

Open Enterprise Architectures for a Substation Password Management System

A. GAUCI, JR. ENG.¹, A. HAMEL, ENG.²
Cooper Power Systems¹ (CAN), Cooper Power Systems² (CAN)

SUMMARY

Utilities have been busily determining which devices inside the substation are critical cyber assets (as defined by the NERC CIP standards), documenting them, and finding ways to enhance the already present security features of these devices. This can be challenging for account management as different IED manufacturers have different means for securing their devices.

NERC CIP-007 makes provisions for account management requiring that a responsible entity implement a policy to minimize and manage the scope and acceptable use of accounts, including factory default accounts. This policy should include methodology to ensure that required accounts have their passwords changed upon being put into service, passwords are easily updatable on a regular basis and upon personnel termination or change of assignment, and include a password change audit trail.

These critical IED devices from multiple manufacturers use many different types of protocols, configuration methods, and communications mediums. A natural connection point to these IEDs would be a secure substation gateway that supports connection of modern devices and legacy devices that can be found in an average substation.

Historically, many utilities' information technology (IT) departments have used password management applications for management of their telecommunications equipment and server passwords. These established tools provide for secure password storage and automated device password changing.

Off-the-shelf Enterprise IED management applications already exist to provide secure communications for services such as automated event retrieval, automated configuration management, and remote IED maintenance capabilities to a variety of substation IEDs.

One such IED management application is being adapted to use a standard interface to connect to many established password management applications. This will allow utilities to utilize the

password management functionality of their preferred choice of IT-established application over the Utility Enterprise Application's secure communication infrastructure. Integration between the IED management application and password management application ensures that automated processes are continually able to access IEDs, even after device password changes.

KEYWORDS

Cyber Security, IED Management, Passwords, Account Management, Standard Interfaces, NERC CIP.

1. INTRODUCTION

With the introduction of standard technologies into the Utilities' telecommunications and control systems, cyber security is becoming a very important and contentious issue. The North American Electricity Reliability Corporation (NERC) has the task of developing guidelines for Critical Infrastructure Protection (CIP). These guidelines are a cyber security framework to protect critical cyber assets that support the operation of the bulk electric system. These critical cyber assets are Intelligent Electronic Devices (IEDs) such as protections, Remote Terminal Units (RTUs), and Digital Fault Recorders (DFRs). These guidelines are described in NERC CIP standards CIP-002 to CIP-009.

Account and password management of critical assets is covered by the NERC CIP standards. Asset account passwords must be changed periodically. This can be a daunting task to consider — manually changing the passwords of hundreds of devices. Using automated services can be difficult also, as the services regularly used in the Information Technology (IT) field lack the required means for changing the password on devices that were designed with proprietary protocols and security schemes, and using diverse means of communications.

Utilities' IT departments utilize password manager services to manage telecommunications devices and servers. These trusted and well-established tools can easily store and manage password changes in a fully encrypted database with full logging.

Some utilities already implement enterprise-level services for managing substation IEDs. These services include automated event retrieval, secure remote maintenance functionalities, and device configuration management. With this communications infrastructure already in place, the next logical step is to utilize it to meet NERC's password management guidelines.

A standard interface could be developed between these two enterprise-level applications to expand the utilities' existing password management application to use the IED management application infrastructure. The IED management application would be allowed to securely access the password information, so that it may continue to access field IED for continuation of its own services.

2. SUBSTATION IED CHALLENGES

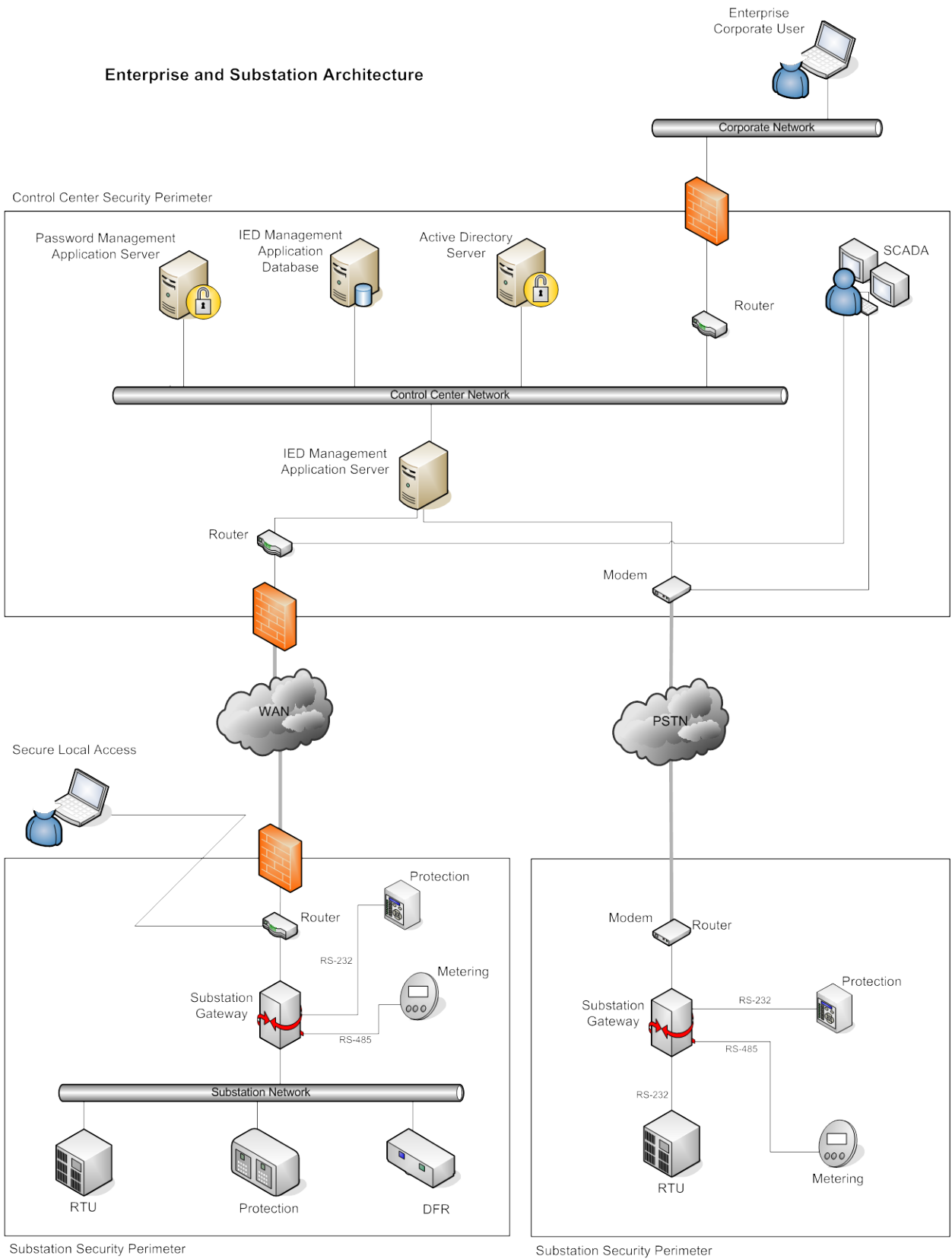
The substation can contain many different types of IEDs, from power system protections to Supervisory Control and Data Acquisition (SCADA) devices to a plethora of telecommunications equipment. These devices may use different communications methods for providing maintenance information such as connection via an Ethernet network or using serial communications such as RS-232 or RS-485.

SCADA connections on these IEDs can also use many different types of Application Layer protocols. The most standard of these are protocols such as DNP3 or MODBUS; but, more obscure proprietary protocols can be found with some older legacy devices. These devices also have different methods for configuration and maintenance access. For example, one commonly used protection utilizes MODBUS for its configuration, while another vendor uses plain text ASCII commands.

These devices also have different security profiles for device access and configuration. Some devices have pre-configured user access levels while others allow the user to set desired

usernames, passwords, and credentials. For example, one common protection manufacturer has two hard-coded security levels; these levels must be accessed in a consecutive order with the lowest first level being accessed first.

Enterprise and Substation Architecture



3. NERC CIP

NERC is the responsible body for developing the CIP standards and determining compliance to the standards through audits. NERC CIP-002 requires identification of critical assets that support the reliable operation of the Bulk Electric System (BES). According to CIP-002-1-R1, the following are considered to be critical assets:

- Control centers and backup control centers.
- Transmission substations that support the reliable operation of the BES.
- Generation that supports the reliable operation of the BES.
- Systems and facilities critical to system restoration, including black start generators and substations in the path of system restoration.
- Systems and facilities critical to automatic load shedding capable of shedding 300 MW or more.
- Special Protection Systems that support the reliable operation of the BES.
- Any additional assets that support the reliable operation of the BES that the utility deems appropriate to include.

Supporting these critical assets is a number of critical cyber assets at both the control centers and substations. For example, some of the applications that would be considered critical cyber assets include real-time monitoring and data exchange, automation, power system modeling, and any cyber asset that has the ability to communicate outside an electronic security perimeter with a routable protocol.

Account management encompasses the administration of local or built-in accounts on any device with communication capabilities. Account management practices for critical assets are defined by NERC CIP-007-1-R5. These practices include managing administrator, shared, and factory default accounts by removing, disabling, or renaming accounts where possible. This is not always feasible, so access to these shared accounts must be minimized and monitored. These accounts are required to be secured using strong passwords with at least six characters and must have their passwords changed annually.

4. EXISTING ENTERPRISE APPLICATIONS

With the requirement to change all IED passwords in an enterprise with a complete audit trail, lays the challenge of trying to implement the process with off-the-shelf, pre-existing enterprise applications.

4.1 Password Management Applications

Password management applications allow utilities to manage and organize the passwords used in their servers and telecommunications equipment. An encrypted database component stores the passwords of all managed devices, ensuring that only authorized users can retrieve the passwords of devices for which they have permission. An automation component can allow for automatically updating device passwords on a periodic basis or on a customized basis. Passwords can be set to expire after a short period, or once they are provided to an authorized user. The password management application can access the device and automatically change the password. Monitoring and

logging is provided for automated password updates and when a password is provided to a user for authorized access.

4.2 IED management applications

IED management applications allow utilities to leverage a sophisticated communications infrastructure in the field to provide such services such as automated power system event retrieval, IED configuration management and pass-through services for remote maintenance and engineering access. Event retrieval services periodically access substation protection IEDs and digital fault recorders, check for any new power system events and if found, retrieve them and store them in a central database accessible to authorized users. IED configuration management services can periodically access substation IEDs and compare the current IED configuration with the last approved configuration in a database — with any inconsistencies reported to an administrator. The pass-through service allows authorized users to remotely access approved substation IEDs in a secure manner — with a complete audit trail of logs and traces. When these applications are used in conjunction with a substation gateway, security can be enhanced by channelling all of these services through a single point of entry into the substation that can be encrypted.

4.3 Standard Interface

Currently a standard interface with an IED management application is being designed that will allow many different password management applications to utilize the extensive and diverse communications infrastructure of the IED management application. Utilities will be able to select the preferred password management system of their choice — allowing them the option of extending their current system to include substation IEDs. The password management systems known in the IT world will then have comprehensive, secure access to the devices available in the substation world — without the difficulty of interfacing with multiple vendors with obscure protocols and different security profiles.

5. INTERFACE DESIGN

The proposed solution is based on open architecture. The use of plug-in architecture allows for the integration of the IED management application with any password management application without being tightly coupled to a specific password management application. Open architecture is defined as a type of software architecture that allows adding, upgrading, and swapping components on-the-fly or with minimal service interruption — to maximize the quality attributes of the overall system.

The IED management application uses plug-in architecture to integrate with a third-party password management application. The plug-in architecture allows the IED management application to be de-coupled from any specific password management application. A configuration file or other mechanism is used to select the specific adaptor that allows the integration of the IED management application with the password management application. Other enterprise-level components can be integrated into the IED management application

using the same plug-in architecture pattern. These other enterprise-level components can be either proprietary or third-party components off-the-shelf (COTS).

Based on the analysis of the Business Use Cases (BUC), it appears that communication between the two enterprise management applications are either initiated by the IED management application or by the password management application. Thus, two interfaces have been defined to handle all of the Business Use Cases (BUC) requirements.

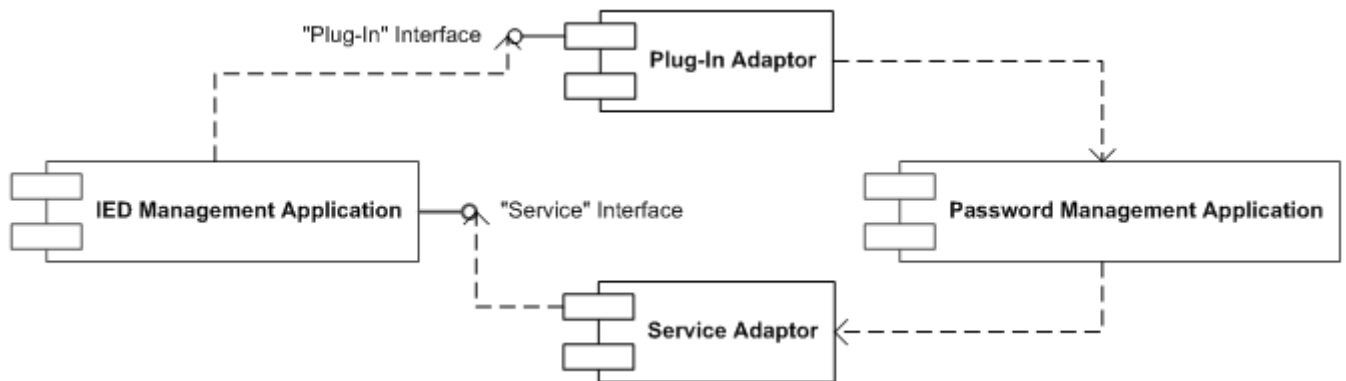
The first interface is referred to as the “call-out” or “plug-in” interface. This is used when the IED management application initiates a call to the password management application. For instance, to get the password information for a given IED to automatically logon an operator located within the corporate network using a pass-through application without divulging to the operator the password used to access the IED. The same “call-out” or “plug-in” interface is used to notify the password management application when a password mismatch occurs or when the password has been shown or divulged to an operator. The later occurring when the IED does not support the automatic logon feature and the operator must manually enter the credentials in the Native Vendor Tool to access the IED. In this case, it is imperative for security reasons that a new password be generated for that IED and sent to the IED management application, so that the IED password is updated.

The second interface is referred to as the “call-in” or “service” interface. This interface is used when the password management application sends new passwords to the IED management application. New passwords can be sent on ad-hoc user requests or be sent automatically on a scheduled basis by the password management application, when required by enterprise policy requirements, or simply when the passwords have been compromised.

By using a well-defined interface to communicate with the password management application, the IED management application allows the possibility to select the appropriate adaptor based on the customer requirements and specific needs — without having to change any code within the IED management application. For instance, an adaptor that uses a messaging system like IBM WebSphere MQ or Microsoft MSMQ could be used for the integration between the two applications. An adaptor that makes a Remote Procedure Call (RPC) could also be used to communicate with the password management application. This ease of integration is made possible by the use of a plug-in architecture. This type of architecture would be stamped as an open architecture.

The IED management application has only a strong reference to the "plug-in" interface. It is only at run-time, through configuration settings, that the specific implementation or adaptor is selected. Thus, based on the customer requirements, this architecture allows for selecting the adaptor that best fulfills the customer needs. The password management application must also communicate with the IED management application; for instance, when the passwords are updated based on the customer policy to meet the NERC CIP requirements, which state that IED passwords should be updated at least once a year. The second interface, the "call-in" or "service" interface, is provided by the IED management application provider to ease the development of a plug-in to be used to easily integrate with the IED management application. A command-line tool could also be used to facilitate the integration of the password management application with the IED management application.

The following diagram in Unified Modeling Language (UML) notation depicts the integration between the IED management application and the password management application for further explanation.



6. CONCLUSION

The password management application manages the policies used for generating the passwords and is responsible for the auditing of password access. The IED management application is responsible for updating the IED password information using a substation gateway as a secure single point of access over a Transport Layer Security (TLS) link. The use of a secure substation gateway and a password management application to hold the IED password information causes this solution to meet the NERC CIP requirements concerning the protection of cyber assets.

BIBLIOGRAPHY

- [1] NERC CIP-002-1, Cyber Security — Critical Cyber Asset Identification.
- [2] NERC CIP-007-1, Cyber Security — Systems Security Management.
- [3] Anthony, R. Garland, J., *Large-Scale Software Architecture*, Wiley.
- [4] Fowler, M., *Patterns of Enterprise Application Architecture*.
- [5] Hohpe, G. Woolf, B., *Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions*, Addison-Wesley.
- [6] Benoit, J., "Meeting IED Integration Cyber Security Challenges," *Eskom Southern Africa Power System Protection Conference*, Johannesburg, South Africa, November 2008.