INFORMATION SYSTEM ARCHITECTURES IN ELECTRICAL DISTRIBUTION UTILITIES

Teodor Sommestad, Gunnar Björkman, Mathias Ekstedt, Lars Nordström
Royal Institute of Technology (KTH)
teodors@ics.kth.se , gunnarb@ics.kth.se, mathiase@kth.se, larsn@ics.kth.se

ABSTRACT

Computerized control systems have been used in many years to supervise and control power distribution. These systems, which often are referred to as SCADA (Supervisory Control And Data Acquisition) systems, have in recent been more and more interconnected to other systems in recent years. In modern utilities various kinds of data are exchanged between the distribution management systems and the administrative systems located in the office network. For example are operational statistics, trouble reports and switch orders often communicated between the office systems and the systems inside the control center.

This paper describes a survey over state-of-practice architectures in electrical distribution utilities. A set of system-services have been identified together with the interfaces that typically exists between these services. How these services are located within different zones within utilities is also identified. The set services, the data flows, and the location of these has been reviewed and validated by vendors of SCADA systems in the electric utility industry.

INTRODUCTION

SCADA (Supervisory Control And Data Acquisition) systems used in electrical power distribution have during the last decades been more and more interconnected to other systems in electrical distribution utilities. In many utilities various kinds of data is exchanged between the control center and services located elsewhere. This includes: historical data, engineering data, commands and status exchanged with other control centers, and data exchanged with remote operator stations.

Based on a survey and a literature review this paper describes a number of architecture patterns or, i.e. commonly deployed solutions, for SCADA systems and systems in their environment. The patterns are represented as a set of descriptions that capture the vast majority of SCADA systems' architecture on a high level. The purpose of the SCADA architecture patterns is to clarify how already installed SCADA systems are employing a stringent model framework. The descriptions show: software services in SCADA systems and software services which SCADA systems exchange data with; the interfaces that can exist between these software services; how the services are typically placed in different security zones (network zones).

The outline of this paper is as follows. The next chapter will briefly describe related work in this field. After that the modeling framework and the survey is presented. In chapter four and five the

architectures are presented together with a summary of their interfaces to external systems. Finally, conclusions are drawn.

RELATED WORKS

This study was initiated with a review of literature where state-of-practice and state-of-art for SCADA system architectures where discussed. There are plenty of textbooks, articles and reports that describe SCADA systems, including:

- Textbooks such as [1,2,3,4,5,6]
- Articles such as [7], [8] and [9,10]
- Reports such as [11], [12], [13] and [14].
- Market surveys such as [15] an those produced by the Newton Evans Company [16]

These references include both schematic overviews of SCADA systems and detailed descriptions of their components. Most of these provide schematic descriptions of SCADA systems. Some also provide empirical data on how common different solutions, services, or configurations are. None of the references found does however provide an encompassing description of common architectures. For example, the descriptions in [8] are limited to Finnish distribution utilities. Many references describing SCADA systems are also dated several years back. Furthermore, many descriptions are explicitly declared as state-of-practice descriptions or likely future architectures (e.g. [10] and [14]) with an unclear applicability to the state-of-practice.

Schematic overviews of SCADA systems can also be found in cyber security related publications. This includes academic writing on this topic can be found in journals (e.g. [17,18,19]), conferences proceedings (e.g. [20,21]), guidelines/standards (e.g.[22,23,24]) and textbooks (e.g. [25] and [26]). The descriptions included in these texts are intended to be general introductions to SCADA systems. Consequently these publications focus on some central aspects and disregard many variations that exist. The security related literature that appears to be most closely related to the work presented in this report is the control system reference model presented in [27]. In this reference model four levels are identified: oversight entity, system and plant control centers, SCADA field equipment and infrastructure equipment. In relation to [27] this report further detail the services, their relationship to each other (interfaces between these), and the levels (zones) related to these systems.

THEORETICAL FRAMEWORK AND METHOD

The architectures presented in this report have been identified through a study of the literature described above and through interviews with a number SCADA system vendor. This chapter will describe the modeling formalism used to document the architectures and the interview procedure as well as the respondents.

Metamodel

The architecture models described in this report include a set of services that has been identified. A service in these models is realized by one or more software component(s). The components as

such are however not explicitly regarded as entities in their own right here. Examples of services include, “Engineering stations (HMI)” and “Data Engineering Server”. A service can be physically distributed on different machines, for example spread over multiple computers. It can also be replicated in the architecture. It is for example common that multiple data engineering stations are instantiated in the architecture to allow simultaneous work. Computers and physical elements are not explicitly covered in this study.

A service belongs to a zone. A zone in this metamodel has a close relationship to a network zone in computer networking. It should however rather be seen as a security domain as defined in [28], i.e. “...a set of security elements subject to a common security policy defined and enforced by a single security policy authority”. In the notation used a zone is represented as a frame around the elements (services) included in it. If there is a tunnel (e.g. a virtual private network, VPN) that makes it possible to join one zone from another zone this is also represented. In that case this represented by a block-arrow between the zones (cf. *Figure 1*).

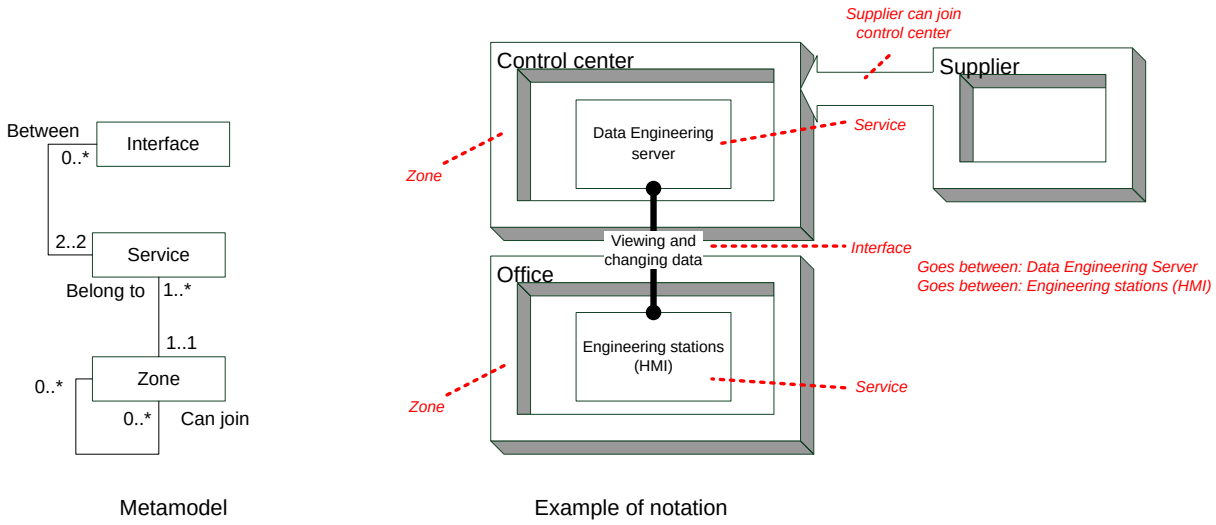

Figure 1 *Architecture metamodel and annotated example.*

Data can be exchanged between services. The element interface represents this. A line connecting two services in the notation used represents an interface; the text written on this line denotes the purpose of the interface. In this report focus is on interfaces and services that hold an apparent and direct business value is included. This means that interfaces that only provide infrastructure services, e.g. the Domain Names System (DNS) are not included.

Architecture survey

A substantial effort has been placed on finding suitable respondents. The following organizations have been contacted for an interview: ABB, Siemens, PSI, Netcontrol, Areva and General Electric. The first four accepted to participate in interviews. In
Table 1 an overview of these vendors and their typical customers is given.

Table 1 *Overview of vendors in this study.*

Organization	**Product**	**Typical customer**

ABB	ABB Network Manager	Larger distribution utilities worldwide.
	ABB MicroScada	Small or medium sized distribution utilities in Europe, the Middle East or Asia.
Siemens	About 10 (including legacy systems)	Larger distribution utilities worldwide.
PSI	PSIcontrol	Larger distribution utilities. Primarily in the German region or Russia.
Netontrol	Netcon 3000	Small or medium sized distribution utilities in Sweden or Finland

The respondents interviewed held a considerable experience in the field. Their experience from SCADA systems ranged from 18 to 41 years and they had been with the vendor they represented for between 7 and 35 years. In total three persons were interviewed about ABB Network Manager's architectures, one person about ABB MicroScada's architectures, three persons about Siemens's architectures, two persons were interviewed about PSI's architectures and two persons were interviewed about Netcontrol's architectures.

The interviews were initiated by an overview of the services included in the models and the data flows between these. This was followed by a presentation of three different network zone models and how services are placed in these zones. These zone models were drawn from literature and with them certain data flows will cross over zones, and some will not.

When presented with the model the respondents were encouraged to give comment to these architecture descriptions and comment unfamiliar or missing components. This comments covered what services that was included in the descriptions, the data flows that go between these, the zones included in the descriptions and how the services were placed in different zones.

The interviews lasted between one and three hours, depending on the amount of deviations identified between the vendor's architectures and the ones presented to them. All comments and deviations where noted throughout the interviews. The initial architecture used as a base model during the interviews remained more or less unchanged throughout the series of interviews. Many of the deviations were also noted by multiple vendors, i.e. it appeared as set of stereotypical variants existed.

In addition to the qualitative comments the respondents were asked to provide quantitative assessments of how common different architectures are in their installed base of systems. This has been used to determine the variants that should be regarded as the basic architecture and what should be regarded as a deviation from it. Once documented in an electronic and readable format the respondents has had the opportunity to review and comment the interview protocols.

ZONE ARCHITECTURES

This chapter will outline the zone architectures identified through the interviews with SCADA system vendors. It will describe how services are placed in different zones in the architectures that are most common for distribution utilities. They will also show the typical interfaces between these services. A number of deviations to these basic architectures have also been identified. The deviations are also presented.

Demilitarized zone architecture

In the demilitarized zone architecture there is a one zone separating the control center zone from the office zone – the demilitarized zone (DMZ). All vendors have some systems installed according to this architecture. There are however a number of variations that exists among these installations.

Figure 2 depict the most common placement of services in this zone architecture. As can be seen from this figure the DMZ normally contains a historian replica, servers for inter-control center communication, and servers for remote HMIs. The control center holds front-end, the SCADA server, a DMS server, the master historian, a data engineering server and the HMI clients.

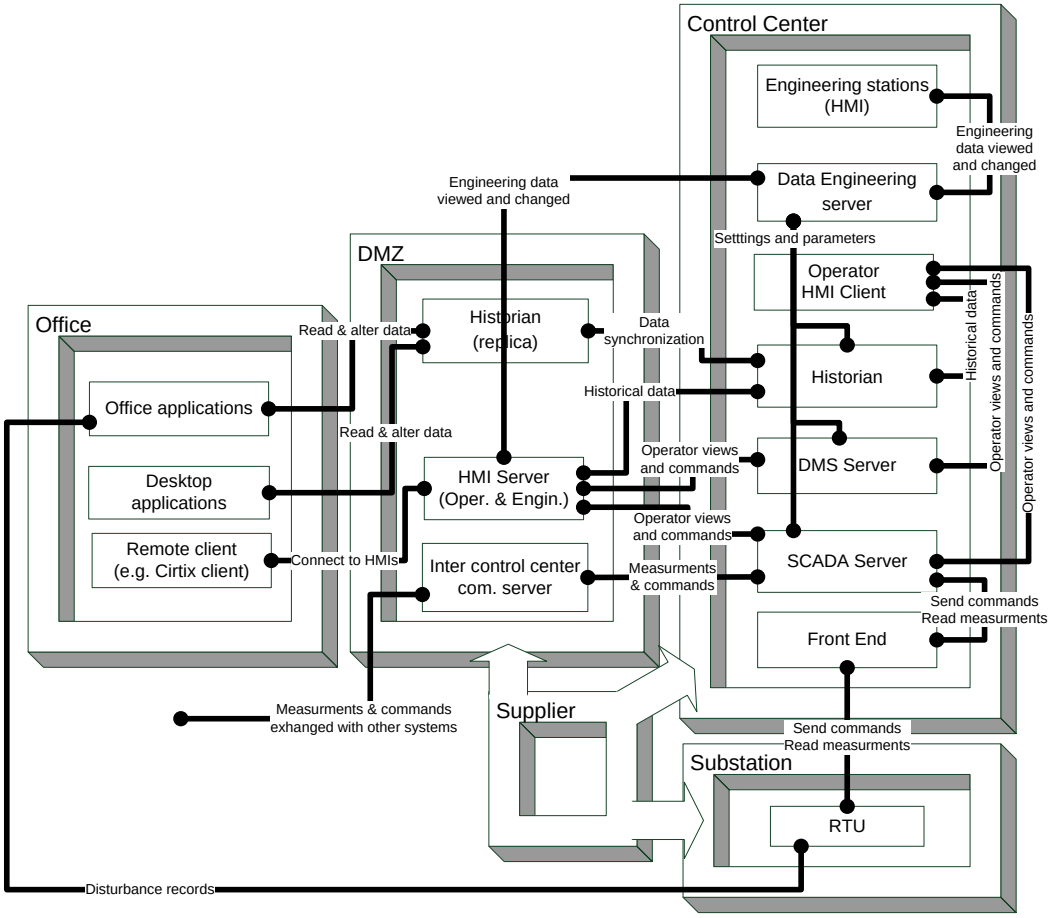

Figure 2 The demilitarized zone architecture.

Figure 2 depicts the most common interfaces between the services in this briefly describe these in text. The DMZ architecture is the architecture that most new SCADA systems use. It is also the zone architecture in which most variation has been found. There are number of more or less common deviations from architecture presented in this figure. These are summarized in *Table 1*.

It should be noted that the DMZ architecture does not always implement a DMZ in the strict sense. With a DMZ, all traffic should terminate in the DMZ and no traffic should go directly through it [24]. As can be deduced from *Figure 2* this is not always the case for the DMZ between control centers. For example, in deviation number four will engineering stations in the

office access the engineering server in the control center and in deviation nine office computers access control centers system's API directly. In both these cases the connection passes directly through the DMZ.

Table 2 Deviations within the demilitarized zone architecture.

#	Deviation
1	A SCADA replica is placed in the DMZ and remote operator stations work towards this replica instead of the primary, operational server.
2	HMI server gives access to Operator station in the control center zone instead of one located in the DMZ. I.e. the HMI server only bridge access to operator stations in the control center.
3	No separate HMI server is used. Instead HMI clients are installed in the office environment or some type of terminal services is activated on control center computers.
4	Engineering stations are placed in the office zone and interface the engineering server from there.
5	A separate web client is possible to use for remote access. This client can only view the status, and not issue commands.
6	A special inter control center communication front end is used when secure MMS is required. This one is placed in the DMZ and the server is placed in the control center zone when a DMZ exits. In other cases it is placed in the control center.
7	An external DMS system is used. This system is placed in the office and exchange data with the SCADA server and historian. In some installations commands can be issued through the interface of this external DMS system.
8	Data from GIS systems located in the office zone is forwarded to the engineering server to update the process models with changes made.
9	Application programming interfaces in the SCADA server and/or DMS server is used to integrate external systems, i.e. office applications and desktop applications (e.g. spreadsheets) located in the office zone.
10	The historian replica is used to move data (e.g. production plans) from the office to the control center application server.
11	A special interface server manages all data exchange between office systems and the control center. No data is allowed to go directly through.
12	A special back-office zone is used for office users which require data exchange with the control center zone. This back-office zone is more secured than the office.
13	Front ends are placed in a special zone between the control center and the network used for substation communication.
14	A quality assurance zone exists for testing of data engineering changes and software updates.
15	Concentrators can be placed in substations between the front ends and remote terminal units (RTUs).
16	Application software for the office (e.g. mail and web surfing) is executed in the control center zone.
17	The data engineering server is placed in DMZ and this server updates the services in the control center zone from there.
18	Data can be exchanged with emergency control centers.
19	RTUs and substation equipment can in some cases be accessed remotely for parameterization and configuration. This can often be done form the office.

Two-zone architecture

In this architecture there are only two zones and the control center is not separated from the office with a DMZ. Instead these two zones interface each other directly with a single firewall. Most of the respondents say that this architecture is uncommon new installations and that today's systems use a DMZ. However, they also state that the two-zone architecture still is common in the installed base of SCADA systems. The percent of system with this architecture on the distribution range from about 20 percent of PSI's installed systems to about half of the installed base level for ABB MicroSCADA, Siemens and Netcontrol.

Figure 3 illustrates the most common placement of services in this architecture. As can be understood by studying this figure this architecture involves a direct data exchange between the control center services and other, external services. For example, use of historical data means that data is read directly from the control center zone.

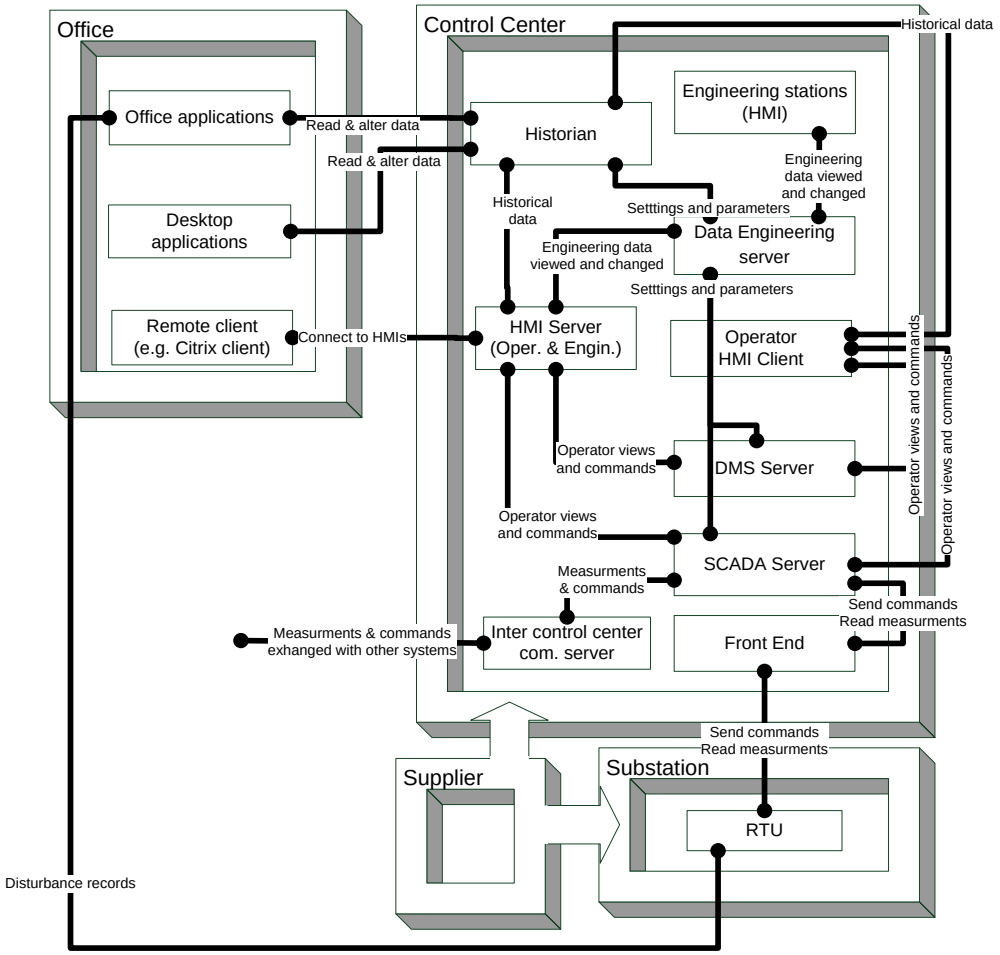

Figure 3 The two-zone architecture.

Just as for the DMZ architecture a number of deviations the basic architecture has been identified. The deviations identified within this architecture are a subset of those in *Table 1*. Three of the ones in *Table 1* are not applicable for the two zone architecture: deviation number one, number eleven and number seventeen.

It should also be noted that some SCADA system installations with the two-zone architecture interface the office network to allow suppliers to connect for debugging and updating, i.e. no other interfaces exists. This is for example the case for about one fifth of Netcontrol's installed base of systems.

Isolated zone architecture

The third zone architecture is the one where the control center is not at all connected to the office or the internet. Although the vast majority of new systems have some connectivity to the office, this architecture is still common in the installed base of SCADA system. The general notion from respondents that have an installed base of with this architecture is that it is used in smaller utilities and in "low-tech-environments".

Figure 4 does not include the office zone or the supplier's zone. These are excluded since the services in the control center do not exchange any data with services in these zones. However, also the isolated architecture does sometimes exchanged data with other control centers. In that case this data exchange comprise of inter control center communication and/or data exchanged with emergency control centers.

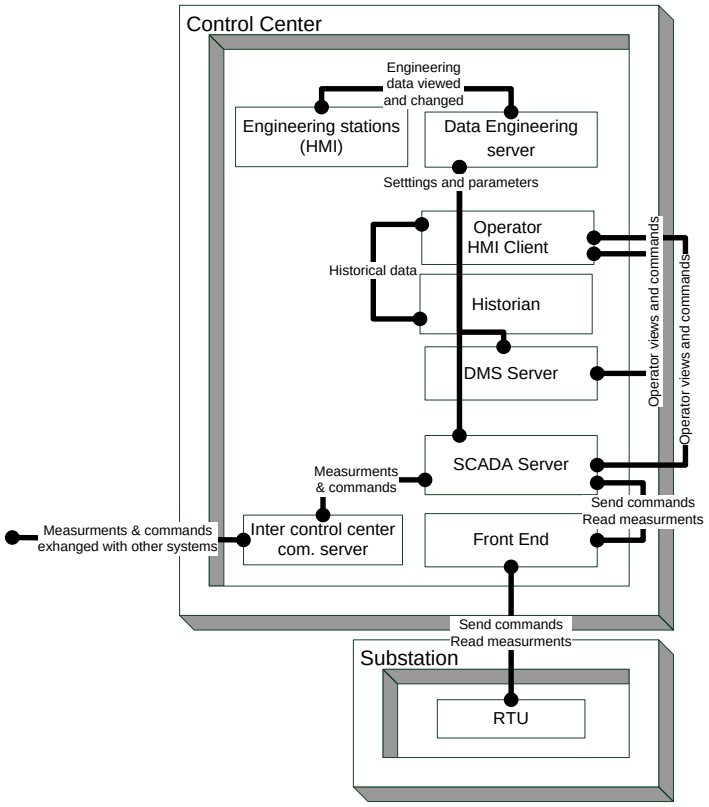

Figure 4 The isolated architecture.

EXTERNAL INTERFACES

This chapter will summarize the external interfaces to SCADA systems which have been identified through the survey.

Substation communication, gateways and disturbance records

All control centers within the domain of electrical power distribution needs to communicate with RTUs and other control equipment distributed in the field, e.g. substation control systems (SCSs). Hence, the communication between the SCADA server and the RTUs is always present in a SCADA system. In addition, two other interfaces to substations have been observed:

- Some RTUs and, and especially SCSs, can locally collect and store disturbance data that is recorded during power system disturbances. This data is a series of very accurately time stamped process values that is later used to analyse the disturbance.
- RTU/SCS parameters can often be loaded from a central site to the local site using dial-in connections, e.g. modems or VPN connections over Internet. The benefit with remote parameter loading is, of course, that the remote sites do not have to be visited when reconfiguration of RTUs/SCSs is required.

These two additional interfaces exist to enhance and simplify analysis support and maintenance. While they are not always present in today's systems general notion among the respondents is that they are increasing in popularity.

Historical data to office

A common and natural data to move out from the control center is historical data. Most SCADA systems that interface other zones also include a historian that is accessible from the office zone. Historians are used to make historical data accessible in the following ways:

- Web interfaces in implemented in the historian.
- Special purpose clients developed for the historian.
- Through the operator HMI clients.
- Programming interfaces (APIs) for custom made connections to other systems.

In the case of a DMZ architecture an historian replica is placed in the DMZ and is kept synchronized with the historian located in the control center. In case of a two zone architecture the historian is made accessible from the office zone.

Engineering data from the office

The data engineering server is sometimes subordinated some other system, e.g. a geographical information system located in the office. This phenomenon is particularly common in larger power distribution utilities where a large quantity of network data is updated each day. To avoid entering these updates multiple times a system located outside the control center is sometimes used as a master data. In this case an API or database interface is used to update the data engineering server.
In addition to the updates received from other application servers the use of engineering stations located in the office appears to be common. A variant is to place engineering station in a back-office zone and only allow updates from there. This does however appear to be less common than the scenario where engineering stations are used from office hosts. Moreover, most vendors seem to integrate the operator HMI client and the engineering station into one software application. In this case all remote operator clients will mean that it could be possible to perform data engineering remotely. If this can be done will depend on the access rights associated with the user accounts.

Remote workstations, and workstations used outside the control center

Remote operator stations of various kinds appear to be commonly used feature in SCADA system. The ones identified in this study can be categorized into eight variants:

- The operator client software is installed on a machine located outside the control center and is allowed (by network interfaces) to connect from an external zone, e.g. the office.
- The operator client software is installed on a machine located outside the control center can be connected after this machine has joined the control center zone, e.g. through a VPN tunnel.
- A remote desktop server (e.g. Citrix, VNC or Windows Terminal Services) is activated and accessible on a host in the control center.
- A HMI server runs in the control center zone and gives access to a number of "virtual" operator HMI clients.
- A HMI server runs in the DMZ and gives access to a number of "virtual" operator HMI clients located in the DMZ.
- A HMI server runs in the DMZ and gives access to a number of "virtual" operator HMI clients located in the control center zone.
- The HMI server's operator HMI clients only connect to a SCADA replica from which no commands is forwarded to the power process.
- A special purpose client with read-only access is available for users outside of the control center.

In addition to the plethora of ways to offer remote access there are also different rule sets that can be applied for where the client must be. For instance, remote access might be limited to a number of dedicated machines in the office, or remote access can be enabled from all addresses (including external internet addresses). In the same way access controls can be implemented and enforced to various degrees.

External power applications and administrative systems accessing control center services

In some installations services in the office interface the SCADA server or application server through an API.

The SCADA server's API is typically used by other services in the control center but can also be used to update or read data of the SCADA server. For instance, data missing in the SCADA server might be replaced with default data or real-time data may be recorded and stored in other (external systems). As exemplified by Netcontrol's integrations with a third-party DMS system APIs can also be used to create custom operator clients and issue commands towards the power process.

In the power application sever a number of functions can be offered. Some of these benefit greatly from data retrieved from external systems. For instance, outage management can be enhanced if call centers can enter trouble calls into the system and if automated crew management systems can be integrated. The data is often exchanged through some enterprise services bus and/or APIs defined in the power application server. Sometimes an interface server is used as an intermediary and the power application server reads data from this interface server.

Suppliers dialing in to the control center for bug fixing and support

The majority of systems with an interface to external network zones allow suppliers to dial in to the control center for maintenance and troubleshooting purposes. The restrictions placed on this type of access appear to vary with the size of the utility. In many cases this type of access will require the vendor to ask for wires to be connected and/or firewall rules to be reconfigured

Office and internet applications used in the control center

Although it is not depicted in the figures above, it appears as office software that access the internet is sometimes used in the control center. This could for example be Lotus Notes clients, email clients or internet browsers. Several vendors notice this as a practice that can be observed in some utilities, in particular smaller utilities where security awareness is on the lower end of the scale. When these applications are in use they are typically used from a machine that also holds the operator HMI client.

CONCLUSIONS

Through the literature study and the interviews with vendors a number of patterns, or stereotypical architectures, has been identified. Three zone architectures has been identified (the DMZ architecture, the two zones-architecture and the isolated architecture). Together with thee variations applicable to these (e.g. use of back-office zones). New systems often include a DMZ, but the legacy in the installed base is substantial.

It is also worth to note that it is possible to speak of SCADA systems as a relevant type of system. A majority of functions/services and data are found in all SCADA systems, and variations with respect to the services used in different installations are few. The software services constituting a SCADA system and the services interfacing these appears to be more or less standardized.

ACKNOWLEDGEMENTS

The authors would like to thank the vendors participating in this study and in particular the individuals who participated as respondents for vendors: Hans-Joachim Diehl, Gilbert Suter, Erich Wuergler, Wolfgang Fischer, Joachim, Lars-Gunnar Lif, Mats Elmgren, Neela Mayur, Erik Johansson, Anders Hellkvist, Frank Hohlbaum, and Mikael Molander.

REFERENCES

[1] G. Clarke and D. Reynders, "Practical modern SCADA protocols: DNP3, 60870.5 and related systems," 2004.

[2] S. Mackay, J. Park, and E. Wright, "Practical data communications for instrumentation and control," 2003.

[3] S. Mackay and E. Wright, "Practical industrial data networks: design, installation and troubleshooting," 2004.

[4] J. Park and S. Mackay, "Practical data acquisition for instrumentation and control systems," 2003.
[5] C. Strauss, *Practical electrical network automation and communication systems*, Elsevier, 2003.
[6] T. Cegrell, *Power system control technology*, Cambridge, Great britain: Prentice hall International, 1986.
[7] M. Qureshi, A. Raza, D. Kumar, M. Park, and B. Park, "A survey of communication network paradigms for substation automation," *2008 IEEE International Symposium on Power Line Communications and Its Applications*, Jeju city, Jeju Island: IEEE, 2008, pp. 310-315.
[8] J. Toivonen, P. Trygg, A. Mäkinen, and P. Järventausta, "A survey of infromation systems in Finnish electricty distribution companies," *Proceedings of NORDAC*, 2006, pp. 1-8.
[9] G. Azevedo and A.O. Filho, "Control centers with open architectures," *IEEE Computer Applications in Power*, 2001.
[10] F. Wu, K. Moslehi, and A. Bose, "Power system control centers: past, present, and future," *Proceedings of the IEEE*, 2005.
[11] J. Andersson, E. Johansson, M. Haglind, and L. Johansson, "State-of-the-art study of commercial industrial control systems," 1997.
[12] IEEE Power Engineering Society, *IEEE standard for SCADA and automation systems, IEEE Std C37.1-2007*, New York, NY: IEEE Power Engineering Society, 2008.
[13] IEC, "IEC 61968-1, Application integration at electric utilities – System interfaces for distribution management – Part 1: Interface architecture and general requirements Reference num," vol. 2003, 2003.
[14] VLPGO, "EMS Architectures for the 21st Century - white paper," 2005.
[15] S. Owen, "Gaining momentum - The 2008 Energy& Resources Global Security Survey," *Viral immunology*, vol. 21, 2008.
[16] Newton-Evans Research Company inc, "Newton-Evans Research Company, Inc.," 2010.
[17] V. Igure, S. Laughter, and R. Williams, "Security issues in SCADA networks," *Computers & Security*, 2006.
[18] I. Nai Fovinoa, A. Carcanoa, M. Maseraa, and A. Trombettab, "An experimental investigation of malware attacks on SCADA systems," *International Journal of Critical Infrastructure Protection*, vol. 2, 2009, pp. 139-145.
[19] T. Sommestad, M. Ekstedt, and L. Nordstrom, "Modeling Security of Power Communication Systems Using Defense Graphs and Influence Diagrams," *IEEE Transactions on Power Delivery*, vol. 24, 2009, pp. 1801-1808.
[20] M. Naedele, "Addressing IT Security for Critical Control Systems," *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 2007, pp. 115-115.
[21] E. Johansson, T. Sommestad, and M. Ekstedt, "Security Isssues For SCADA Systems within Power Distribution," *Nordic Distribution and Asset Management Conference (NORDAC)*, 2008.
[22] US Department of Homeland Security, "Catalog of Control Systems Security: Recommendations for Standards Developers," *Analysis*, 2008.
[23] G. Finco, "Cyber Security Procurement Language for Control Systems," *Idaho National Labs*, 2007.

[24] K. Stouffer, J. Falco, and K. Kent, "Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology," *Nist Special Publication*, vol. 800, 2008.
[25] R.L. Krutz, *Securing SCADA systems*, Indianapolis, Indiana, USA: Wiley Publishing, 2006.
[26] J. Wiles, T. Claypoole, P. Henry, P. Drake, and L. Johnson, "Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure," 2008.
[27] J. Stamp, M. Berg, and M. Baca, "Reference Model ofr Control and Automation Systems in Electrical Power," 2005.
[28] J. Sherwood, A. Clark, and D. Lynas, *Enterprise Security Architecture: A Business-Driven Approach*, USA: CMP Books, 2005.