Honeywell

General Security Best Practices

SYSTEM ENGINEERING GUIDE

APPLICATION

Honeywell hereby expressly states that its controllers are not inherently protected against cyber-attacks from the Internet and that they are therefore intended solely for use in private networks. However, even private networks can still be subject to malicious cyber-attacks by skilled and equipped IT individuals and thus require protection. Customers should therefore adopt the installation and security best practices guidelines for Honeywell IP-based products to mitigate the risk posed by such attacks.

The following guidelines describe the General Security Best Practices for Honeywell IP-based products. They are listed in order of increasing mitigation.

The exact requirements of each site should be assessed on a case-by-case basis. The vast majority of installations implementing all of the mitigation levels described here will be far in excess of that required for satisfactory system security. Incorporating the items 1-5 (relating to Local Area Networks) will generally meet the requirements for most automation control network installations.

LOCAL AREA NETWORKS (LAN) INCORPORATING WEBS CONTROLLERS

Ensure the systems operate on an appropriate password policy for user access to all services. This guideline would include, but is not limited to:

1. The use of strong passwords.
2. A recommended password cycle time.
3. Unique user names and passwords for each user of the system.
4. Password disclosure rules.
5. If remote access to IT-based building control systems is required, use VPN (Virtual Private Network) tech-nology to reduce the risk of data interception and protect the controls devices from being directly placed on the internet.

Further Considerations

- Prevent unauthorized access to the network equipment that is used in conjunction with systems provided by WEBs solutions. With any system, preventing physical access to the network and equipment reduces the risk of unauthorized interference. Security best practices with IT installations would ensure that the server rooms, patch panels, and IT equipment are in locked rooms. WEBs equipment should be installed within locked control cabinets, themselves located in secured plant rooms.
- When completing commissioning, ensure the device is password protected. Ensure appropriate user levels are assigned for the site users.
- Adopt an appropriate update policy for the infrastructure installed at the site as part of a service level agreement. This policy should include, but is not limited to, updating the following system components to the latest release:
  - Devices firmware for controller, I/O modules, HMI, etc.;
  - Supervisor software, such as WEBStation AX software;
  - PC / Server operating systems;
  - Network infrastructure and any remote access systems.
- Configure separate IT networks for the automation control systems and the customer's corporate IT Network. This may be achieved by configuring VLANs (Virtual LANs) within the customer's IT infrastructure or by installing an air-gapped separate network infrastructure dedicated to the automation control systems.
- Once the system has been commissioned, restrict IP traffic on the automation control network (for example using access lists) to the types of protocols required for normal operation, i.e., C-Bus, BACnet, etc... Further information regarding the communications traffic required for normal operation can be found in the product documentation.
- When interfacing with WEB controllers using a centralized system supervisor (e.g., WEBStation-AX) and where the system does not require direct access to the individual devices web server, the network infrastructure should be configured to restrict web server access.
- Dynamic VLANs using MAC address allocation can protect against the unauthorized connection of a device into the system and can reduce the risk associated with an individual monitoring information on the network.

For more information, see also section "Network Security" of the Product Data of the given controller.

31-00129-01

Home and Building Technologies

In the U.S.:

Honeywell

715 Peachtree Street NE

Atlanta, GA 30308

customer.honeywell.com

Honeywell

31-00129—01 M.S. 09-17
Printed in United States