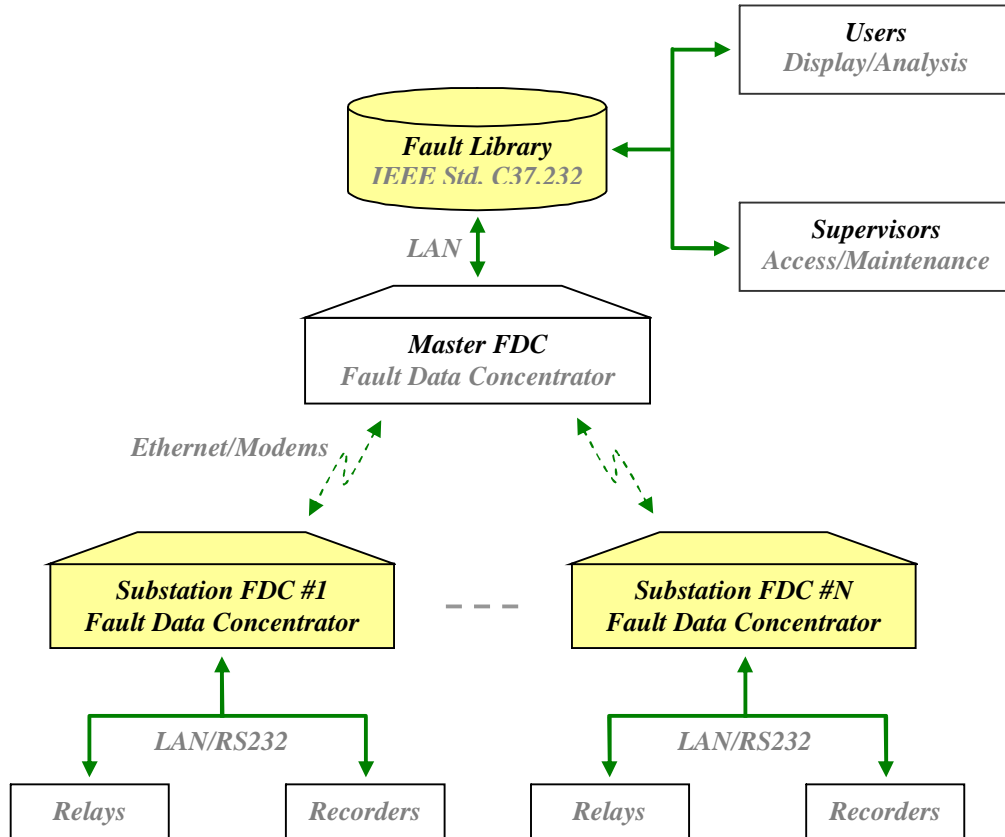


Fault Data Concentrator (FDC)

Automated Collection of Fault and Disturbance Data Records System Description and Security Issues (October 10th, 2010)



I – Definition of Terms

Wavewintm: Is a universal program for collection and analysis of transient and steady state waveform signatures (fault records) from various types of substation protection and measurement devices such as numerical relays, digital meters, and fault recorders (hereinafter, smart devices).

Fault Data Concentrator (FDC): Is a hardened, embedded computer equipped with multiple serial and Ethernet ports, a modem, and a copy of the Wavewintm program.

Substation FDC: Is used to communicate with the smart devices in the substation. Its main purpose is to retrieve the latest fault records from each device.

Master FDC: Is used to communicate with the Substation FDCs. Its main purpose is to collect the retrieved fault records from each FDC and store them on a shared drive on the company network (fault library) for access by protection and equipment engineers. In the event Substation FDCs are not deployed, then the Master FDC can be used to remotely poll and collect the latest fault records directly from the smart devices.

II – Security Features

At the basic level, the FDC is a state of the art computer that uses the latest in operating systems technology which offers the benefit of using the full depth and breadth of a wide range of commercially available security applications. At the system level, the FDC provides a number of specialized security measures designed specifically to deal with smart devices and fault records. The overall objectives of the specialized security measures are to:

- Ensure a safe journey for fault records from the smart devices all the way to the fault library (whether retrieved upon occurrence or by demand).
- Provide protection against remote access to substation FDCs and smart devices (implemented at the substation FDC level).
- Provide protection against unauthorized file transfers including malware to the fault library (implemented at the Master FDC level).
- Report on communications integrity, log all access requests, and archive all data communications between FDCs and smart devices.

The basic features of the specialized security measures include, but are not limited to, access protection, file transfer verification, data encryption, compression and logging, password management, and proprietary protocols. The following is a high level description of these security features:

Access Protection: For manual maintenance, remote or local access to critical FDC information is permitted for authorized users only (requires a valid user-id and a strong password). For automated communications, a unique 32 bit access key is used to seed a CRC algorithm that authenticates all file transfers between the Master and each Substation FDC.

File Transfer Verification: All fault records retrieved by the Substation FDCs and collected by the Master FDC are initially quarantined at the local levels. Once the records are quarantined, the FDCs will inspect their contents by parsing out file extensions and key fault information such as date and time of occurrence and name of originating equipment. If the extensions are proper and if the key information exists in the proper places then the fault records are transferred otherwise they will remain quarantined and a file transfer error message will be logged.

Base50 Encryption: The FDCs are also equipped with base 50 encryption algorithms used to encode key filename information of fault records being transferred between the Substation and Master FDCs. The encoding process can be programmed to operate based on a scrambling character set which is useful for compression. The calculated average compression ratio is 40%.

Data Logging: All communications (each and every byte) between the Substation FDCs and the smart devices, and between the Master and the Substation FDCs, are saved to log files. All access requests and error messages are also saved. The resulting log files are maintained and archived on a periodic basis. The period is user defined but due to performance requirements it is recommended not to exceed 90 days.

Password Management: Both the Master and Substation FDCs support strong passwords in compliance with NERC CIP Standards and are capable of changing the passwords of the smart devices on a periodic and/or upon demand basis. The passwords are randomly generated using at least 6 alphanumeric characters and the random function generator is seeded upon initial execution in order to ensure even distribution across the spectrum of characters (equally likely outcomes).

Proprietary Formats and Protocols: In addition to the above specialized measures, the nature of fault records is an added security benefit. The formats of fault records and the communication protocols needed to retrieve them are today mostly proprietary and most of which are complex binary structures. Knowledge of such structures is not commonly available and is rather difficult to attain.

III – Risk Factors

The risk factors vary depending on the type of topology used (report by exception or poll upon demand) and the level of security measures taken (such as applying strong passwords, providing multiple access levels, periodically changing passwords, enabling encryption and compression features, and disabling cyber space or any other form of remote access capability). If all of the available security measures are utilized and if the selected topology is report by exception then the FDC system is deemed risk free.

IV – CIP Compliance Matrix

If an FDC is used to monitor bulk protection assets that are deemed critical then the FDC is designated as a critical cyber asset (as defined by NERC CIP Standards) especially because the FDC handles sensitive information such as baud rates, IP addresses, user ids, passwords, relay settings, targets, and fault and disturbance data records. The FDC is a very useful tool for helping protection and security personnel investigate and classify fault records (whether they are due to real life operations/mis-operations or are caused by malware and/or cyber attacks). The FDC is in effect a monitor of protection assets which

in turn makes it a fundamental component of CIP compliance and provides an advanced tool for security planning. The following matrix provides details of the FDC compliance features for CIP requirements:

CIP-001-1a: Sabotage Reporting:

- **R1) Awareness:** Provides fault and disturbance waveform signatures which help security and protection personnel recognize and become aware of sabotage events and multi-site sabotage affecting larger portions of the interconnection.
- **R2) Reporting:** Provides management and reporting functions which help security and protection personnel report and maintain fault records.

CIP-002-3: Critical Cyber Asset Identification (Bulk System):

- **R3) Critical Cyber Asset Identification:** Provides a device management interface which helps security and protection personnel develop and maintain a list of critical cyber protection assets that support the reliable operation of the Bulk Electric System.

CIP-003-3: Security Management Controls:

- **R1) Cyber Security Policy:** Provides an array of automated communication topologies (such as report by exception topology) and security measures (such as access protection) which help security and protection personnel implement and enforce cyber security policies for their protection assets.
- **R4) Information Protection:** Provides an inference engine and an array of advanced analysis tools to help identify and classify fault record signatures from various types of protection assets.
- **R5) Access Control:** Provides an array of access control measures (such as multi-level passwords) to manage access to information of/from protection assets.
- **R6) Change Control and Configuration Management:** Provides a manual process to add, modify, replace, and/or remove information from protection assets and to document vendor related changes (such as firmware and protocols).

CIP-004-3: Personnel and Training:

- **R1) Awareness:** Helps increase situational awareness by automatically reporting fault and disturbance waveform signatures whether due to sabotage or due to protection operations.
- **R2) Training:** Softstuf provides a qualified team to train on proper access and handling of information of/from protection assets.

- **R4) Access:** Maintains a list of personnel ids and passwords for authorizing access to information of/from protection assets.

CIP-005-3: Electronic Security Perimeter (ESP):

- **R1) Electronic Security Perimeter:** Establishes an electronic security perimeter around the protection assets perimeter in the substation with only one defined access node for reporting information back to the Master FDC.
- **R2) Electronic Access Control:** Denies access by default and secures and locks all serial and dialup links (takes exclusive control of them, no other applications can have access to them).
- **R3) Monitoring Electronic Access:** Supports strong passwords and provides detailed access logs (unauthorized access attempts are highlighted and all bytes to/from protection assets are logged 24/7). Access banners are also provided.
- **R4) Cyber Vulnerability Assessment:** Provides detailed access logs and exception reports (communication errors) to help with vulnerability assessment of access points and to report on their integrity.
- **R5) Documentation review and Maintenance:** Documentation logs are automatically maintained on a periodic basis. The recommended period of maintenance is on a 90 days basis.

CIP-006-3c: Physical Access Security:

- **R1) Physical Security Plan:** Provides multilevel password protection against physical access via the local mouse and/or keyboard (for both the operating system and the polling application levels).
- **R5) Monitoring Physical Access:** Monitors physical access requests at the polling application level and reports on unauthorized access attempts.
- **R6) Logging Physical Access:** Computerized physical access logs are generated and automatically maintained on a periodic basis. The recommended (default) period is on a 90 days basis.

CIP-007-03: Systems Security Management:

- **R1) Test Procedures:** Provides an array of tools for testing communication links which help security and protection personnel evaluate access and throughput especially after significant changes are made to the existing cyber assets.

- **R2) Ports and Services:** The FDC only enables the ports and services that are needed for collecting/reporting fault and disturbance data records, all other ports and services are disabled.
- **R3) Security Patch Management:** For the Substation FDCs, security patch management is not required because they are embedded operating systems with all Server and Browser services disabled, removed, or deleted. To that extent, security patches most probably will not properly install. As for the Master FDC, security patch management is needed especially if the FDC is a standard office work station and the polling application is defined as a “user” on the company network with access to the internet.
- **R4) Malicious Software Prevention:** The FDCs communicate using a proprietary protocol that only allows for files that are actual fault and disturbance data records to be transferred among them, all other types of files including malware are blocked/quarantined. The protocol users CRC checks and looks for the presence of key data elements including data, time, type and location of fault occurrence. The protocol also checks for proper types of file extensions.
- **R5) Account Management:** Each FDC provides two levels of password protection (system and application) and generates detailed access logs. The passwords are a minimum of 6 characters and allow for use of numeric, alpha, and/or special characters. In addition, the FDCs are capable of automatically changing and managing the passwords of the smart devices being polled.
- **R6) Security Status Monitoring:** The collected FDC fault records and the generated access and integrity logs are archived and maintained on a shared folder on the company network (called the fault library). To that extent, and because it provides detailed documentation on fault and disturbance signatures, the library is a very useful resource for protection and security personnel especially for supporting incident response activities.
- **R7) Disposal or Redeployment:** The uninstall/removal procedure for the FDC polling application permanently deletes all of the configuration information and access parameters including any sensitive information such as phone numbers, IP addresses, passwords, and history/access logs.

CIP-008-3: Incident Reporting:

- **R1) Cyber Security Incident Response Plan:** The collected fault library data records and logs along with their corresponding display and analysis interfaces provide protection and security personnel with an advanced array of analysis tools specifically designed to help them classify and characterize various types of fault and disturbance data signatures (whether caused by real life events on the power system or are due to sabotage and/or cyber attacks).

CIP-009-3: Recovery Plans for Critical Cyber Assets:

- **R1) Recovery Plan:** The FDC polling application provides a high level script language interface for protection and security personnel to program triggers and alarms (such as for detecting changes in relay settings) and also to define remedial actions schemes (such as notifications for initiating recovery plans).
- **R2) Exercises:** The provided fault data analysis tools are also designed to support static and dynamic relay testing procedures. To that extent, the fault library data records can be used by security and protection personnel to model the effects of a cyber attack and initiate standard response exercises.
- **R3) Change Control:** The FDCs provide user friendly interfaces that allow authorized users to change configuration and programming parameters as needed to adapt and evolve the system based on lessons learned and/or based on applied changes to protection assets.
- **R4) Backup and Restore:** The FDC operations and maintenance guide provides detailed procedures for periodic backup and for restoration of configuration files, access parameters, and executable programs. In addition, the FDC architecture supports the use of backup FDCs at both the Master and Substation levels and is also capable of initiating restoration procedures automatically.

V – Additional Information

For additional information please visit www.softstuf.com, or contact:

Amir Makki
609-338-7735 (Cell)
215-922-6880 (Phone)
amir@softstuf.com