Honeywell

Augmented Remote Operations

Product Information Note

Experion® Augmented Remote Operations Solution (ARO) allows you to maintain full production with minimal on-site staff by augmenting your local control system with remote operations capabilities. Utilize available resources from any location to maintain operations and business continuity through a range of challenging scenarios.

Key Benefits

Maintain production during periods of on-site staff shortages
Ensure sufficient operational staff are always available by enabling remote personnel to monitor and/or control operations.

Run process operations from any facility
Utilize process operators and repurpose existing engineering stations or spare Orion consoles available at other locations.

Multi-site operations
Enable any site to share their operations with other process operations centers or remote workers at offices on your intranet.

Quick deployment
An Augmented Remote Operations Solution can be installed and running quickly with no HMI re-engineering or client installation required.

Remote expert support for critical operations
Process experts can quickly access the control system information they need to provide troubleshooting assistance and operations support from wherever they are.

FEATURES & BENEFITS

Fully Functional

- Full Experion Station and Orion Console functionality.

Secure

- User authentication enforcement with support for multi-factor authentication prevents access to Experion for unauthorized users.
- Configure read-only or read-write access to Experion assets based on the user's scope of responsibility.

Minimal Engineering

- Experion Augmented Remote Operations re-uses your existing displays and Station configuration.
- No need for modifications or migration.

Access anywhere

- Securely connect from your business intranet or via corporate VPN.

Lifecycle Assurance

- Fully supported as part of standard Experion platform.

Remote Client Connection Options

No Experion software is required on the remote client machines. Experion ARO uses Microsoft Remote Desktop technology to connect business network machines to Station or Experion Engineering tools running on the Experion ARO server. There are three client options supported.

Preferred Client

Microsoft Remote Desktop

This client provides the most flexibility for use with the standard ARO topology.

Microsoft Remote Desktop is the only client to support multiple monitors and must be used when connecting to multi-window Station (such as Orion or quad screen Consoles). This client is also recommended for remote access to single-window Station and Experion Engineering tools.

Microsoft Remote Desktop client supports up to 20 concurrent Station sessions per ARO server, 5 of these can be multi-window Station sessions.

Alternate Clients

The following clients are available for customers preferring remote access through a web browser or where more than 20 concurrent Station sessions are required.

Web Client

Remote Desktop Web client is recommended for customers requiring remote access to Station in a web browser.

This client supports a single monitor only, making it suitable for single window Station access. It may also be used for remote access to Experion Engineering tool on sites without a DMZ network.

The Web Client supports up to 20 concurrent single-window Station sessions per ARO server.

RemoteApp

RemoteApp client is recommended for customers requiring more than 20 concurrent Station sessions.

This client supports a single monitor only, making it suitable for single window Station access. It may also be used for remote access to Experion Engineering tool on sites without a DMZ network.

RemoteApp supports 40-100 concurrent single-window Station sessions per ARO server.

ARO Topologies

Standard Topology

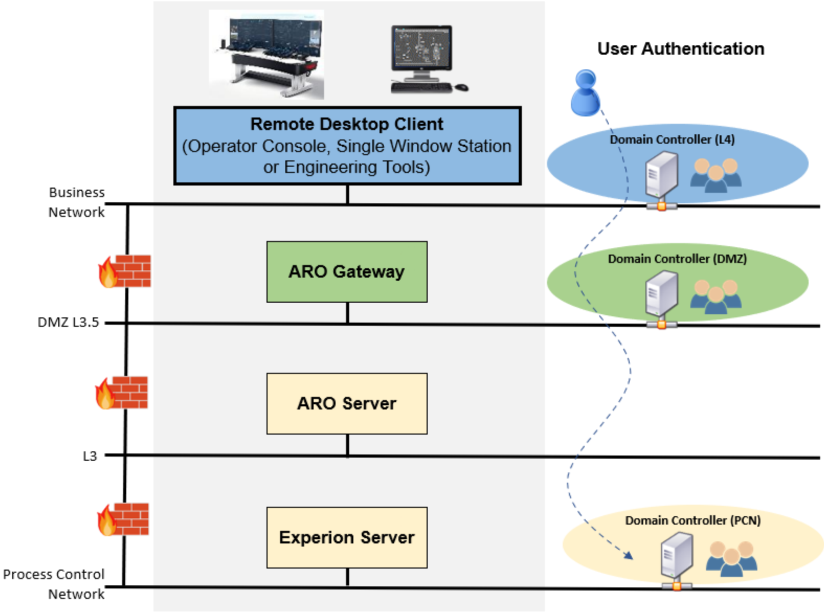


Figure 1: Standard Topology with ARO in DMZ domain

The standard topology shown in Figure 1 is best practice deployment providing the highest level of security. The topology consists of thin client machines on the business network, an ARO gateway on the DMZ, an ARO server on L3 and Experion servers on the Process Control Network (PCN). Client machines in the L4 domain connect to the ARO server via the ARO gateway. The ARO server hosts Experion Stations which connect to Experion servers on the PCN.
Users need an account on the business network, DMZ and the L3/L2 domains. The user first logs in to the client machine using their business network domain account credentials. When connecting to the ARO server the user must provide their DMZ domain account credentials. Finally, the user logs in to Station using their L3/L2 PCN domain account credentials.

Topology Variation for Remote App and Web Clients

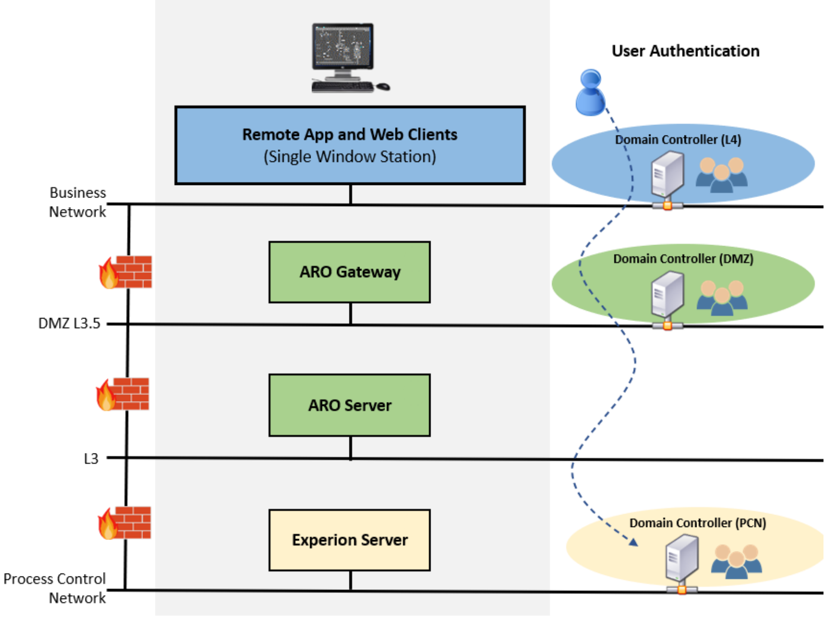


Figure 2: Topology Variation for Remote App and Web Clients

Use of Microsoft Remote App or Web clients requires both the ARO Gateway and ARO Server to be part of the same domain (DMZ). This variation is showing in Figure 2 above.

Multi-release Support Topology

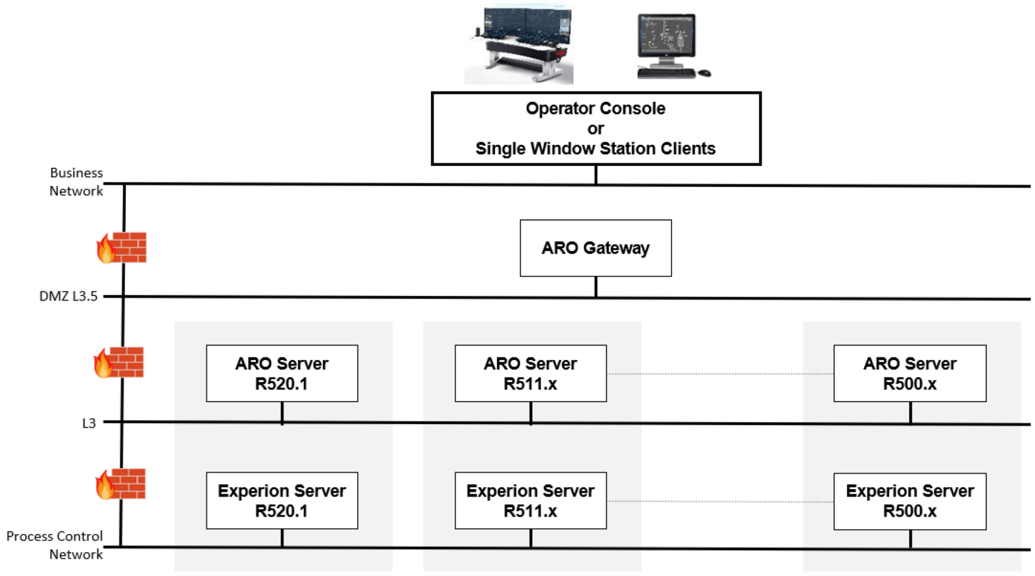


Figure 3: Multi-release support topology

As shown in the figure above a single ARO gateway node can support multiple ARO servers and releases. Each Experion release requires its own ARO server. For example, a site with R500.1, R510.1 and R520.1 would require a single ARO gateway and three ARO servers, one for R500.1, R510.1 and R520.1.

Optional Additional Security Safeguards for Standard Topology

Additional security safeguards, provided by Honeywell Cybersecurity services, are available for the standard ARO topology.

These safeguards include:

Multi-Factor Authentication (MFA)

MFA, sometimes referred to as two-factor authentication or 2FA, is an additional layer of security which requires two authentication methods to verify user identity. It is an effective way to protect against security threats which target user identification and passwords, such as phishing, user credential exploitation, or brute force attack.

Firewall pre-authorization

Traditional firewalls, which provide protection at the network and transport layer, are no longer effective against the complexity of modern cyberattacks and hacking methodologies. With the introduction of the Next Generation Firewall (NGFW), remote-access requests are filtered based on the identify-based security policies and application-layer inspection.

Additional Node Hardening Services

Additional bastion end-point security solutions can be provided to compliment the standard ARO node hardening. The hardening services include the development and configuration of additional hardening policies for the ARO nodes, enforcing security best practices and the principle of least privilege for remotely connected users. This service can be applied as a standalone solution with the ARO deployment or as part of the larger security hardening effort to secure entire DCS systems, which is also known as Honeywell PCN Hardening.

Application Whitelisting

Whitelisting is the process of preventing unwanted programs from running on a system by defining a compressive list of files and programs that are allowed to run on a system. The application whitelisting solution is effective against the execution of all unauthorized application components on higher risk client systems, including ARO servers and client nodes.

Sites without a DMZ

Note: Where it is not possible for the site to deploy a DMZ network to support the standard topology, the following topology can be used. Optional additional safeguards such as multi-factor authentication are not supported on this topology.

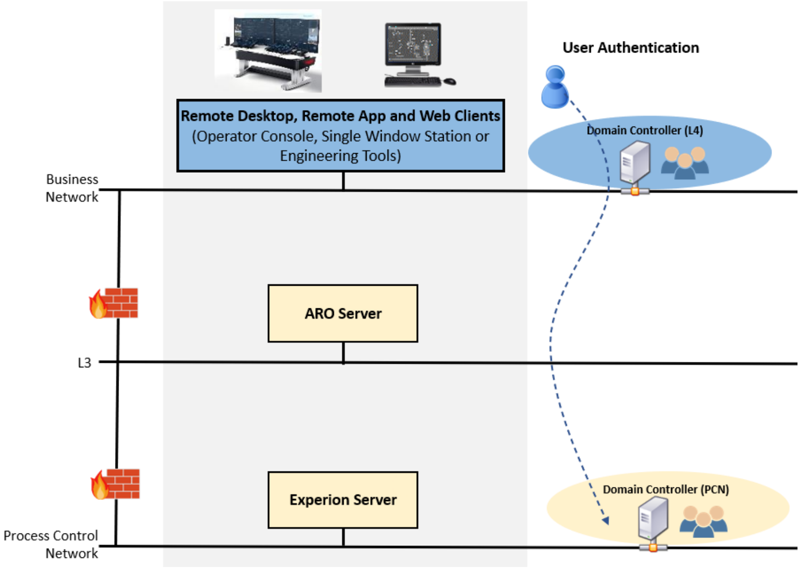
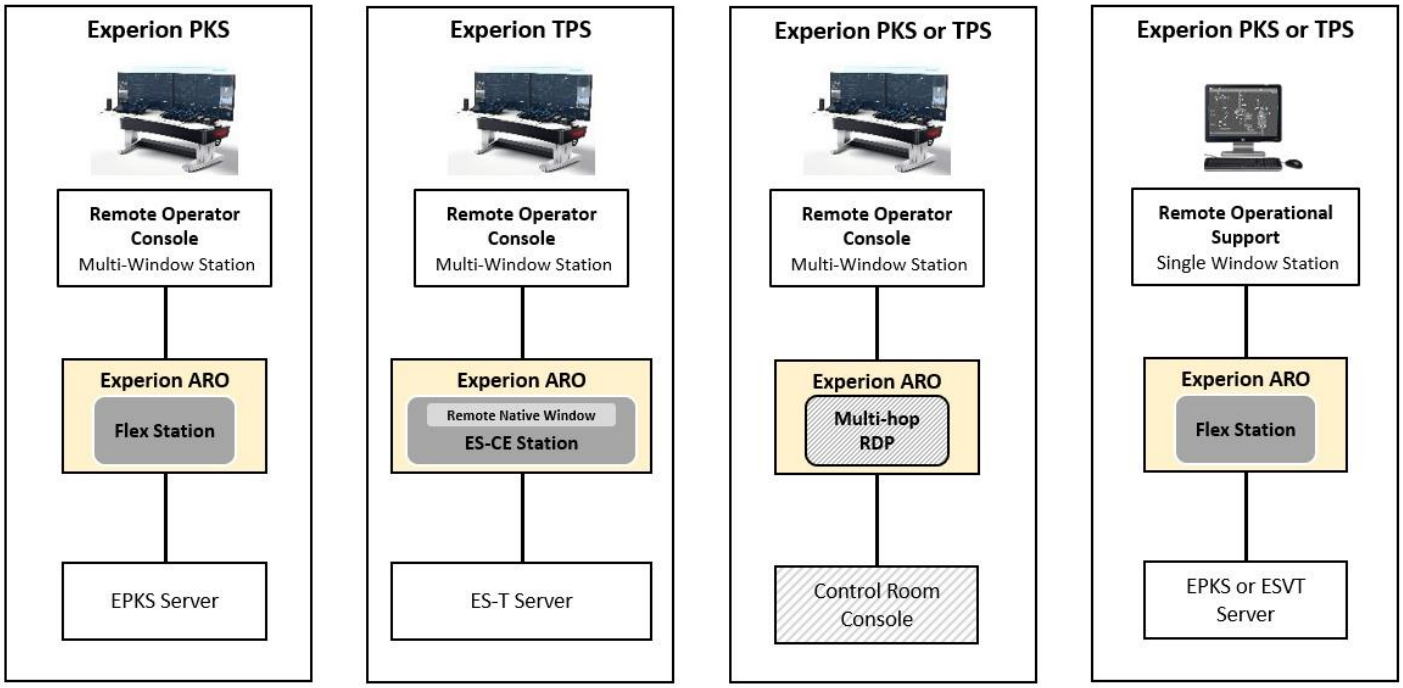


Figure 4: Topology for sites without a DMZ

This topology consists of client machines on the business network, an ARO server on L3 and Experion servers on the PCN. The ARO server is be part of the PCN domain in this topology. Users need an account on the business network and process control network domains. The user first logs in to the client machine using their business network domain account. When connecting to the ARO server the user must provide their PCN domain account credentials.

ARO Station Options



Experion ARO supports multi-window remote operator consoles and single window remote operational support / engineering Stations.

- For Experion PKS systems, Flex Stations are used on the ARO server.
- For Experion TPS systems requiring multi-window remote operator consoles, Console Extension Stations are used on the ARO server. The Console Extension Stations connect to ES-T servers on the process control network. For native window access, Remote Native Window is required. Only one Station session per ES-T can view Native Window.
- For Experion TPS systems requiring single window remote operational support / engineering Stations, Flex Stations are used on the ARO server. The Flex Stations connect to ESVT servers on the process control network.

Alternatively, the ARO server can also be used as a multi-hop RDP gateway to connect to a Station in the control room. In this scenario the remote Station takes over the Station running in the control room

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road,
Zhangjiang Hi-Tech Industrial Park,
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

September 2021