RTAC R153 Technical Note

With the addition of firmware version R153-V0 to the RTAC product line, the following are some notes and additional comments about new additions or changes in the firmware. These items are compiled from the release notes found in *Appendix A: Firmware and Manual Versions* of the ACSELERATOR RTAC® SEL-5033 Software Instruction Manual. Please note that this document does not discuss each release note, but rather just those with additional context or conversation points. This information can also be found in the SEL-5033 instruction manual in the appropriate sections for the new or modified behavior.

Some new features or enhancements to existing features in R153-V0 include the following:

- [Cybersecurity Enhancement] Added the Security and Auth web APIs to manage the X.509 certificates, CA certificates, and LDAP settings.
- [Cybersecurity Enhancement] Enhanced the Network web API to manage the Hosts settings.
- [Cybersecurity Enhancement] Enhanced the OPC UA server and client protocols to support the Sign and Encrypt security mode.
- [Cybersecurity Enhancement] Enhanced the IIoT library packages to support the HTTPS and MQTTS TLS-based connections.
- Added the Network Event Capture tool to allow the automatic creation of trigger-based Ethernet communication monitor captures with configurable pre- and post-trigger durations.
- Added support for licensed features to allow temporary demonstration periods for as many as 90 days for licensed protocols and libraries.
- Enhanced the SEL-3350 to support as many as 50,000 tags in a project.
- Enhanced the Modbus server to support shared tag maps.
- Enhanced the SEL Protocol Client so that collected CEV event records can be converted into equivalent COMTRADE records.
- Enhanced the Axion Protection CT/PT and AC Metering EtherCAT modules to provide IEEE C37.118 PMU streaming rates of 120 Hz and 100 Hz.
- Enhanced the Axion touchscreen capabilities to support an alarm summary screen and customized annunciator screens.
- Enhanced the IP Alias support to allow use with interfaces that are bridged, bonded, or configured in a PRP pair.

ACSELERATOR RTAC enhancements include the following:

- Added a Tag Selector tool to allow browsing and easy selection of all tags in a project with drag-and-drop operations so that these tags can be copied into supported fields, such as the Simple Tag Mapper and Tag Processor.
- Enhanced the project tree to display the connection status of devices as offline, online, or disabled while connected to an RTAC with firmware version R151 or later installed.

- Enhanced the project tree to allow copy and paste operations for IEC 61131 User Logic elements (Programs, Functions, Function Blocks, Data Types, and GVLs) in RTAC projects with a firmware version of R148 or later.
- Added an Other column to the Start Page project list that indicates the presence of the Advanced Read-In components (Ethernet Settings, HMI Projects, etc.) in a project.
- Enhanced the task re-ordering dialog to support bulk assignment for the order of items in the main and automation tasks when using a custom order.

Library Extension additions and enhancements:

- Added the Grid Connect extension.
- Added the DMA Link extension.
- Added the 87L Comm Monitor extension.

The following are additional comments on new features and changes in the RTAC product line.

Security, Auth, and Network Web APIs

When managing a large number of RTACs, it can be challenging to perform system-wide modifications, such as rotating the CA certificates or changing the LDAP settings. The addition of the Security and Auth web APIs allows these aspects of the RTAC settings to be retrieved or modified programmatically and accommodates mass remote updates of certificates and settings to multiple RTACs. The specific capabilities of these new and enhanced APIs include the following:

LDAP General Settings

- Retrieve or update LDAP general settings

LDAP Group Mappings

- Create LDAP group mappings
- Retrieve a list of all LDAP group mappings
- Retrieve, update, or delete a single LDAP group mapping

Hosts

- Retrieve a list of all hosts
- Create a new hosts entry
- Retrieve, update, or delete a single hosts entry

CA Certificates

- Retrieve a list of all CA certificates
- Upload a certificate in PEM format
- Retrieve the information from a single certificate
- Delete a single certificate
- Retrieve a single certificate in PEM format
- Update a single certificate

X.509 Certificates

- Retrieve a list of all X.509 certificates
- Generate a new X.509 certificate
- Upload an existing X.509 certificate in PKCS#12 format

- Retrieve the information from a single X.509 certificate
- Delete a single X.509 certificate
- Retrieve a single X.509 certificate in PEM format
- Update a single X.509 certificate
- Retrieve the Certificate Signing Request (CSR) from a single certificate
- Activate an X.509 certificate

Figure 1 shows an example of retrieving the information from an X.509 certificate via the Security API:

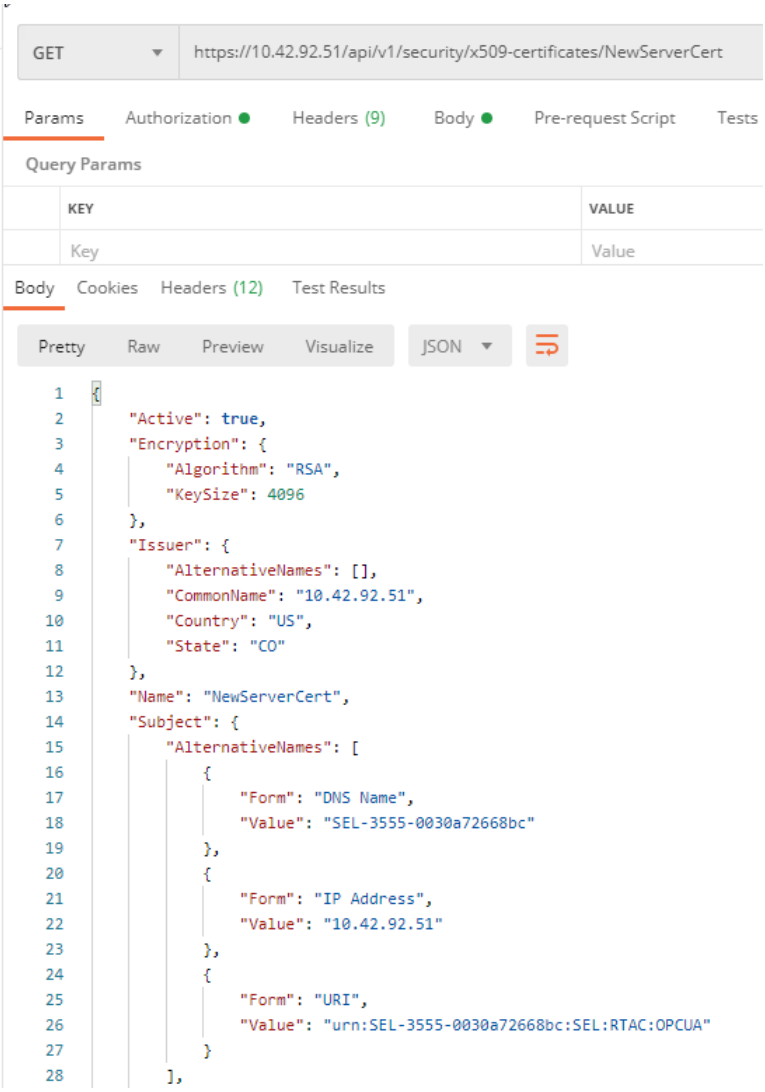

Figure 1 Retrieving the X.509 Certificate Information

Enhanced the OPC UA Server and Client Protocols to Support the Sign and Encrypt Message Security Modes

The OPC UA server and client protocols were introduced to the RTAC in firmware versions R150 and R151, respectively. A common request is that these protocols allow for secure TLS-encrypted conversations between the RTAC and an OPC UA endpoint by supporting Message Security Modes. From an RTAC settings standpoint, this requires adding two new settings: **Message Security Mode** and **Security Policy**. On the server, these two settings represent a minimum message security mode and policy to which the client must conform. To the client,

these settings represent a preferred method of communication with the server. These two settings should match between the client and server. For example, the RTAC OPC UA client settings of Sign and Encrypt and Basic256Sha256 (shown in *Figure 2*) should match the appropriate server settings for the allowable security policies.

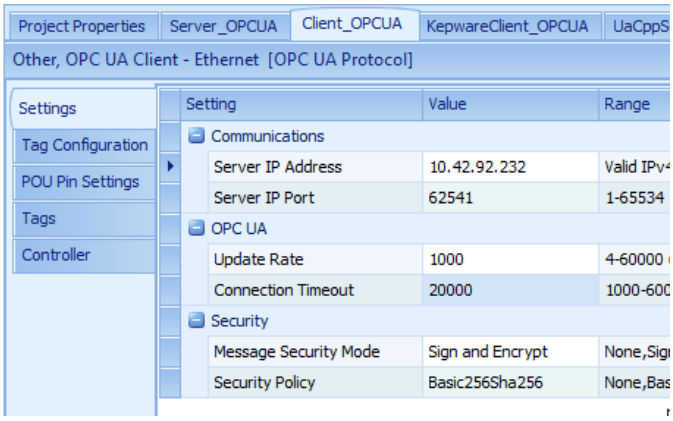

Figure 2 RTAC OPC UA Client Settings

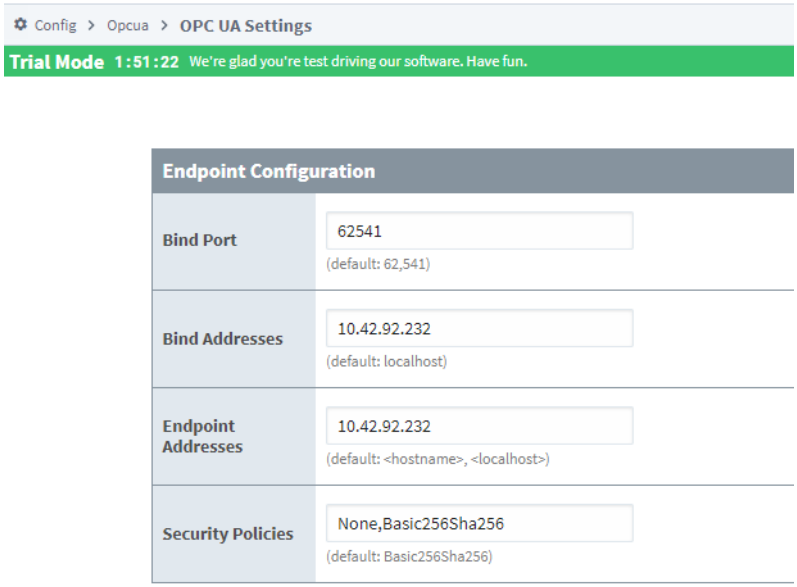

Figure 3 Third-Party OPC UA Server Security Settings

When configuring the certificates in the RTAC to allow for secure OPC UA messaging, refer to the OPC UA section in your instruction manual for instructions on how to create a valid RTAC certificate and how to trust the remote certificate(s).

IIoT Library Packages With TLS-Based Connection Support

Firmware version R151 added support for the IIoT library package that allowed the RTAC to create MQTT and HTTP client requests to server endpoints by using over-the-wire plaintext messaging. A common requirement of these types of server endpoints is a security requirement that all requests to the server be encrypted using TLS. Firmware version R153 adds support for wrapping these requests in TLS encryption by using the RTAC's active X.509 certificate to provide the public key for the conversation. This feature allows the RTAC to interact by using secure versions of the HTTPS and MTTQS protocols. See *Figure 4* and *Figure 5*, respectively, for an example of a password vault response from an

RTAC web API, first using an HTTPS request generated with a third-party tool and then the same response when the RTAC generates the HTTPS by using the WebClient IIoT library package.

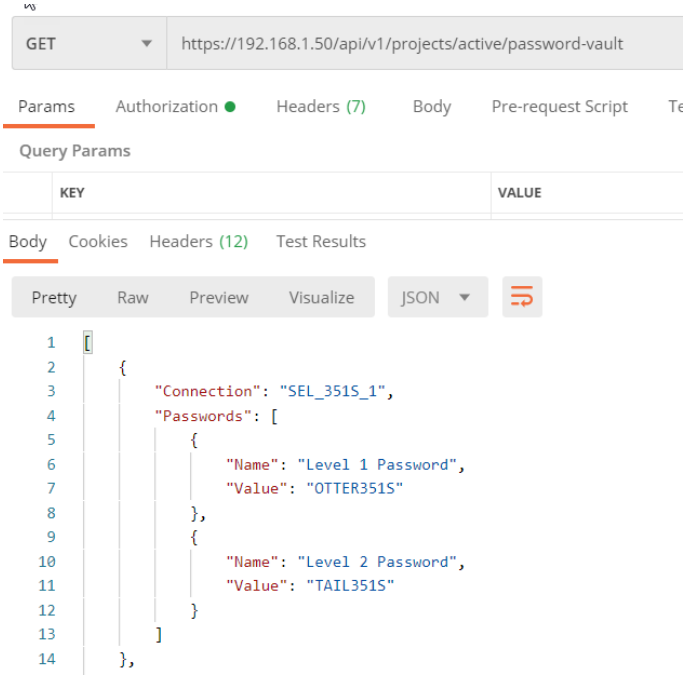

Figure 4 RTAC Password Vault API Response

Type	Value
STRING	'https://192.168.1.50/api/v1/projects/active/password-vault'
BOOL	FALSE
WEB_CLIENT.BasicAut...	
REQUEST_TYPE	GET
CONTENT_TYPE	NONE
WEB_CLIENT.HttpResult	
INT	200
WSTRING(g_udiMaxHe...	"Server: nginx$R$NDate: Fri, 26 Jul 2024 14:24:37 GMTRNContent-Type: application/json$R$NTransfer-Encoding: chunked$R$NConnec
WSTRING(g_udiMaxRe...	"[{"Connection":"SEL_351S_1","Passwords":[{"Name":"Level 1 Password","Value":"OTTER"},{"Name":"Level 2 Password","Value":"TAIL"}]}]
STRING(g_udiMaxHea...	'Server: nginx$R$NDate: Fri, 26 Jul 2024 14:24:37 GMTRNContent-Type: application/json$R$NTransfer-Encoding: chunked$R$NConnect
STRING(g_udiMaxResp...	'[{"Connection":"SEL_351S_1","Passwords":[{"Name":"Level 1 Password","Value":"OTTER"},{"Name":"Level 2 Password","Value":"TAIL"}]}]'
DINT	130

Figure 5 RTAC Password Vault API Response in RTAC User Logic by Using the WebClient IIoT Library

Network Event Capture Tool

The SEL-3350, SEL-3555, and SEL-3560 hardware with firmware version R153 or later support a licensed feature called Network Event Capture that allows for the creation of trigger-based PCAP records. When the feature is active, a running buffer of all Ethernet communications traffic is maintained. Upon activation of a user-logic-based trigger, a configurable pre- and post-trigger duration of Ethernet traffic is written to a PCAP file in the RTAC file manager. This is useful for capturing network conditions during brief, unpredictable scenarios, such as a device going temporarily offline or receiving trip signals contained in GOOSE messages.

When a Network Event Capture is configured, the pre-trigger duration is assigned a value from 1 to 60 seconds and the post-trigger duration is assigned a value from 0 to 60 seconds. PCAP files are written to a NetworkEventCaptures directory in the RTAC file manager. PCAP files are named in the time-stamped

COMNAME format, with the Station Name, Device GUID, and Company Name elements extracted from the matching RTAC System Tags values configured in the project.

Temporary Licensed Features

Newly supported temporary licensed features give the SEL application engineering team the ability to issue RTAC licenses for a 90-day demonstration period to allow customers to try out the many licensed features and protocols offered by the RTAC.

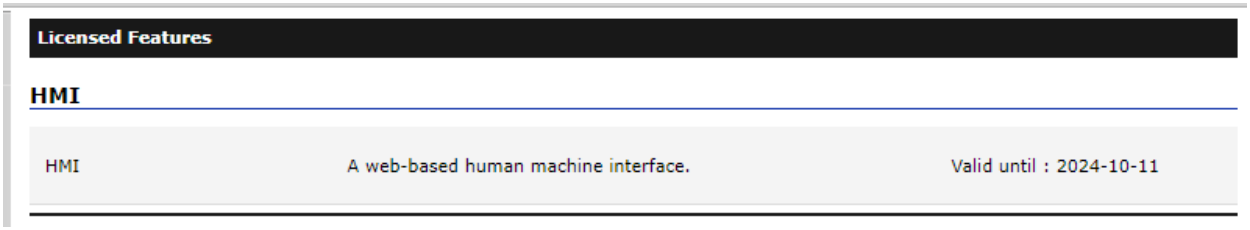

Figure 6 Temporary RTAC HMI License

Modbus Server Shared Maps

Modbus servers in firmware version R153 or later support the concept of Server Shared Maps. These are useful in applications where there is a primary and backup connection to a SCADA or HMI system. The primary and backup connections are often represented with two separate Modbus servers in an RTAC project. Modbus Server Shared Maps allow the creation of a single unified tag map that is assigned to both Modbus server devices and used to represent the identical register layout shared between those two servers.

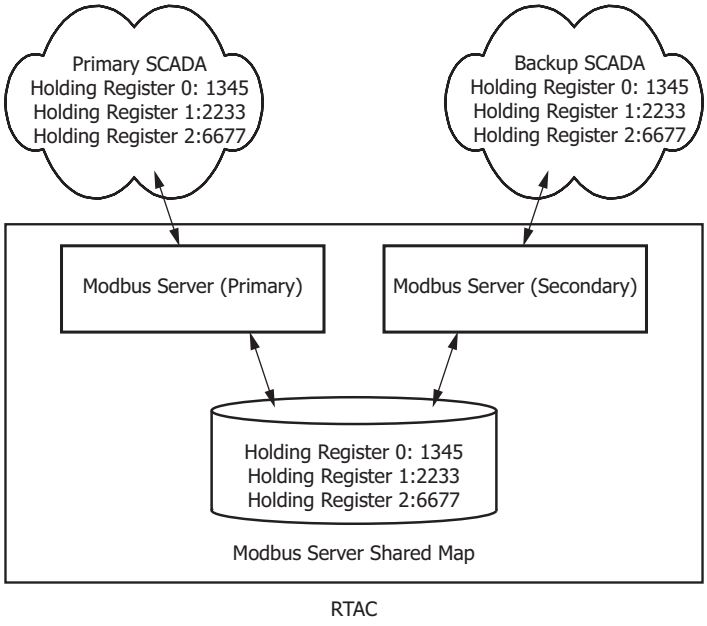

Figure 7 Modbus Server Shared Map Application

Axion Touchscreen Annunciator and Alarm Summary Support

The Axion Bay Controller's 7-inch color touchscreen display now features a built-in alarm functionality. This update supports as many as 25 alarm screens, offering flexible tile layouts and a variety of tile colors to suit your preferences. Additionally, the new alarm summary screen provides a comprehensive overview

of all active alarms, ensuring you stay informed and in control. These features combine to deliver an intuitive and visually engaging interface, making it easy to monitor and manage your substation alarms.

The alarm panels provide a visual indication of alarm conditions such as faults or other abnormal conditions. The alarm screens consist of a series of tiles arranged in a matrix form. The tile layout is flexible, with options including 2x2, 3x3, 3x4, 3x7, 4x4, 4x5, and 5x5 grid formats. Additionally, you can select ten color options for each tile.

Assign each tile to a specific alarm point defined in the RTAC. The tile background flashes and changes colors to represent the Active, Inactive, Acknowledged, and Unacknowledged state of the alarm point. As many as 25 alarm screens can be configured in the SEL touchscreen. If the touchscreen configuration in the RTAC project does not include alarm pages, then the touchscreen disables the Alarms application. *Figure 8* shows an alarm panel that uses a 3x3 tile layout.

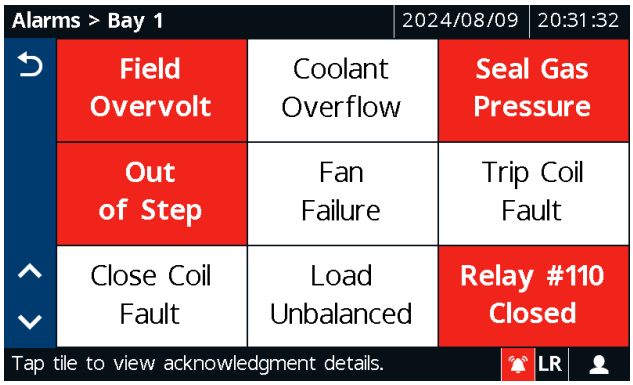

Figure 8 Touchscreen Alarm Panel

The Alarm Summary application is similar to the Sequence of Events (SOE) application, with the exception that it uses tags with alarm logging enabled via the Tag Processor or user logic. The Alarm Summary application displays the most recent 1,024 unacknowledged or active alarms and provides users the ability to view, acknowledge, or unacknowledge the alarms. *Figure 9* shows an example of the Alarm Summary screen displaying active and unacknowledged alarms. Active alarms display in red text and inactive alarms display in black text.

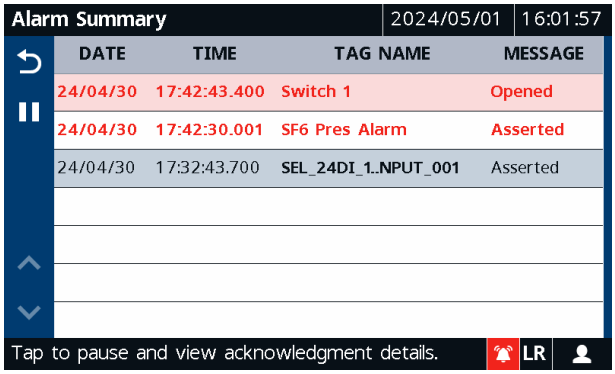

Figure 9 Touchscreen Alarm Summary

Alarm acknowledgement is intuitive and fast. You can acknowledge active alarms via the alarm panels or alarm summary screen. Tap on an alarm tile or alarm summary row to access the acknowledgement screen for the alarm. You can view the

alarm state and active timestamp, acknowledge the alarm, or exit the screen by using the close button. *Figure 10* shows an example of the alarm acknowledgement screen.

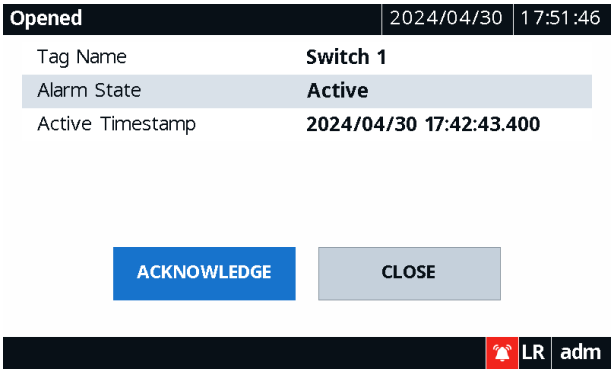

Figure 10 Touchscreen Alarm Acknowledgement

Tag Selector

During configuration of RTAC project settings, many operations require that project tag names be entered into various fields for mapping operations, such as those performed in the Tag Processor or the Simple Tag Mapper. Previously, the only way to populate these fields was by typing in the tag name(s) or copying and pasting the information from another source. The Tag Selector allows for drag-and-drop operations of one or more tags into the tag entry fields of the project. The following project items are acceptable sources for tags in the Tag Selector:

- Devices
- Shared Tag Maps (e.g., DNP server shared maps)
- Virtual Tag Lists
- System Tags
- Contact I/O

Tags can be added from the Tag Selector into the following destinations:

- Tag Processor **Destination Tag Name** and **Source Expression** fields.
- Extension fields that accept tags, such as the **Monitored Data** tab in the Dynamic Disturbance Recorder or the client-to-server mapping tabs in the **Generated_Map** subitem of the Simple Tag Mapper.

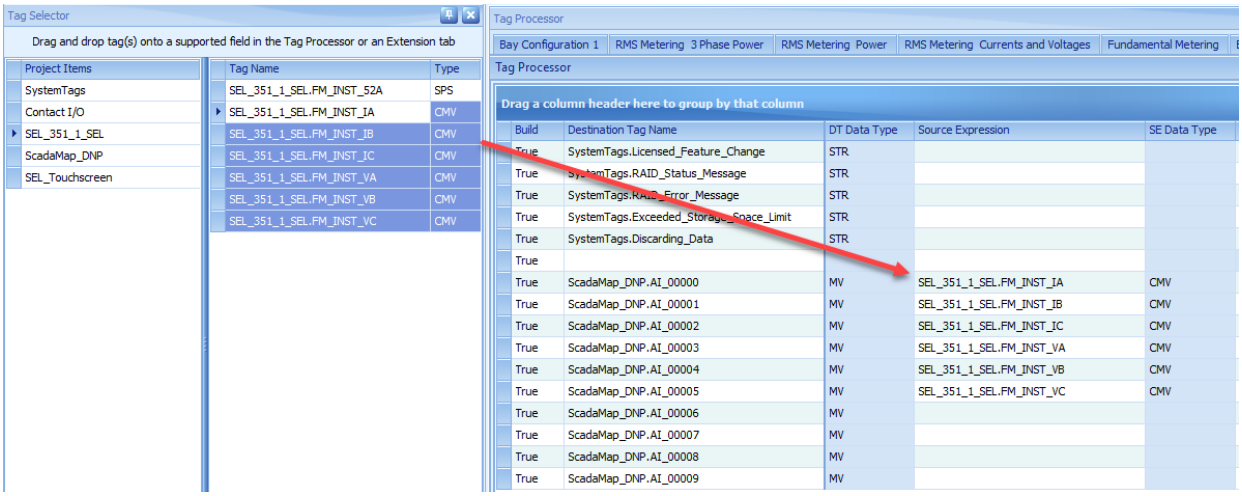

Figure 11 Tag Selector

Project Tree Device Communication Status

Status icons in the project tree now indicate a device's communication status when an RTAC with firmware version R151-V0 or later is offline, online, or disabled. When the RTAC is offline, the status icon for each device is blue, as shown in *Figure 12*.

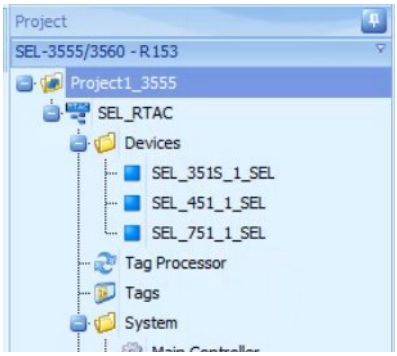

Figure 12 Project Tree Status–Offline

When the RTAC is online, the device icons change color based on the communications status of the device. Green indicates the device is online, red indicates the device is offline, and gray indicates the device is disabled, as shown in *Figure 13*.

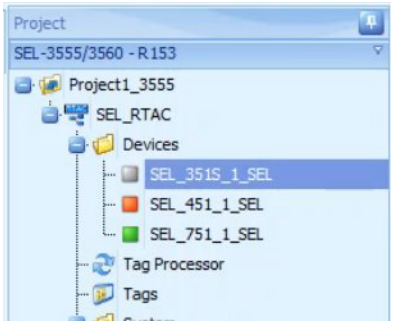

Figure 13 Project Tree Status–Online

Other Column in the Main Menu

For several years, the ability to read advanced project items from an RTAC and embed them into a project has allowed configuration performed via the web interface to be preserved with the project file itself. However, it was not immediately obvious which advanced components were embedded in a project. This enhancement adds an Other column to the main menu that displays a list of the advanced project items when hovered over, as shown in *Figure 14*.

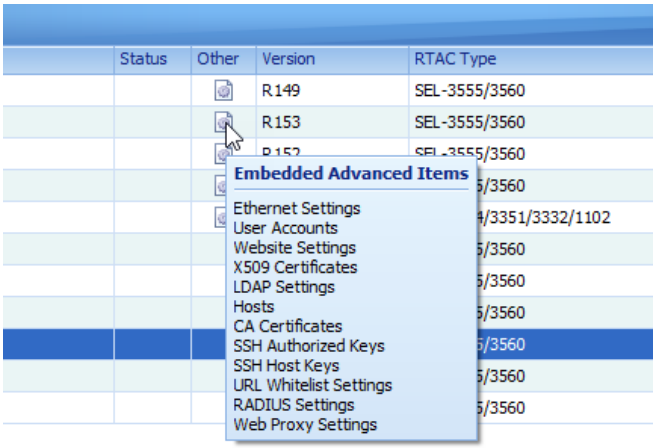

Figure 14 Embedded Advanced Items

Bulk Task Re-Ordering

Traditionally, creating or re-arranging a custom task order for the main task or automation task has involved a lot of manual effort to move items up or down in the task execution order. In firmware version R153 or later, you can drag-and-drop items to relocate them in an execution order. In *Figure 15*, for example, the HMI_MAP_DNP Order 1 item can be relocated by dragging and dropping it between the existing Order 9 and Order 10 items, as shown in *Figure 16*.

Figure 15 Sample Execution Order

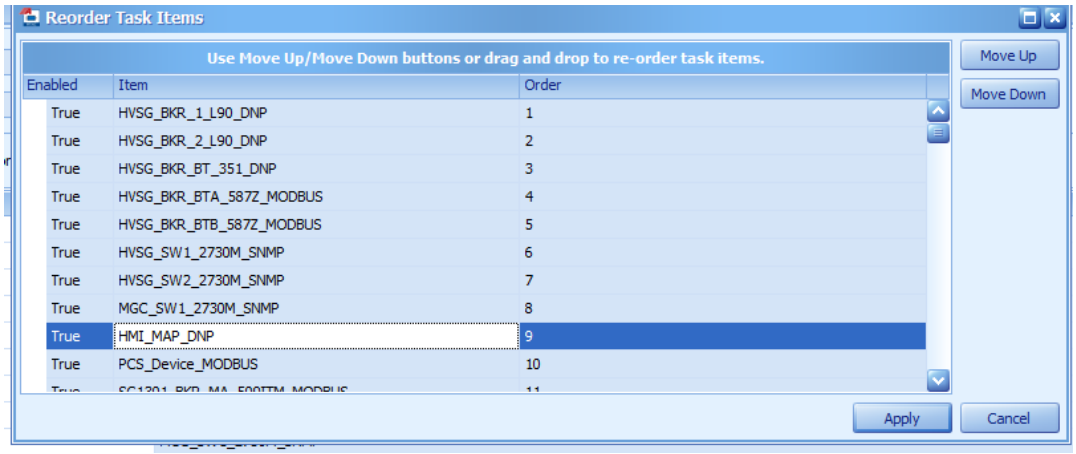

Figure 16 Relocating HMI_MAP_DNP in the Sample Execution Order

Grid Connect Extension

This extension provides a comprehensive interface to manage a complete distributed energy resource (DER) configuration by using the IEC 61131 logic engine components built into the RTAC's GridConnect library solution. The extension provides all functionality necessary to organize data mapping between individual generation and storage assets by using their Modbus communications and the respective I/O necessary to interact with the GridConnect control blocks. The extension also configures the logic necessary for coordinating these control interfaces to manage the configured site from the perspective of the point of common coupling (PCC) or the point of interconnect (POI).

DMA Link Extension

This extension automates the process of configuring an RTAC project file to integrate with the SEL Blueframe® Data Management and Automation (DMA) application suite. It is used with existing RTAC project files to quickly and reliably ensure that SEL Client and SEL Server devices in the project file are configured for DMA Disturbance Monitoring, DMA Credential Management, and DMA Configuration Monitoring. The extension automatically configures and manages the following project aspects:

- SEL Protocol Clients: Password monitoring, event collection (CEV or COMTRADE), device GUID, ASCII SER collection, configuration monitoring
- SEL Protocol Servers: the SEL server provides unsolicited notifications for new events, configuration monitoring changes, and new ASCII SER entries

87L Comm Monitor Extension

This extension automates the process of configuring an RTAC to collect, monitor, and report on the communication health indicators of differential protection schemes. With initial support for the SEL-411L Advanced Line Differential Protection, Automation, and Control System, this application assesses relevant unsolicited SER points as well as data points from the COM 87L report and provides alarm indicators and status updates to the logic engine, RTAC SOE, and RTAC file system.

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
selinc.com • info@selinc.com