COMMON DATACOMMUNICATION INFRASTRUCTURE FOR METERING, OPERATIONS & MAINTENANCE

Main author

S. Bakker

The Netherlands
ABSTRACT

To reduce cost and keep data communication networks manageable the aim is to develop a common data communication infrastructure for all corporate business processes. The main requirements are that this data communication infrastructure must provide all network services to meet the specific requirements of the separate process information streams and all at maximum security. It has been recognized that security is very important for a corporate network because business processes rely heavily on a corporate data communication infrastructure and a poor secured network can make the corporate business very vulnerable.

Because the common data communication infrastructure must fulfill the specific requirements of all business processes at a high level of security this cannot be accomplished easily by integrating and adapting existing networks and devices. The bottom line of security is to get and stay in control! In other words, whenever a device, system or complete network is being connected to the common data communication infrastructure, strict configuration procedures must be in place to assure secure operation.

For this reason a total new network design is made with security as an integral part of it. Only when security is planned from the beginning a corporate network can be well secured. This implies also that during the operational phase of the network security is an ongoing process conform the proactive model. The proactive model enables network administrators to perform risk analysis, network monitoring, intrusion detection, protect systems and establish controls and policies.

Because the final common data communication infrastructure must be capable of connecting hundreds or even thousands of systems in the future an IP number plan is developed. With a well designed IP number plan the network is strictly divided in network segments to separate network traffic depending on the characteristics of the data streams such as the required integrity, authenticity, security, availability and bandwidth. The IP numbers of host are predefined because of the strict hierarchical network structure which reduces complexity and therefore improves network security and maintainability.

In addition to a well designed network the devices connected to the network must be considered also, in order to implement a secure networking environment. Therefore after selecting an operating system the operating system was completely hardened for the target application. For communication outside the secure network a perimeter network was designed with proxy servers to provide information outside the network in a secured way.

Conclusions

Information demand of the gas transport process is increasingly growing due to the additional services provided for the open gas market over the last few years. Therefore the data communication facilities have been expanded and resulted in several separate and dedicated networks to implement these services. However the evolved diversity of data communication networks had a negative impact on the maintainability and complexity of the networks and so lead to an increase of costs. For this reason a new common data communication infrastructure has been designed to reduce cost, but requires a more secure networking environment which can be achieved more easily for a less complex network.
# TABLE OF CONTENTS

1. Abstract
2. Introduction
3. Problem description
4. Targets
5. Strategy
6. Network design
7. Network implementation
8. Results
2. Introduction

As a result of the open gas market the business activities gas transport and gas trade are unbundled now and shippers have gained access to the gas transport network enabling further evolvement of the gas market. Because the gas transport component is a significant part of the total result of a business transaction the information demand of gas transport is increasingly growing. The network operator however is responsible for the information provision of metering data to shippers and the required data communication facilities are therefore extremely important for the network operator.

Metering data is however only one component of the numerous information streams required to perform gas transport business. Continuous operation of the gas transport network in order to execute all transport contracts also requires an extensive telemetry network for remote monitoring and control and a complex central transaction system with data communication facilities to shippers to process all hourly based transport allocations, perform contract verification, evaluate balancing and as a result submit confirmations. In addition the operational and maintenance staff is responsible to keep the gas transport network including all equipment in optimal condition and perform modifications and upgrades to the gas transport system with little or no impact on transport capacity and all at minimum cost. This means that for the operations and maintenance process the information need is also growing and therefore data communication facilities are installed for this purpose too.

The rapid expansion of information demand during the last few years required many modifications and extensions to the data processing infrastructure and resulted in a dedicate and separate network for each separate business process and therefore lead to an increase in cost of the data communication infrastructure due to an increase in inefficiency and complexity. Due to this complexity new projects to implement new functionality or modifications to the current data processing infrastructure requires more project execution time while the market requires fast changes. In addition transport business becomes more and more dependant on the corporate automation and data communication infrastructure and so the availability requirements increase also.

3. Problem description

The automation of the gas transport system consists of the central systems, data communication facilities and de-central systems. The central systems collect data from the de-central systems in the field via data communication facilities. This data is mainly used for monitoring and control of the gas transport system via the telemetry system and billing via the metering system. The de-central systems consist approximately of:

- flow capacity metering systems on 1100 locations;
- quality metering systems on 100 locations;
- export metering systems on 16 locations;
- telemetry systems on 600 locations;
- blending, compressor and nitrogen station control systems on 30 locations;
- pressure reduction, flow injection station control systems on 20 locations;
- pressure reduction and flow measuring systems on 80 locations;
- peak shaving system on 1 location;
At this moment all metering systems for gas volume and quality data are connected to the central metering system for billing via a dedicated network. The telemetry outstations are connected via another dedicated network and used for monitoring and control of valve, blending, compressor, nitrogen, pressure reduction, peak shaving and injection stations.

It is foreseen that most of the de-central systems must be replaced in the near future and in addition the X25 networks for telemetry and metering must be replaced by a IP VPN network because of the end of life declaration of the X25 network in 2010. Because of the required upgrade of the network and field systems this offers not only an opportunity but also a need for optimization of the network and field equipment. Optimization will obviously result in cost reduction but in order to realize the replacement of such a large amount of systems and network connections a detailed project plan is required to meet the deadlines at a high quality level.

4. Targets

To meet the primary targets related to cost, time and quality the following derived targets have been identified:

- decrease hardware diversity;
- functional integration and flexibility;
- increase lifecycle of new or upgraded systems;
- uniform control and presentation;
- uniform construction and installation;
- maximum use of market standards;
- improve knowledge of engineering/maintenance employees;
- improve knowledge of operational employees;
- reduce project execution time;
- reduce maintenance effort;

Over the past 10-15 years many systems were installed in the field by many system integrators and each system integrator used equipment from different suppliers which resulted in an installed base of a vast variety of equipment, systems, controllers, I/O boards, parts etc. Although there was a list of preferred vendors and system integrators in the past it was only applicable for a short period of 3-5 years where after a new selection was performed on the market. The diversity of hardware in the field requires at the moment a great effort for the maintenance and support staff, and a lot of knowledge of maintenance personnel in the field. Spare parts must be available of all systems and equipment, maintenance people need to have knowledge of all this equipment, training is required frequently to keep people in the field skilled and up to date. It is evident that only a decrease of hardware diversity will reduce this effort.

Many small and similar systems are build only as a solution for one problem because normally, when a particular solution was needed, a project for that particular problem was initiated and executed conform the standard procedures. However when the same problem arose more often, again an another complete separate project was executed and so lead to many similar systems but each implemented with complete different equipment, software and/or interfacing. Systems should however not be build just to solve one single problem but to solve a whole range of problems. So if possible more flexibility should be build in from the beginning by means of the installation of optional hardware, and application configuration. In addition functionality of other systems can often be
integrated at minimum cost but reducing total cost of ownership because of the reduced installed base/diversity.

One of the targets to reduce the diversity and amount of equipment is to increase the lifecycle of systems and equipment. When spare parts cannot be guaranteed the lifecycle will normally be less than 7 years and therefore the number of projects for system replacement will increase and so will lead to a diversity of systems. Therefore we decided lifecycle must be guaranteed for a minimum of 15 years.

Although hardware construction and installation is important for every system, software engineering becomes more and more important because of the required increasing functionality and complexity of systems. However, while hardware engineering is mature and quality is high due to many international standards, software engineering is still poor for the same reason, a lack of international standards. In addition when distinct system integrators are implementing similar systems the diversity in control strategies and process visualization/control is again considerable. For the maintenance and support staff it is therefore very time consuming to perform bug fixes, software changes or functional changes and this is getting even more worse when different types of systems are involved. Operational people need to have knowledge and expertise of every separate system concerning presentation and control. For example similar functions will probably react on each separate system differently which could lead to unsafe situations.

As said before the quality of hardware construction of an installation is at a high level now. However to keep similar systems uniform and to guarantee spare parts for the future the use of materials and equipment must be prescribed comprehensively. In addition the design and construction of system cabinets needs to be specified in detail to avoid differences. For example, to comply with the EMC requirements construction is very important and because only a few experts have knowledge of these requirements, strict guidelines for construction are very important.

In the past most control systems where making use of proprietary hardware and software. This required experienced people for every part of the system in order to implement or modify hardware and/or software. Because of the required special knowledge it was only possible to have a few well trained and experienced system managers of every system for maintenance and once the system was obsolete again the knowledge was worthless. In order to achieve more flexibility and efficiency of the human resource pool, investment in knowledge must be more sustainable and so useful for many different systems. For this reason systems are required which make extensively use of standards for hardware as well as software. Because of the use of standards, maintenance people can be employed for many different systems and job rotation can be performed without great impact while the knowledge is preserved. The same is valid for engineers. For example the use of the IEC 1131 standard will preserve the programming language knowledge of employees and in addition, efforts in engineering are also preserved when adopting another process control system.

Knowledge of maintenance, engineering and operational people can only be retained if the knowledge is sustainable by making use of both international standards and corporate standards. Only in this way it is possible to keep the knowledge within the company which is essential for the core business of a company.

During engineering and construction many activities are very time consuming and not strictly necessary because people quite often are reinventing the wheel. For example for several reasons loop diagrams or software diagrams are often completely rebuild. To decrease project execution time these repetitive activities must be recognized and organized centrally, apart from the projects, where multiple projects can make use of it.

Because of standard hardware and software for PCS and SCADA less maintenance effort is required however without effective maintenance facilities maintenance effort will still increase again. Because of the ever increasing information demand all systems will be connected to an IP network for data flows such as telemetry, metering, performance data, support and remote operation of plants and
so this is a potential security risk and requires more maintenance effort. In addition, because of the rapid changing gas market, modifications to the gas transport system must be performed more often and within shorter time periods. Therefore remote maintenance facilities are required to keep the system secure by monitoring the system and installing the required security patches and upgrades. In addition, modifications to a PCS or SCADA system can be performed remotely without the need for a to travel to each station for a minor change. Also when local support is required from a specialist (supplier or system manager) this can be performed secure and managed via the network instead of installing dial in modems for remote access.

5. Strategy

To meet the targets to reduce the diversity of systems, increase knowledge, realize uniform process control and presentation, perform fast project execution the following activities are required:

- Design of a common data communication infrastructure for all systems;
- Standardization of Process Control System (PCS);
- Standardization of SCADA system;
- Selection of preferred system integrators for the long term;
- Building standard software libraries for the PCS system;
- Building standard software libraries for the SCADA system;
- Building hardware standards;

The existing data communication networks for metering, telemetry, maintenance and back office must be integrated in one common data communication infrastructure. This will not only reduce the amount of equipment in the field for network connectivity but also the number of data communication lines/points for the network provider. In addition network management can be integrated and carried out by one department and it will be easier to develop corporate wide network management policies. Every station in the field will have only one physical network connection with many logical network connections available, which means connectivity everywhere for all business processes at minimal cost. Once a network connection is required for telemetry or metering it is a minor change to add a logical network connection for the back office or maintenance and support.

For standardization of the Process Control System a European selection of a single supplier was performed. The aim of the selection was to choose one process control system for a period of 10 years with an option for another 5 years. In this selection the use of international standards for the Process Control System was very important. For example it was required that the SCADA interface complies with the OPC standard and the programming language complies with the IEC-1131 standard. This does not only guarantee that investments in knowledge will be preserved but also engineering efforts will be preserved because software can be reused in the future if a different PCS would be selected after the contract period.

Standardization of the SCADA system was similar to the PCS system which means the selection of a single supplier for a period of 10 years with an option for another 5 years. A separate European selection was done for both, PCS and SCADA in order to get the best of both worlds. For connectivity with PCS an OPC interface was required. Experience from the past showed that SCADA systems where already obsolete within 7 years and had to be replaced. For the selected SCADA supplier support is guaranteed for the contract period of maximum 15 years which is very decisive because of the short life cycle of PC hardware and the Windows operating system.
Two system integrators were selected in an European selection procedure. It was required for the system integrators to adopt and apply the selected PCS and SCADA systems for all future projects. An important advantage of selecting for PCS and SCADA a single supplier was of course commercial, more discount because of the purchased product volume, and building up a strong relationship with these suppliers. Because the cost of both PCS and SCADA is relatively small when compared to the total project cost of a process control system two system integrators have been selected for competitive reasons.

In order to realize uniform control and presentation for all future systems standard software libraries are build for both PCS and SCADA. The feature of creating libraries was one of the requirements of the PCS and SCADA selection to enable the reuse of software but also to perform software updates with minimal engineering effort. The software libraries must be used by system integrators for every new process control system and will reduce the project execution time significantly.

With the selection of a PCS and SCADA supplier the hardware components of these systems are also standardized. Standards are also developed for loop diagrams, power supply and installation materials. To avoid diversity of construction a detailed standard specification is available with special attention concerning EMC. Once the system integrators are experienced with construction in projects it is expected the systems are highly uniform.

6. Network design

For the network design the requirement was to develop a common data communication infrastructure for all corporate business processes. Because the data flow for each business process can have completely different requirements in terms of availability, response time, band with, security etc. the network must support logical networks to ensure a logical segregation of data flows. For example a logical telemetry network requires a high availability and fast response time in comparison with an office network which requires a high bandwidth and lower requirements on availability and response time. A common data communication infrastructure must be able to implement such a logical segregation of networks. Most network providers can provide this kind of network services today as a Virtual Private Network. One important issue of a data communication network involves network security.

It has been recognized that security is very important for a corporate network because business processes rely heavily on a corporate data communication infrastructure and a poor secured network can make the corporate business very vulnerable. Security must be an integral part of a network design and is only effective when planned from the beginning of a corporate network. Risk management of a corporate network is an ongoing process and must be implemented conform the proactive model to enable network administrators to perform risk analysis, protect systems, network monitoring, intrusion detection and establish controls and policies. The bottom line of security is to get and stay in control! In other words, whenever a device, system or complete network is being connected to the common data communication infrastructure, strict configuration procedures must be in place to assure secure operation.

For a complete design of network at least the following activities are required:

- building a business process model;
- identify digital assets and business data flows;
- identify risks;
- protect digital assets and business data flows;
- identify and remove vulnerabilities;
- establish policies;
- specify requirements of digital assets and business data flows;

Only when you have a complete business process model you know exactly where the digital assets reside and how data flows over the network. Only when this picture is complete, risks can be identified and appropriate measures can be taken for protection. The risks can be:

- loss of data or corrupt data;
- unauthorized access to confidential/classified data;
- uncontrolled inbound/outbound data flow;
- server/workstation compromise;
- application compromise;
- denial of service;

These risks can be expected from hackers and crackers who can reside inside as well as outside your company. In addition many risks originate from Viruses, Worms, Trojans, Hoaxes, Malicious application/web Scripts or Denial of Service Attack. To protect against these risks measures are required on both network level and server/workstation level.

Protection of the common data communication network alone is not sufficient but in addition all connected host systems must be protected adequately. As a summary the following protective measures are required:

- **Network**
  - Physical access of network equipment;
  - Logical access of network equipment;
  - Network monitoring/event logging;
  - Minimize protocols and complexity;
  - Intrusion detection;
  - Network separation;
  - Network isolation;

- **Host systems**
  - Physical access of host systems;
  - Logical access of host systems;
  - Operating System hardening/stripping;
  - Operating system updates/patches
  - Audit trails/Event logging;
  - Virus scanner;

**Network**

It is obvious that physical access to network routers, switches, firewalls etc must be restricted for unauthorized personnel. So network rooms must be locked including cabinets of network equipment. Only routers and managed switches shall be used to avoid unwanted access which is for example the case with hubs. Hosts shall be connected via managed switches only with minimal MAC address protection, line detection and event logging on a central management system.
Management of routers and switches is normally possible via both, local ports and network connections. Local access must be blocked by password protection and any access must be logged on a central network management system.

Routers and switches shall send events when an abnormal situation occurs in a network such as an increase in network traffic, connecting/disconnecting lines, unexpected IP addresses, configuration changes etc. All network management traffic shall be send via a dedicated management network connected to a central management system. In addition to event logging it shall be possible via the management network to change and verify router/switch configurations and verify constantly if network equipment is still up and running.

To keep the network manageable and secure it is necessary to minimize network complexity. A minimum number of protocols should be allowed on the network. For example for process control networks NetBIOS is only allowed on the local LAN segment and because the network for process control is very static, DHCP is not used but static IP addresses are used. It is preferred that data flows are predetermined so that a small network configuration change cannot lead to unpredictable network problems. Therefore for process control static address routing is used and routing protocols are disabled which could be another potential security risk.

An Intrusion detection system or IDS is a system that automatically detects, alerts and takes protective measures when an intruder is attempting to gain unauthorized access to the network. Preventive protection of the network is not enough but in addition the network traffic must be monitored all the time to signal an intruder at an early stage. When installing a network based IDS all traffic is scanned for any anomaly and an alert is sent to the network management system. To keep the IDS system simple it should be placed only on vital spots of the network.

Network separation means that different kinds of data flow with different requirements are separated on one physical network by means of logical networks. Because of the different requirements is must be possible to implement for each logical network a Quality of Service (QOS) including requirements on throughput, delay, jitter, availability etc. By means of network separation the network can be optimized for all network traffic and security is enhanced because data flow in one logical network cannot influence a data flow in another logical network. Most of the routers of today provide enhanced functionality for network separation next to the normal routing functionality of network traffic. The router configuration must be performed conform the exception model when implementing the routing rules. This means that the configuration is started with blocking all traffic first and subsequently open only what is required.

Network isolation is the physical separation of network traffic. For example when connecting servers/workstations to the network these are connected directly to a switch. Separate logical networks can terminate in one common switch or separate switches. One can imagine that for some important and large plants each logical network is terminated in a separate switch while on a lot of less important and small plants where only two logical networks are required a common switch is used. Because of the two distinct network addresses the connected servers/workstations of one logical network will not be able to communicate directly with the server/workstations of the other logical network. However as a consequence there may be some influence on bandwidth off each logical network.

Host systems

Physical access to network equipment must be restricted as well as for the host systems. As a minimum, servers must be installed in secured areas and installed in locked server cabinets. In addition the use of modems and notebooks should be restricted or forbidden as well as access to removable media to avoid the risk of bypassing security measures.
Logical access of host systems involves the local access via the console and remote access via the network. Local access must be restricted via strong passwords or preferably via smart cards/keys. Rebooting of a server by means of a floppy or CD should not be possible and the power-on password should be set as well as the BIOS password. Remote access via the network must be possible only after user authentication and the use of logical networks must restrict access to hosts via the network. So a host can only be reached from predetermined points in the network as configured in the routers. Note that the routers are configured conform the exception model. So initially all network traffic is blocked where after for each data flow a rule is configured.

Operating system hardening/stripping is the process of improving the security of an operating system by the configuration of security settings and removing applications and network services. The configuration of security settings in the Windows environment is performed by means of security policies. Many security guides are available on the internet to assist you such as the Windows 2000 Security Configuration Guide of Microsoft or the security guides of the National Security Agency. In addition all applications and network services which are not used or required for a host system should be uninstalled or at least disabled to eliminate each potential security risk. Note that the operating system hardening/stripping should be part of the operating system installation procedure to avoid an possible early compromise of your system.

Despite all the measures to secure the operating system, exploits or leaks are discovered from time to time. Therefore it is important that all host systems are kept up to date with the latest security patches and upgrades. For the process control plants all issued security patches must be reviewed in advance and gathered to be installed at a appropriate moment in time. All security patched must be tested in combination with the applications where after the roll out and installation will be done manually by each system manager. Manual installation of patches and updates is required, first to avoid an undiscovered fault to spread out over all systems in a short period of time and second because automatic installation requires an additional network service which is another security thread.

To monitor the performance of the system and signal any misbehavior concerning security in an early stage the policy settings must be configured to log audit trails and events. In case of a direct threat an alert must be sent to a central management system for proper action. To guarantee the availability of a system performance alerts must be sent also.

Another counter measure of security risks is the use of virus scanners. This is especially important when the system can communicate with the internet and email. For the process control systems and networks, internet and email is prohibited and so none of these network services are installed. In addition the use of removable media is normally blocked with the exception of a few workstations where a virus scanner must be installed.
7. Network Implementation

The common data communication infrastructure is implemented as a strict hierarchical network which can be completely redundant. Refer to figure 1.

All process control plants are connected to a IP VPN provider by means of a single physical network connection which provides connectivity of all plants to the head office. In addition the IP VPN provider is responsible that each plant can have only direct access to the head office (Black lines in figure 1). This means that when two plants have to communicate the data path must go up first to the
head office and then back to the other plant. The allowed communication paths including the initiation of a connection must be configured in the routers (Red arrows in figure 1). When a high availability is required the network can be installed completely redundant including an alternative central location.

A hierarchical network topology is very cost effective because first off all, network configuration and management is straightforward. Only one connection to every plant with possible multiple logical networks can exist. Because the network topology is strictly hierarchical which coincides the logical network structure the routing configuration is simple by making use of Classless Inter-Domain Routing (CIDR). Even when encryption is required one IPSec tunnel for each plant will be effective in most cases and only in very high secure applications IPSec is required directly from the host. Another reason a hierarchical network is cost effective is because expensive and high maintenance effort equipment such as firewalls and intrusion detection systems are installed at one central location where specialized personnel is available.

To implement logical networks for data flow segregation, determine routing rules and IP numbers an IP number plan is an absolute necessity. With a well designed IP number plan the network is divided into sub networks by means of CIDR to separate data traffic of different logical networks. In addition the IP numbers of the hosts are static to improve security by enabling IP filtering and removing the DHCP network service. Also routing is completely static and so no routing protocols are active. More important is that with a strict hierarchical network the router configuration is predetermined and so can be automatically generated. Although this is not implemented yet the intention is to generate the router configurations in the near future and load/verify the configurations in each router. For the network only (border) routers and managed switches are used and for vital plants a dedicated switch is used for every logical network.

At the central location some common network services are installed and a perimeter network including proxy servers for communication outside the network in a secured way. One of the central services is a login server. In fact this is a domain controller however it is only used for the purpose to enable users to login with a single user account on the network. No policies are configured on the domain controller for the host systems because a fatal error of an administrator might spread out to all systems in a very short time which is not acceptable. All host systems must be able to run autonomously for a long period of time without domain controller. Windows allows a maximum of 50 logins, if configured, before the account is locked when the domain controller is not available. The perimeter network is used for connection with the outside world. All inbound/outbound network traffic has to pass the perimeter network including a firewall and IDS system. Proxy servers are installed so that no direct connection to a host system in the network is possible to obscure any internal IP number for the outside world for security reasons.

8. Results

A pilot is started at the end of 2005 and involved the upgrade of 2 gas plants and the installation of central systems connected to the common data communication infrastructure. The purpose of the pilot is to verify if the installation of the network connections and servers/workstations can be performed fast and properly and if all security measures are adequate under the condition that the gas plants are functioning correctly with sufficient performance. If necessary correction measures will be taken where after the installation and maintenance procedures will be formalized. One of the main efforts was the hardening of the operating system for the SCADA systems and engineering work stations. This resulted in a DVD for a complete unattended setup of a hardened operating system including all required applications and network settings. Also the IP number plan has been finished and tools are developed now for the automatic generation of network diagrams including
IP numbers/network masks, host table and router configurations. To limit human errors in the router configuration the automatic generation of router configurations are planned.