RIO Security Checklist

Recommended:

Host

- □ Network Firewall
- □ Anti Virus
- □ OS Updates
- □ OS ‘Limited User Accounts’
- □ VI Passwords
- □ Build EXEs, remove source code
- □ VI Server Access
- □ NI Auth Settings

RIO Device

- □ VI Server Access
- □ NI Auth Settings
- □ SSL System Web Server
- □ SSL App Web Server with Web Service
- □ Disable FTP
- □ RIO on internal network
- □ FPGA Bounds
- □ FPGA Safe States
- □ RTEXE, not interactive mode

Optional:

Host

- □ Limit Physical access
- □ Disable/Encrypt I/O (USB hub, CD Drive, etc.)
- □ Status signal to RT
- □ Change default ports

RIO Device

- □ Limit Physical access
- □ VPN Hardware Firewall/Router
- □ Status signal to host
- □ Change default ports

Extreme:

Host

- □ Application Whitelisting
- □ Change default ports

RIO Device

- □ Software Checking
- □ Hardware Checking
- □ Encrypt Communication between FPGA and RT

Resources:

DevZone Article: Overview of Best Practices for Security on NI RIO Systems

Contact your local rep and/or support