L03 - Design, Implement, and Manage FactoryTalk Security
Background: What is FactoryTalk Security?

Use FactoryTalk Security to...

Manage the insider threat by authenticating the user and authorizing the use of Rockwell Automation software applications to access automation devices.

How does it work?

Provides a security authority to verify identity of each user and grants or deny user's requests to perform a particular set of actions on resources within the system.

- User Roles (FT groups or Windows groups)
- User Accounts (FT users or Windows users)
- Computers and Computer Groups
- System Policies (plant wide)
- Product Policies
- Controllers to be secured
- Secure Controllers by Area (resource groups)
Let's Learn about Fred
Creating User Accounts

“Fred”; user name and PW
Let’s Learn about Fred
FactoryTalk System Policies

“Fred’s” PW expires in 30 days
Let’s Learn about Fred
Assigning Users to a Group or Role

“Fred” is an Engineer
Let’s Learn about Fred
Assign FactoryTalk Software Permissions

“Fred” can use Logix Designer
Let’s Learn about Fred
Assign Groups or Roles Permissions

Engineers can Modify AOI’s
Let’s Learn about Fred
Resource Assignment to Areas of Applications

Finally; “Fred” is an Engineer who can Modify AOI’s on all controllers in “Area2”
FactoryTalk Security in Logix Controllers Using the Security Authority Identifier (SAID)

- With FactoryTalk Services Platform SR5 and Logix V20 (and later)
  - Configures Logix Controllers to require that all users be authenticated from a specific instance of the FactoryTalk Directory before they can access the controller (Security Authority Identifier)
  - Security Authority Identifier gets stored in the project (“project binding”) – secures the offline file

Anyone working on a project (on-line or off-line) with the “Security Authority ID required” box checked...

Is first required to “Log On” ....

... using the FactoryTalk Directory used to secure the project
Backing up the SAID

- Use the FactoryTalk Administration Console, the **Security Authority Identifier** can be…
  - Encrypted with a passphrase or password to allow for secure backup copies (disaster recovery)
  - Allows secure duplication and distribution to allow multiple FTDirectories to share the same ID!
    - Can be used to replace the CPU Lock functionality that was deprecated in v20
Secure Slot for Communications

Controller Properties - Security Hardening

Security Authority: FactoryTalk Security (\SERVER\rest_of_the...

Require Matching Security Authority ID for Authentication and Authorization

Restrict Communication Except Through Selected Slots

Select Slots:

Communication Restricted Through Controller Ports

RSLogix 5000

Configuration and Programming of the Logix 5000 family of controllers
Pick and Choose: Data Access Control

- Users can assign External Access settings of Read/Write, Read Only, or None to tags
  - Useful to control which tags can be modified from an HMI or other external application
- A cryptographically licensed trusted connection is established between RSLogix™ 5000 and the Logix controller
  - Ensures the “External Access” attribute can only be changed by RSLogix 5000
  - “Who” can use RSLogix 5000 to change this attribute controlled by FactoryTalk® Security
- Users can also define tags as Constants
  - Constants can not be modified by controller logic

Improves security of tags especially when used in conjunction with FactoryTalk® Security
Pick and Choose: FactoryTalk View SE Security

- FactoryTalk View SE Security can be applied to:
  - Displays
Pick and Choose: FactoryTalk View SE Security

- FactoryTalk View SE Security can be applied to:
  - Displays
  - Objects
Pick and Choose: FactoryTalk View SE Security

- FactoryTalk View SE Security can be applied to:
  - Displays
  - Objects
  - Applications
Pick and Choose: ControlLogix Real-Time Change Detection

- Real-time monitoring of ControlLogix V20 or higher for changes via “Audit Value”
- On Detect will get activities via controller “Change Log”
- On Detect complete will consolidate all activities in a Report via Event Log
- Will detect Rogue changes
Pick and Choose: FactoryTalk AssetCentre Audit / Change Reporting

- Search FactoryTalk AssetCentre
  - Events
  - Audits
  - Archive history
- Schedule a Report or “Run Now”
- Email reports per a Schedule

**Examples**

- Search audit log for changes made during last four hours to a specific asset that has failed
- Search archive history to determine what files a user has modified during last month
- Search event logs for upload tasks that failed
- Search audit log at the end of every shift for any forces or empty branches to improve plant-floor safety
Main Sections of the Lab:

1. FactoryTalk Overview: Everyone Must Complete
2. Deploy Initial RSLogix Project to Controller: Everyone Must Complete
3. Securing RSLogix 5000: Everyone Must Complete
5. Securing Controller Data & Access: Pick & Choose
6. Protecting RSLogix 5000 Source Code: Pick & Choose
7. Real-Time Change Management for ControlLogix: Pick & Choose
Main Sections of the Lab:

1. FactoryTalk Overview: **Everyone Must Complete**
2. Deploy Initial RSLogix Project to Controller: **Everyone Must Complete**
3. Securing RSLogix 5000: **Everyone Must Complete**
5. Securing Controller Data & Access: **Pick & Choose**
6. Protecting RSLogix 5000 Source Code: **Pick & Choose**
7. Real-Time Change Management for ControlLogix: **Pick & Choose**