NATIONAL INSTRUMENTS™

Addressing Security in LabVIEW RIO Systems

Carlos Pazos

Product Marketing Manager

Embedded Software

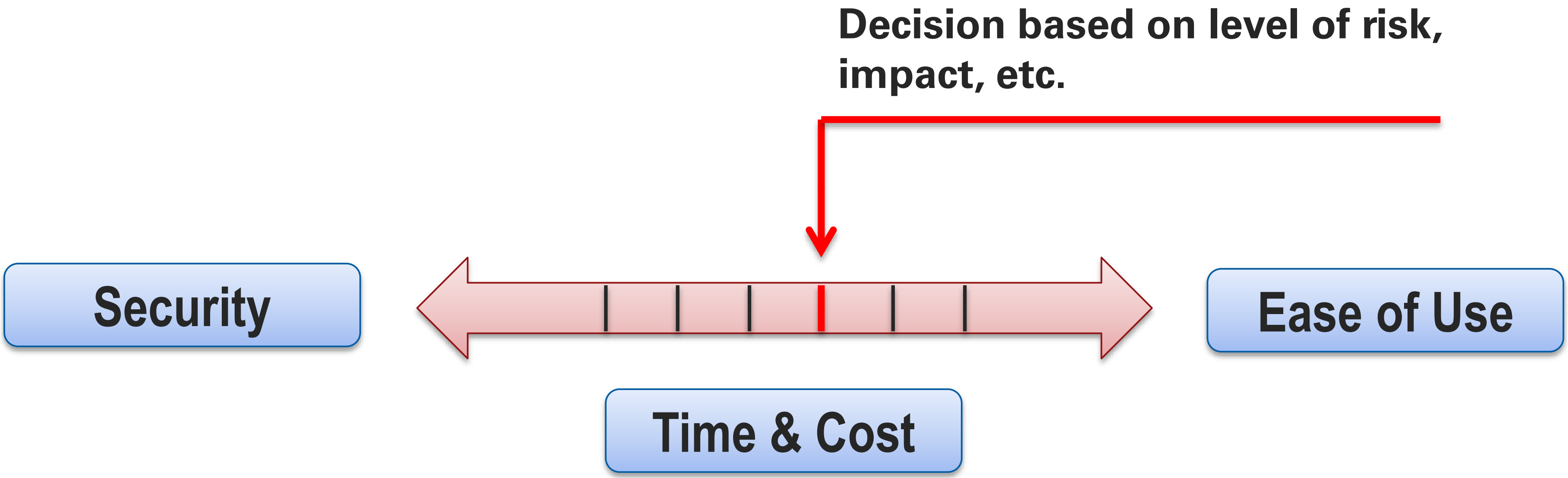
NI Knows Its Customers Care about Security

- Customers: Define security objectives, assess application-specific risks, evaluate and implement security steps

We want to work with our customers to help tackle this complex challenge.

How much time should be invested in security?

Balancing Security with Other Constraints



Decision based on level of risk, impact, etc.

Security

Ease of Use

Time & Cost

The Challenge

Development is hard:

Build a system that functions as designed

Security is <u>really</u> hard:

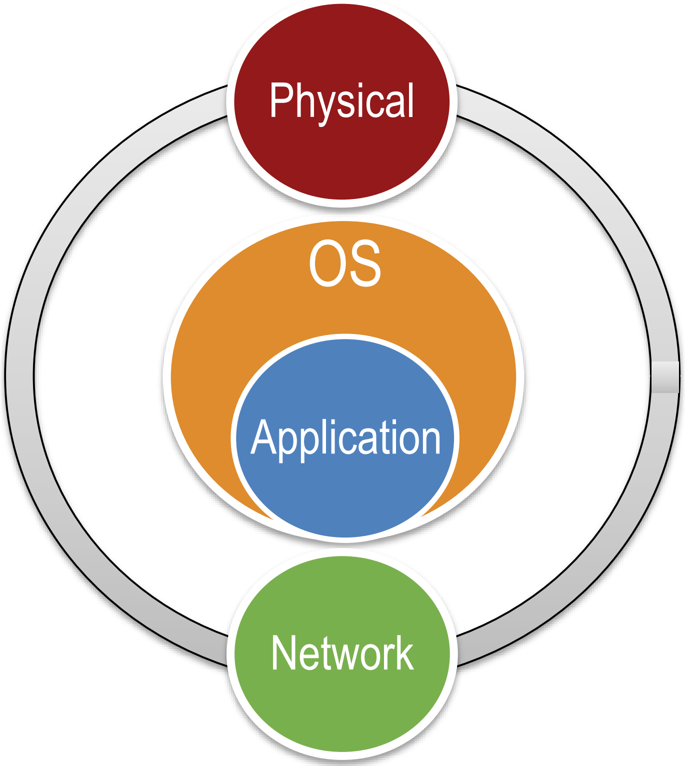
Build a system that *can't be used any other way*

Examples: Surveillance, theft, impersonation, base of operations

"A system's security is a function of its weakest link."

Layered Model of Security

- Security can be defined at many layers
- A breach at any layer can compromise other layers
- “Don’t invest in a retinal scanner for your house if you are going to leave your window open”
- “Defense in Depth”



CompactRIO Development Stages

NOTE: Can you make the symbol for the application deployment something a little more innocuous like a computer or a start button or something like that?

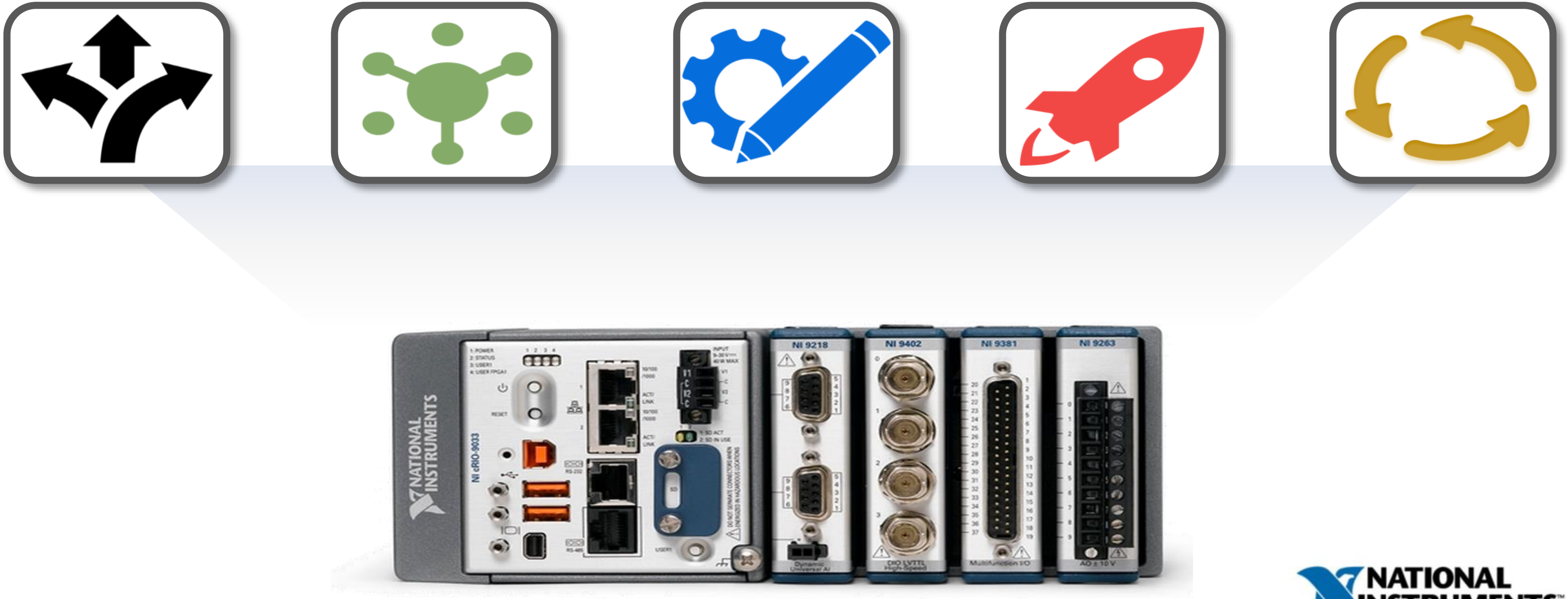
Platform Selection

System Configuration

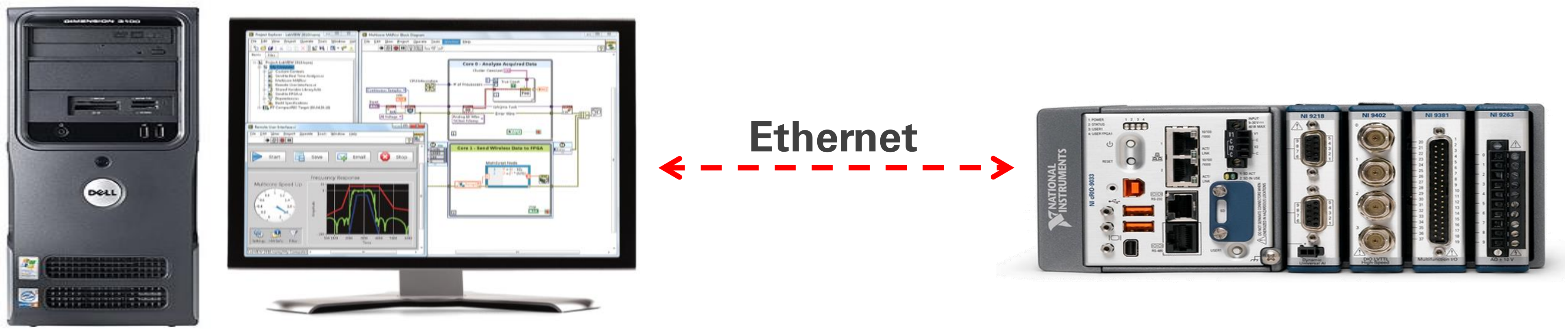
Application Development

Application Deployment

Application Maintenance



CompactRIO Development Stages



Ethernet

Development and/or Deployment PC

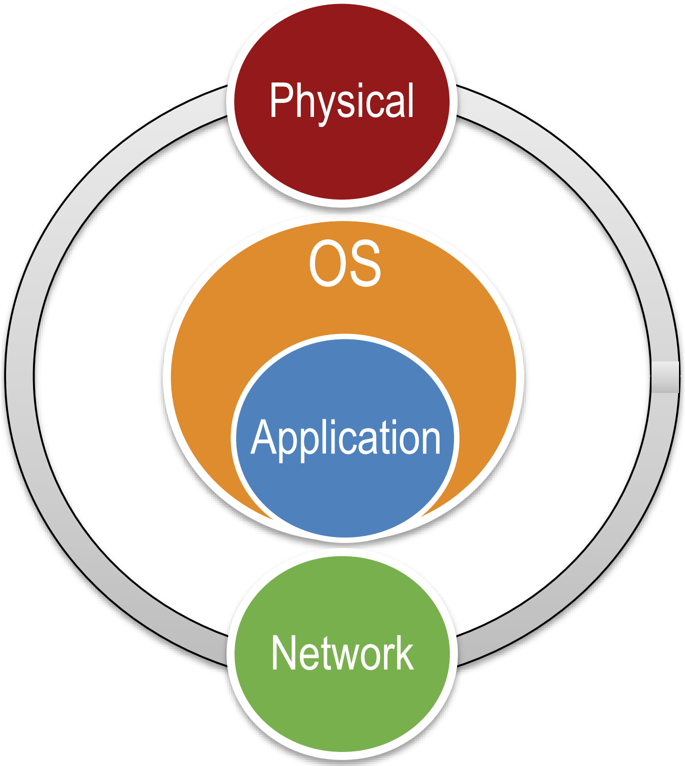
CompactRIO Embedded System

Security Best Practices

1. Physical Security

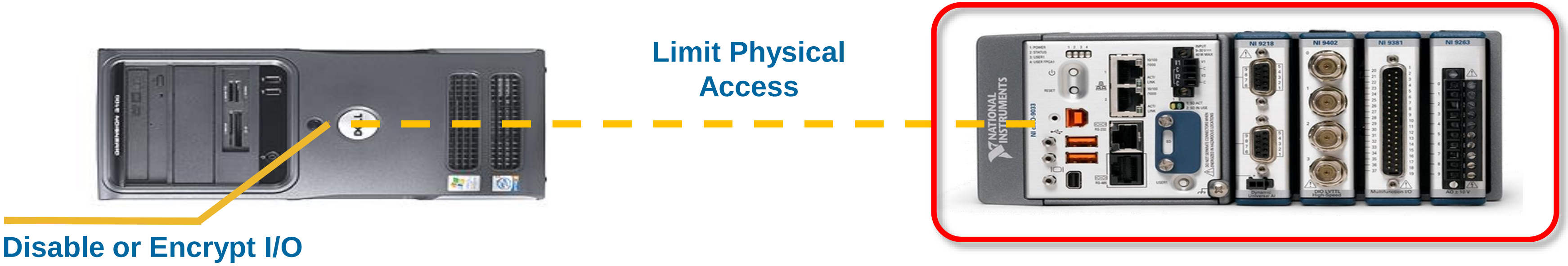
2. Network Security

3. Application & OS Security
   - NI Linux Real-Time



Physical Security

Physical Security



Limit Physical Access

Disable or Encrypt I/O

- Limit environmental/physical access to Host PC and physically enclose the real-time target
- Disable or require encryption on I/O (USB, CD Drive, etc.)
- Implement hardware checking
  - USB dongle for IP Protection
  - Digital I/O to validate that enclosure is properly secured

Network Security

General Network Security

- **Secure network**
  - Isolated network if possible; firewall if you connect to public infrastructure

- **Use web services for network communication**
  - HTTPS provides integrity and confidentiality
  - SSL certificate-based authentication between devices
  - Password-based user authentication between services

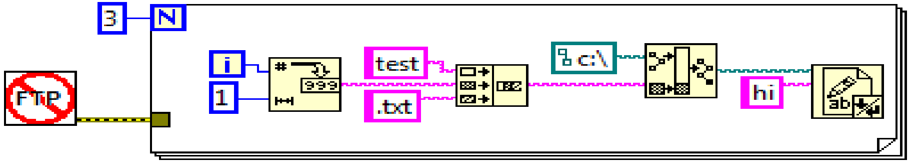
- **Understand the security risk of network protocols.** No authentication nor confidentiality for:
  - Remote Front Panel, Remote VI Server, Network shared variables
  - Mitigation:
    - **Good:** Use IP address access control, blacklist Exported VIs
    - **Better:** Use lower-layer tunnel (e.g. VPN or SSL)

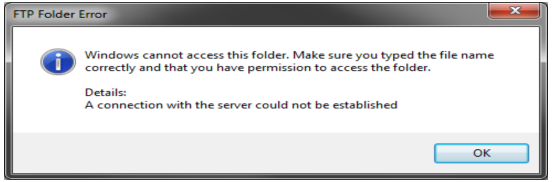
Disabling the FTP Server

- Only on **VxWorks** & **Phar Lap**
    - There is no unsecured FTP by default on NI Linux RT

- Use Shutdown RT FTP Server VI in your RT application

- Must reboot to enable FTP server
    - Disable RT Startup App to enable FTP



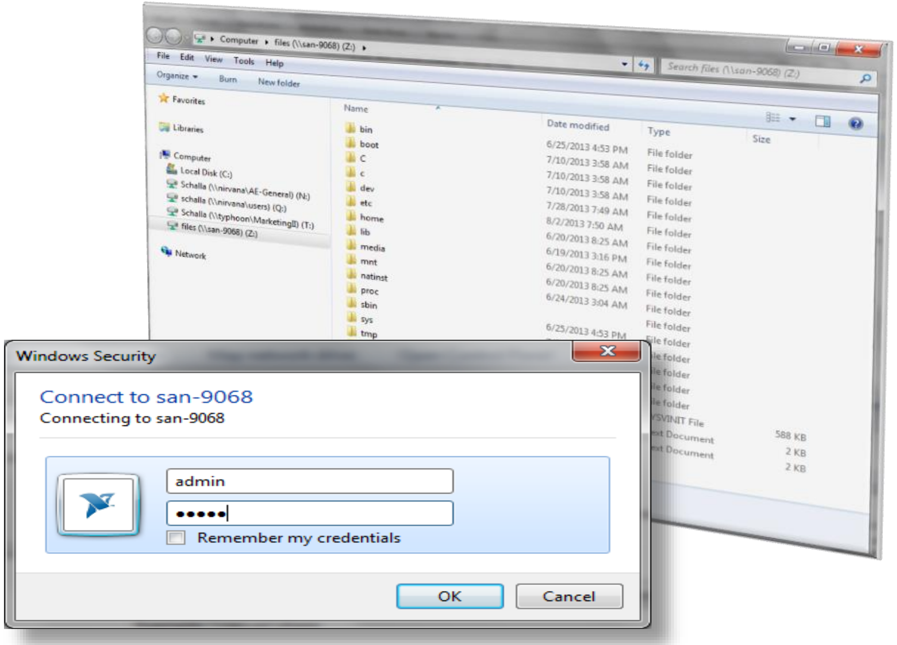

FTP Folder Error

Windows cannot access this folder. Make sure you typed the file name correctly and that you have permission to access the folder.

Details:
A connection with the server could not be established

File Transfer: WebDAV

- Industry Standard Protocol
- Manage files on targets remotely over HTTP(S)
- Secure File Access
    - Authentication & Encryption
- Supported by all modern OSes and Web Browsers
- LabVIEW API for programmatic access
- WebDAV File Browser


Computer ▸ files (\\san-9068) (Z:) ▸
File
Edit
View
Tools
Help
Search files (\\san-9068) (Z:)
Organize ▾
Burn
New folder
Favorites
Libraries
Computer
Local Disk (C:)
Schalla (\\nirvana\AE-General) (N:)
schalla (\\nirvana\users) (Q:)
Schalla (\\typhoon\MarketingII) (T:)
files (\\san-9068) (Z:)
Network

```
Name       Date modified        Type           Size
bin        6/25/2013 4:53 PM    File folder
boot       7/10/2013 3:58 AM    File folder
C          7/10/2013 3:58 AM    File folder
c          7/10/2013 3:58 AM    File folder
dev        7/28/2013 7:49 AM    File folder
etc        8/2/2013 7:50 AM     File folder
home       6/20/2013 8:25 AM    File folder
lib        6/19/2013 3:16 PM    File folder
media      6/20/2013 8:25 AM    File folder
mnt        6/20/2013 8:25 AM    File folder
natinst    6/24/2013 3:04 AM    File folder
proc                            File folder
sbin       6/25/2013 4:53 PM    File folder
sys                             File folder
tmp                             File folder
                                ile folder
                                ile folder
                                ile folder
                                ile folder
                                ile folder
                                YSVINIT File
                                xt Document    588 KB
                                xt Document    2 KB
                                               2 KB
```

Windows Security

Connect to san-9068

Connecting to san-9068

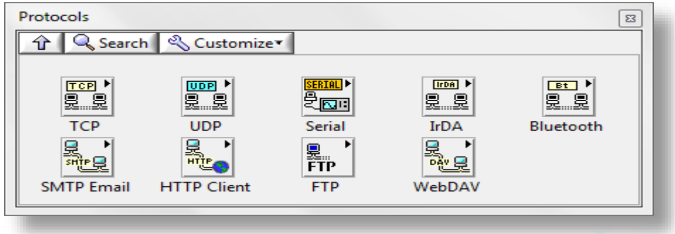
admin

•••••

☐ Remember my credentials

OK

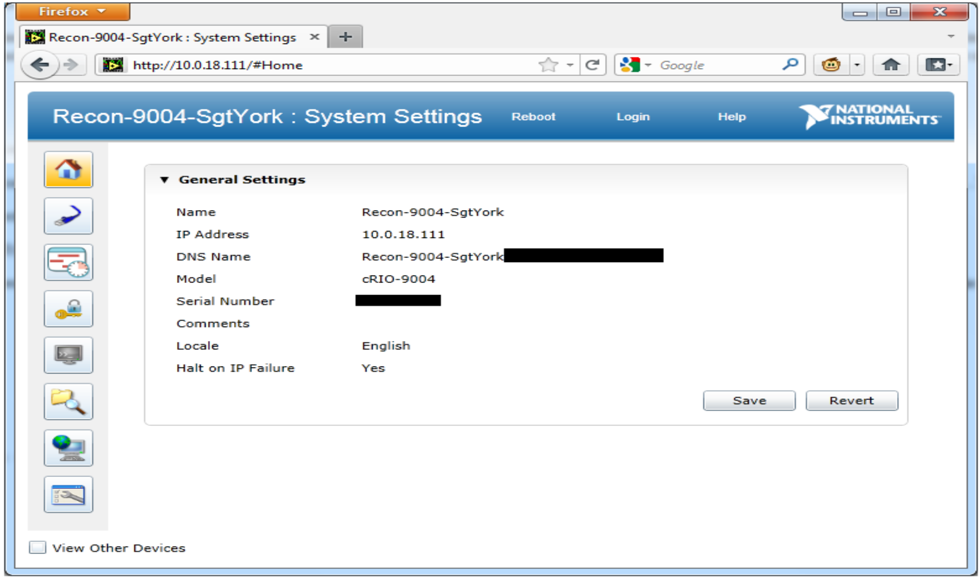
Cancel



NATIONAL INSTRUMENTS

Web Based Configuration and Monitoring

- Use to access
  NI Auth settings
- cRIO:
  - http://<cRIO_ip.addr>
- Host PC
  - http://<host_ip.addr>:3582



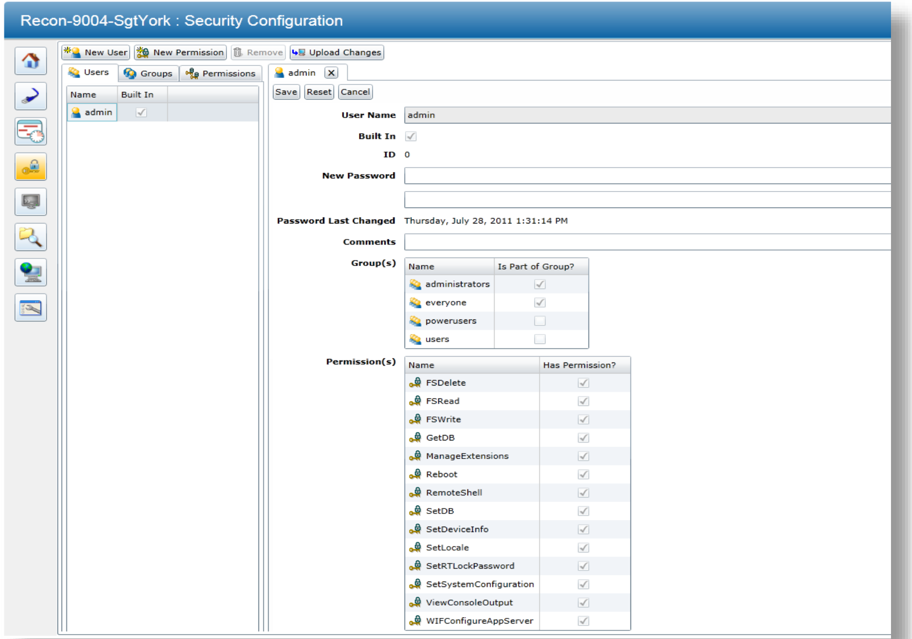
Recon-9004-SgtYork : System Settings

▼ General Settings

Name	Recon-9004-SgtYork
IP Address	10.0.18.111
DNS Name	Recon-9004-SgtYork[redacted]
Model	cRIO-9004
Serial Number	[redacted]
Comments	
Locale	English
Halt on IP Failure	Yes

□ View Other Devices

NI-Auth Users & Permissions



Recon-9004-SgtYork : Security Configuration

Name	Built In
admin	✓

User Name	admin
Built In	✓
ID	0
New Password	
Password Last Changed	Thursday, July 28, 2011 1:31:14 PM
Comments	

Group(s)

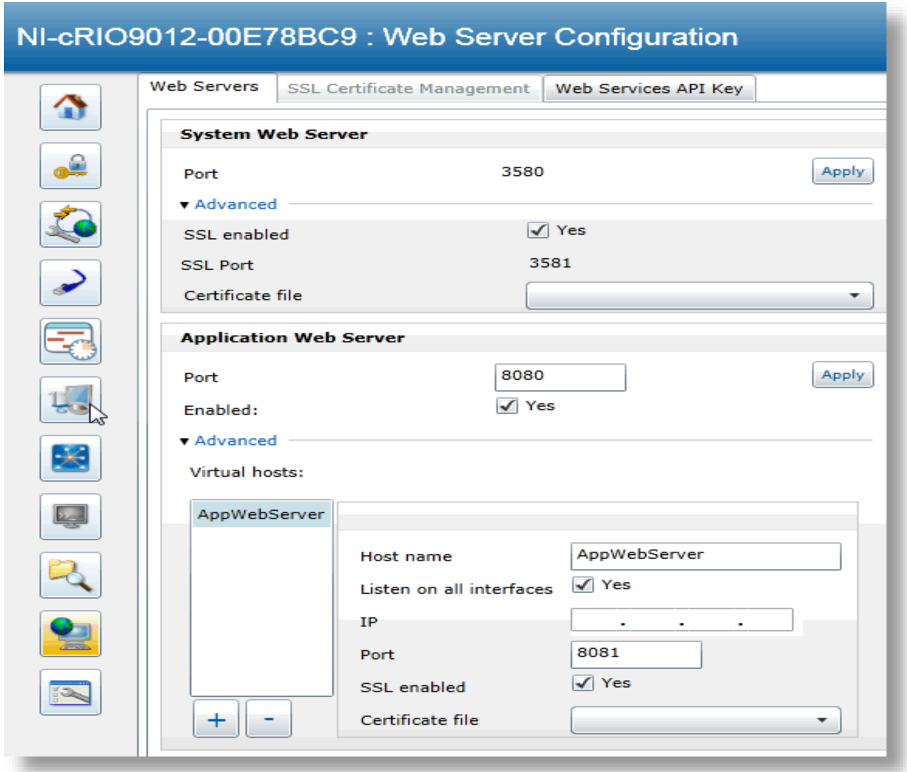
Name	Is Part of Group?
administrators	✓
everyone	✓
powerusers	□
users	□

Permission(s)

Name	Has Permission?
FSDelete	✓
FSRead	✓
FSWrite	✓
GetDB	✓
ManageExtensions	✓
Reboot	✓
RemoteShell	✓
SetDB	✓
SetDeviceInfo	✓
SetLocale	✓
SetRTLockPassword	✓
SetSystemConfiguration	✓
ViewConsoleOutput	✓
WIFConfigureAppServer	✓

- **Change password on ‘admin’ account**
- Set permissions on users and groups to restrict users & groups to only activities they are responsible for
- Currently applicable only to web services and web management

Enable SSL



NI-cRIO9012-00E78BC9 : Web Server Configuration

System Web Server

Port 3580

SSL enabled ☑ Yes

SSL Port 3581

Certificate file

Application Web Server

Port 8080

Enabled: ☑ Yes

Virtual hosts: AppWebServer

Host name AppWebServer

Listen on all interfaces ☑ Yes

IP . . .

Port 8081

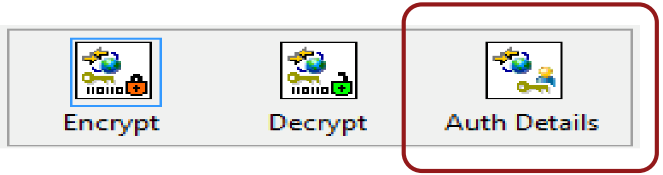
SSL enabled ☑ Yes

Certificate file

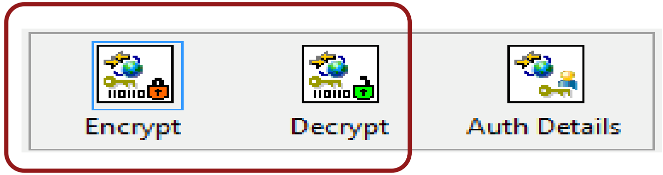
- Enable SSL for both System and Application Web Servers
- Turn off HTTP version and rely only on the HTTPS version
- Select and setup self signed certificates or go through a CA
- System Web Server available at
  - https://<cRIO_ip.addr>
  - https://<host_ip.addr>:3581

Web Services Security palette

- Allows web service to retrieve NI-Auth attributes
  - User name
  - Group
  - Permissions
  - Session key (320 bits)

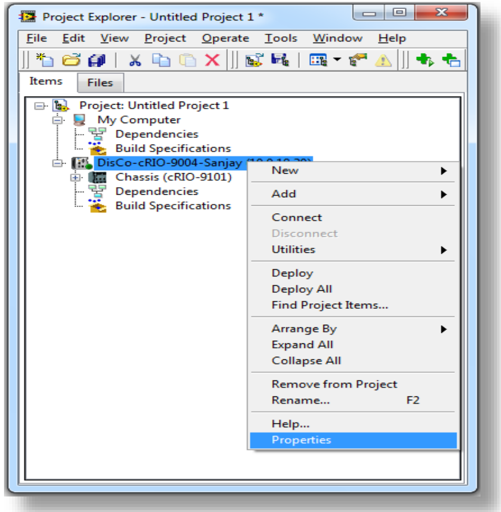


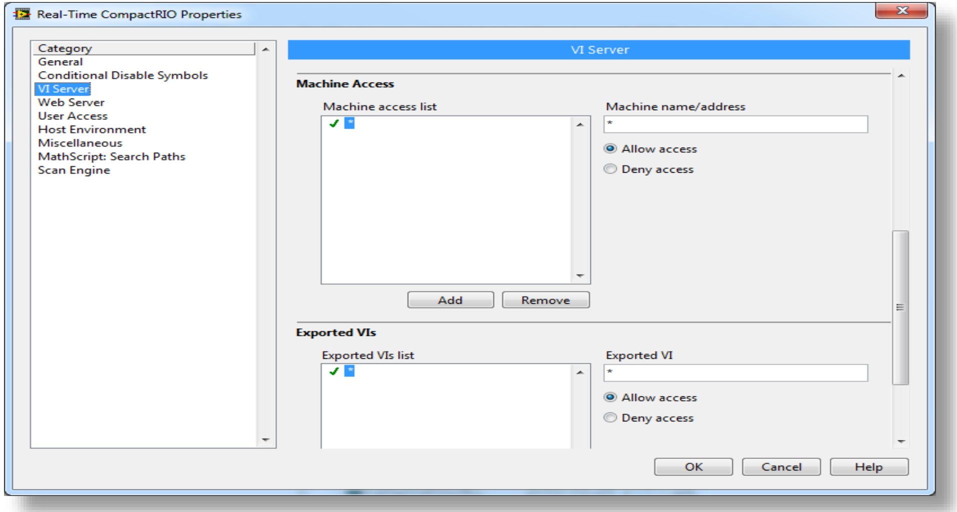
- Encryption functions that use the session key
  - Secure Remote Password (RFC 2945) using SRP_SHA1
  - Message confidentiality
  - Message authentication/integrity using third-party HMAC



Managing VI Server Access

- Manage VI Server (TCP) Access to help prevent ‘LabVIEW’ viruses
    - Prevent remote access & execution of code on your PC or RT target
- For Host PC: Tools » Options » VI Server
- For cRIO: use Project Explorer as shown here





Machine Access

Machine access list: ✓ *

Machine name/address: *

● Allow access
○ Deny access

Exported VIs

Exported VIs list: ✓ *

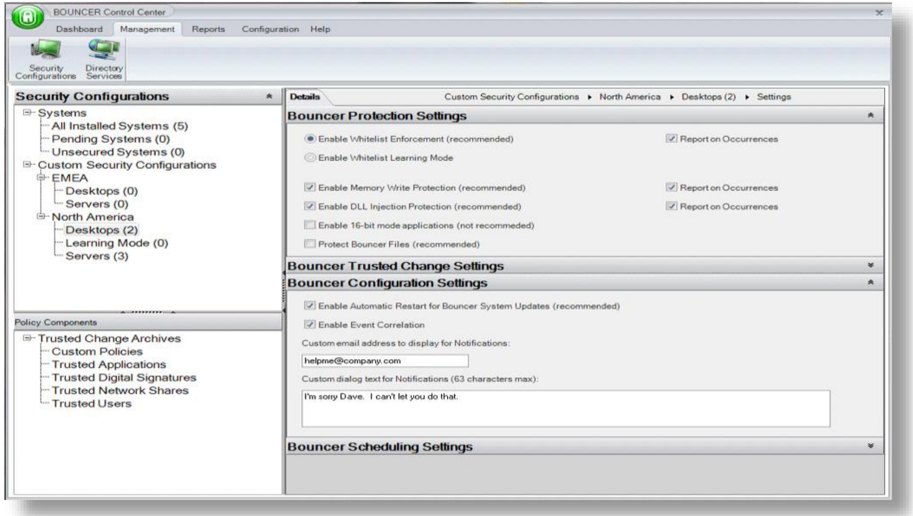
Exported VI: *

● Allow access
○ Deny access

Application & OS Security

Application Whitelisting

- Use to regulate code execution on host computer
- Compute and store checksum in a known good state
- Compare checksum against table
- Solutions:
  - CoreTrace Bouncer
  - McAfee Application Control
  - Bit9 Parity Suite
  - Microsoft AppLocker



Bouncer Protection Settings

● Enable Whitelist Enforcement (recommended) ☑ Report on Occurrences

○ Enable Whitelist Learning Mode

☑ Enable Memory Write Protection (recommended) ☑ Report on Occurrences

☑ Enable DLL Injection Protection (recommended) ☑ Report on Occurrences

□ Enable 16-bit mode applications (not recommeded)

□ Protect Bouncer Files (recommended)

Bouncer Trusted Change Settings

Bouncer Configuration Settings

☑ Enable Automatic Restart for Bouncer System Updates (recommended)

☑ Enable Event Correlation

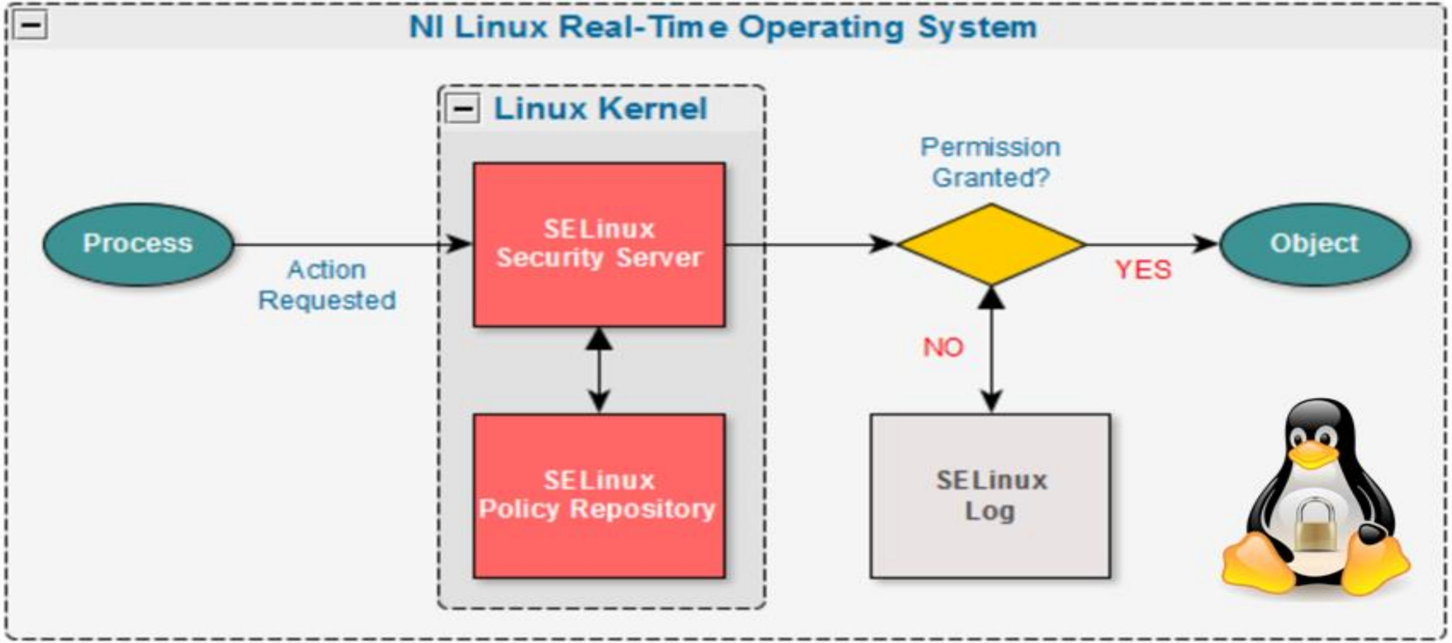
Custom email address to display for Notifications: helpme@company.com

Custom dialog text for Notifications (63 characters max): I'm sorry Dave. I can't let you do that.

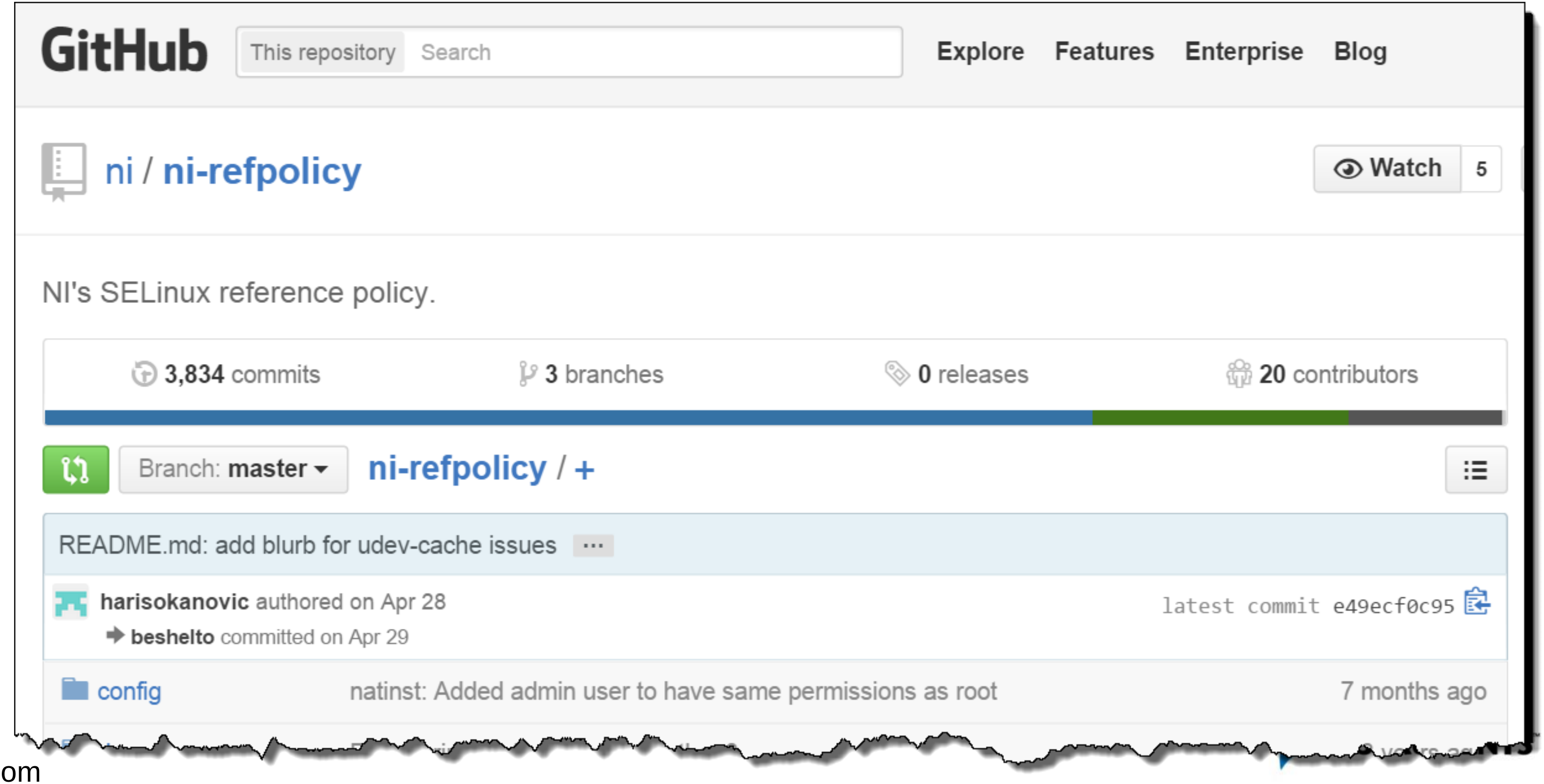
Bouncer Scheduling Settings

Malicious Code Prevention

Security Enhanced Linux (SELinux)



GitHub Reference Policy



ni / ni-refpolicy

NI's SELinux reference policy.

3,834 commits | 3 branches | 0 releases | 20 contributors

ni-refpolicy / +

README.md: add blurb for udev-cache issues …

harisokanovic authored on Apr 28

beshelto committed on Apr 29

latest commit e49ecf0c95

config	natinst: Added admin user to have same permissions as root	7 months ago

Sensitive Data Protection

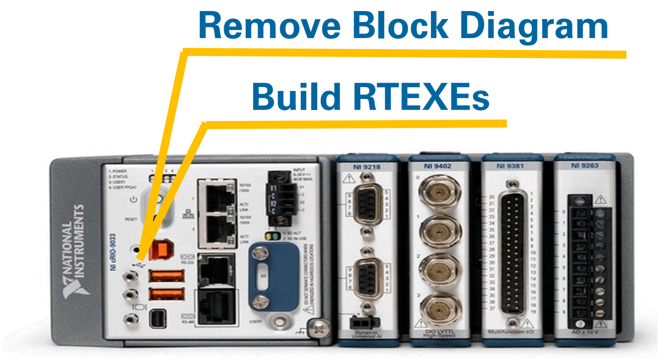
- Options for encrypting data in storage
  1. Several individuals offer LabVIEW VIs
     - Caution: Much slower than C/C++ implementations
  2. Use .NET library in LabVIEW
     - system.security.cryptography library
     - Add reference to mscorlib.dll
  3. Use DLL calls to the host OpenSSL/CAPI library
- General principle: " *Ensure the confidentiality of sensitive data through its entire lifecycle.*"

LabVIEW and LabVIEW Real-Time

Application Security

Remove Block Diagram

Build EXEs



Remove Block Diagram

Build RTEXEs

- Remove the block diagram: LabVIEW Help: Removing Block Diagrams from VIs
- Use Build Specifications such as EXEs & RTEXEs
- Remove the source code and the development environment from host computers on the deployed network

LabVIEW FPGA

Application Security

FPGA Bounds

FPGA Safe States

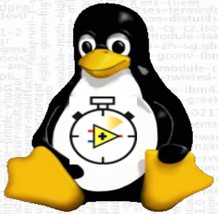
- Implement bounds checking on FPGA I/O to prevent damage
- Use an FPGA Watchdog over RT and default to FPGA ‘safe states’ if something is erroneous on RT

NI Linux Real-Time

NI Linux Real-Time

- Maintained by NI
  - Custom built and optimized for NI embedded hardware
    - Supports ARM and x64, with cross-compilers provided
  - Easier integration of third-party peripherals and applications as most have Linux drivers or packages available
  - NI Package Repository: download.ni.com/ni-linux-rt/
    - Over 3,000 packages
  - OS source: github.com/ni
- PREEMPT_RT
  - Enables real-time reliability through pre-emption, priority inheritance, and scheduling
  - Standard approach to real-time performance on Linux

LINUX FOUNDATION
SILVER MEMBER



NATIONAL INSTRUMENTS

Linux Ecosystem

Database

Raima
MySQL
SQLite
MongoDB
CouchDB

Security

SELinux
OpenVPN
IP Tables
System Logging
fail2ban
denyhost

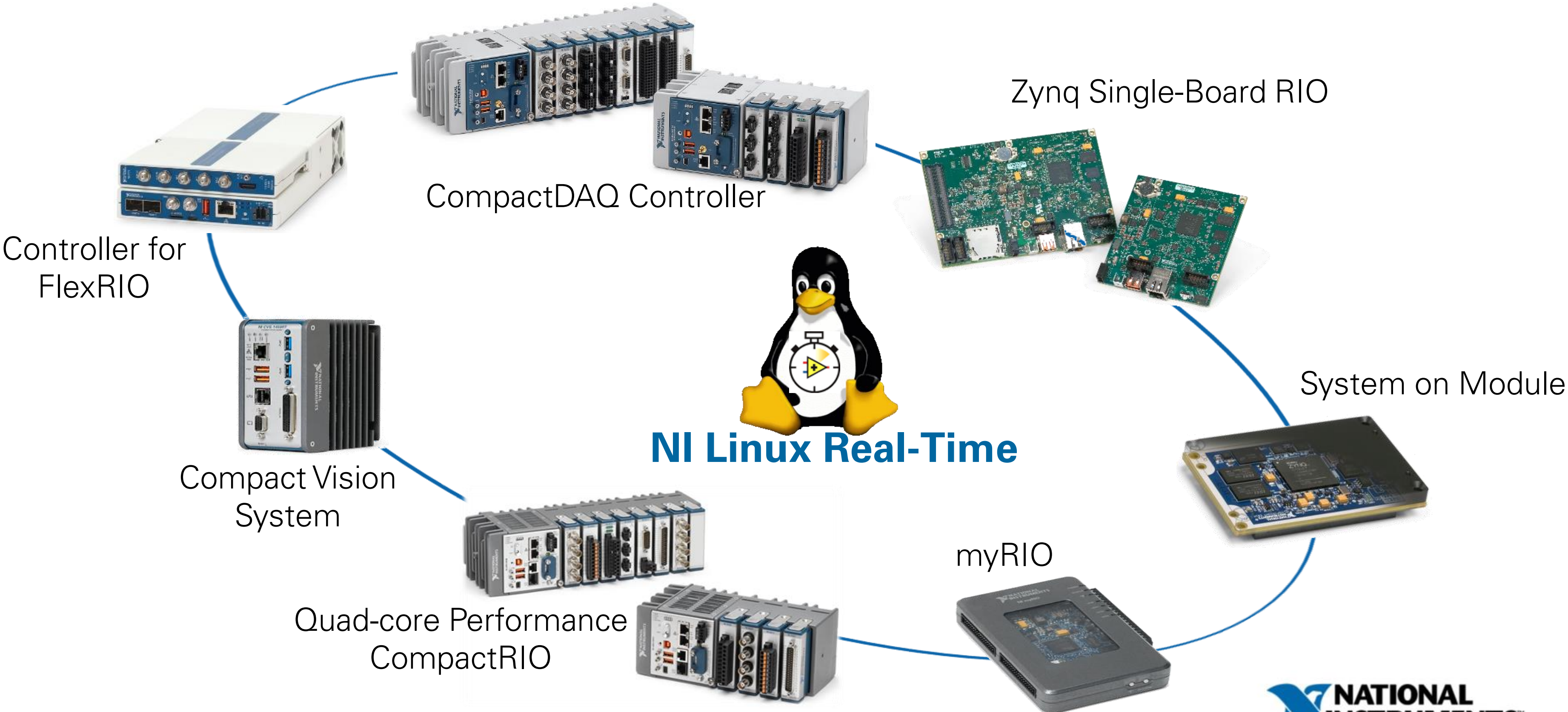
Code Re-use

C/C++
Shell scripting
Python
Ruby
Perl

Connectivity

Isshd
IPv6
SNMP
NTP
netstat

Integration with the Latest Hardware Products



CompactDAQ Controller

Zynq Single-Board RIO

System on Module

myRIO

Quad-core Performance CompactRIO

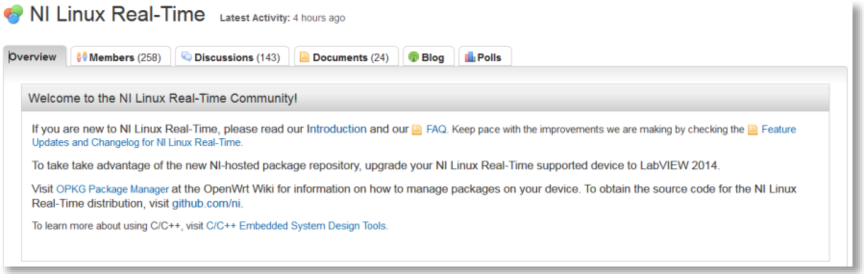
Compact Vision System

Controller for FlexRIO

NI Linux Real-Time

Key Resources

- ni.com/linuxrtforum
  - Tutorials
  - Documentation
  - Forum for discussions
- ni.com/linux
  - Links to whitepapers
  - Embedded and Desktop uses
- download.ni.com/ni-linux-rt/
  - Package Repository
- github.com/ni
  - OS Source



NI Linux Real-Time **Latest Activity:** 4 hours ago

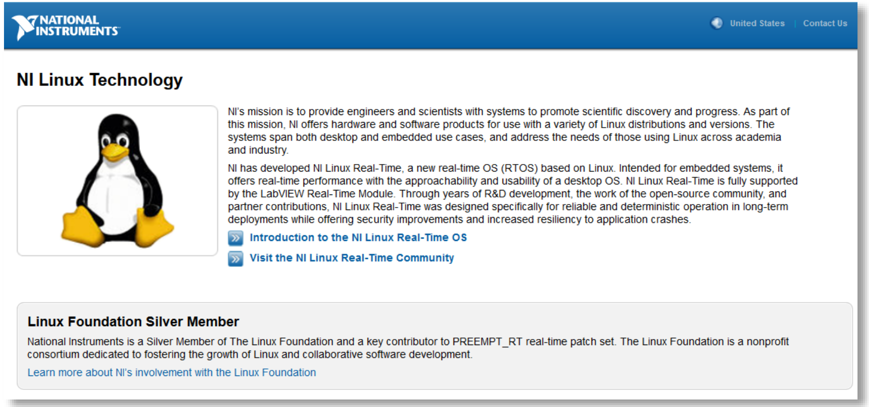
Welcome to the NI Linux Real-Time Community!

If you are new to NI Linux Real-Time, please read our Introduction and our FAQ. Keep pace with the improvements we are making by checking the Feature Updates and Changelog for NI Linux Real-Time.

To take take advantage of the new NI-hosted package repository, upgrade your NI Linux Real-Time supported device to LabVIEW 2014.

Visit OPKG Package Manager at the OpenWrt Wiki for information on how to manage packages on your device. To obtain the source code for the NI Linux Real-Time distribution, visit github.com/ni.

To learn more about using C/C++, visit C/C++ Embedded System Design Tools.



NI Linux Technology

NI's mission is to provide engineers and scientists with systems to promote scientific discovery and progress. As part of this mission, NI offers hardware and software products for use with a variety of Linux distributions and versions. The systems span both desktop and embedded use cases, and address the needs of those using Linux across academia and industry.

NI has developed NI Linux Real-Time, a new real-time OS (RTOS) based on Linux. Intended for embedded systems, it offers real-time performance with the approachability and usability of a desktop OS. NI Linux Real-Time is fully supported by the LabVIEW Real-Time Module. Through years of R&D development, the work of the open-source community, and partner contributions, NI Linux Real-Time was designed specifically for reliable and deterministic operation in long-term deployments while offering security improvements and increased resiliency to application crashes.

» Introduction to the NI Linux Real-Time OS

» Visit the NI Linux Real-Time Community

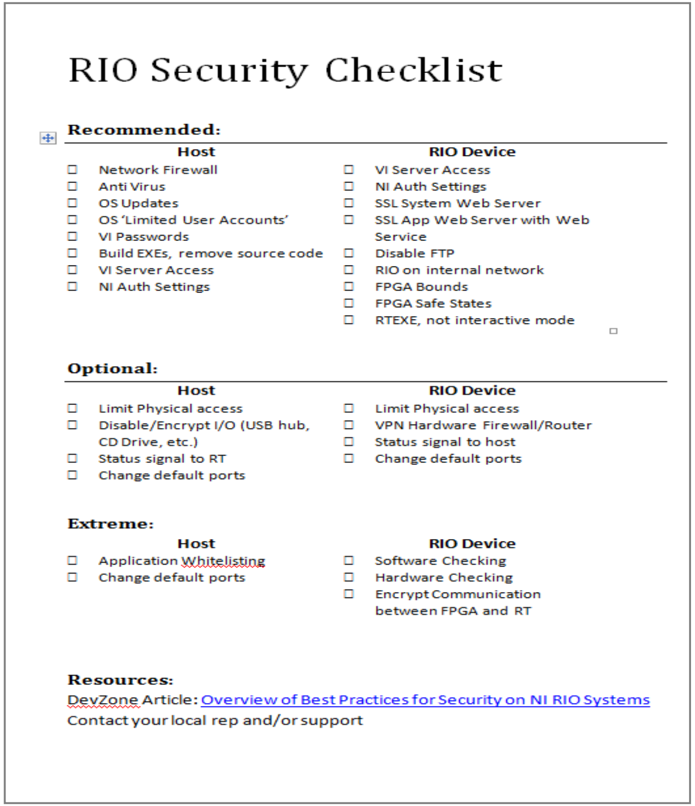
Linux Foundation Silver Member

National Instruments is a Silver Member of The Linux Foundation and a key contributor to PREEMPT_RT real-time patch set. The Linux Foundation is a nonprofit consortium dedicated to fostering the growth of Linux and collaborative software development.

Learn more about NI's involvement with the Linux Foundation

Next Steps

- Sign up at ni.com/security
- Leverage online resources: Overview of Best Practices for Security on NI RIO Systems
- Engage NI with security needs such as security certifications (NERC CIP, IEC 62351, etc.)
- Use the Best Practices Checklist to evaluate and secure your system



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

Questions?

Carlos Pazos
Product Marketing Manager
Embedded Software
carlos.pazos@ni.com

NATIONAL INSTRUMENTS™