TECHNICAL DESCRIPTION

System 800xA Mobility

Extended Automation in the palm of your hands

The use of mobile devices in industrial facilities is now widely accepted and can provide tremendous value to day-to-day operations. Utilizing standard technologies, proper network design, and best practices, mobile devices can access the 800xA system over a secure wireless network. Everyone associated with a system can benefit from having immediate access to real-time information.

—
01 System 800xA workplace being viewed on a mobile tablet

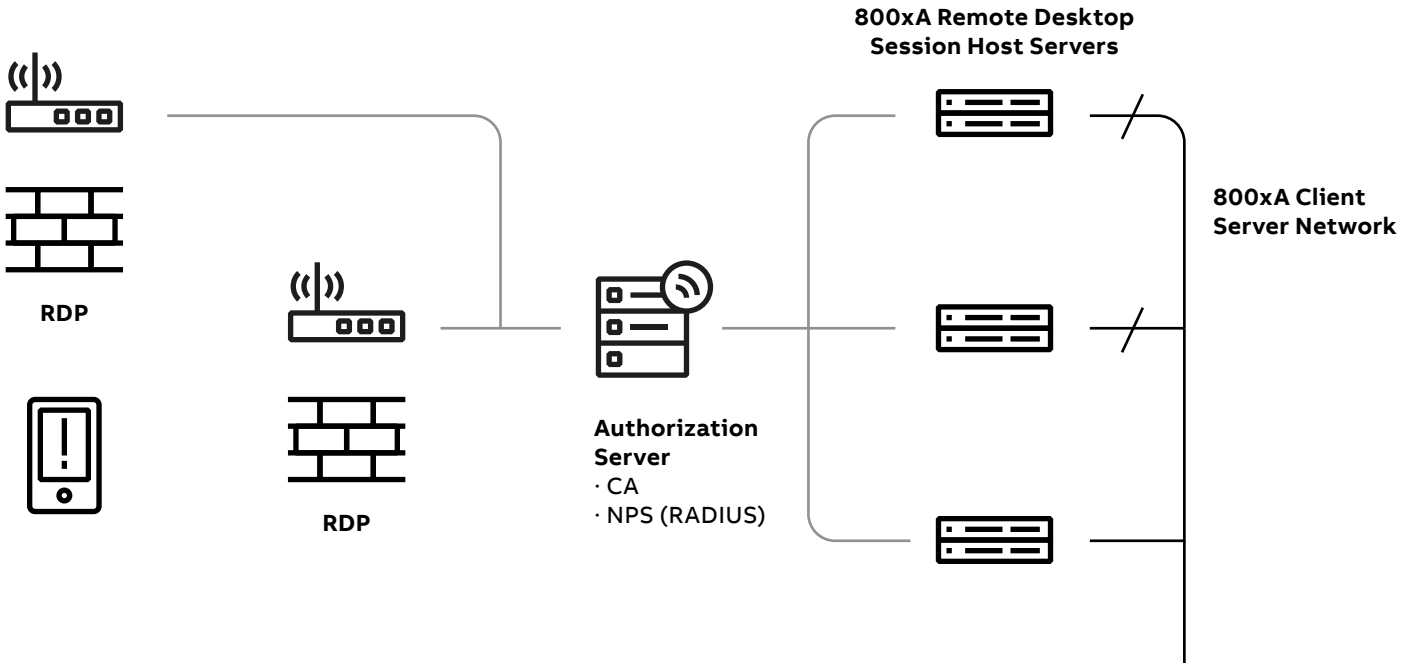
02 Overview concept for mobile device access

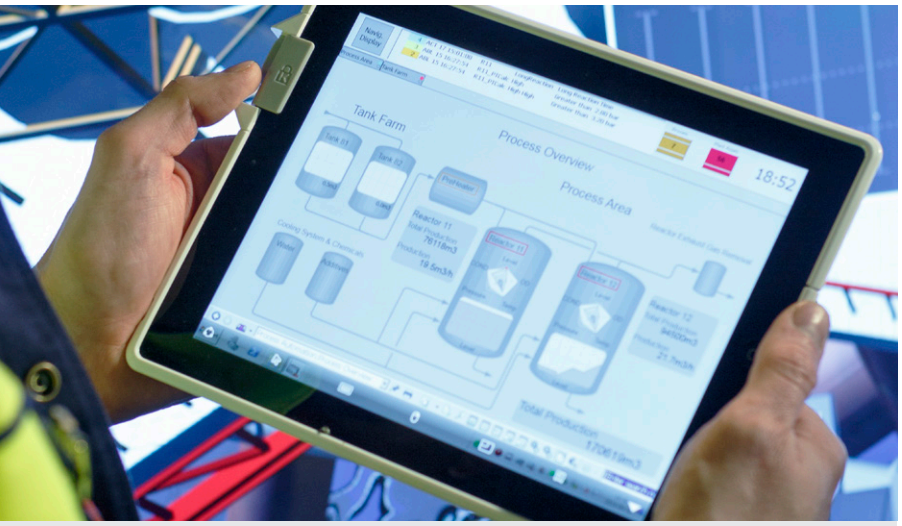
Benefits

- Improved visibility into current plant status regardless of user's location.
- Remote monitoring and control for field operations and maintenance activities.
- Ability for subject matter experts, supervisors, and plant manager to "see what they see" reducing the time to correct problems.

Overview

An overview of the concepts involved in providing wireless access is shown in figure 2. As most tablets do not have a native remote desktop client, a third party application may be required. Mobility is enabled through multiple wireless access points that also implement firewall and intrusion detection systems.





Customized workplace
The customized 800xA iPad operator workplace, available via the ABB Library, provides a starting point for developing a workplace which is more suited to the smaller screen size of the iPad. The customized workplace is in the form of an .afw file which can be imported into the 800xA system. It comprises the following:

iPad Operator Workplace object
- The date and time application bar item has been removed
- The tool bar time item used instead of the application bar

iPad Operator Workplace panel object
- This defines the startup display for the iPad Operator Workplace

iPad Alarm & Event List Configurations object
- This contains the 3 line alarm list which has been defined for a smaller screen to eliminate the horizontal scroll bar from occurring

Certificate Authority
The certificate authority is responsible for providing certificates which are used in the authentication of the wireless device to the wireless access point. As it is expected to have limited number of mobile devices used in conjunction with the 800xA system, it is preferable to have one certificate per device. This provides a more concise control over device access to the wireless networks.

The certificates of individual devices can be created after adding the Certificate Authority (CA) role to the Remote Desktop Session Host server. Each new certificate appears identical in the list. To differentiate between certificates, a friendly name such as the device name is added to the certificate after the certificate is produced.

Security
Multiple layers of defense should be used where possible. A separate network is recommended for the connection from the access points to the Remote Desktop Session Host servers. Both the access point and the Remote Desktop Session Host server have active firewalls.

The technology that is recommended for this solution is part of the IEEE 802.1X standard. EAP-TLS, which uses certificates, is used to establish connection between wireless devices and wireless networks. This requires a Certificate Authority (CA) server to be present in the network.

To provide security authorization, at least one Network Policy Server (NPS) server is used. This provides Re-mote Authentication Dial-In User Service (RADIUS) authorization functionality.

A separate network is used for the server side of the wireless network. The wireless access points are connected to one or more 800xA Remote Desktop Session Hosts (previously called Terminal Servers) which provide the login sessions for the remote desktop connection.

Establishing connectivity from the mobile device to the wireless access point uses WPA encryption and a certificate that has been generated in the Certifi-cate Authority. Furthermore, RADIUS is used for the authentication where the user must provide domain credentials to establish a connection. This provides a central method to remove the access to a lost mobile device by revoking the certificate or removing a user who should no longer have access to the system.

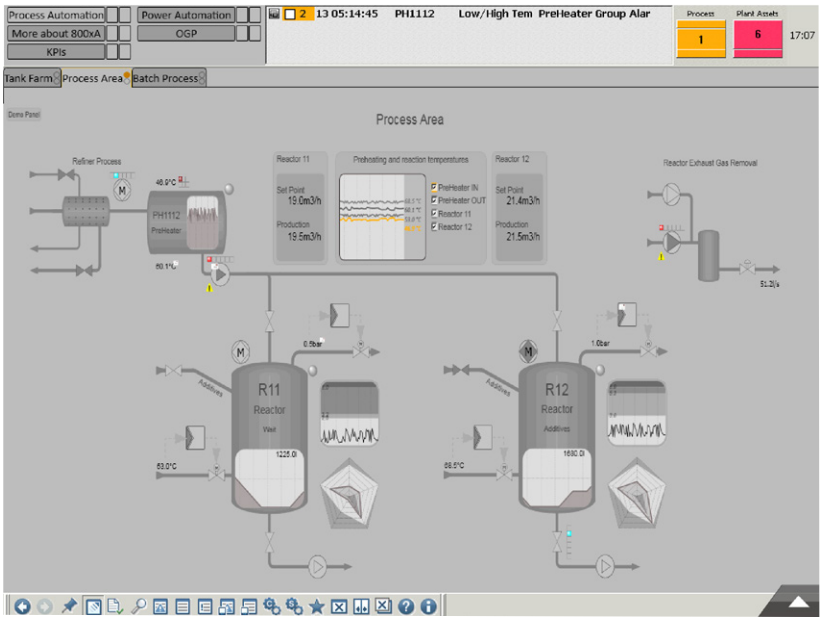
Additional security measures should also be implemented to restrict who can log into the system, and that those users can or cannot operate equipment. Security also needs to be configured for the mobile device and RDP application to provide the necessary level of security protection. (see 03)

Safety
Mobile support for 800xA is not intended for remote over the internet operation of a production environment. It is intended for production environment mobility where operators and production staff can view the process. Any operation of the system without physical visual contact should be avoided. The iPads should be dedicated to remote operation within the production environment and not be taken home or used in the office. There should also be no 3G/4G capabilities in the iPad.

Regulations should be in place which dictates that no usage of phone based hotspots is allowed in conjunction with the iPads.

Best Practices

Due to the demanding requirements of industrial systems, it is highly recommended that specialists in WIFI industrial deployments are consulted for planning and implementation of the wireless solution.



Requirements

Infrastructure

- Remote Desktop Session Host with Remote Desktop Services role
- Windows Server 2008 R2 node running NPS and CA

System 800xA

- 800xA 5.1 (running on Windows Server 2008 R2)
- System 800xA Operator Workplace License (for mobile devices)
- System 800xA Mobility guide (2AA….)

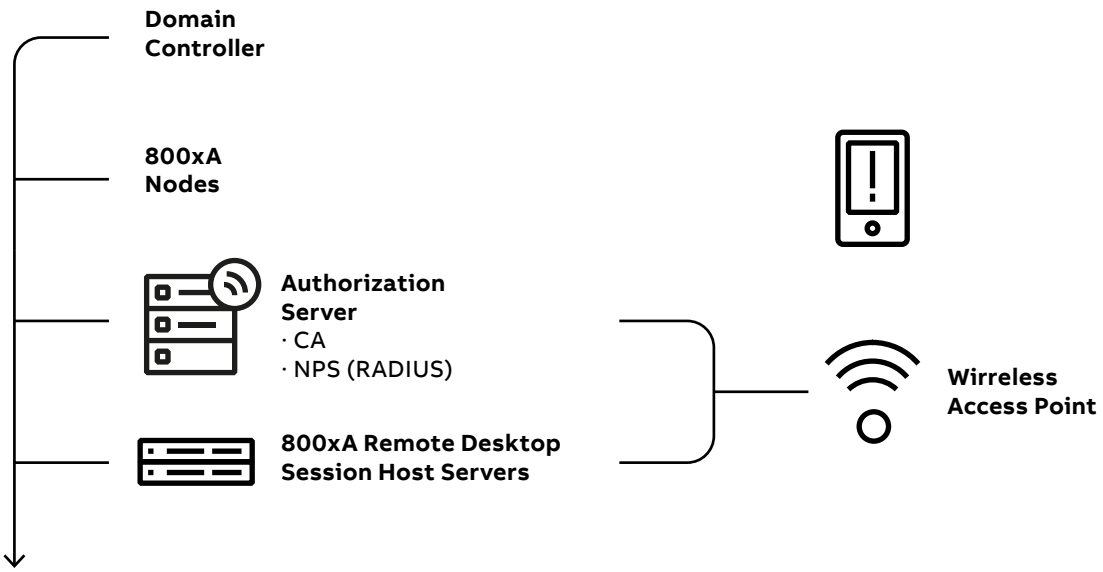
Other

- Remote Display Protocol (RDP) Application for mobile device (if RDP not natively available)

—

03 Example of Personalized Workplaces

04 Overview concept of data collection points for 800xA mobility



solutions.abb/800xA
solutions.abb/controlsystems

3BSE077629 en D