Pakistan. He is member of IEEE and has approximately ten years of experience in the field of controls and automation. He has contributed to projects with various utilities and industrial customers in the Middle East and North Africa region.

Husam Ahmed is a technical business development manager with Schweitzer Engineering Laboratories, Inc. (SEL), Middle East. He has a B.S.C. in electrical engineering from the University of Bahrain. He has 12 years of experience with SEL, where his focus is on substation automation systems and power management solutions. Recently, he has been involved in the cybersecurity field for electrical systems. Prior to SEL, Ahmed worked for five years in the fields of process automation, metal manufacturing automation, and electrical systems.