DeltaV Remote Operations

This document examines the technologies and architectures required to meet remote operational requirements as part of a larger iOps strategy.

Remote Operations functionality connects multiple production facilities to a central control room with secure network technologies. It is based on standard DeltaV hardware solutions integrated into the corporate infrastructure to bring the same local user environment to the remote operators. It is an integral part of the overall iOPs solution from Emerson.

Table of Contents

Introduction

In the competitive business landscape within the process industries, controlling and reducing operating costs is front-of-mind for all industry executives and plant managers. When it comes to operating and managing production facilities located in remote geographic areas of the world, high operating costs, employee safety, staff retention, and operational excellence are key issues. Reducing the size of the workforce in these remote locations represents a significant opportunity to drive cost from these operations by relocating Operations personnel and key support staff to more central urban locations.

This paper looks at the challenges associated with remote operations and the methods Emerson leverages within the DeltaV distributed control system to meet these challenges. This paper is intended to document a control system architectures for both remote operations as well as remote access. The goal here is to identify key requirements for a successful control system deployment for a Remote Control Room, a key component for some organizations migrating to integrated Operations business models.

Executive Overview

For some organizations, Remote Operations is a corner stone in moving to an Integrated Operations operating strategy. To do so, delivering high performance control room capabilities to remote control centers which enable real time operations is a requirement. The key to providing this capability lies in the Network Infrastructure and Cyber Security architecture that links the production facilities to the central control room. DeltaV has been used for remote operations for decades, first with Remote Access Services embedded in the control system, and more recently with Remote Client Servers. With the evolution of remote connection solutions in the Information Technology space, end users are now able to access the control system Operator environment more easily and more securely than ever before. DeltaV provides this connectivity using standard technologies based on Remote Desktop Protocol which is embedded in the Windows Operating system as a native Remote Client product, to deliver the additional security required in industrial process control applications.

With modern virtualization technology, standard DeltaV products, and common network infrastructure, a highly secure, robust connection between the control room and the production operation need no longer be constrained to local plant networks. Today, the geographic location of the Control Room can be independent of that of the production facility. They can be located hundreds or even thousands of miles away from the operation just as easily as next door if required.

Drivers for Remote Operations Initiatives

The business drivers associated with relocating the control room away from the physical operation: the high operating cost of operating remotely, health and safety considerations, business performance improvement, and the location of key skilled resources. Housing staff on an off-shore platform and the Helicopter flights to and from the asset represent added expense as well as greater HSE risk for organizations for organizations operating in off-shore oil and gas. Relocating workers to a central onshore location eliminates both cost and risk to the organization and allows workers be home when their shift is done. Similarly, at Fly in / Fly out operations, flights and the added expense to accommodate workers at remote operations is a strong business driver for organizations to closely look at remote operations. High employee turnover is another factor considered by organizations with remote operations. Relocating staff can improve employee retention, driving down HR and training costs, and help extend the careers of experienced employees.

Emerson differentiates between Remote Plant Operations and Remote Plant Access. The critical functions provided by the Control Room Operator requires a responsive Operator Console with 24x7 availability. The Control Room enables the real-time operation of the facility in a secure environment where authorized individuals monitor and take actions to ensure the safe and reliable operation of the facility. Operator Consoles are dedicated stations designed for a specific purpose in a demanding service.

In addition to operations staff, access to the control system is often required by Engineers, technical staff and 3rd party service providers for a variety of engineering and support functions. For these users, the system must be flexible enough to allow access from a wide range of physical locations, including internet access via VPN secured networks.

DeltaV solves both connectivity requirements with the same underlying technology, Remote Desktop Protocol from Microsoft. For **Remote Access**, the user is connected to a Remote Desktop Server over the existing network infrastructure with standard products familiar to IT professionals. These connections are important, but not critical to the 7x24 operation of a facility. They are widely dispersed and must be secured to protect the networks at all levels. Alternately, for **Remote Operations** the remote connections are restricted and isolated to deliver performance as well as high availability.

The combination of Remote Operations and Remote Access provides the flexibility to deliver DeltaV operator and engineering access to all users where they are located. Both solutions are based on standard DeltaV products, designed to be integrated into the customer's operations philosophy.

DeltaV Remote Access Architecture

The DeltaV Remote Client product is specifically designed for Remote Access users, wherever they may be located. The architecture is based on the Microsoft Remote Desktop servers (RDS). The DeltaV Remote Client server runs DeltaV software to serve Remote Windows sessions running DeltaV applications. Each session can be dedicated to specific users and/or specific Client Stations, such as production engineers, technical staff, or off site users at the business level. Access could be extended to users over the internet with appropriate controls.

DeltaV Remote Client users may be located anywhere in the company's network infrastructure. The Remote Client Server is located on the highly secure Control System network and is connected securely to the production facilities site network, or L3 network DMZ via firewall. Users at the L3 layer, such as production engineers, technicians or mobile workers can access the remote sessions over this network. For users in the L4 or Business LAN layer, an interim "Jump" server is placed in the L3 DMZ, allowing these upper level users to gain secure access to the L3 layer, and then make a connection to the Remote Client server. This jump server functionality is a standard feature of Microsoft Servers, known as an RD Gateway. This server allows security credentials from the L4 network to remain separate from the L3 and L2 security credentials. External users may access the L4 network via VPN, and from their, access the RD Gateway and Remote Client server. RDP protocol provides an efficient connection that adjusts to network performance to maintain a responsive connection.

The design of this network infrastructure typically follows the ISA95 model which defines the connectivity from the least trusted external networks to the highly trusted production network. Cyber Security concerns drive many of the design features of this network, including the use of DMZs and interim jump servers. Because of the wide range of possible users and reduced physical security of their locations, this network must apply a layered approach to protect the mission critical Control System and associated assets. The DeltaV system provides integrated tools and complementary products to meet the Cyber Security standards as recommended in IEC62443. These are detailed in the DeltaV Cyber Security manual.

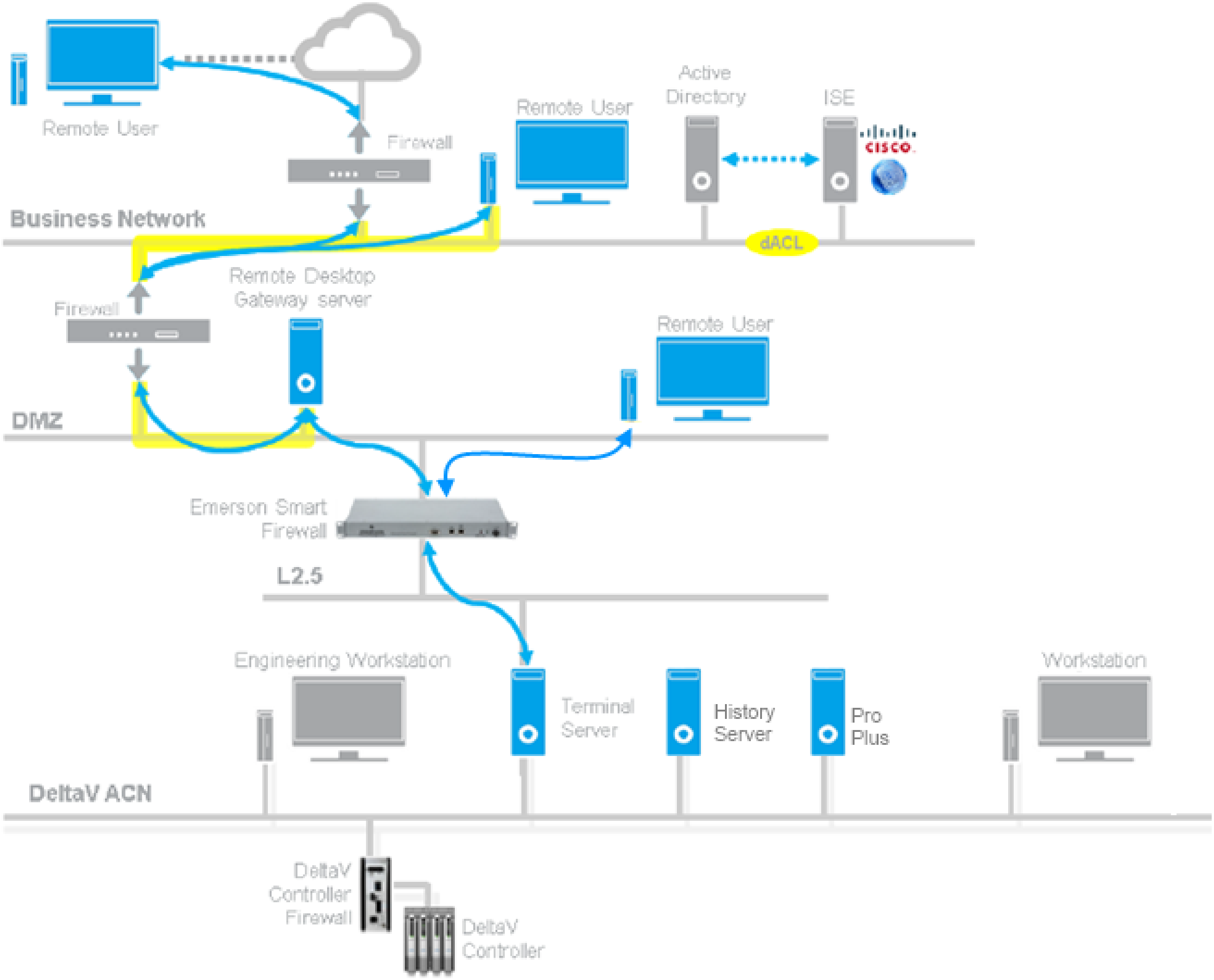

Figure 1 - DeltaV Remote Client architecture

The architecture in Figure 1 shows the flexibility provided by Remote Client Servers and a well designed Cyber Secure network infrastructure. There are many variations on this topology and many solutions for increasing availability. However, in this model, loss of network connectivity is not uncommon as server maintenance or security threats may force a shutdown of network sections or affected servers. For Remote Access users, interruptions to system connectivity is tolerable, within reason. This network is a balance of access with security, and the priority is security.

DeltaV Remote Operations Architecture

The Remote Operations solution from Emerson serves a different kind of user. Production Operators require access to the process as the utmost priority. Loss of view to the process is not an acceptable situation. To serve this high availability requirement, a different network architecture must be considered. The Remote Operations solution is based on standard DeltaV products deployed in a secure Network infrastructure to connect the central control room to the remote production facilities. At the core of this architecture is the DeltaV Virtualization Environment, based on the Dell VRTX hardware and DeltaV Virtual Studio software, creating a robust, high availability platform for mission critical Operator nodes. The VRTX hardware is installed at the production facility, connected directly to the production Area Control Network (L2). The Operator Station virtual machines are connected to the Operator consoles via the Thin Client network, which is extended from the production facility to the Central control Room.

This Thin Client network is reserved for the Remote Desktop Protocol connections between the Operator console and the Virtual Machines. No other connections are permitted on this network. The secure nature of this network is therefore extended to the remote control room and remains isolated from all L3 and L4 users. Where available, dedicated Optical Fibers should be used, connecting the remote facility to the central control room.

Extended Thin Client network

The design of the Extended Thin Client Network is dependent on several factors. The primary influence is the available network bandwidth and latency between the remote production facility and the central control room. Another important factor is the availability of this remote network connection. In many cases, this connection is leased from commercial suppliers in the form of dedicated Fiber connections. No other traffic shares these fibers. Fault tolerance is also highly recommended where the production facility is de-manned and loss of view is not acceptable. Separate redundant fiber connections should ideally use separate paths to avoid loss of both connections at the same time. A redundant network delivers the highest availability.

For a given implementation, the network design takes all the technical challenges into consideration, along with the Cyber Security requirements of the customer to design an acceptable infrastructure. The goal of the design is to connect a secure network segment in the central Control Room to the secure Thin Client network at the production facility. The requirement is for this connection to be fast, reliable and secure, and it must be affordable.

The required bandwidth of a DeltaV Thin Client station is dependent on the type of information contained in the Operator Displays. Detailed Bitmaps add to initial display call up time, while more complex animations can add a constant baseload. Integrating CCTV into Operator Displays will also increase RDP bandwidth baseload requirements. For this reason, separate CCTV monitoring on dedicated screens allows the network bandwidth to be prioritized through Quality of Service and VLANs over the remote network link. This ensures Operator station responsiveness, sacrificing bandwidth on less critical data streams in times of increased network demand.

Table 1 – Network bandwidth load for RDP Monitor

Number of Monitors	Typical HCD display	Highly animated displays	Integrated CCTV*
4	2 MB	4 MB	10 MB
8	3 MB	6 MB	19 MB
16	5 MB	10 MB	29 MB
32	8 MB	15 MB	72 MB

* Integrating CCTV streams into Operator increases RDP bandwidth and can impact the required network bandwidth to display these video images on the Operator Console monitors.

Thin Client Network Security

The preferred architecture is to extend the Thin Client network directly to the central control room via a secure network. The ISA95 model identifies network layers and application connectivity but does not speak to physical hardware or specific security solutions. The Central Control room requirements must be balanced with cost, security, and performance that are in line with the business goals of the end user. The number of remote Operator consoles and available network bandwidth may allow a user to leverage their existing infrastructure to accomplish Remote Operations and meet their availability needs. However, sharing network infrastructure through VLANS and relying on Firewalls to secure the Thin Client network may also require the addition of jump servers. This adds complexity to the network and ultimately impacts availability and cost.

The DeltaV Thin Client network is available as simplex or redundant. By extending a redundant network infrastructure through disparate paths, over dedicated fiber, the secure control room network is extended without compromise in security and with the highest level of responsiveness. Additional measures can be taken to manage the content of this network, including encryption and Quality of Service (QoS). Each application requires careful consideration and attention to meet the user’s requirements at the best possible cost. By isolating the Thin Client network, access to this network is only available from the endpoint devices. No access is provided to users at the L3 and L4 layers of the infrastructure.

The Thin Client computers in the central control room are secured by both physical access means, as well as password and optionally biometric authentication. Additional security mechanisms such as Access Control Lists and tight Firewall rules ensure that only authorized users on specific workstations/consoles have access to the Thin Client network to the remote production facilities.

Thin Client Availability

Availability is one of the critical elements to Remote Operations. Loss of view due to network outages cannot be allowed. To that end, the network must be designed with Fault Tolerance. The remote network design will use alternate paths and even different suppliers to ensure high availability for mission critical communications. Within this infrastructure, the Thin Client network is carved out with appropriate bandwidth. The RDP protocol is perfectly suited for this environment. There are no proprietary protocol requirements to consider for the Thin Client network, only availability, bandwidth and security.

A typical network diagram shows how the Remote Control Room Operator stations are connected to the site Workstations virtual machines. In this scenario, the L4, L3, and L2.5 networks are bypassed by a secure, segregated network dedicated to the Operator Interface environment. There are no connection paths to this network from any other network. This provides the highest throughput and lowest latency between the control system and remote control room.

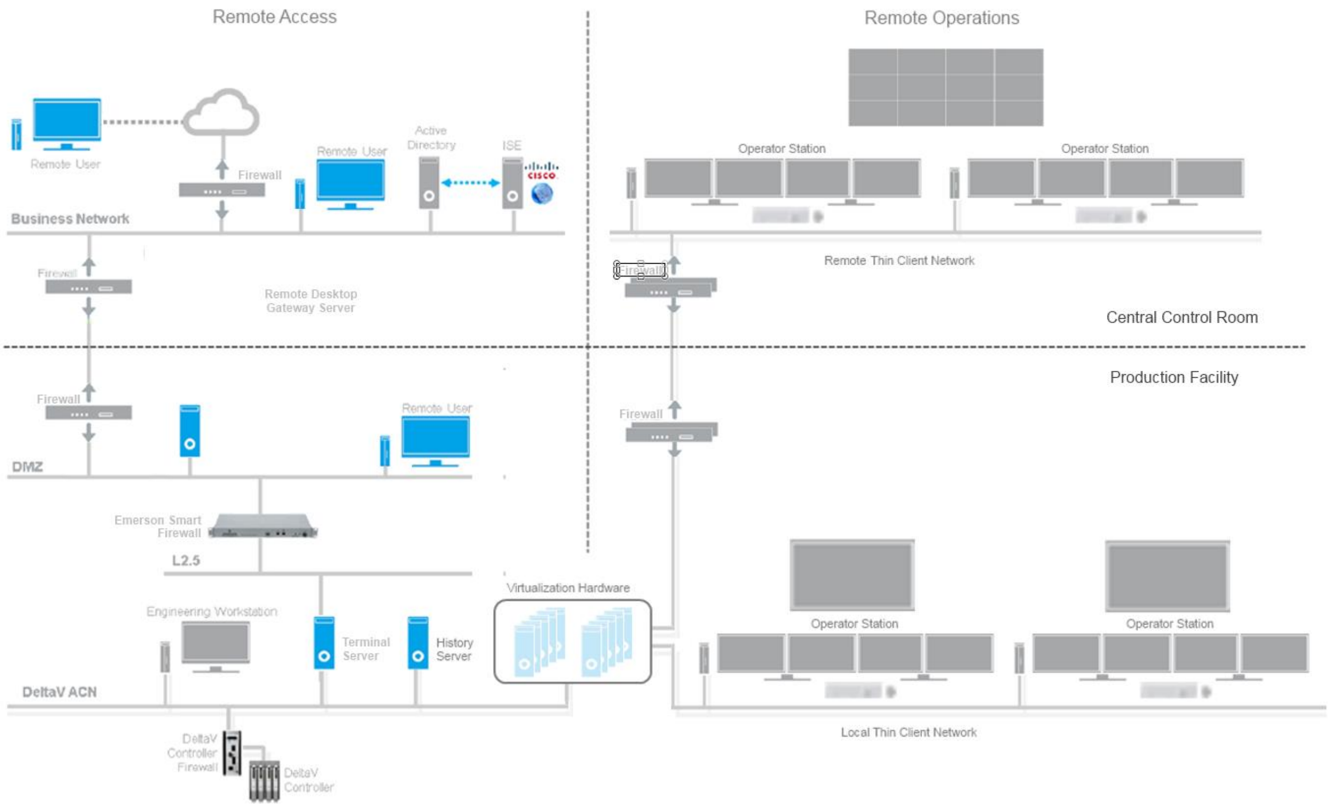

Figure 2 – *Remote Operations Topology*

In the architecture above, Operator Stations are located both at the Production Facility, and the Remote Operations Control room. The system has been setup with separate local and remote Thin Client networks. A Remote Client Server is connected through the L2.5 network to the L3 Jump server for Remote Access users on the business layer. The Remote Thin Client network is an isolated, secure and redundant network connecting the Operator Stations to their Remote Thin Client consoles located in the remote Command Center control room, delivering high availability and real-time responsiveness to these remote operators. Note that only Operator Thin Client stations are connected to this isolated network. The Operator Station software and computers are isolated from these supplemental information sources as dictated by Cyber Security guidelines of the end user.

Collaboration Workstations for iOPs

The secure network connection from the central control room location can extend to multiple remote facilities, allowing operators to manage multiple sites at the same time. It also allows these operator consoles to incorporate enhanced collaborative tools. The Workspace servers provide a highly evolved video management software to allow operators to access many different sources of data in a single user environment. One of the key features of this solution is its collaboration interface, which allows a data source to be shared as a web page with other users, allowing both to see the same live image streaming to both user’s computers. The remote Thin Client network is an enabling technology for this collaborative Workspace environment.

Summary

The combination of Remote Operations and Remote Access provides the flexibility to deliver DeltaV Operator and engineering access to all users wherever they are located. Remote Operations provides the 24/7 system access for Operators to allow de-manning of remote facilities and improving the operational efficiencies across multiple production facilities with integrated operations. These solutions are based on standard DeltaV products, designed to be integrated into the customer's operations philosophy.

The DeltaV System provides proven remote connectivity with proven, standard products designed and tested for mission critical Control Room operation and highly distributed geographical access by remote users. These products can be integrated into existing network infrastructures to meet the network and cyber security guidelines of the site. For enterprises seeking to implement highly integrated operations in Command Centers remotely located from their production facilities, the DeltaV Remote Operations architecture delivers the real-time response that production Operators need in a highly secure environment.

References

References:

IEC62443 Cyber Security standard

DeltaV Cyber Security Manual

Other related Whitepapers, available at

http://www2.emersonprocess.com/en-US/brands/deltav/whitepapers/pages/whitepapers.aspx

1. DeltaV Remote Client
2. DeltaV Remote Access Services
3. DeltaV Mobile

Emerson
North America, Latin America:
✆ +1 800 833 8314 or
✆ +1 512 832 3774

Asia Pacific:
✆ 65 6777 8211

Europe, Middle East:
✆ +41 41 768 6111

www.emerson.com/deltav

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.