A SOFTWARE PLATFORM FOR IEC 61850 SUBSTATION CONFIGURATION AND MANAGEMENT

Petter HÄGGMAN
Vattenfall Eldistribution AB – Sweden
petter.haggman@vattenfall.com

Johan GRELSSON
Vattenfall Eldistribution AB - Sweden
johan.grelsson@vattenfall.com

Niklas SIGFRIDSSON
Vattenfall Eldistribution AB – Sweden
niklas.sigfridsson@vattenfall.com

Peter SÖDERSTRÖM
Vattenfall Eldistribution AB – Sweden
peter.soderstrom@vattenfall.com

ABSTRACT

The introduction of IEC 61850 as a standard for Protection & Control in MV and HV substations introduces new demands for a software platform present in the substations. Multiple vendors equipment and new tools for communication analysis introduce the need for several different software tools to be used configuring and maintaining the substation, which must be accomplished by a secure, flexible and cost efficient platform.

This paper describes Vattenfalls experience with a pilot design and installation of a virtualized pc platform concept, designed to fulfill the defined requirements on a MV and HV substation software platform. The concept is based on standard IT products available on the market and the concept is tested in a pilot installation at ÄT89 Upplands Väsby in Sweden. [1] gives the background on the pilot installation.

INTRODUCTION

The use of IEC 61850 in substation automation systems (SAS) introduces the software defined automation system. The complete SAS is defined by software settings, from communication to configuration. There are several different software needed in a SAS with multiple vendors, as each vendor have their own configuration tools, the integrator might have a third party tool and maintenance use another set of software tools for troubleshooting. All these tools produce and require different types of software configuration files, all of which constitutes the complete SAS.

In order to preserve and maintain the SAS over time, all configuration files must be archived and managed in a controlled, traceable and secure way. Also the different versions of the software used in a specific SAS must be managed in order to ensure the ability to recreate the SAS. This introduces the need for software version management and configuration management, which are novel processes to the branch, but well known in the software development branch.

From a maintenance perspective, the SAS will require access to all used software tools, in the correct versions, in order to analyze and correct problems with the SAS. As software versions will be different between substations over time, this will create a problem.

Security of the communication network will require that no unknown computers are connected/allowed to connect to the network within the substation. This will inhibit the use of technical personnel computers.

The software defined and controlled SAS opens up the possibility to remotely access all functions. This will introduce new work processes for problem solving and maintenance, saving both time and environment.

All of the above drives the need for a software platform in the substation. The platform must support centralized authentication, authorization and auditing together with efficient backup methods in order to be utilized at thousands of sites in the grid. The need for multiple operating systems is dictated by the equipment vendor’s software and the need of full functionality remote access is dictated by efficient economics in service and maintenance.

REQUIREMENTS

The requirements on the software platform, called ServicePC, were formulated in several groups.

Network design

The Vattenfall network security design of the process IT network is based on a zone model. Zone 1 through 3 are mission critical, where zone 1 is the actual automation process, zone 2 is supervisory management and control of the automation process and zone 3 is measurement and monitoring.

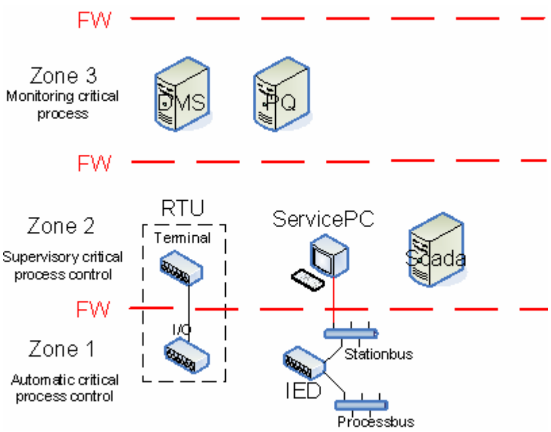
FW
Zone 3
Monitoring critical process
DMS
PQ
FW
Zone 2
Supervisory critical process control
RTU
Terminal
ServicePC
Scada
FW
I/O
Zone 1
Automatic critical process control
Stationbus
IED
Processbus

Figure 1 – Security zone model

The ServicePC will have a direct connection to zone 1, where the stationbus is located, and a direct connection to zone 2 for the external interface. This is important, as it could, if not handled correctly, create a network connection between zone 2 and zone 1, which is prohibited according to the security design principles.

Hardware

The hardware of the ServicePC shall fulfil the requirements of an industrial commodity, which means that it shall be rugged, fanless, use solid state storage and be temperature resilient. Power supply voltage shall be between 24-48 VDC.
The external interfaces should consist of a minimum of two network interfaces, two RS232 serial interfaces (RS485 optional) and four USB 2.0 interfaces.

Operating systems

The ServicePC shall support two simultaneous operating systems, Windows XP and Windows 7. These demands are defined by the software that are to be used and which operating system a specific vendor's software is supporting. This is out of control for Vattenfall, therefore we must support at least these two versions. In a SAS designed with multiple vendor equipment, the support for different operating systems must be simultaneous and a data sharing mechanism is required between the different operating systems.

Image management

In order to be able to manage ServicePC in thousands of substations, there must be an efficient image management. As SAS are built over time, there will be a large number of versions of different vendor software that are in use at the same time and each substation SAS will have to be considered a unique individual when it comes to software tool versions.
This will lead to the management of hundreds/thousands of client images with regard to software updates, security updates and backups.

Backup

Backup is a critical issue for a software platform in a substation. The backup has until now primarily meant disaster recovery, meaning the ability to restore a substation computer after a hardware failure.
The difference with the new IEC 61850 concept is that the backup now must be continuous in order to ensure the restore of single software files from a previous date, as every change to the configuration in the SAS will produce new versions of software files and traceability over time is important.
The backup solution will introduce demands on the communcation bandwidth in order to be able to maintain a sufficiently short time window for running backups. This is an important design factor as the communication to substations can be limited in terms of bandwidth.

User policies

As a part of Vattenfall process IT network, all users are managed centrally in a specific Directory service. User policies are defined and enforced by requiring all connected computers to join the domain.
The ServicePC shall be a part of the domain and all user policies shall be centrally managed.

Security policies

Like user policies, security policies are enforced by the use of a Directory service. However, as the ServicePC will be a multiple session client, it must allow local security principles to be enforced in order to ensure the security design locally in the platform.

Data sharing

As the SAS of the substation is software defined, the different configuration files will work as a complete documentation of the SAS. This documentation shall be available centrally as well as locally in the substation, which requires some data sharing mechanism between the local substation and the central process IT network.
This will also be used for keeping updated equipment manuals, instructions and other technical documentation available at the substation in an efficient way.

Remote access

All functions in the ServicePC shall be available by remote access from within the Vattenfall process IT network. This means that anything that can be done in the substation, can also be done at a computer connected to the process IT network, located elsewhere in the network.
This functionality requires that a combination of user policies and security policies can ensure what functions are available, to whom and at what location.

Communications

The need for communication is quite complex, as the ServicePC shall be able to deliver functionality of different sorts. A principal demand is that all functions in the ServicePC shall be locally available even if the external communication is down. This is critical to ensure that the SAS always can be managed locally in a situation when the external communication is disturbed.

The main communication need is the ethernet connections to the station bus and the external network interface towards the process IT network. The ethernet connection to the station bus is used for communicating with the IED :s and to analyze traffic on the station bus in a service situation. The connection to the process IT network is used for remote access, backup, data sharing and platform management. This means that there must be at least two ethernet interfaces that are strictly separated in order to not cross connect zone 1 and zone 2.

There is also a need for serial interface communication, primarily RS232, but could be RS485 in some cases. These communication interfaces are used by software to connect to console interfaces of specific IED:s. By this, any software used to communicate with an IED console, can be available on the ServicePC platform.

The USB interfaces are used for connection of keyboard and mouse, but can also function as spare serial and ethernet interfaces by the use of converters. There might also be IED:s that offer a console function by the use of USB.

SOLUTION DESIGN

The solution designs primary parameter is our choice of a virtualized client platform. The requirement of simultaneous operating systems that can be separated from each other on network connection level is a strong argument to virtualize the clients.

There are two main virtualization designs to choose from, Type 1 Hypervisor and Type 2 Hypervisor. The Type 1 Hypervisor is a virtualization platform that runs directly on top of the hardware, i.e. there is no traditional operating system running below the clients. The Type 2 Hypervisor is based on a traditional operating system, i.e. there is platform operating system below the clients. The main argument for choosing a Type 1 Hypervisor is that there is no platform operating system that needs management in terms of patches and security.

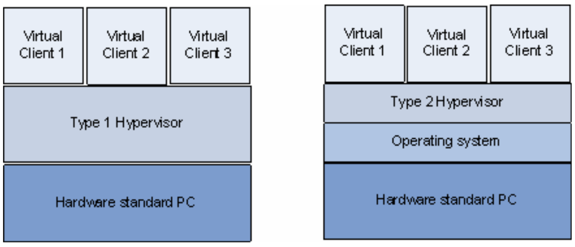

Figure 2 – Hypervisor types 1 and 2

We opted for a Type 1 Hypervisor named Citrix Xenclient as the platform for our design. It is a relatively new product on the market and its main development purpose is laptop management in large organizations.

The choice of Xenclient brought a number of requirement fulfilments with it and the management of Xenclient is via two central servers, the Synchronizer and the Image server.

Network design

The choice of virtualized clients makes it possible to completely separate clients between zone 1 and zone 2. Xenclient allows for a hypervisor separation of network interfaces, which means that a network interface can be completely excluded from the hardware visible to a client.

Operating systems

Xenclient allows any choice of client operating system between Windows XP, Windows 7 and Windows 8. The limitation of number of virtual clients is dictated by the processing power of the hardware.

Image management

Xenclients image management is completely centralized by the use of Synchronizer and Image server. Any client image can centrally be updated and transferred to the local hypervisor.

Another positive factor is that restoring a client on new hardware is a quick and easy task. As the client is virtualized, a restore only includes a quick installation of the hypervisor on new hardware and then the correct image is dispatched to it.

Backup

The Synchronizer is able to perform delta backups of the client image on a file block basis. This means that any backup performed consists of a delta change of file blocks on the local disk since the last backup. This way the amount of data that is transferred is kept to a minimum, which is preferable on low bandwidth communication links.

The downside to a block based backup is that restoration of a single file will be more time consuming.

User policies

As the clients running on top of Xenclient are regular windows clients, user policies are managed by the use of a Directory service in the same manner as physical clients on the process IT network.

Security policies

Aside from the policies enforced by the Directory service, Xenclient have security policies that can be used to enforce hardware limitations to the clients. This includes access to network interfaces, access to USB devices and access to serial ports. The local console of Xenclient can be visible or not, controlled by policies.

Data sharing

As the clients are regular windows clients in this solution, data sharing can be set up with ordinary windows mechanisms. This includes both sharing between local virtualized clients and sharing between central storage and local virtualized clients.

Remote access

The chosen solution for remote access to the ServicePC clients is VNC (a public free software). VNC gives remote access to the desktop and thereby all software functions available at the local client. It was also chosen not to use windows sharing for file transfers to and from the ServicePC client (by security reasons), but instead to use the file transfer functionality within VNC. This way, access to VNC is controlled by the Directory service policies and, at the same time, the permissions to transfer files to and from the clients.

Communications

The communications capabilities are restricted by the hardware chosen for the ServicePC. The chosen hardware, an industrial PC, offered two ethernet interfaces, two serial ports and six USB 2.0 ports, but was available in other configurations.

The serial ports were used for a console software, connected to two Alstom MU on the process bus, giving access to configuration and monitoring of these units. Another console software was configured to use the station bus to connect to earth fault detection equipment.

Software for IED configuration and monitoring was using the station bus in a standard way.

PILOT EVALUATION

The evaluation of the pilot tests at ÄT89 Upplands Väsby gave by hand a number of identified areas that need further development.

A main issue of concern was the inability of Xenclient to handle more than one ethernet interface. It turned out that the version used only managed one ethernet interface, which lead us to create a special network design for the substation, using VLAN as traffic separating mechanism between virtual clients. This lead to a more complex setup of the substation switch and is not considered a permanent solution to build on. The lack of ethernet support also lead us to not install the station bus sniffer tool, as this can be used to induce harmful traffic on the station bus and therefore is of highest security level. Without a dedicated ethernet interface, it was decided to be excluded from the ServicePC setup.

A second area of challenges was that Xenclients support for serial port speed turned out to be limited to 19200 bps. The Alstom MU:s demanded 38400 bps on their console interfaces and a workaround solution was managed by using serial-to-USB converters instead. This issue is expected to be resolved in a later version of Xenclient.

The third area of challenges was that the USB support of Xenclient was not fully developed. If connecting two identical devices, for example serial-to-USB converters, the hypervisor only managed to detect one of them. This is expected to be resolved in a later version of Xenclient.

The fourth problem area detected was backups over low bandwidth communication links. The substation was connected over a cellular network link with a speed of approximately 200 kbps and it turned out that the image backups timed out before finishing. The amount of data in the backup was limited, but the Xenclient hypervisor seems to expect the backup to transfer at a certain speed or it will timeout at the application level. As soon as the substation was connected to its regular fiber optic communication link, the backups were performing as expected. This issue will need some more investigation as Xenclient is expected to be able to use a slow communication link.

CONCLUSIONS

Other than the above technical issues, the evaluation shows that the concept of a virtualized ServicePC with multiple clients will deliver according to the requirements and expectations. It offers a flexible, centrally managed, secure, standardized platform solution for a ServicePC in substations, working as a software platform for the IEC 61850 based SAS.

The ability to offer remote access to the SAS will open up new ways of working with service, support and maintenance.

The platform can also function as a development platform for new functions that is made possible by a standard windows client in the substation, hosting different software used for data collection, state monitoring and other novel applications.

REFERENCES

[1] A. Johnsson, N. Sigfridsson 2013, "Deployment of smart substation standard IEC 61850", *Proceedings CIRED 22nd International Conference on Electricity Distribution*