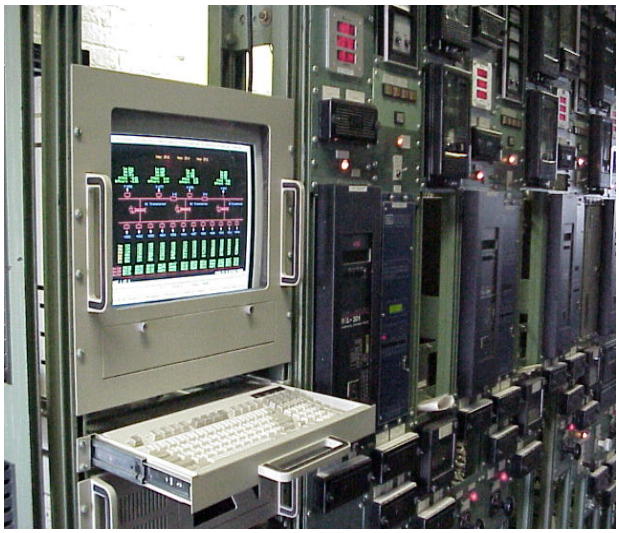
WAVEWIN™ SECURITY

An Expert System Security Program for Relaying Equipment (Protection and Monitoring)



Draft 2.0 (June 17th, 2010)

EXECUTIVE SUMMARY

This document describes how Wavewin (trademarked by Softstuf) can be used to do both secure and monitor protection infrastructure including numerical relays and digital fault recorders (hereinafter, critical devices). The main concept is to provide security and enhance the business at the same time. Security is achieved by periodically changing passwords and the business is enhanced by continuously monitoring protection equipment and automatically reporting on trouble spots (targets, fault and disturbance records, and so forth). In the event that any breaches or trouble spots are discovered, the appropriate alarms and reports are generated upon occurrence.

The intent of security is protection. To that extent, protection relays are a fundamental component of security. It is therefore necessary to communicate with these relays and read their data in order to determine whether a particular threat has evolved or an actual breach is in progress. However, current cyber security systems are mainly designed to deal with communication links and are restricted to the point of access or entry (the front door). These systems do not provide security beyond the front door. Accordingly, a good security program must be an expert system for securing communications and for analyzing power system performance at the same time (system security). The Wavewin solution provides this type of expert system capability and is commonly used in line

restoration, fault and disturbance analysis, dynamic relay testing, and for monitoring evolving loads. The main objectives are to increase security and reliability while reducing engineering time. Other objectives include helping expose faulty wires, faulted equipment, bad configurations, nasty harmonics, unbalanced circuits, overloaded assets, and so forth.

BACKGROUND

Before we get started, it is worthwhile to mention that a house with no doors or windows is a very secure environment but the problem with such a house is that you can never enter or ever leave. The same is also true when securing critical devices. We can disable communications with all of them but this will severely hinder operations, maintenance, and development. In other words, the more security we have the less access we get. We have to strike a balance between security and access, a balance that does not hinder the business but at the same time provides a sufficient level of security (including threat assessment and breach containment).

The Wavewin program is designed to provide such balance and has been evolving and growing for over twenty years (there is no foreseeable limit to its potential growth). The program is battle hardened and is used by a large number of utilities in the United States including but not limited to Bonneville Power Administration, Con Edison of New York, National Grid, Progress Energy, Southern Company, and Vermont Public Service.

INTRODUCTION

Twenty five years ago, cyber security was not a big concern for power systems because protection systems were mostly electromechanical and because dial-up and internet technologies were young and restrictive. Today, however, and after an incredible amount of advances in communications and embedded systems technology, protection systems are computer based and internet technologies are making their way into the substation. Consequently, cyber security is now a big concern and the extent of damage resulting from a large scale attack is mind boggling and is being repeatedly enumerated by many news agencies.

A considerable number of utilities have heeded the call and are actively working to secure their assets. Unfortunately, their collective energies have focused on access and have not addressed security from a system perspective.

The Wavewin program addresses security from the system perspective. The program can simultaneously communicate with large numbers of critical devices, old and new, and secure them by periodically changing their passwords and monitor them by continuously gathering and processing their collective

information. This is a complex process achieved by using a device independent architecture supported by a large library of “drivers” for interfacing with various types of critical devices and for implementing specific types of measurements, calculations, and remedial schemes. Wavewin offers a number of security layers that can be used independently or collectively. A functional description of each layer is provided in the following sections.

FUNCTIONAL DESCRIPTION

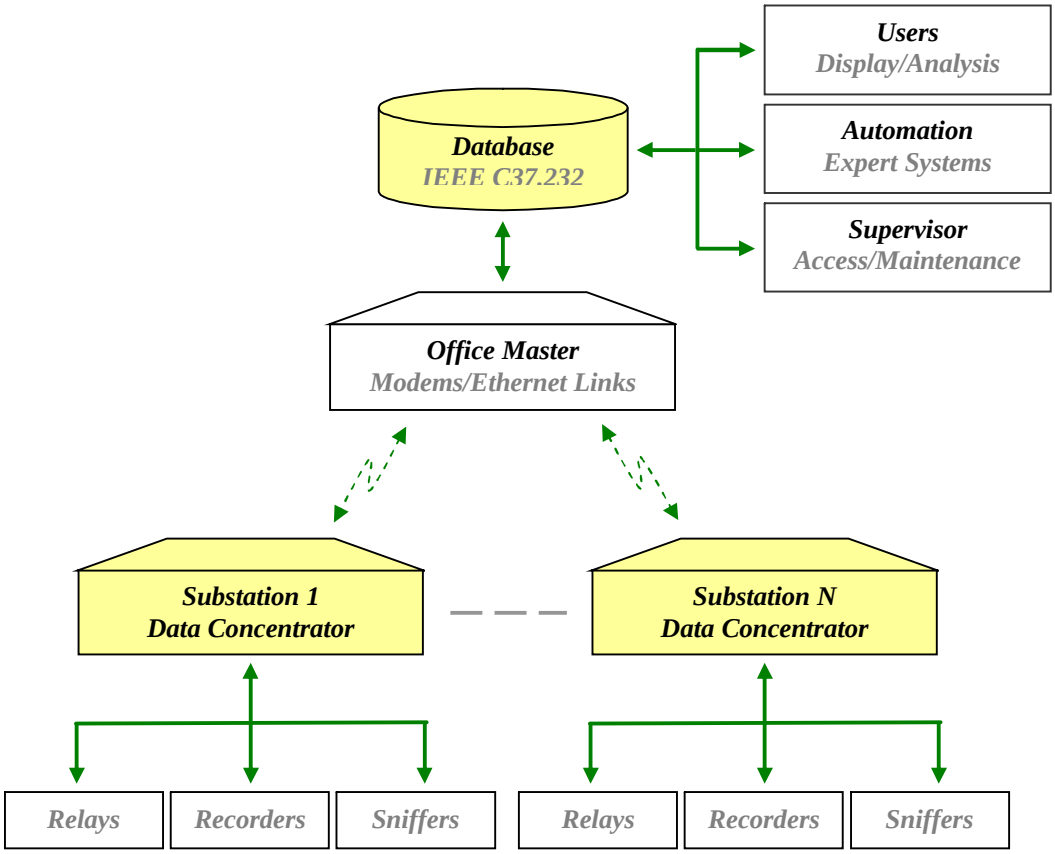


Figure-1: Wavewin Topology for System Security (High Level Diagram)

As shown in Figure-1, a hardened embedded system (data concentrator) is placed in each substation and a central computer is placed in the office (office master). Each data concentrator communicates with the devices in its substation and the office master communicates with the data concentrators. Any information acquired by the office master is archived to a shared database and is therefore available for access and analysis by authorized users, supervisors, and automated applications from any point on the company network. The archived information is stored in compliance with IEEE Standard C37.232-2007.

The above topology is a common model for integrating and securing critical devices. However, the capabilities of such models are limited by the software programs being used to operate the concentrators and masters. The extent of functionality available for analysis and automated processing is basically limited by the software programs being used. In other words, the hardware needed to provide an adequate level of integration and security is commonly available but the universal programs needed to operate such hardware are not widely available. Wavewin is the exception. The next section provides a description of the basic system security layers provided by Wavewin.

SECURITY LAYERS

The basic concept behind this type of security is that all communications with critical devices are rerouted through the data concentrator (whether they originate from a remote location or from within the substation fence). The security scheme is composed of four layers: access security, encryption, threat assessment, and breach containment:

1) Access Security: This is about defending against the use of telephone or internet systems to control critical devices from a remote location. This type of security is realized by automatically changing passwords on all critical devices on a periodic basis. Each period, each device receives a new, randomly generated password from the data concentrator (no one password can be used to access the system). The period is programmable and can be set as low as once/hour or as high as once/year, or can be manually triggered. This process ensures that passwords are always changing which in turn locks out the system and no one has access. In order to access a specific device, a user has to call a supervisor at another location and request access permission. If the user is authorized then the supervisor disarms the security functions to the specified device and restores its default passwords. Once the user is done, or upon expiration of the access timer, the security functions are rearmed automatically.

2) Encryption: This is the second layer of security and is designed to guard against use of specialized gadgets such as port and phone splitters or wireless transceivers to hijack legally established connections. This type of security is realized by encrypting all transmissions from the concentrators. Such encryption protects legally established connections from being hijacked by requiring proper decoding on both ends of any connection. The encryption algorithms are based on keys that are unique to each device and are periodically changing. And to double the trouble for anyone trying to hijack the connection, the encryption functions are augmented by a cyclic redundancy code whose transfer coefficients are also changing along with the keys and passwords.

3) Threat Assessment: This is the third layer of security and is designed to guard against other types of specialized gadgets such as null modem cables,

cross over cables, and modem emulators. Such gadgets are used to control critical devices directly from the front or rear panel inside a substation. This type of security is realized by monitoring “connection integrity” and immediately reporting on any communications errors (broken link detection). This monitoring is a form of ongoing threat assessment with the aim of protecting against threats emanating directly from the vicinity of critical devices. If a broken link is detected then it could mean that someone has disconnected the existing connection and is trying to establish their own or it could simply be a bad cable. Regardless, the integrity monitoring functions will issue a “broken link alarm”. Upon restoration of a broken link, the monitoring functions will automatically retrieve the protection settings from the affected devices and check to ensure that they have not been tampered with. If the protection settings did change then a “tamper alarm” is immediately generated.

4) Breach Containment: This is the final layer of security designed to defend against those who have gained access and have begun to assert multiple outputs. This type of security is realized by periodically collecting and analyzing target, status, fault, and load information with the aim of detecting any abnormal patterns in the behavior of the protection system (good/bad operations). If a rapid sequence of bad operations is detected then a breach may be in progress or most probably some critical device miss-operated. Clearly, having access to such information provides containment but more importantly it helps improve the reliability of the power system.

CONCLUDING REMARKS

As global communication systems and digital instruments continue to make their way into the substation environment replacing old, reliable and “digitally” secure electromechanical systems with new, globally available cyber space assets, the security concerns continue to grow and are becoming more challenging day by day. The most difficult part of this growing security phenomenon is the balancing act between security and access. As mentioned in the opening section of this document, we can’t in the name of security build a house without doors and windows. The house must have the necessary doors and windows but should be closely monitored to provide the ability to react instantly to any unauthorized access or breach.

Wavewin has been proven to bestow the right type of balance by providing the right type of system security that actually helps improve the business. Wavewin is almost 20 years in development and is based on intellectual property acquired from most of the major players in the industry (utilities and manufacturers). The program has acquired a considerable user base that includes most of the largest utilities in the United States. As such, Wavewin has become the premier program for analyzing power system performance during disturbance and switching operations and is the right platform for securing critical devices. In conclusion,

Wavewin is good news for those that have implemented security schemes and ended up with restricted operations and for those that lack security because the program supports rapid deployment, is cost effective, non-intrusive, and works with the existing communication infrastructure.

Additional Information

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

Amir Makki
(215) 922-6880 (Phone)
(800) 818-3463 (Office)
amir@softstuf.com

ANNEX - A: BACKGROUND ON WAVEWIN FEATURES

1) Scalability: Wavewin is designed to operate office masters and data concentrators and is capable of polling up to 999 critical devices simultaneously per copy. The 999 number was chosen because the designers did not want to exceed the computing power of standard off-the-shelf computers by overloading them with too many connections. In the event more than 999 connections are needed then multiple masters and/or data concentrators can be used.

2) Availability: Computer hardware and operating system failures do occur and especially so when running unmanned over long durations of time. Therefore, it is highly recommended that the master and data concentrators be equipped with watch dog timers in order for Wavewin to quickly restore services after a crash or lockup condition occurs. If a watch dog timer can not be provided then an external remote boot switch is alternatively recommended to help the supervisor restore services remotely without having to physically visit the location of the master or data concentrator.

3) Applicability: Wavewin is designed to poll a list of various types of devices over a hybrid set of communication networks and protocols. The list is specified in the device manager configuration table as shown in Figure-2. The polling period can be specified in seconds, hours, days, weeks or months. Devices that are in a multi-drop topology are polled one at a time (in ascending order) and those that are in a star topology are polled simultaneously.

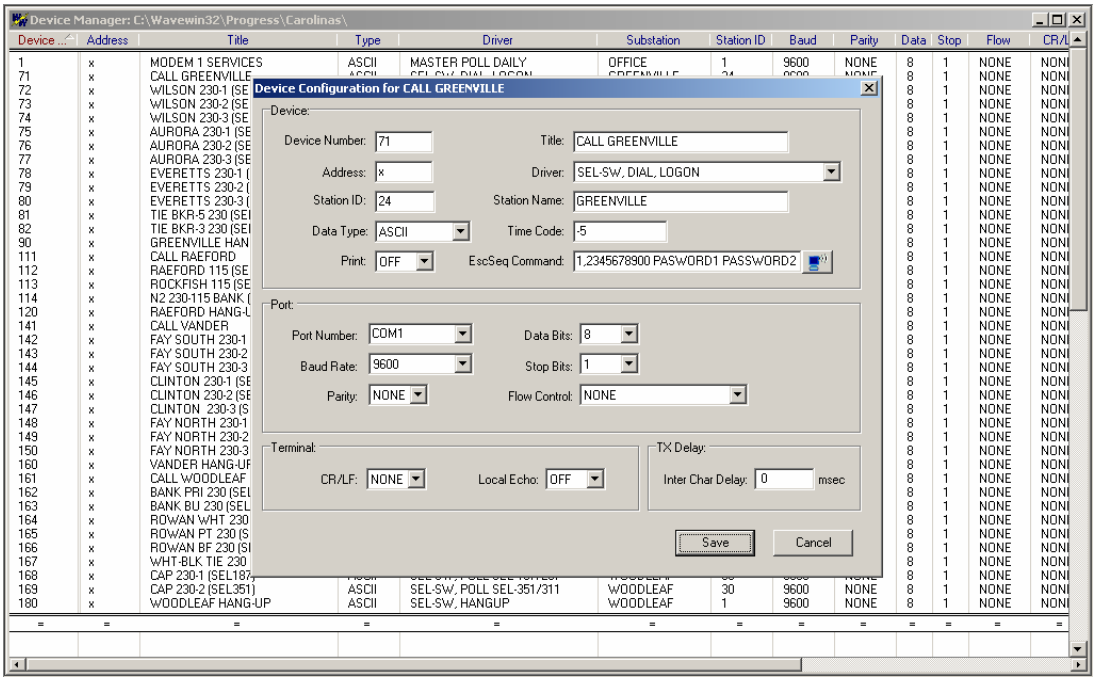


Figure-2: Wavewin Device Manager Configuration Table

4) Storage: Collected data records are discerned and processed by the Wavewin browser and the results are saved to a shared folder on the company network called the database. Immediate and secure access to the database records is concurrently available to authorized users from any point on the company network. The database records are considered legal records and are always maintained in their original proprietary format. The size of the database varies from small (mega bytes) to extremely large (terra bytes) depending on the selected polling periods and on the total number of devices being polled. A directory structure is normally set up for archiving database records by month or by year so that records can be easily retrieved for future analysis.

The database records have complex inter-relationships (multiple events can be in one record, or one event can span multiple records) and they have varying naming conventions. The browser uses an inference engine to determine date and time of event occurrence and type of originating equipment. The browser's search, sort, and query engines operate based on the outputs of this inference engine. The database browser is depicted in Figure-3.

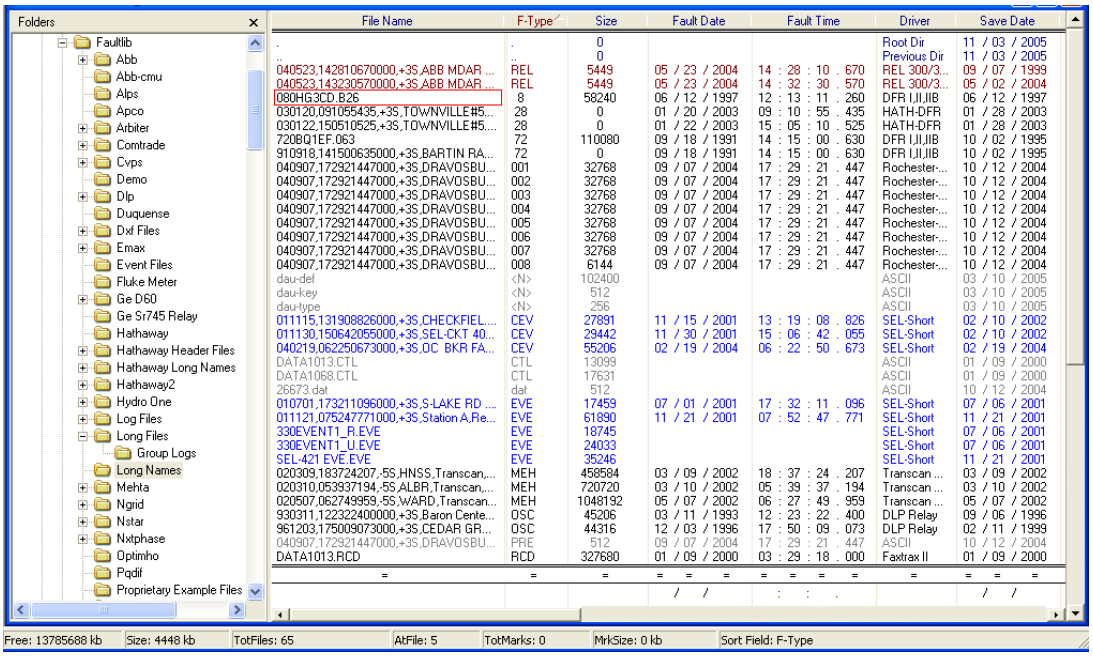


Figure-3: Wavewin Browser and Database Records

5) User Interfaces: User interfaces are needed for protection and engineering personnel to analyze collected information (transient and steady state) in order to evaluate the performance of their protection systems. Wavewin provides a powerful array of such interfaces. These interfaces are used to inspect fault and disturbance records, to check targets and status information (which contacts closed and which control inputs energized), to identify exceptions (which settings changed and which devices failed their self-test), and so forth. Wavewin also

provides a set of automated interfaces that continuously search and identify any circuits that are imbalanced, overloaded and/or inefficient. The automated interfaces using a network of adaptive algorithms collectively aspiring to rank circuit behavior (good/bad conditions). A number of these interfaces are depicted in Figures 4 through 7.

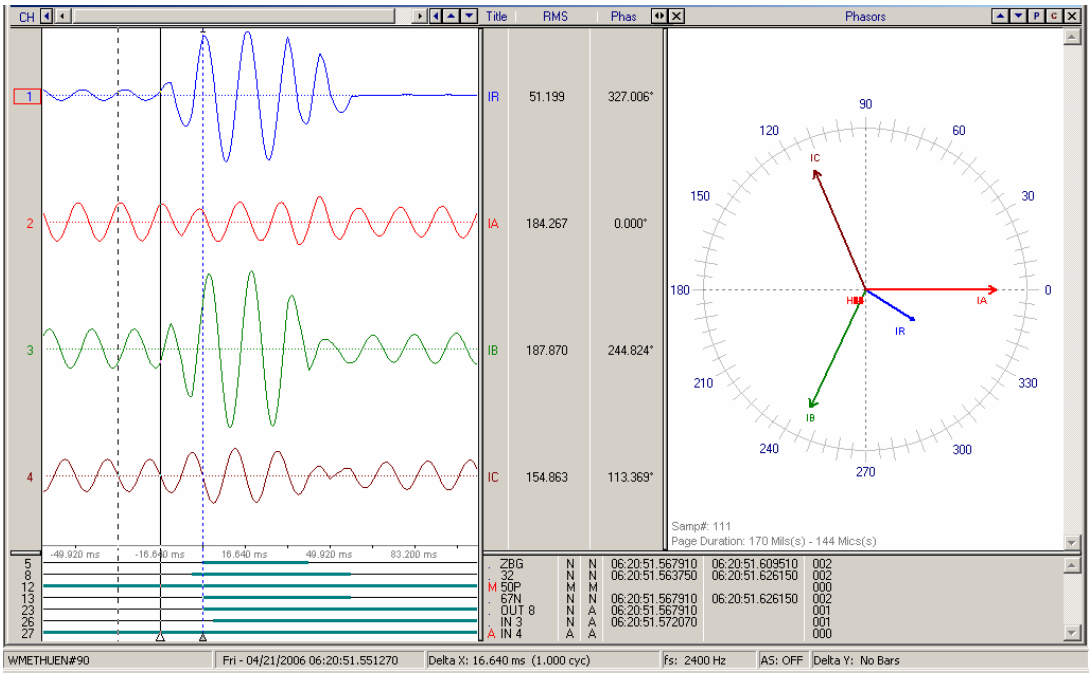


Figure-4, Fault & Disturbance Interfaces (Transient Data Analysis)

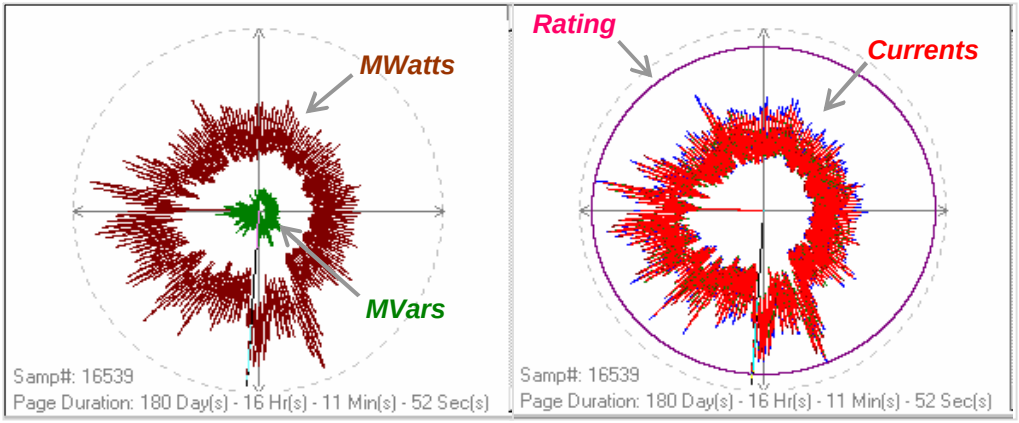


Figure-5, Evolving Loads and Seasonal Averages (Steady State Analysis)

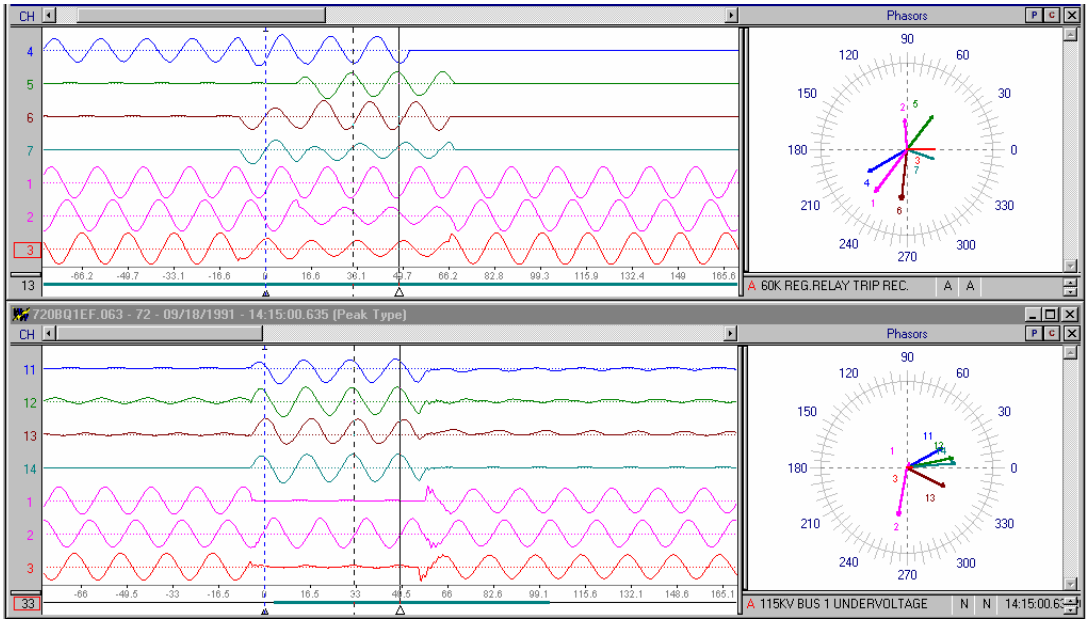


Figure-6, End to End Interfaces (Data Synchronization)

```
* File Information:
* ------------------
            Station: EXAMPLE 1 - SEL151
             Device: SEL 151
          File-Name: C:\Faultlib\910918,141500625000,+3S,EXAMPLE 1 - 151, 151,ARKEY ELECTRI
          File-Size: 5541 Bytes
     Prefault-Time: 9/18/91 14:15:00.562510
        Fault-Time: 9/18/91 14:15:00.625000
         Save-Time: 06/04/2004 09:46:02
      Process-Time: 01/03/2006 22:48:50
  Start Date & Time: 09/18/1991 14:15:00.562510
    End Date & Time: 09/18/1991 14:15:00.741648
      File Duration: 179 Mils(s) - 138 Mics(s)
 Sampling Frequency: 240.000000, 4166 Microsecond Reading
    Line Frequency: 60.000000

* Fault Information:
* -------------------
  01 - Event    : AG T    Location:   3.30    Shot:   3   Targets: INSTAQN
       Currents (A pri), ABCQN:   2229      0      0   2229   2212

* Highest/Lowest Analog Peaks Chart:
* ----------------------------------
>    Max-Val       Min-Val      LPeak-Up      LPeak-Dn      OneBit   pUnits   Description
   3131.069     -3131.069       675.994       -77.782      0.0010     Amps   1-IR
   3153.696     -3153.696       685.894       -84.853      0.0010     Amps   2-IA
      0.000         0.000         0.000         0.000      0.0010     Amps   3-IB
      0.000         0.000         0.000         0.000      0.0010     Amps   4-IC
  14570.642   -14570.642     14570.642   -14570.642      0.0010    Volts   5-VA
  15792.523   -15792.523     15792.523   -15792.523      0.0010    Volts   6-VB
  17249.163   -17249.163     17249.163   -17249.163      0.0010    Volts   7-VC

* Events/Sensors Activity Summary:
* ---------------------------------
> Fst Lst  Fst-Change         Lst-Change      Changes  Description
   N   N  14:15:00.608336  14:15:00.683324  002      1-P51
   N   N  14:15:00.625000  14:15:00.674992  002      3-P50H
   N   N  14:15:00.608336  14:15:00.683324  002      5-Q51
```

Figure-7, Reports and Summary (Fault Location and Sequence of Events)

ANNEX - B: BACKGROUND ON WAVEWIN COMMUNICATIONS

Monitoring protection systems is a complex undertaking because there are many types and vintages of critical devices in place today. Communicating with and retrieving data from such devices requires the use of a universal platform to deal with the hybrid nature of connection types, topologies, protocols and interfaces. A flavor of what is involved is provided below:

1) Connections: Legacy devices are primarily equipped with modem, RS-232, and/or RS-485 serial connections while new devices provide wide area Ethernet connectivity. Connections can be established remotely using phones and wide area networks or locally using null-modem and cross-over cables.

2) Topologies: Critical devices are organized in groups of local area networks, one or more in each substation. The network connections could be either serial or Ethernet or could be a combination of both. The network topology is either multi-drop or star. The multi-drop topology limits communications to one device at a time whereas the star topology does not. A star topology can be used to communicate with all of the devices at the same time. RS-232 networks are mainly star topologies, RS-485 networks are multi-drop topologies, and Ethernet networks support both topologies (if there is enough bandwidth then the network can be used as a star topology).

3) Protocols: There are many types of protocols that are needed for communicating with critical device, standard and proprietary. Examples of standard protocols include and are not limited to IEC 61850, IEEE C37.118, Modbus, DNP, Zmodem, and FTP. Examples of proprietary protocols include SEL, GE-Modem, Incom, Faxtrax, Transcan, BPA, and RIS. This large number of needed protocols is because of the complex nature of critical devices and the lack of an industry wide standard that can deal with such complexities.

4) Integration: In order to integrate critical devices, companies have historically chosen the phone system. A phone switch is usually placed in each substation and then a bank of host modems is made available at the office. The host modems are usually placed as standalone peripherals on an unmanned computer in the office called the master station. Today companies are adding Ethernet connectivity to place their critical devices on a wide area network. Such wide area connectivity provides better speed and availability than the telephone system. These enhancements open up new horizons for protection, planning, and real-time monitoring applications (such as reporting power system faults as they happen or anticipating equipment failures before they happen).

5) Interfaces: Software interfaces are needed to configure critical devices and to test them and to collect and analyze their data. Here too, each type of critical device has its own set of interfaces. The net result is a large number of interfaces with a wide variety of operating nuances producing disconnected islands of

information. There are some interfaces that are designed to work with standard formats and naming conventions such as IEEE Standards C37.111 and C37.232 but the majority of them are proprietary. Most of these interfaces, if not all of them, are available for download from the internet or can be purchased from the original manufacturer. In other words, these interfaces are available to anyone who wants them. Securing such interfaces is a main priority.

The extensive variations in available connection types, protocols, and interfaces are the main reason behind the inception of the Wavewin program. The program can simultaneously communicate with various types of critical devices over a hybrid set of connections and topologies.