WAVEWIN™ SECURITY

Using Wavewin to Secure Large Arrays of Microprocessor Based Protection and Control Equipment

Draft 5.0 (October 7th, 2007)

Executive Summary

The subject of this document is to show how the Wavewin™ Security program (trademark by SoftStuf, inc. 1991-2007) can be used to secure the power system's digital control and protection infrastructure which includes digital relays, remote terminal units and programmable logic controllers (critical devices) against any group or individual having a criminal agenda and equipped with the means, technology and knowledge needed to carry it through (such as a terrorist organization or a foreign intelligence agency or a disgruntled employee).

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 leave or ever enter. The same is also true with securing critical devices. We can disable communications with all of them, but this will severely hinder operations, maintenance, construction, 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 evolving threat assessment and rapid breach containment. This type of balance can be realized by implementing the Wavewin Security program as follows:

Remote access: This is about defending against the use of the telephone system and/or the internet to control critical devices from a remote location. This type of security can be realized by installing Wavewin's password management drivers. The drivers are used to periodically change all of the passwords on all of the critical devices. Each device receives a new, randomly generated, password on each pass (no one password can be used to access multiple devices). The period is normally set by the user and can be defined as low as once every 5 minutes or as high as once per year, or can be manually operated. This process ensures that the passwords are always changing, which basically locks out the system and no one has access. In order to access a specific device, the user has to first call the system operator and ask for permission. If the user is authorized then the operator will grant such permission by disarming the drivers for the specified device. The disarming sequence also restores the device's default passwords. Once the user is done, or upon expiration of the access timer, the drivers are automatically rearmed.

Link tapping: This is the second layer of security designed to guard against the use of specialized gadgets in order to hijack a legally established connection (such as port and phone splitters, or wireless transceivers). This type of security can be realized by installing Wavewin's data encryption drivers. The encryption drivers are used to encode and decode all of the transmissions to and from all of the critical devices. Such encryption protects legally established connections against being hijacked by requiring that the proper drivers be available on both ends of any connection to any critical device. The data encryption drivers are 64 bit algorithms based on keys or seed values that are unique to each device and that are also being periodically changing along with the passwords as mentioned above. And, on top of that, and just to double the trouble of anyone trying to hijack a legally established connection, the data encryption drivers are augmented by a 32 bit cyclic redundancy check whose transfer coefficients are also changing along with the keys and passwords.

Direct access: This is the third layer of security and is designed to guard against other types of specialized hardware gadgets (such as null modem cables, cross over cables, and modem emulators). Such gadgets are used to access and control a critical device directly from the front or rear panel while physically standing inside a substation. This type of security can be realized by installing Wavewin's integrity monitoring drivers. The integrity drivers are used to continuously monitor all of the available connections on all of the critical devices and automatically report, upon occurrence, on any errors in communications or broken links or on any unauthorized changes to the protection settings on the critical devices. This type of monitoring is a form of ongoing threat assessment with the aim of protecting against any threats emanating directly from within the vicinity of any array of critical devices. If a broken link is detected then it could mean that someone has disconnected the existing Wavewin connection and is trying to establish their own, or it could simply be a bad cable. Regardless, the integrity drivers will issue a warning message because the passwords are no

longer changing and because the data transmissions are no longer encrypted. Upon restoration of a lost connection, the integrity drivers will automatically retrieve the settings and check them to ensure that they have not been tampered with, otherwise the drivers will alarm.

Domino Effect: This is the fourth and final layer of security designed to defend against those who have gained access and have begun to assert multiple trip outputs. This type of security can be realized, in stages, by deploying Wavewin's postmortem analysis drivers. The analysis drivers are used to periodically collect and analyze status, fault, and load information with the aim of automatically detecting any abnormal patterns in the behavior of the critical devices (good/bad operations). The analysis information is collected directly from the critical devices but is also complimented with an array of additional information from other types of non-critical devices such as trip information systems, digital fault recorders, sequence of events recorders, and phasor measurement units. The analysis drivers are based on "artificial intelligence" techniques with the specific aim of pointing out where the trouble spots are. This is accomplished by ranking circuit behavior including event occurrences on a scale from 000 to 999 (with the later being the worst case scenario). If a rapid sequence of bad operations is detected then a breach may be in progress, or most probably some critical device miss-operated resulting in a cascading event. Clearly, having access to such information helps provide containment but more importantly it also helps improve the overall reliability of the power system.

There are a number of market available programs that can provide some of the above mentioned schemes but there is only one program that has addressed all of them at the same time, and that program is Wavewin. The Wavewin program is a specialized platform designed to communicate with a hybrid array of critical devices, old and new, over a hybrid array of connections, old and new, and to gather, discern, process, and analyze complex data as well. The main concept here is to provide security at access time and at run time (basically for as long as the connection exists) by alarming on any critical devices or communication links that have been compromised and by doing so upon occurrence. In what follows, a brief background is provided on communications and data retrieval, and then a high level description is presented on the hardware and software components that are needed in order to implement a fully working version of the Wavewin Security program as described above.

Background On Communications

25 years ago, "cyber" security was not a big concern for the power industry because protection systems were mostly electromechanical and because the dial-up and internet technologies were young, restrictive, and slow. Today, however, and after an incredible amount of advances in communications and embedded systems technology, or intelligent electronic devices (IEDs), the

protection system is going digital and the internet technology is rapidly making its way into the substation. Consequently, cyber security is now a big concern. The extent of damage resulting from a large scale attack is mind boggling and is being repeatedly enumerated by many of the news agencies on television, radio, internet, and in print.

Having said the above, securing the protection system is a complex undertaking because there are too many different types/vintages of critical devices already in place today. Communicating with and retrieving data from such devices requires a universal platform that can deal with a hybrid mix of connections, topologies, protocols and interfaces. A flavor of what is involved is provided below:

Connections: Historically speaking, the primary methods used for connecting with critical devices are modems and serial ports (RS-232 and RS-485). In addition, most of the new devices are also being equipped with Ethernet ports. Connections to these devices can be established either remotely using modems and Ethernet networks or directly using null and cross over cables.

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. Clearly, the star topology is much more “dangerous”. In general, RS-232 networks are star topologies, RS-485 networks are multi-drop topologies, and Ethernet networks can be either or depending on the addressing scheme being used and on the maximum amount of available bandwidth (if each device has a unique address and if there is enough bandwidth then the network is a star topology).

Protocols: After gaining access to a particular device, the language used to communicate with that device is called the protocol. There are many different types of protocols in circulation today, 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. Manufacturers have to produce their own protocols because of the complex nature of critical devices and the lack of an industry wide standard that can deal with such complexities. Consequently, new devices today are being designed to support multiple types of protocols simultaneously from separate ports. Clearly, standard protocols that are simple to decipher and that are well documented are the most dangerous ones (such as Modbus and DNP).

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 standard such as IEEE-C37.111 and IEEE-C37.232 but the majority is proprietary. Most of these interfaces, if not all of them, are available for download from the internet or can be purchased by contacting the original manufacturer. In other words, these interfaces are available to anyone who wants them. Clearly, securing against these interfaces is a main priority and especially so because such interfaces can be used to awaken hidden code segments and/or open backdoors (the Trojan horse threat).

The extensive variations in the types of connections, topologies, protocols and interfaces mentioned above are the main reason behind the inception of the Wavewin program. The program is used to automatically communicate with various types of critical and non-critical devices over a hybrid set of connections and topologies without having to rely on any interfaces from any manufacturers (this is a third part guarantee that eliminates the Trojan horse threat). The program is designed to provide security by improving operations, maintenance, construction, and development procedures. A description of the hardware and software components is provided in the following section.

Hardware Description

Master Station: In order to integrate critical devices, companies have historically chosen the phone system. A modem is usually placed in each substation LAN and then a bank of host modems is made available at the office. The host modems are usually placed, as standalone peripherals, on some unmanned computer in the office called the master station. The master station uses the Wavewin program to service these modems on a 24/7 basis and acts as a "firewall" between them and the company network. Many companies today are also adding Ethernet capability using fiber loops and frame relays in order to place all of their critical devices and master stations on the same network. This is much more useful as compared to the telephone system because it saves on long distance telephone bills and it allows for having the master station poll all of the connected devices on a continuous basis. A graphical depiction of the overall integration scheme starting with the substation devices and ending with the users on the company network is shown in Figure-1.

Data Concentrators: Many companies have also added computers to their substation LANs. Such computers are called data concentrators, or substation servers, or communication processors, and are used to run the Wavewin program in order to continuously poll all of the critical devices and check their data for any trouble spots. Upon detection of any trouble spots, these computers will use the LAN modems or the Ethernet connections to immediately report their findings to the master stations (report by exception). Alternatively, the computers can be configured to hold on to their findings until some master station asks for them (report upon demand).

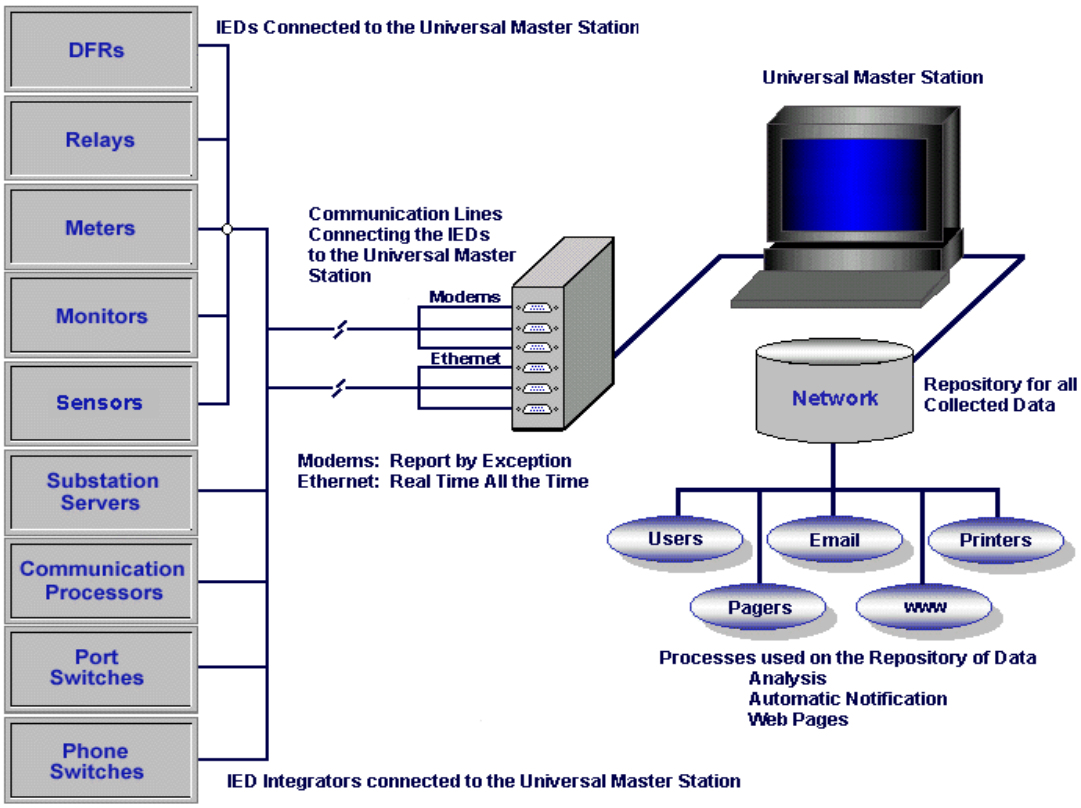

Figure-1; Wavewin Security Integration Diagram

Software Description

Scalability: The Wavewin program is designed to reside on a master station and/or on a data concentrator and is capable of polling up to 999 critical devices. The 999 number was chosen because the designers did not want to overload the program with too many connections. In the event that more than 999 connections are needed then multiple master stations and data concentrators can be used. Or alternatively, multiple copies of the program can be run on the same master station or data concentrator. Theoretically, there is no limit on the total number of copies that can be ran from the same computer, however, and because today's computers do fail, it is recommended that only one (1) copy be used with each master station or data concentrator.

Availability: It is highly recommended that the master stations and data concentrators be equipped with watch dog timers in order for the Wavewin program to quickly restore service after a crash or a lockup condition. However, this recommendation is difficult to realize because: 1) computers on the company network are standard issue without watch dog timers, and 2) the computers are

not configured to start automatically without having the user first enter his/her password. If a watch dog timer can not be easily provided then an external remote boot switch is alternatively recommended in order to help the operator restore service using the phone system without having to physically visit the location of the master station or the data concentrator.

Functionality: The Wavewin program is designed to poll a hybrid list of devices. The list is specified in the device 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.

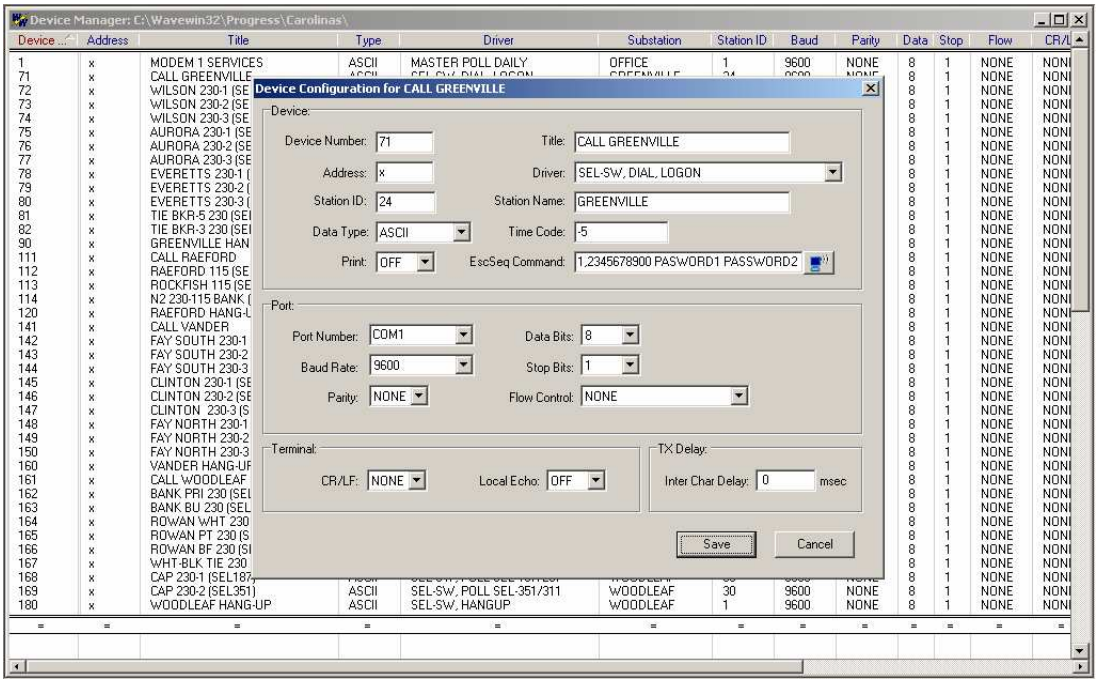

Figure-2; Wavewin Device Configuration Table

Repository: The information collected from each poll is discerned and processed and the results are saved on a shared folder on the company network called the repository. Immediate and secure access to the repository information is concurrently available to all of the authorized users on the company network. The repository files are considered legal records and are always maintained in their original proprietary format. The size of the repository varies from very small (mega bytes) to extremely large (terra bytes) depending on the selected polling period and on the total number of devices being polled.

Automation: The Wavewin program automatically checks all of the collected data and reports on any exceptions; e.g., settings have changed or self-test has failed. The program parses the digital information from the captured fault records

(see Figure-3) and reports on any outputs that closed or inputs that energized during protection operations. The program also looks for unbalanced, overloaded and inefficient circuit conditions (good/bad performing circuits).

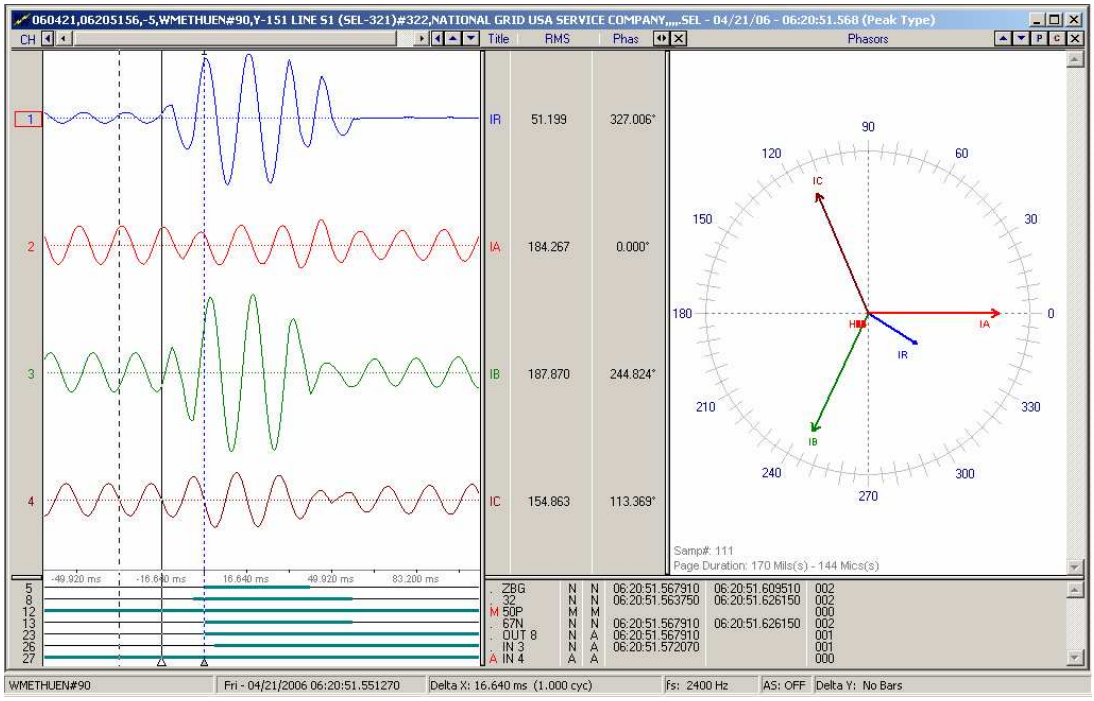

Figure-3; Fault Record with Parsed Analog and Digital Data

Pilot Installation

Wavewin is almost 20 years in development. It is based on intellectual property acquired from most of the major players in the power industry, utilities and manufacturers alike. The product 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 has proven to be a positive asset for fast line restoration, dynamic relay testing, contingency planning and monitoring of evolving loads. Consequently, and because security has become a big concern, the Wavewin development group and the Progress Energy system protection group teamed up in 2003 with the objective of modifying Wavewin to also secure all of the critical devices at Progress Energy as detailed in the executive summary section at the beginning of this document.

After a considerable amount of development and testing, the first working version of the “Wavewin Security” program was commissioned at Progress Energy on 26 May 2005. Today the program is running on two (2) master stations: one for the critical devices in the Carolinas and one for the devices in Florida. For the

purposes of this initial “pilot”, each master station was equipped with one modem only. The Carolinas master was configured to secure and poll 90 devices spanning 10 LANs across 8 substations. The Florida master, on the other hand, was configured to secure devices in over 150 substations. The program is operating successfully and the performance is as specified.

User Comments

1) NERC: “Wavewin was indispensable in the blackout investigation of August 14th, 2003.”

2) PSEG: “Wavewin has helped us tune our relays, improve system reliability, and reduce engineering time.”

3) NGRID: “After the August 14th blackout it has become clear that we should all be using Wavewin, we now tell our vendors that compatibility with Wavewin is a must.”

4) APC: “Softstuf has always tried to support additional devices in the same consistent manner in which they started the Wavewin application years ago. That basic manner was to provide the neatest and slimmest operational package they could. They always prided themselves in producing a "lean mean fighting machine" with no excess baggage. The result was a "universal" display application with no peer.”

5) Hydro One: “Wavewin was used extensively in the August 14th blackout analysis and was invaluable especially to view digital fault records.”

6) BPA: “We were so pleased to see that Wavewin works as advertised.”

7) Con Edison: “SoftStuf has delivered on their commitment and the performance of their Wavewin product has exceeded our expectations.”

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, security concerns continue to grow and are becoming more challenging day by day. The most difficult part of this growing security concern 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 windows and doors. The house must have the necessary windows and doors but they should have tamper resistant locks to restrict access and they should also be

closely monitored to provide the ability to react instantly to any unauthorized access. The Wavewin program has been proven to bestow the right balance by providing the type of security that actually improves system operations. In addition, one of the main prime directives behind the design of Wavewin is the ability to rapidly deploy its capabilities. The Wavewin Security program can be fully implemented throughout the United States within a few years.

Additional Information

For additional information please visit www.softstuf.com.

Prepared By

Amir Makki
609-338-7735 (Cell)
800-818-3463 (Office)
amir@softstuf.com

Acknowledgments

The author thanks the experts for their help in preparing this document.

Tony Giuliante (ATG Consulting)
Maria Rothweiler (SoftStuf)
George Semati (TIS Labs)
Mark Taylor (SoftStuf)
Steve Turner (Progress Energy)
John Walsh (SBT Services)

