Rockwell Automation

# Innovation & Technology Forum

## Logix Intellectual Property Protection

Roman Foukal

Commercial Engineer A&S

# Agenda

- SECURITY OVERVIEW
- SOURCE PROTECTION
- FactoryTalk® SECURITY
- LICENSE PROTECTION
- TAMPER PROTECTION

# Secure Automation & Information

## Defending the digital architecture

### Secure Network Infrastructure

**Control Access** to the network, and **Detect** unwanted access and activity

### Access Control & Policy Management

Control **Who, What, Where & When** access is allowed, to which application & device

### Content Protection

**Protect** viewing, editing, and use of specific pieces of control system content

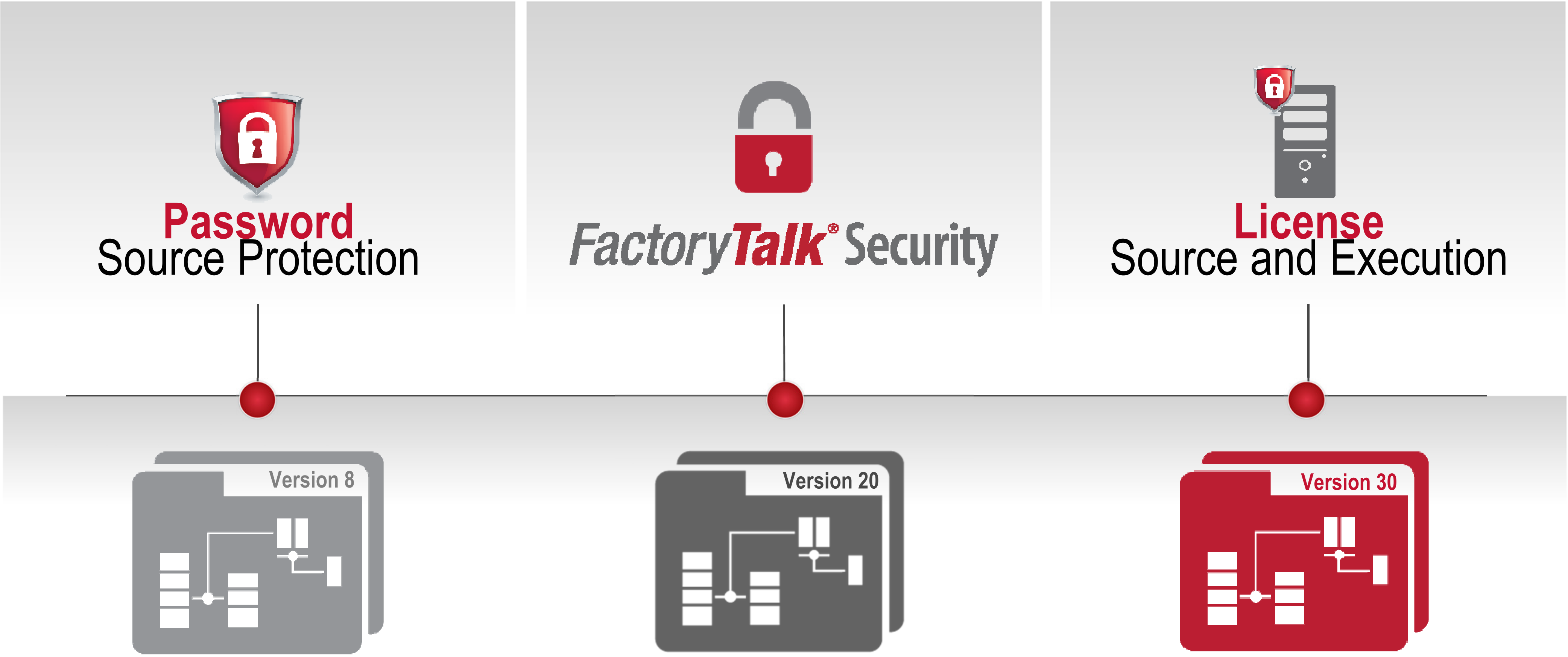
### Tamper Detection

**Detect** & **Record** unwanted **Activity & Modifications** to the application

**INDUSTRIAL SECURITY**

MUST BE IMPLEMENTED **AS A SYSTEM**

# Studio 5000 Logix Designer®
# Content Protection History



Password
Source Protection

FactoryTalk® Security

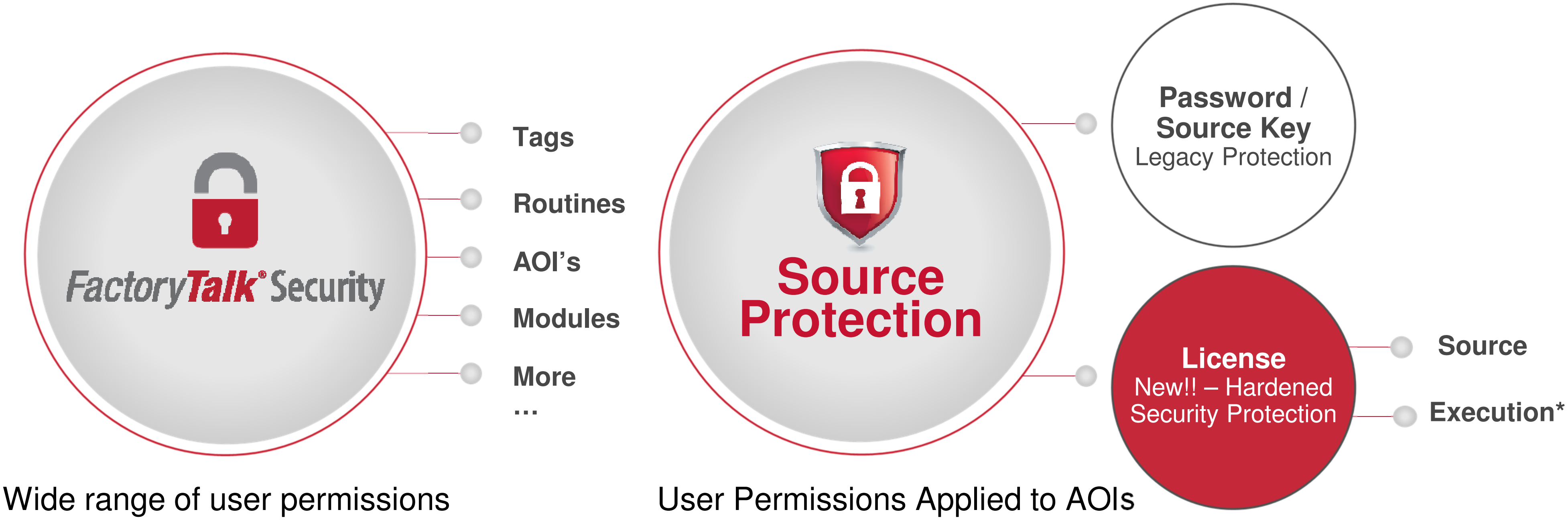
License
Source and Execution

Version 8

Version 20

Version 30

# Summary of the Options – V30



FactoryTalk® Security

- Tags
- Routines
- AOI’s
- Modules
- More
- …

Source Protection

- **Password / Source Key** Legacy Protection
- **License** New!! – Hardened Security Protection
  - Source
  - Execution*

Wide range of user permissions applied to vast range of objects

User Permissions Applied to AOIs and Routines: Protect, Edit, Copy, Export, View

*Supported by ControlLogix® 5580, CompactLogix™ 5480, CompactLogix™ 5380 controllers

# Password Source Protection

Simple Control of Who Accesses Content

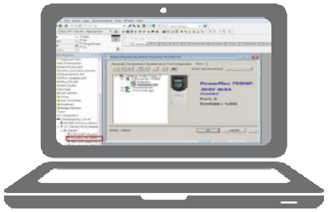
*Some control over who accesses content, but chief concern is simplicity*

USE CASE

**Password**
Source Protection

SOLUTION

**Studio 5000®**
*Logix Designer®*



REQUIRES

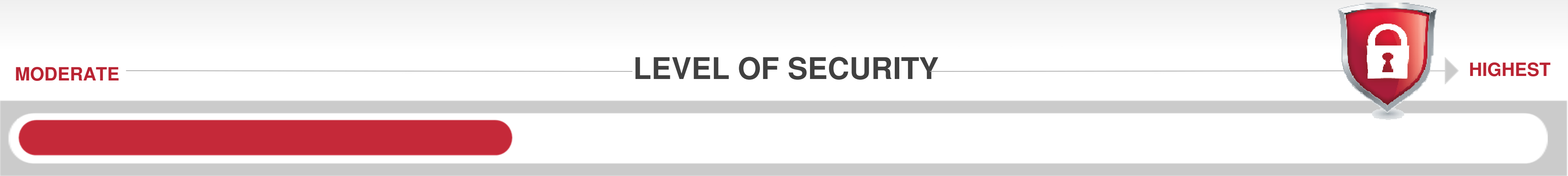
**CUSTOMERS WITH FEW USERS**

User 1

User 2

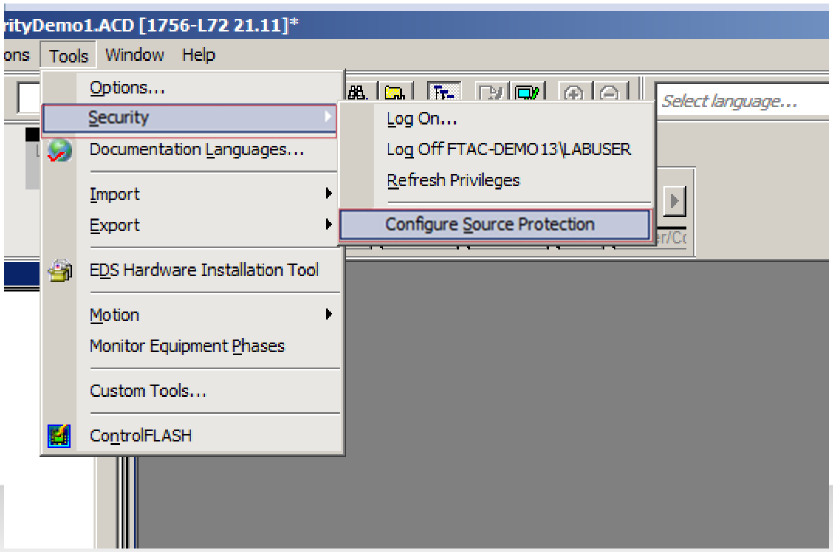
User 3

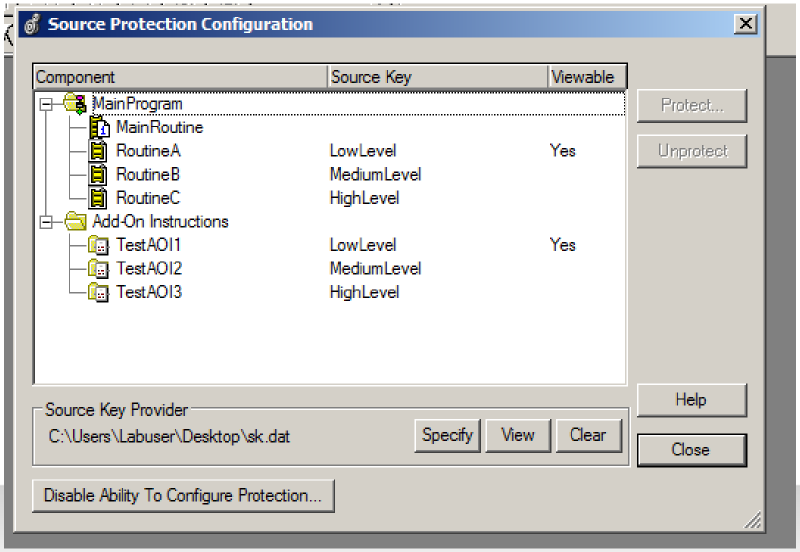
USER TYPE



# Password Source Protection

## ASSIGN A PASSWORD TO ANY ROUTINE OR ADD-ON INSTRUCTION



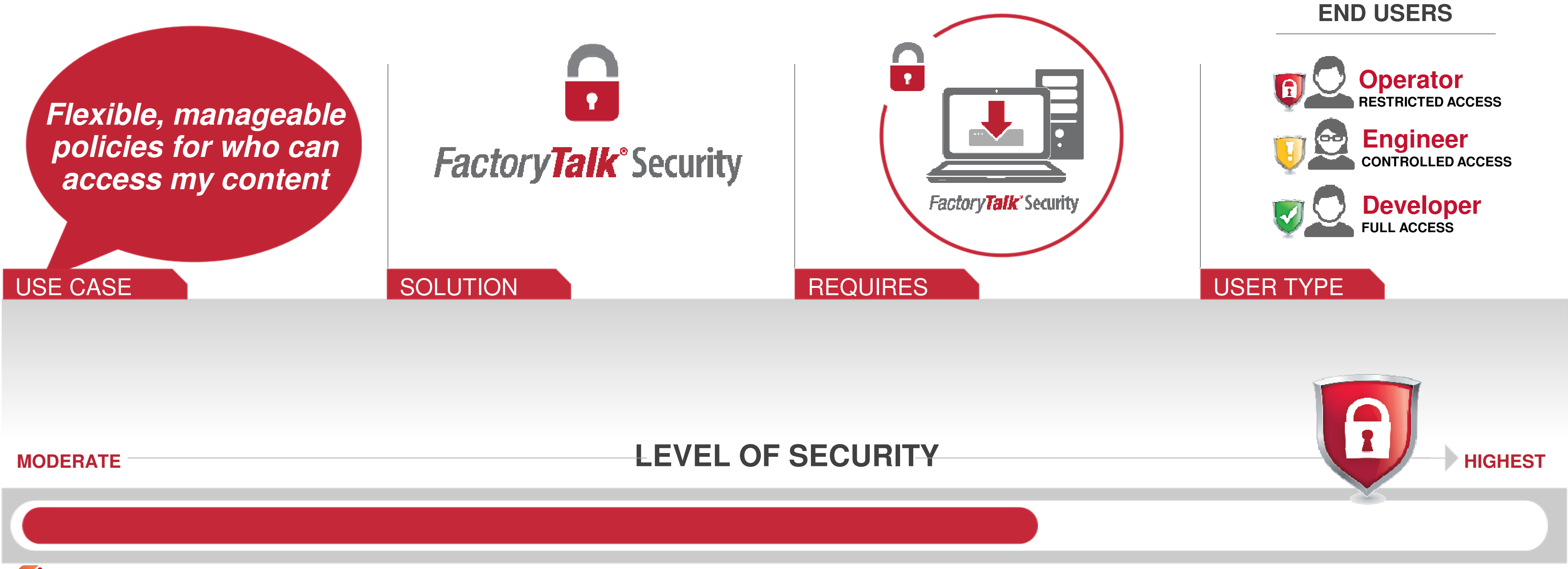

Source Protection Configuration
Protect...
Unprotect
Help
Close
Specify
View
Clear
Disable Ability To Configure Protection...

| Component | Source Key | Viewable |
|---|---|---|
| MainProgram | | |
| MainRoutine | | |
| RoutineA | LowLevel | Yes |
| RoutineB | MediumLevel | |
| RoutineC | HighLevel | |
| Add-On Instructions | | |
| TestAOI1 | LowLevel | Yes |
| TestAOI2 | MediumLevel | |
| TestAOI3 | HighLevel | |

Source Key Provider: C:\Users\Labuser\Desktop\sk.dat

# FactoryTalk® Security

## Flexible, Manageable Policies for Content



USE CASE

*Flexible, manageable policies for who can access my content*

SOLUTION

FactoryTalk® Security

REQUIRES

FactoryTalk® Security

USER TYPE

END USERS

**Operator** RESTRICTED ACCESS

**Engineer** CONTROLLED ACCESS

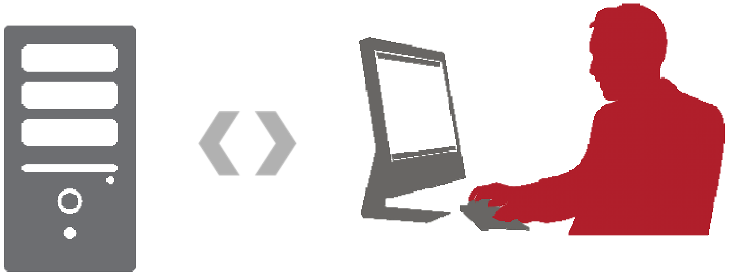
**Developer** FULL ACCESS

LEVEL OF SECURITY

MODERATE

HIGHEST

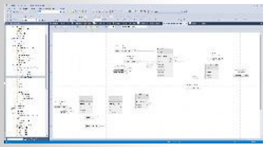
# FactoryTalk® Security



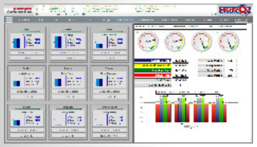
FactoryTalk® Directory

- Authenticate the User
- Authorize Use of Applications
- Authorize Access to Specific Devices

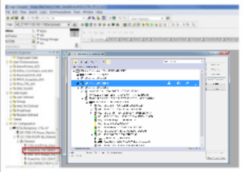
## FactoryTalk® SECURITY ENABLED SOFTWARE EXAMPLES



Studio 5000®



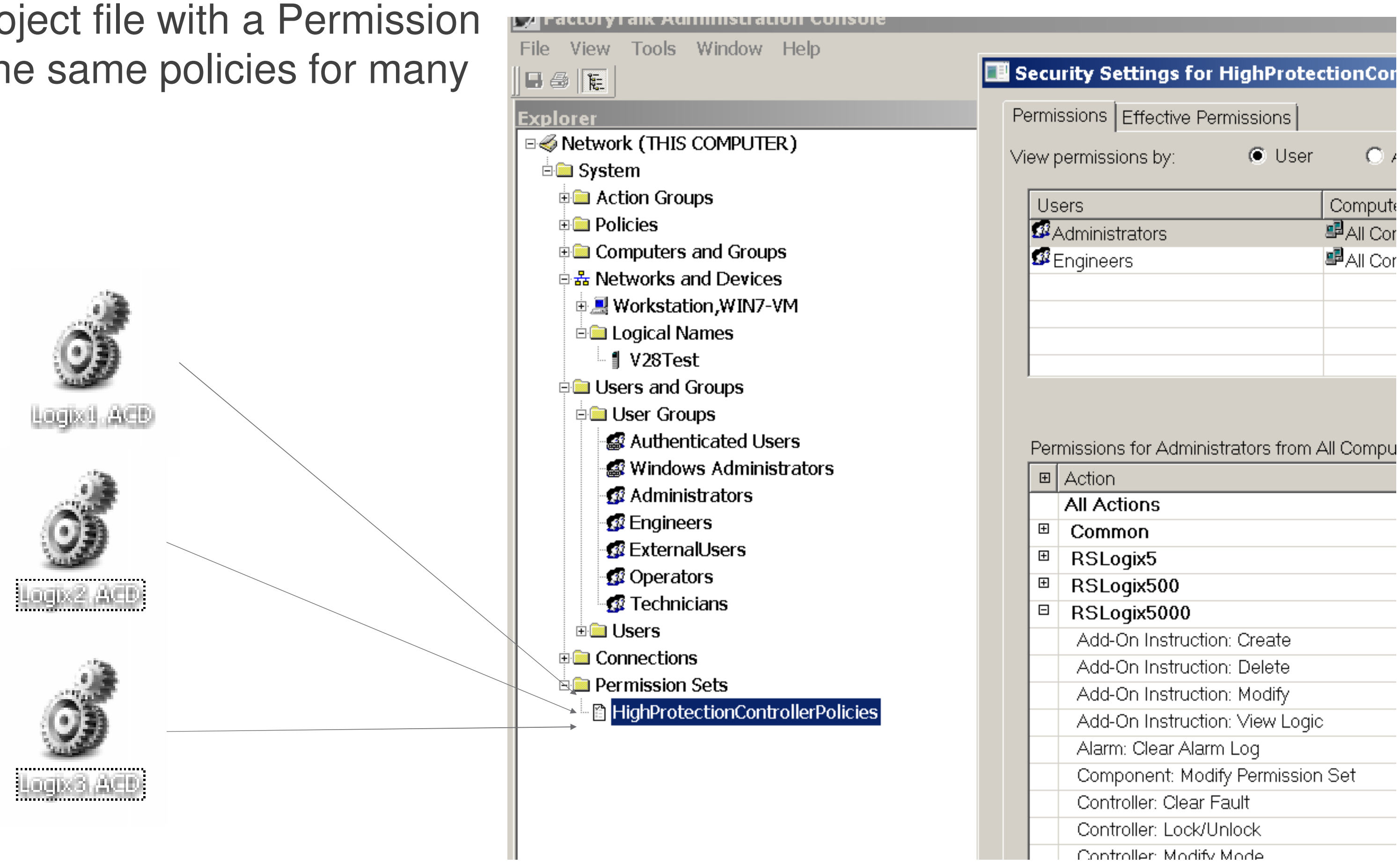
FactoryTalk® View SE



RSLinx® Enterprise

# Permission Sets for Securing Projects

- Secure a project file with a Permission Set to use the same policies for many controllers


Logix1.ACD
Logix2.ACD
Logix3.ACD
FactoryTalk Administration Console
File View Tools Window Help
Explorer
Security Settings for HighProtectionCon
Permissions
Effective Permissions

Network (THIS COMPUTER)
- System
  - Action Groups
  - Policies
  - Computers and Groups
  - Networks and Devices
    - Workstation,WIN7-VM
    - Logical Names
      - V28Test
  - Users and Groups
    - User Groups
      - Authenticated Users
      - Windows Administrators
      - Administrators
      - Engineers
      - ExternalUsers
      - Operators
      - Technicians
    - Users
  - Connections
  - Permission Sets
    - HighProtectionControllerPolicies

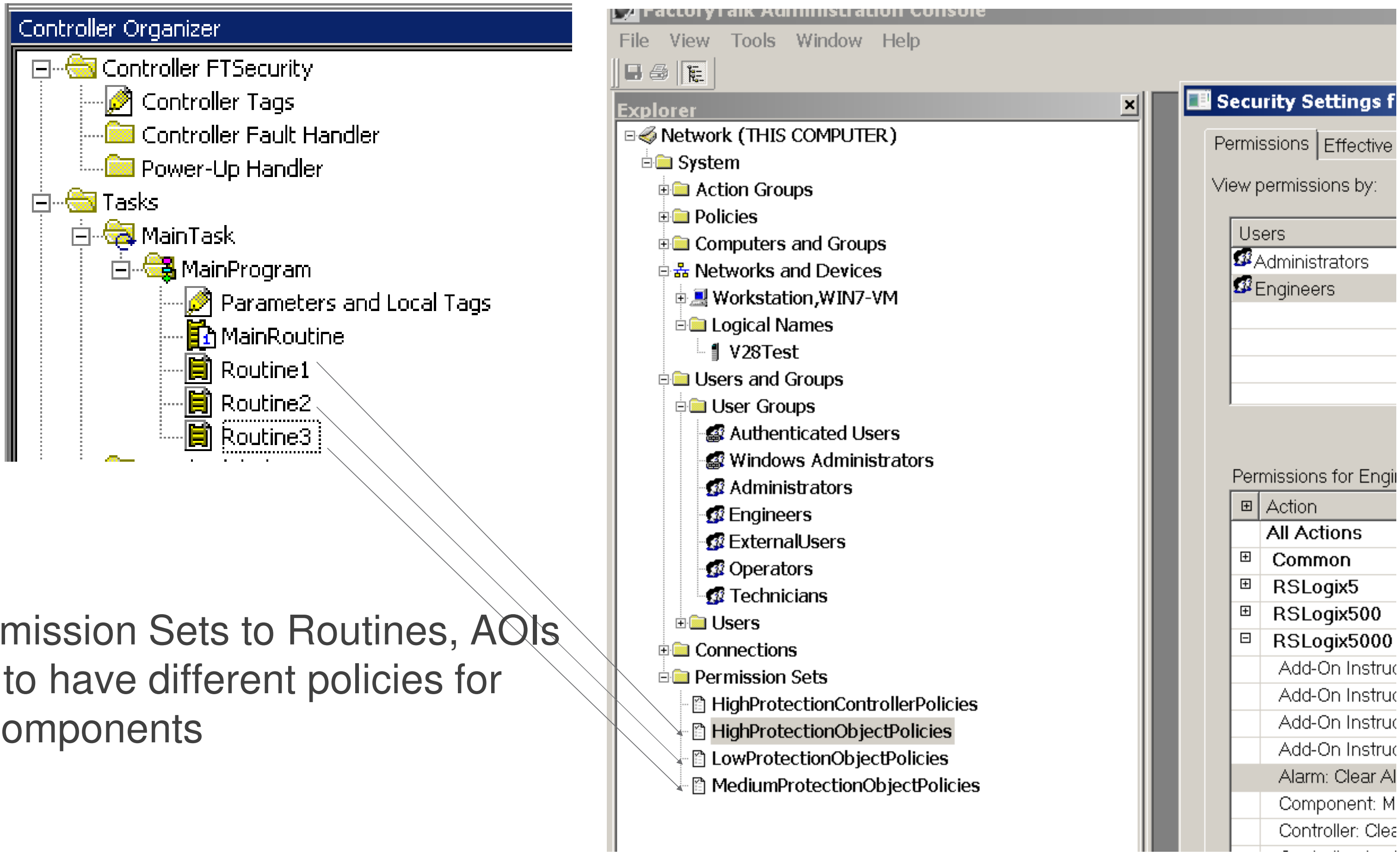
View permissions by: ● User ○

| Users | Compute |
|---|---|
| Administrators | All Cor |
| Engineers | All Cor |

Permissions for Administrators from All Compu

| ⊞ Action |
|---|
| All Actions |
| ⊞ Common |
| ⊞ RSLogix5 |
| ⊞ RSLogix500 |
| ⊟ RSLogix5000 |
| Add-On Instruction: Create |
| Add-On Instruction: Delete |
| Add-On Instruction: Modify |
| Add-On Instruction: View Logic |
| Alarm: Clear Alarm Log |
| Component: Modify Permission Set |
| Controller: Clear Fault |
| Controller: Lock/Unlock |
| Controller: Modify Mode |

# Permission Sets for Securing Routines, AOIs and Tags



Controller Organizer

- Controller FTSecurity
  - Controller Tags
  - Controller Fault Handler
  - Power-Up Handler
- Tasks
  - MainTask
    - MainProgram
      - Parameters and Local Tags
      - MainRoutine
      - Routine1
      - Routine2
      - Routine3

FactoryTalk Administration Console

Explorer

- Network (THIS COMPUTER)
  - System
    - Action Groups
    - Policies
    - Computers and Groups
    - Networks and Devices
      - Workstation,WIN7-VM
      - Logical Names
        - V28Test
    - Users and Groups
      - User Groups
        - Authenticated Users
        - Windows Administrators
        - Administrators
        - Engineers
        - ExternalUsers
        - Operators
        - Technicians
      - Users
    - Connections
    - Permission Sets
      - HighProtectionControllerPolicies
      - HighProtectionObjectPolicies
      - LowProtectionObjectPolicies
      - MediumProtectionObjectPolicies

Security Settings f

View permissions by:

| Users |
|---|
| Administrators |
| Engineers |

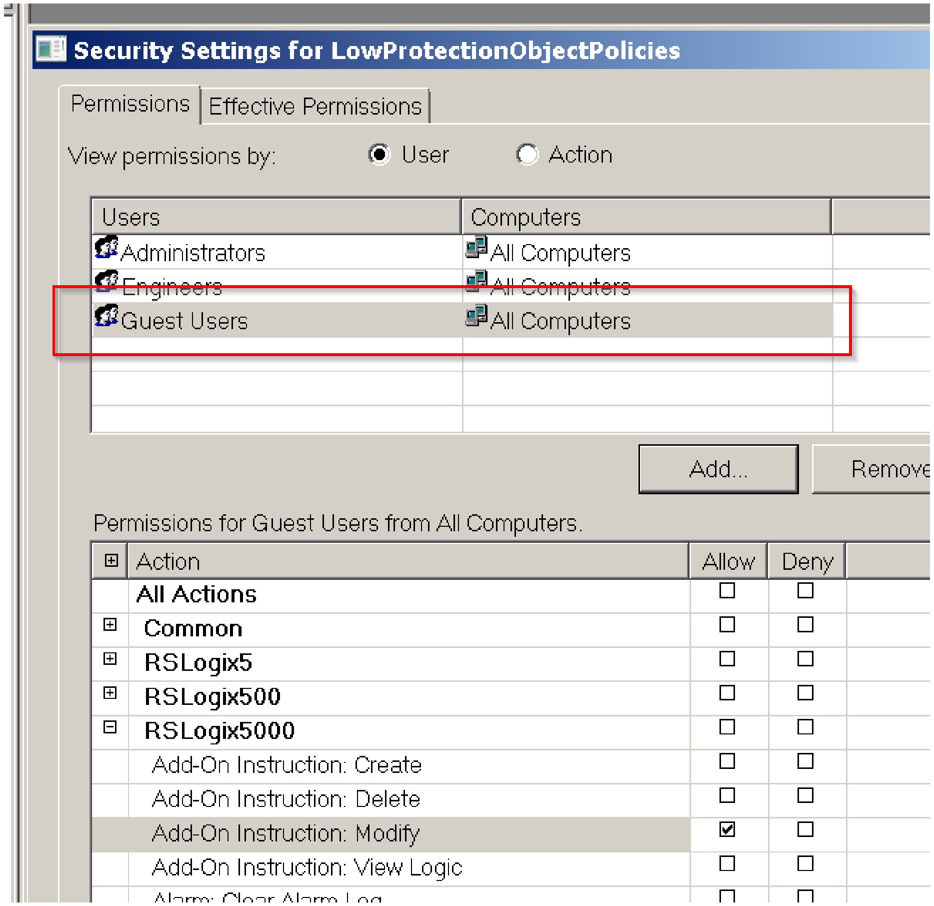
Permissions for Engi

| Action |
|---|
| All Actions |
| ⊞ Common |
| ⊞ RSLogix5 |
| ⊞ RSLogix500 |
| ⊟ RSLogix5000 |
| Add-On Instruc |
| Add-On Instruc |
| Add-On Instruc |
| Add-On Instruc |
| Alarm: Clear Al |
| Component: M |
| Controller: Clea |

- Apply Permission Sets to Routines, AOIs and Tags to have different policies for different components

# Guest User Access

- With Guest Users, grant limited permissions to users who aren’t members of your FactoryTalk® Directory



**Security Settings for LowProtectionObjectPolicies**

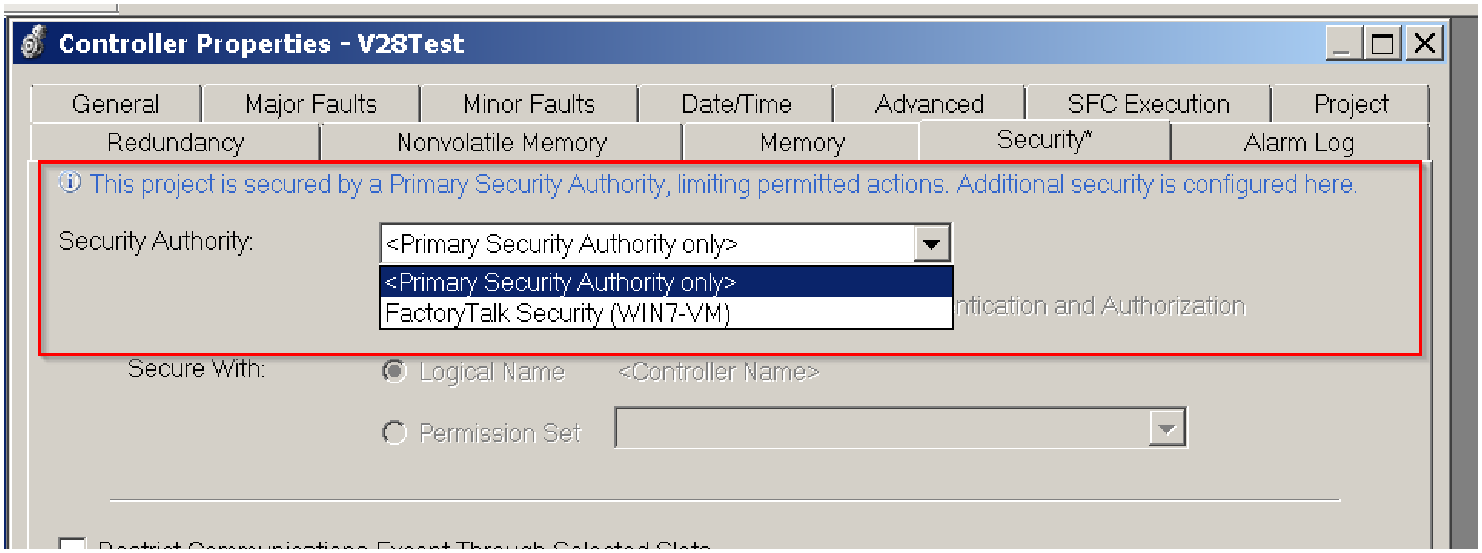
View permissions by: ● User ○ Action

| Users | Computers |
|---|---|
| Administrators | All Computers |
| Engineers | All Computers |
| Guest Users | All Computers |

Permissions for Guest Users from All Computers.

| ⊞ | Action | Allow | Deny |
|---|---|---|---|
| | All Actions | □ | □ |
| ⊞ | Common | □ | □ |
| ⊞ | RSLogix5 | □ | □ |
| ⊞ | RSLogix500 | □ | □ |
| ⊟ | RSLogix5000 | □ | □ |
| | Add-On Instruction: Create | □ | □ |
| | Add-On Instruction: Delete | □ | □ |
| | Add-On Instruction: Modify | ☑ | □ |
| | Add-On Instruction: View Logic | □ | □ |
| | Alarm: Clear Alarm Log | □ | □ |

# Secondary Security Authority



ⓘ This project is secured by a Primary Security Authority, limiting permitted actions. Additional security is configured here.

Security Authority: <Primary Security Authority only>

<Primary Security Authority only>
FactoryTalk Security (WIN7-VM)

ntication and Authorization

Secure With: ● Logical Name <Controller Name>

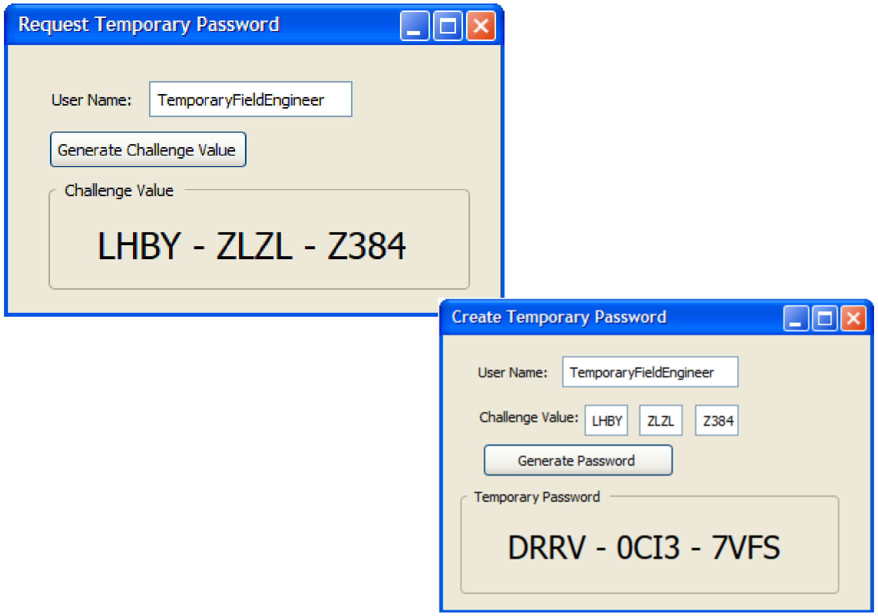
○ Permission Set

□ Restrict Communications Except Through Selected Slots

- Guest Users can further limit access to a project file with a Secondary Security Authority

# FactoryTalk® Temporary Users

- Use FactoryTalk® Temporary Users to temporarily give someone access to privileges of a different user group



Request Temporary Password

User Name: TemporaryFieldEngineer

Challenge Value

LHBY - ZLZL - Z384

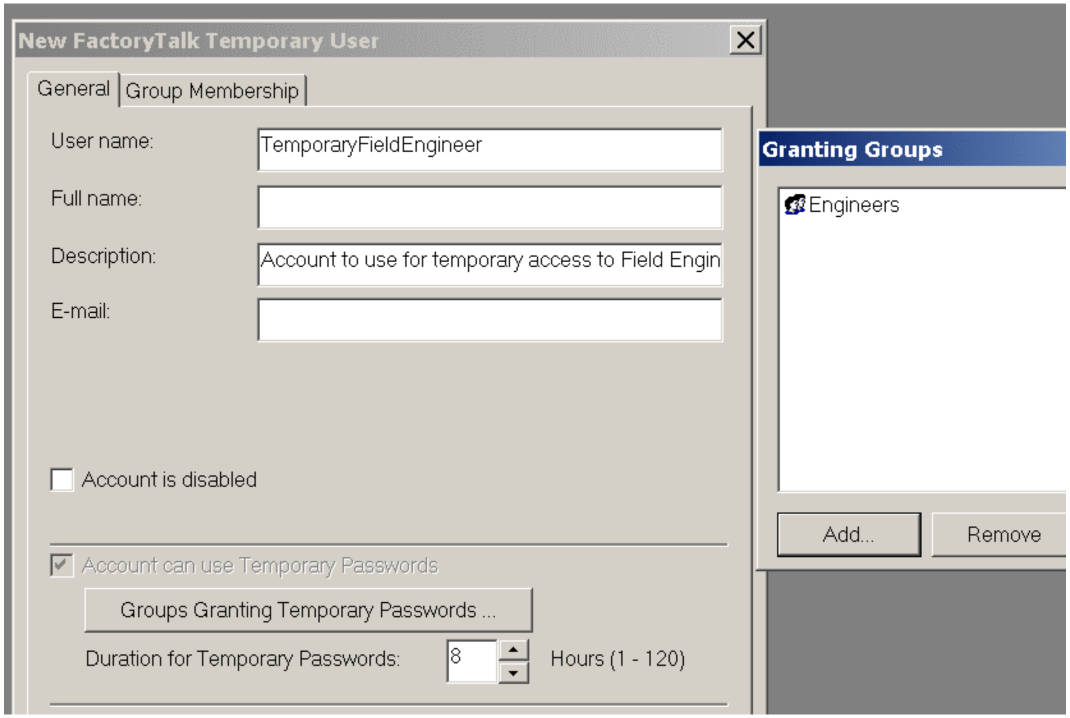
Create Temporary Password

User Name: TemporaryFieldEngineer

Challenge Value: LHBY ZLZL Z384

Temporary Password

DRRV - 0CI3 - 7VFS



New FactoryTalk Temporary User

User name: TemporaryFieldEngineer

Full name:

Description: Account to use for temporary access to Field Engin

E-mail:

□ Account is disabled

☑ Account can use Temporary Passwords

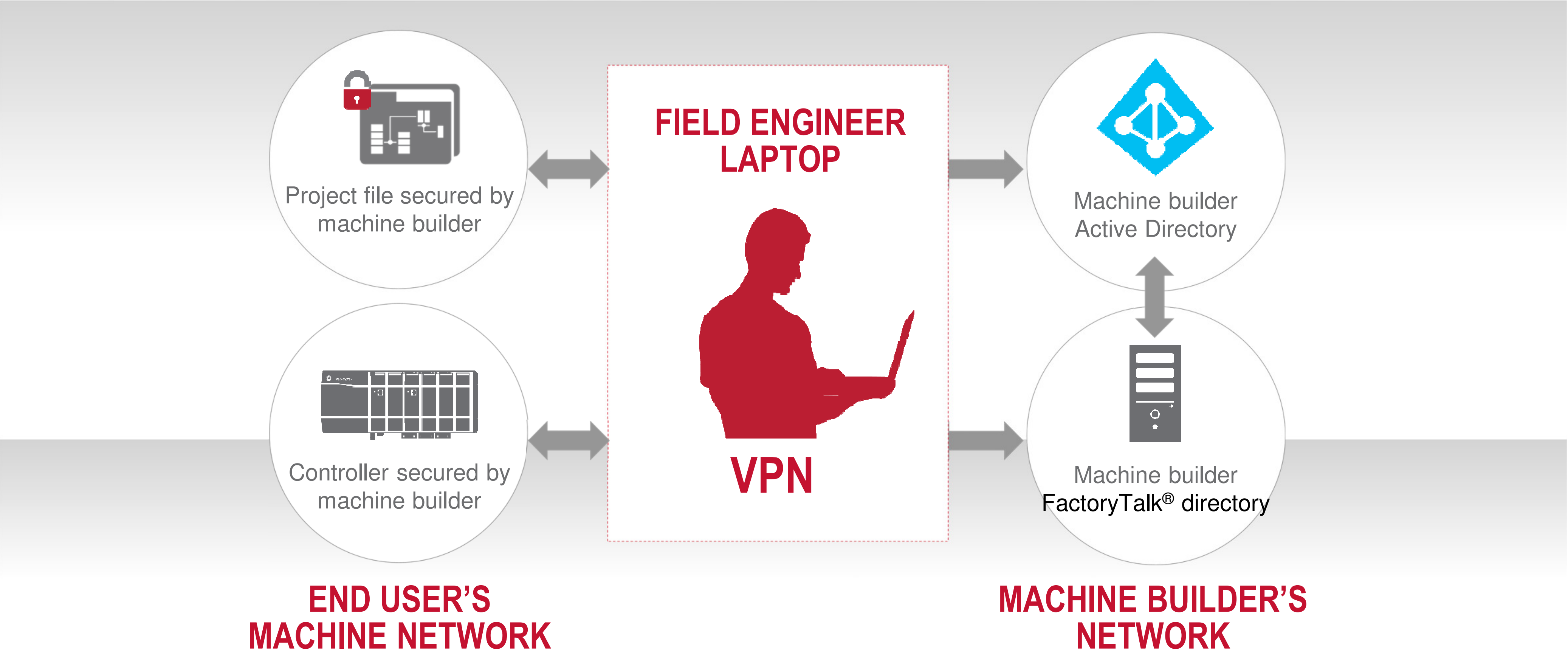
Duration for Temporary Passwords: 8 Hours (1 - 120)

Granting Groups

Engineers

# FactoryTalk® Security

## Machine Builder Environment


Project file secured by machine builder
Controller secured by machine builder
FIELD ENGINEER LAPTOP
VPN
Machine builder Active Directory
Machine builder FactoryTalk® directory
END USER'S MACHINE NETWORK
MACHINE BUILDER'S NETWORK

# License Source & Execution Protection

## Secure Hardened IP Protection of Content

USE CASE

***Most secure protection possible for intellectual property.***

SOLUTION

**License**
Source and Execution

REQUIRES

Activated
Secure Device

Subscription to
License Portal

USER TYPE

**OEMS**
HIGHLY SENSITIVE IP

**END USERS**
THEFT OF CONTENT
IS CONCERN

MODERATE — LEVEL OF SECURITY → HIGHEST

Rockwell Automation

# Content License Protection

## Robust protection of Intellectual Property

### DEVELOPER
FULL ACCESS

- Easily Edit and Deploy IP protected content

### MAINTENANCE ENGINEER
CONTROLLED ACCESS

- Can Diagnose / Modify unprotected parts of the program
- Add new content as needed
- Force IO, modify a signal, replace/add devices, manage performance data, etc
- Uptime! Less support needed

### END USER
RESTRICTED ACCESS

- Can still use FactoryTalk® Security (V28+) for additional control / access regulation
- Multiple IP Owners in one system
- Retains Access to Unprotected Content

# WORKING TOGETHER

**Password**
Source Protection

FactoryTalk® Security

**License**
Source and Execution Protection

**CONTENT PROTECTION CAN EXIST TOGETHER LIKE MULTIPLE DIFFERENT LOCKS ON A DOOR**

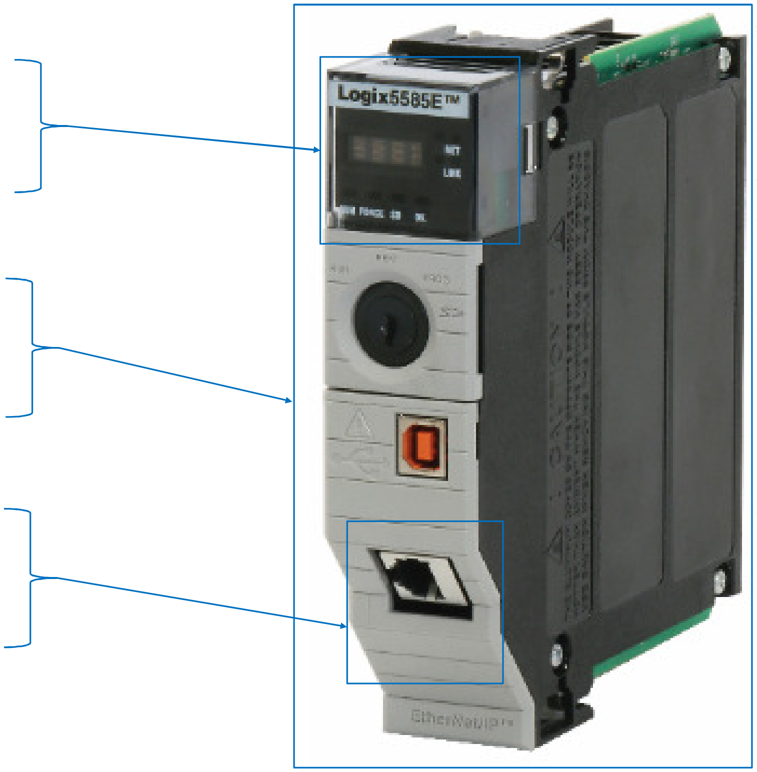
# Which Do I Choose?

| USE CASE | SECURITY OPTION |
|---|---|
| I want **limited control** over who accesses my content, but my chief concern is simplicity | **Password** Source Protection |
| I want **flexible, manageable** policies for who can access my content | FactoryTalk® Security |
| I want the **most secure** protection possible for my content | License **Source** Protection |
| **I want to control** the use of my content | **License** Execution Protection |

# Logix 5580 & 5380 – Controller MSG to SELF

User configurable functionality for an additional layer of security

- Programmatic ability enable/disable via Message to “SELF”
- Configurable “*Masking*” of Scrolled Fields 4-Char LCD
- Embedded Web Page Disable/Enable
- Embedded Ethernet port Disable/Enable



# Logix 5580 & 5380 4-Char LCD

User configurable “Masking” for an additional layer of security

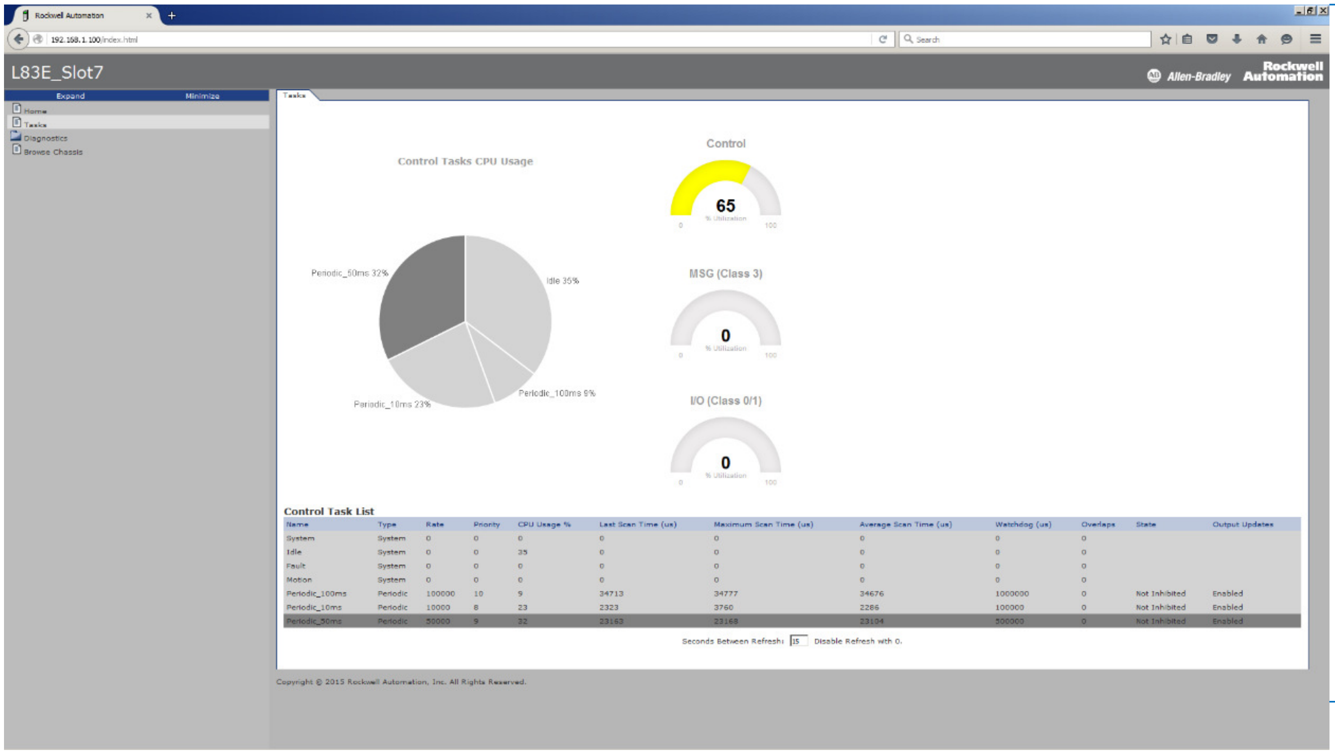
- Normal Scrolling Messages on the LCD Display:
  - 1.) Controller Name - (**Controller_Name**)
  - 2.) Link Status - (**Link 1 - Down**)
  - 3.) Port Status - (**Port A - 192.168.1.1**)

- Configurable “*Masking*” of Scrolled Fields with a MSG to SELF
  - Default (All shown)
    - **Controller_Name    Link 1 – Down    Port A - 192.168.1.1**
  - Controller Name and Link Status (only)
    - **Controller_Name    Link 1 – Down    --------------------------**
  - Port & IP Address (only)
    - **------------------------    --------------------    Port A - 192.168.1.1**
  - Completely OFF
    - **------------------------    --------------------    --------------------------**

# Logix 5580 & 5380 Embedded Web Page

User configurable Disable/Enable for an additional layer of security

- Configurable Disable/Enable of Controller Embedded Web Page



Control Task List

| Name | Type | Rate | Priority | CPU Usage % | Last Scan Time (us) | Maximum Scan Time (us) | Average Scan Time (us) | Watchdog (us) | Overlaps | State | Output Updates |
|---|---|---|---|---|---|---|---|---|---|---|---|
| System | System | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| Idle | System | 0 | 0 | 35 | 0 | 0 | 0 | 0 | 0 | | |
| Fault | System | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| Motion | System | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| Periodic_100ms | Periodic | 100000 | 10 | 9 | 34713 | 34777 | 34676 | 1000000 | 0 | Not Inhibited | Enabled |
| Periodic_10ms | Periodic | 10000 | 8 | 23 | 2323 | 3760 | 2286 | 100000 | 0 | Not Inhibited | Enabled |
| Periodic_50ms | Periodic | 50000 | 9 | 32 | 23163 | 23168 | 23104 | 500000 | 0 | Not Inhibited | Enabled |

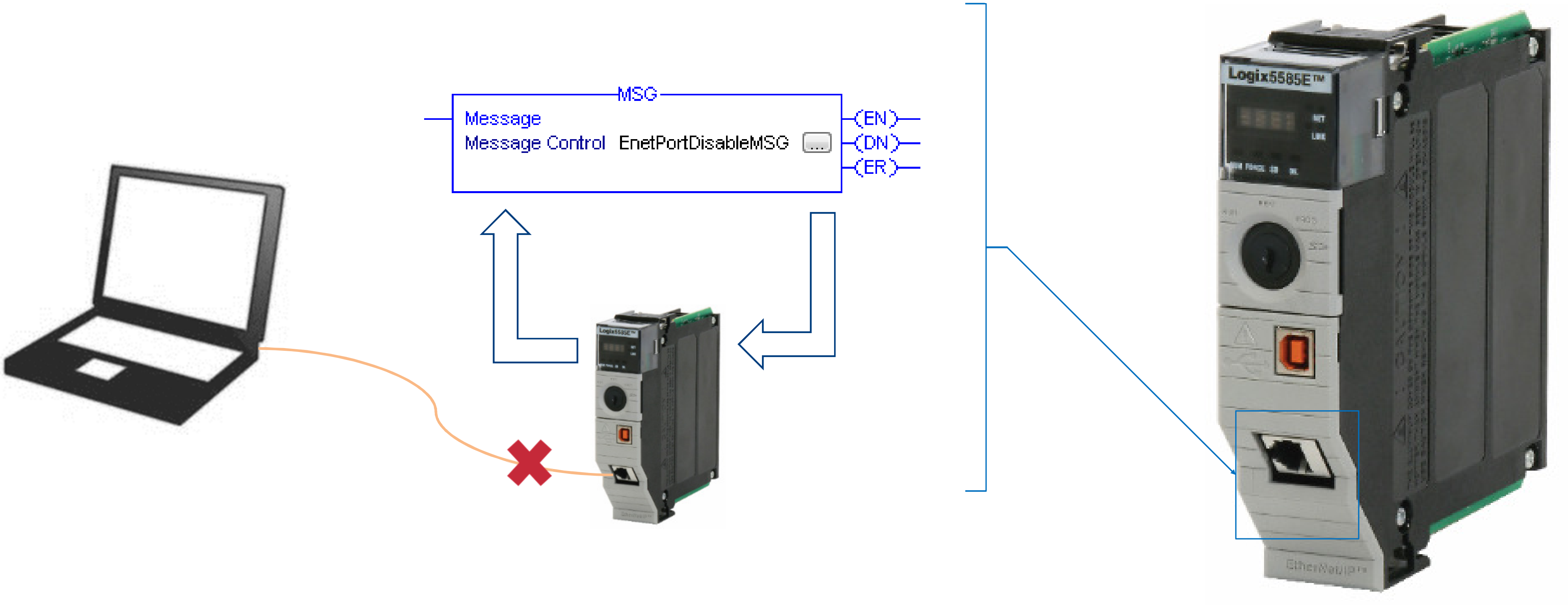
Seconds Between Refresh: 15 Disable Refresh with 0.

Copyright © 2015 Rockwell Automation, Inc. All Rights Reserved.

# Logix 5580 & 5380 Embedded Ethernet Port

User configurable Enable/Disable for an additional layer of security

- Configurable Disable/Enable of Controller Ethernet Port



MSG

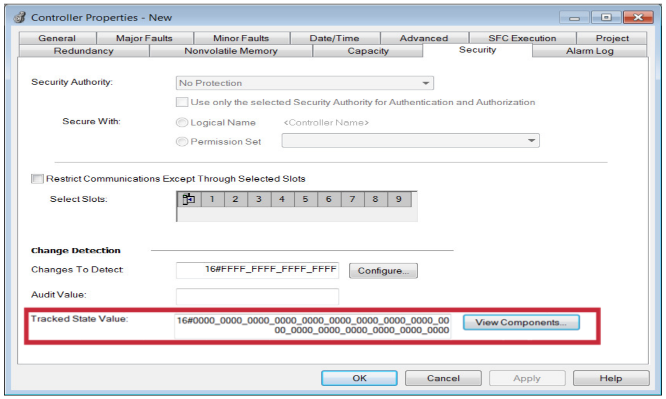
Message

Message Control EnetPortDisableMSG

# Component Change Detection

Determine if the state of key components in a program have changed (5570)

- Quickly determine if changes were made to a program offline.
- New Tracking Group setting enables the tracking of changes on a granular basis for tags, I/O modules, and routines within a program.
- In the event that changes are made to components within a “Tracked Group”, the group signature will change.



Security Authority: No Protection

□ Use only the selected Security Authority for Authentication and Authorization

Secure With: ○ Logical Name <Controller Name>

○ Permission Set

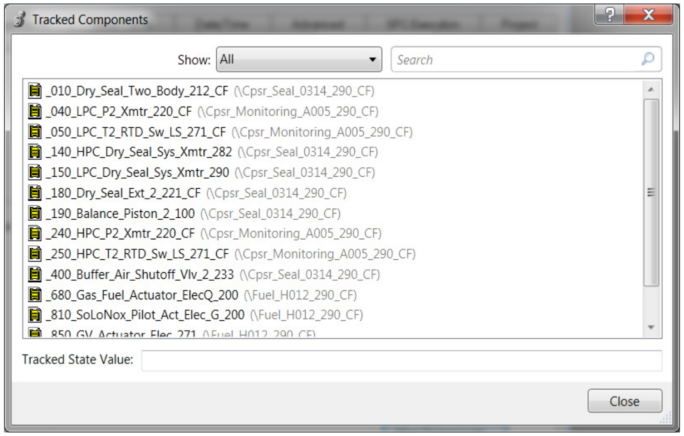
□ Restrict Communications Except Through Selected Slots

**Change Detection**

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF

Audit Value:

Tracked State Value: 16#0000_0000_0000_0000_0000_0000_0000_0000_0000_0000_0000_0000_0000_0000_0000_0000



Show: All

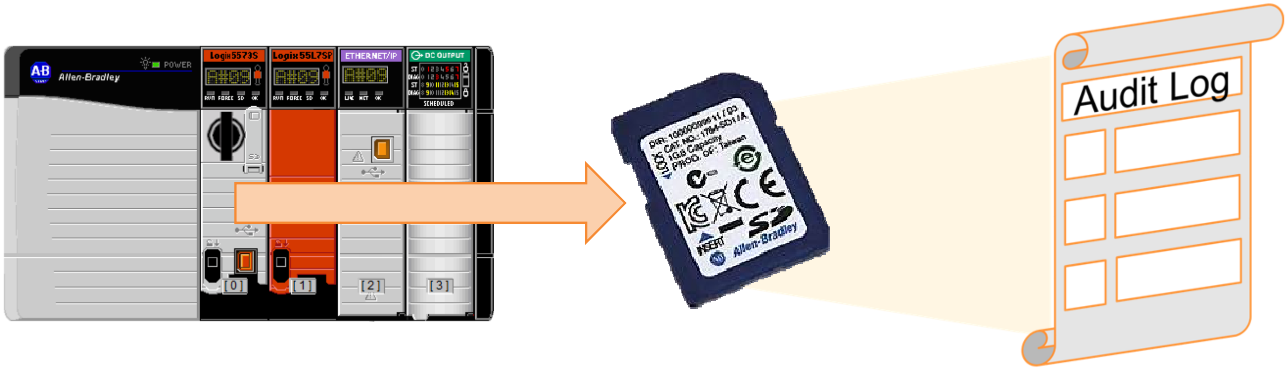
_010_Dry_Seal_Two_Body_212_CF (\Cpsr_Seal_0314_290_CF)
_040_LPC_P2_Xmtr_220_CF (\Cpsr_Monitoring_A005_290_CF)
_050_LPC_T2_RTD_Sw_LS_271_CF (\Cpsr_Monitoring_A005_290_CF)
_140_HPC_Dry_Seal_Sys_Xmtr_282 (\Cpsr_Seal_0314_290_CF)
_150_LPC_Dry_Seal_Sys_Xmtr_290 (\Cpsr_Seal_0314_290_CF)
_180_Dry_Seal_Ext_2_221_CF (\Cpsr_Seal_0314_290_CF)
_190_Balance_Piston_2_100 (\Cpsr_Seal_0314_290_CF)
_240_HPC_P2_Xmtr_220_CF (\Cpsr_Monitoring_A005_290_CF)
_250_HPC_T2_RTD_Sw_LS_271_CF (\Cpsr_Monitoring_A005_290_CF)
_400_Buffer_Air_Shutoff_Vlv_2_233 (\Cpsr_Seal_0314_290_CF)
_680_Gas_Fuel_Actuator_ElecQ_200 (\Fuel_H012_290_CF)
_810_SoLoNox_Pilot_Act_Elec_G_200 (\Fuel_H012_290_CF)
_850_GV_Actuator_Elec_271 (\Fuel_H012_290_CF)

Tracked State Value:

# Controller Based Audit Log

Updates to the Controller Logs (5570)

- Detailed log files created and stored to the SD Card
  - As detailed as the records that Logix Designer currently sends to AssetCentre
- The Controller “cryptographically” signs the log files that are written to the SD card, as well as verify the authenticity of those log files.



Rockwell Automation

Innovation & Technology Forum

# Thank you