21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2016 Grid of the Future Symposium

Considerations and Challenges with Automated Oscillography and Sequence of Event Record Retrieval

J. ALLEN, C. STILWELL
Burns & McDonnell
USA

SUMMARY

Disturbance monitoring equipment can collect and summarize transmission and distribution system events in an automated fashion. Organizing this data and making it available to business groups can vastly improve troubleshooting and maintenance analysis. Data can be used to understand misoperations, outage events, as well as protective operations. The benefits of using this data are substantial, but how can the system be architected to reach maximum benefits and usability? This document reviews design and security topics that should be considerations, and are sometimes challenges, during the implementation of disturbance monitoring equipment.

KEYWORDS

Disturbance
Monitor
Compliance
Automation
Storage
Design
Network
Record
COMTRADE
Security

cstilwell@burnsmcd.com

Oscillography and event data are valuable tools for engineers to perform irregularity analysis on an electrical system. The oscillography data is helpful enough in determining the cause of outages that many regional coordination councils now require that the data be available for analysis after an outage or system misoperation. In the past, stand-alone fault recorders were deployed to collect disturbance data from the electrical system by direct connection to current and voltage transformers. Fault recorders were fairly simple, having little or no provision for remote access and relatively limited data storage capacity. As the industry evolved, microprocessors ushered in technology with higher data resolution and additional features that reduce operational and maintenance costs. This technology, known as disturbance monitoring equipment (DME), consists of a wide array of devices that can be specifically suited to the operators' needs and preferences. This article introduces several design considerations for deploying an automated DME system that retrieves data from intelligent electronic devices (IEDs) that are part of the electric grid.

The installation or automation of many DME systems is driven by compliance with regional or national regulatory requirements. Therefore, a good place to begin the development of a list of system requirements is the governing bodies with jurisdiction over the region. Regulatory requirements will provide the minimum conditions that the system must attain. Utility-specific requirements should also include requests from any corporate groups or departments that could use the accumulated data for business or engineering purposes. Groups that may be interested in DME data may include: security, automation, protection and control, maintenance, and system planning. During the planning phase, all groups should consider the quality of the data being collected, how the data will be used, and how each group would like the data to be presented or available to them. The security and compliance groups must have critical input to the system design to assist in meeting all requirements.

Prior to design, accurate surveys should be performed of any existing IEDs that have DME capabilities or will otherwise be connected to the DME system at each site. Information gathered in the survey must include connection types, number and type of open ports, protocols, and data transfer speeds. The survey should also include the communication facilities between each device and the enterprise-level servers, as communication path upgrades may be needed depending on the technology chosen. Collecting this information early during the planning phase will help streamline the design process and inform decisions about potential alternatives.

The communications infrastructure, system requirements, and data presentations are key elements influencing the design and dictating the overall dataflow for the oscillography information. The intelligent portion of the system is responsible for the collection of the oscillography data from the end devices. This component of the DME system can be either centralized or distributed, or a hybrid of both, depending on whether the collection mechanism will be polling, listening (notifying), or push-type communications. The collection type will have a strong influence on the system architecture due to the bandwidth implications that it creates for the overall system.

The next component of a DME system that can also be centralized, distributed, or hybrid is data storage. Data storage may, however, be needed at multiple levels for redundancy considerations. Another important consideration for storage location will be end-user presentation. To avoid delays when fetching or searching for data, each site should transfer the data to an enterprise server where it can be accessed and viewed readily. If end users do not require quick access to the oscillography data, a distributed storage solution may be acceptable.

A centralized intelligence and storage solution, which collects data from remote IEDs and stores them in a top-level system, is the simplest and fastest form of collection. This solution is best suited for a listening or push-type collection mechanism in theory however, IEDs are not available with protocols that support that many open channels. Therefore, polling is recommended for a centralized design. Devices should be polled on a defined schedule, downloading any new event records in a report-by-exception method (i.e. downloading the records only when new events have occurred since the last poll.) There are challenges with this centralized approach as well, including increased bandwidth requirements for the wide area network (WAN), lower polling frequency, and possible loss of data if communications to the site is interrupted. Furthermore, this centralized system architecture is less scalable than the distributed architecture because a centralized server can become resource constrained.

A distributed system architecture collects event data from IEDs through a local area network (LAN) or through serial connections, then aggregates the information to a local and/or an enterprise storage location. Typically, a cache of the data is kept at the remote site even when storage is centralized to maintain continuity of the data if communications to the server are temporarily lost. This more costly approach allows for higher frequency of polling, reliable device connections with lower latency, reduced WAN bandwidth usage, and better reliability. This approach can be more challenging to manage because there are local instances of the intelligence software application at each site, all requiring security patches, upgrades, and compatibility with previous versions as well as any centralized instances running for data synchronization. Careful management of the local and synchronized storage is needed to avoid replicating data needlessly.

The entire vision of the DME system should be documented during the design phase, including IEDs, event formats, device capabilities, intelligence structure and data flows at the local and enterprise level. The design should also include the data visualization and presentation methods in detail. The final design should take into account the data collection mechanism at each level, any security or unique connection issues (communication managers or remote terminal units), and where applicable, the rate at which the primary interface(s) is updated. A key element to the design is the connection to the IEDs themselves. When using protection assets such as protective line relays to collect oscillography data, care must be taken to ensure that connection and password security is protected.

Once the architecture is determined, there are design considerations at the device level. There are different types of event record formats, such as sequence of events record (SER), compressed event file (CEV), and Common format for Transient Data Exchange (COMTRADE) standard IEEE C37.111. It is important to determine the device settings based on the information gathered from the regulatory bodies during the planning phase of the project. File format, resolution, duration, and even file naming convention may have minimum requirements set by the regulatory bodies.

When an event does occur, it can take significant time to transfer the event data files from the IED to the storage system, depending upon the connection type (Ethernet or serial.) This should be one of the considerations when determining the polling rate to prevent data from being overwritten and lost due to IED storage constraints conflicting with event creation frequency.

In many cases, an automated oscillography system must work in a multi-vendor environment, so the capabilities of every asset type must be considered. Many devices that support the recording of oscillography and system event data have limited storage capacity, file retrieval methods, and/or protocols. Additionally, the capabilities of a particular IED may vary depending on the version of firmware running on the device, or the hardware revision. These nuances may require a change in collection rate, connection sharing, or even device replacement. It is a time-consuming endeavor to attempt connecting a minimally complaint device (which does not support many standard formats, protocols, or collection mechanisms) to a system that needs to be reliable for compliance purposes.

Cyber security is a prime concern that encompasses the entire DME system. Many IEDs require proper authentication to retrieve the oscillography data files. This condition stipulates that the intelligence system, which polls the IEDs, must know the secure and fluctuating credentials to enable the login process. Under the best cases, this requires synchronization between databases in a secure way to avoid tedious updating of passwords between the engineering access system and the event collection system. Some systems currently do not support password synchronization, and most IEDs do not support central authentication. These difficulties can complicate the design and security functions should be tested end-to-end prior to deployment.

Once all the data is collected and brought to the centralized location, it is important to consider the specifics of how the system event data will be used. There are significant differences between collecting data solely for the purpose of meeting regulatory compliance, and reviewing or presenting collected data frequently to identify stability, potential maintenance issues, or other analytics. Several solutions are available that present drastically different user interfaces. A system architecture designed solely for archival purposes could use a system that simply delivers collected records into a directory structure at the designated location. Other intelligence packages compile all records into a database (either centralized or distributed) for searching. Some are able to be customized and integrated into an existing database or dashboard for system operators and engineers. The software tools must be able to run quickly and be scalable for large (and possibly distributed) data sets as event record databases grow very large as more IEDs are integrated into the system, especially if high sampling rates are used. Time should be devoted to evaluating current event data viewing software.

Deploying an automated DME system to meet regulatory compliance is a challenging task with many considerations. It is critical to invest time mapping out the design with the stakeholders, discussing end-user presentation, and testing the design in a lab that has a real-world configuration to maximize deployment efficiency. During this stage, the lab equipment can be used to create documentation, find connection and setting information, and test system functions. In the case of a customized solution, this lab environment will be essential to the development of a functional and reliable system. Automated DME systems can greatly increase efficiency in troubleshooting system events and providing root cause analysis, ultimately making the grid more reliable.