SCHWEITZER ENGINEERING LABORATORIES, INC.
WHITE PAPER

Leveraging Security – Using the SEL RTAC's Built-In Security Features

Darrin Kite

INTRODUCTION

Cyberthreats to critical infrastructure represent a growing and persistent risk to a nation's security and prosperity. The SEL Real-Time Automation Controller (RTAC) product platform serves as the information hub for substations in electric utilities as well as many other critical industries. It provides essential services, such as data aggregation, logic processing, oscillography, event report collection, and secure engineering access. Securing RTACs and the associated communications is critical to the confidentiality, integrity, and availability of data that are essential for maintaining and operating critical infrastructure.

There are many technologies and best practices underlying the architecture of the SEL RTAC that contribute to security. When considering antivirus technology, secure communications, or security patch management, it is essential to understand the concepts that are incorporated into these devices to mitigate today's cyberthreats. This white paper discusses these concepts and provides configuration examples to empower engineers, technicians, and security personnel to protect critical cyberassets.

Figure 1 serves as a topological guide for the security topics covered in this white paper (indicated by the section numbers). Each topic covered in this document is independent, so you can focus on topics pertinent to your organization's infrastructure.

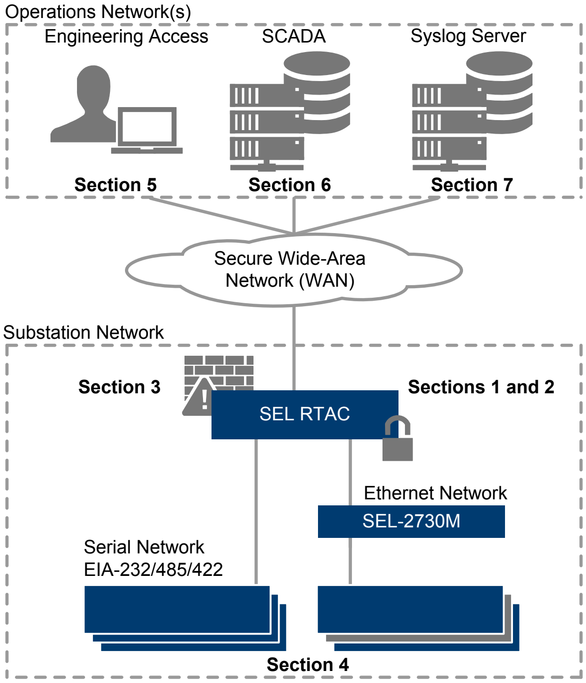


Figure 1 RTAC Security Diagram and Topic Sections

SECTION 1: VERIFYING APPLICATION INTEGRITY – WHITELISTING TECHNOLOGY

The sheer volume of new malware and zero-day exploits makes it difficult to deploy blacklisting technology for critical infrastructure due to the lack of available bandwidth and connectivity to sites. Instead of providing constant updates for malware signatures (for blacklisting technology), whitelisting technology provides a different approach that only allows known, trusted applications to execute on computing systems. This is the approach taken in the SEL RTAC product platform.

SEL designed and built the exe-GUARD® utility as a cooperative project with the U.S. Department of Energy (DOE), Dominion Virginia Power, and Sandia National Laboratories. Exe-GUARD provides protection against rootkits, implements kernel-level whitelisting, and incorporates secured memory privileges with enforced mandatory access controls. It also provides powerful resistance to code injection by whitelisting only known authorized executables.

Exe-GUARD features are enabled by default in SEL RTAC firmware Version R134 and above. These features are not controllable by the user, meaning they cannot be disabled by user configuration. Four tags (detailed in Table 1) that relate to the exe-GUARD utility are available through the SEL RTAC logic engine.

Table 1 Tags Available for Security Logging Through the Tag Processor

Tag Name	Description
SystemTags.ExeGuard_Enabled	Status of the exe-GUARD utility.
SystemTags.Whitelist_Alert	An executable file not authorized by SEL attempted to execute.
SystemTags.ExeGuard_Security_Alert	A system executable attempted an unauthorized action.
SystemTags.Whitelist_Alert_Action	Action taken when a security incident is detected. Configurable in SystemTags > Settings.

These tags are configured in the ACSELERATOR RTAC® SEL-5033 Software Tag Processor by default. This means that any change in the tags will create a log entry in the RTAC's Sequence of Events (SOE) log. The SOE log is downloadable through the SEL RTAC web interface. Alternatively, SOE logs can be collected using ACSELERATOR TEAM® SEL-5045 Software, accessed via ODBC-compliant connections, sent via syslog (see Security Auditing – Event Monitoring and Reporting [Section 7]), or tied to a supervisory control and data acquisition (SCADA) protocol, such as DNP3. An example of the last configuration is shown in the following code.

```
IF SystemTags.Whitelist_Alert.strVal <> ‘’ THEN
      DNPServerSharedMap1_DNP.BI_00000.stVal := TRUE;
      DNPServerSharedMap1_DNP.BI_00000.q.validity := BOOL_TO_DINT(NOT
              SystemTags.ExeGuard_Enabled.stVal);
      DNPServerSharedMap1_DNP.BI_00000.t := SystemTags.Whitelist_Alert.t;

ELSE
      DNPServerSharedMap1_DNP.BI_00000.stVal := FALSE;
      DNPServerSharedMap1_DNP.BI_00000.q.validity := BOOL_TO_DINT(NOT
              SystemTags.ExeGuard_Enabled.stVal);
      DNPServerSharedMap1_DNP.BI_00000.t := SystemTags.Whitelist_Alert.t;
END_IF

IF SystemTags.ExeGuard_Security_Alert.strVal <> ‘’ THEN
      DNPServerSharedMap1_DNP.BI_00001.stVal := TRUE;
      DNPServerSharedMap1_DNP.BI_00001.q.validity := BOOL_TO_DINT(NOT
              SystemTags.ExeGuard_Enabled.stVal);
      DNPServerSharedMap1_DNP.BI_00001.t := SystemTags.Whitelist_Alert.t;
ELSE
```

```
        DNPServerSharedMap1_DNP.BI_00001.stVal := FALSE;
        DNPServerSharedMap1_DNP.BI_00001.q.validity := BOOL_TO_DINT(NOT
                SystemTags.ExeGuard_Enabled.stVal);
        DNPServerSharedMap1_DNP.BI_00001.t := SystemTags.Whitelist_Alert.t;
END_IF
```

This example logic maps the SystemTags.Whitelist_Alert tag and SystemTags.ExeGuard_Security_Alert tag to DNP3 binary inputs. This example assumes that a DNP3 server and a DNP3 server shared map are configured in the project. For instructions on inserting a DNP3 server, shared map, or program, refer to the ACSELERATOR RTAC Instruction Manual [1]. Note that the quality (.q.validity) for the exe-GUARD tags has an initial value of invalid. The reason for this is that the tags are not updated until a change occurs, i.e., a security event occurs. In DNP3, depending on group and variation type, that quality information is transmitted to SCADA. In the preceding code example, the tag quality is tied to the SystemTags.ExeGuard_Enabled tag. By tying this tag to the enabled status for the exe-GUARD application, the operator can determine if the information stored in the DNP3 binary inputs is valid.

SECTION 2: SECURING UPDATES – MANAGING SECURITY PATCHES

On the discovery of a security vulnerability that affects the SEL RTAC product platform, SEL updates firmware in a timely manner to resolve the issue. The affected SEL RTACs can then be upgraded locally or remotely. All firmware is digitally signed by SEL and the signature is included as part of the firmware upgrade. As such, if firmware authenticity cannot be verified using the provided signature, it is rejected. For firmware upgrade instructions, refer to the appropriate hardware instruction manual for your SEL RTAC.

Visit the Industrial Control System Cyber Emergency Response Team (ICS-CERT) and/or National Vulnerability Database websites to stay informed about vulnerabilities relevant to industrial control systems [2] [3]. In addition, sign up for SEL Vulnerability Notifications [4], which provides up-to-date security notifications for potential issues affecting SEL products.

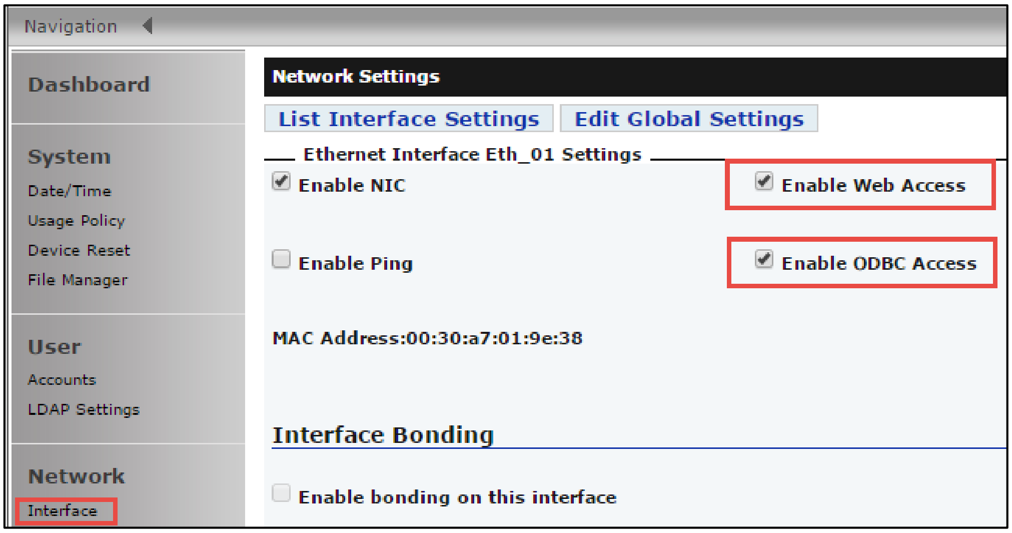
SECTION 3: AUTHORIZING COMMUNICATION – SELF-CONFIGURING STATEFUL FIREWALL

The SEL RTAC has a self-configuring stateful firewall. A stateful firewall tracks the state of network connections when filtering IP packets. It also provides context-aware traffic inspection. If the communication is initiated by the SEL RTAC, then all traffic associated with that socket connection is permitted. However, incoming traffic is only permitted if it meets the criteria defined within the ACSELERATOR RTAC project. The firewall is not directly configurable by the user; instead, the SEL RTAC platform configures the firewall based on the communications settings in the ACSELERATOR RTAC project and those configured through the web interface. Table 2 shows the four service ports for all Ethernet interfaces, including the USB-B interface. The Network Time Protocol (NTP) port is open by default and is configured in the ACSELERATOR RTAC project.

Table 2 Default Open Ports for Ethernet and the USB-B Interfaces

Port Number	Description
5432	ACSELERATOR RTAC project download and retrieval
443	HTTPS (Transport Layer Security-encrypted [TLS-encrypted] RTAC web server session)
80	HTTP (connections migrated to Port 443)
123	NTP time synchronization (assuming a default ACSELERATOR RTAC project is loaded on the SEL RTAC)

The default ports can be disabled through the web interface for all Ethernet interfaces, except the local USB-B interface on the SEL-3530, SEL-3530-4, SEL-3505, and SEL-3505-3 RTAC hardware options. Deselecting the **Enable Web Access** check box in the web interface removes the firewall exemption for Ports 80 and 443, and deselecting the **Enable OBDC Access** check box removes the firewall exemptions for Port 5432 on the selected Ethernet interface (as shown in Figure 2). To remove the exemption for Port 123, users can disable NTP in the ACSELERATOR RTAC project under **System_Time_Control > POU Pin Settings** (as shown in Figure 3).



Ethernet Interface Eth_01 Settings

☑ Enable NIC

☑ Enable Web Access

□ Enable Ping

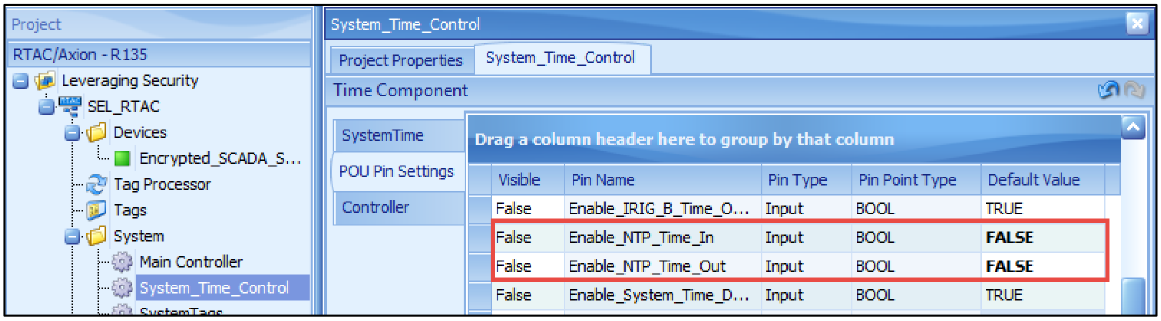
☑ Enable ODBC Access

MAC Address:00:30:a7:01:9e:38

Interface Bonding

□ Enable bonding on this interface

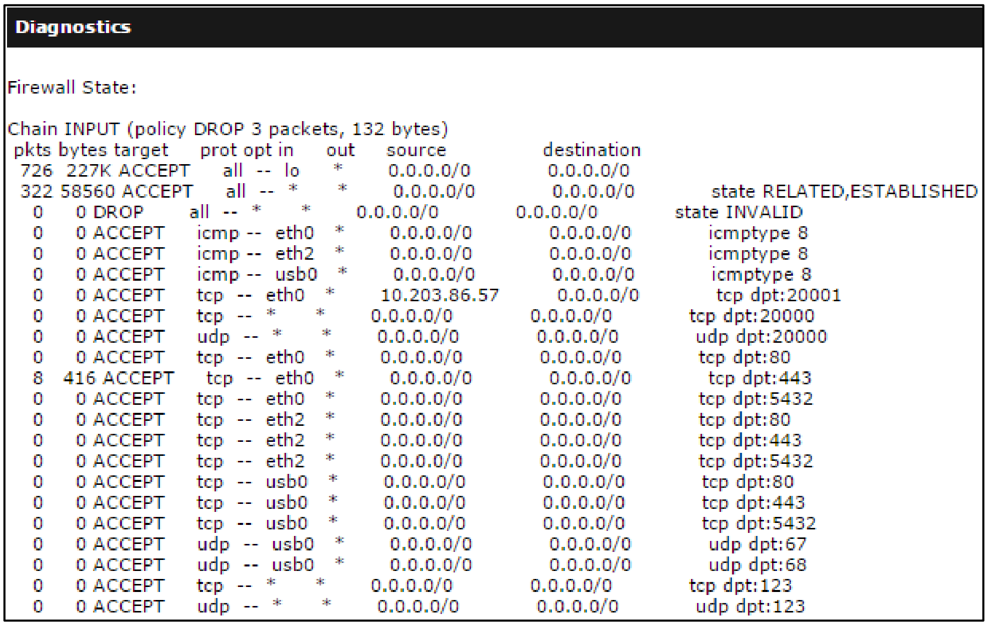
Figure 2 The Network > Interface Menu in the SEL RTAC Web Interface – Uncheck Services to Disable Default Port Access in the Firewall



Visible	Pin Name	Pin Type	Pin Point Type	Default Value
False	Enable_IRIG_B_Time_O...	Input	BOOL	TRUE
False	Enable_NTP_Time_In	Input	BOOL	**FALSE**
False	Enable_NTP_Time_Out	Input	BOOL	**FALSE**
False	Enable_System_Time_D...	Input	BOOL	TRUE

Figure 3 Disable the NTP Services in an ACSELERATOR RTAC Project

To view the present firewall state, navigate to **Reports > Diagnostics** in the RTAC web interface (Figure 4 shows the report). A table entry is created when an outgoing connection is initiated by the device. When traffic returns, the RTAC compares the packet's information to the table information to determine whether it is part of a presently logged communications session. If the packet is related to a present table entry, it is allowed to pass. A table entry is also created when a port is opened by configuring a communications server (i.e., a DNP3 server instance) or when a generic listening port is configured (i.e., an access point [AP]). The latter is used in conjunction with AP routers (APRs), which allow a user to route traffic from a source to a predetermined serial port or Ethernet destination (for more information, see the ACSELERATOR RTAC Instruction Manual).



```
Firewall State:

Chain INPUT (policy DROP 3 packets, 132 bytes)
 pkts bytes target     prot opt in     out     source               destination
  726  227K ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
  322 58560 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 ACCEPT     icmp --  eth2   *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 ACCEPT     icmp --  usb0   *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 ACCEPT     tcp  --  eth0   *       10.203.86.57         0.0.0.0/0           tcp dpt:20001
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:20000
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:20000
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    8   416 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5432
    0     0 ACCEPT     tcp  --  eth2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  eth2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  eth2   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5432
    0     0 ACCEPT     tcp  --  usb0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  usb0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  usb0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5432
    0     0 ACCEPT     udp  --  usb0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:67
    0     0 ACCEPT     udp  --  usb0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:68
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:123
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:123
```

Figure 4 Diagnostic Report Showing the Present Firewall State

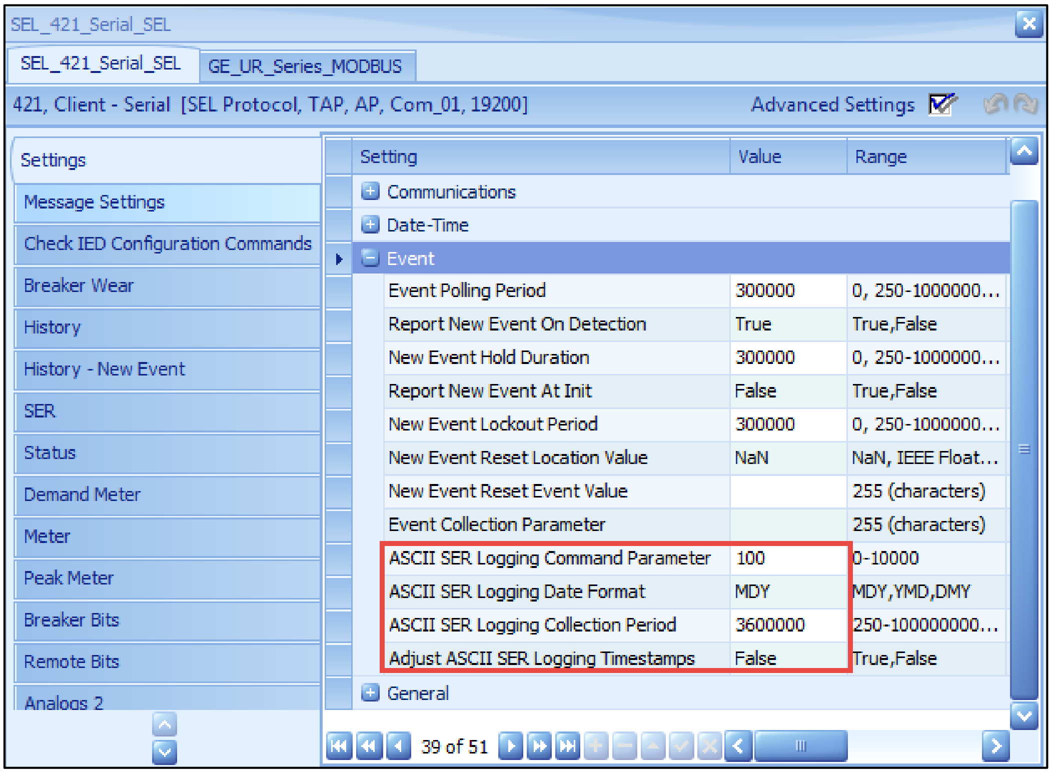
Note that in Figure 4 the Ethernet interfaces in the firewall report are zero-indexed, which means **eth0** corresponds to **Eth_01** in the **Network > Interface** menu. This firewall example is associated with a very simple ACSELERATOR RTAC project, which has one DNP3 client and one DNP3 server. The DNP3 client uses Port 20001 to connect to an intelligent electronic device (IED). The DNP3 server is listening on Transmission Control Protocol (TCP) Port 20000 and User Datagram Protocol (UDP) Port 20000. The default services are disabled on **Eth_02** (**eth1**), which means the default ports and associated services are not shown in Figure 4.

SECTION 4: MONITORING IEDS – ASCII SEQUENTIAL EVENTS RECORD (SER) LOGGING

The IEDs in a substation or industrial plant process and analyze essential information to protect and control power systems and industrial processes. These devices are usually purpose-built and have limited storage capability to support the detailed logging required for event and security analysis. RTAC contact I/O is useful for creating SOE records in the RTAC of IED alarm points, when those devices lack native SER storage. Monitoring, logging, and concentrating IED SER data in a centralized location provides a valuable check against unauthorized changes and produces an audit trail essential for regulatory compliance.

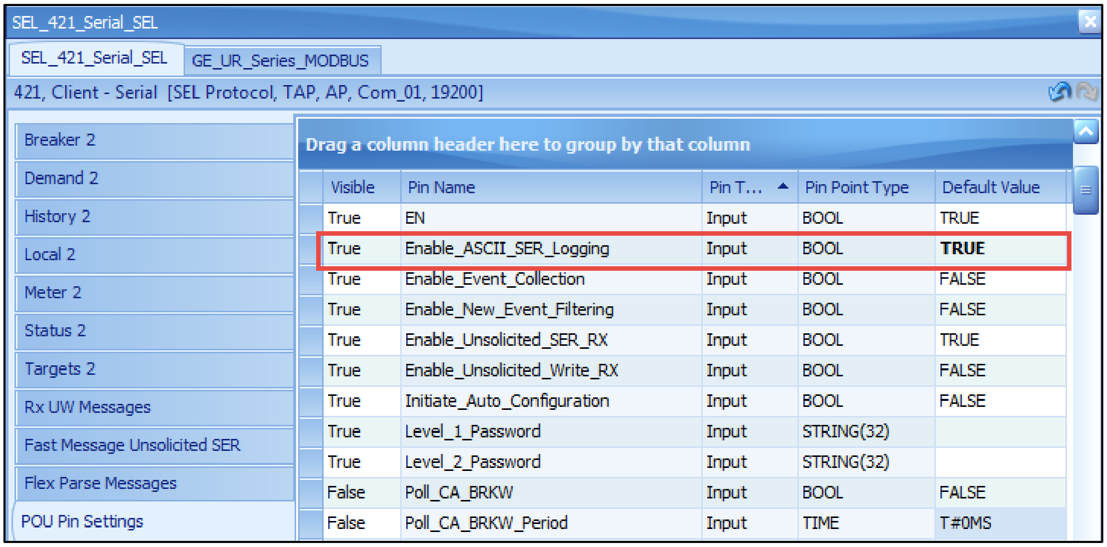
The SEL RTAC supports automatic ASCII SER collection from SEL IEDs and General Electric (GE) UR series IEDs. Refer to the IED's instruction manual for instructions on adding the relay data to the SER log. In SEL IEDs, Relay Word bits can be added to the SER equation through the command line interface or via ACSELERATOR QuickSet® SEL-5030 Software. The information available for logging is dependent on both the IED type and firmware version.

The parameters for the ASCII SER collection are in the settings tab in both an SEL and Modbus® clients (shown in Figure 5 for an SEL client). For GE UR series devices, the Modbus client is used. A different mechanism is used to collect ASCII SER data from SEL IEDs as opposed to GE UR series relays. However, the settings are similar and the results are identical. In SEL IEDs, the **SER** command is used to collect events. This command has an option to only view a certain number of events at a given time. By default, the **ASCII SER Logging Command Parameter** is set to **100**. This means that when the polling period (**ASCII SER Logging Collection Period**) expires, the SEL RTAC issues the **SER 100** command and parses all the new events. Also, the format that an IED records SER date and time information in needs to be specified in the **ASCII SER Logging Date Format** to log the correct time. If needed, the SER time stamp can be normalized to the SEL RTAC's time base by selecting **Adjust ASCII SER Logging Timestamps**. If this is set to **True**, then the settings configured in the **Date-Time** settings are used to determine the necessary adjustment. To enable the SER collection service, the **Enable_ASCII_SER_Logging** is set to **TRUE** in the **POU Pin Settings** (as shown in Figure 6). ASCII SER collection for GE devices is similar, with the notable absence of the **ASCII SER Logging Date Format** and **ASCII SER Logging Command Parameter**. Each individual ASCII SER entry is logged with a time stamp or an adjusted time stamp, based on settings, into the SEL RTAC SOE log.



Setting	Value	Range
Communications		
Date-Time		
Event		
Event Polling Period	300000	0, 250-1000000...
Report New Event On Detection	True	True,False
New Event Hold Duration	300000	0, 250-1000000...
Report New Event At Init	False	True,False
New Event Lockout Period	300000	0, 250-1000000...
New Event Reset Location Value	NaN	NaN, IEEE Float...
New Event Reset Event Value		255 (characters)
Event Collection Parameter		255 (characters)
ASCII SER Logging Command Parameter	100	0-10000
ASCII SER Logging Date Format	MDY	MDY,YMD,DMY
ASCII SER Logging Collection Period	3600000	250-100000000...
Adjust ASCII SER Logging Timestamps	False	True,False
General		

Figure 5 The ASCII SER Logging Parameters in an SEL Client



SEL_421_Serial_SEL

SEL_421_Serial_SEL | GE_UR_Series_MODBUS

421, Client - Serial [SEL Protocol, TAP, AP, Com_01, 19200]

Visible	Pin Name	Pin T...	Pin Point Type	Default Value
True	EN	Input	BOOL	TRUE
True	Enable_ASCII_SER_Logging	Input	BOOL	**TRUE**
True	Enable_Event_Collection	Input	BOOL	FALSE
True	Enable_New_Event_Filtering	Input	BOOL	FALSE
True	Enable_Unsolicited_SER_RX	Input	BOOL	TRUE
True	Enable_Unsolicited_Write_RX	Input	BOOL	FALSE
True	Initiate_Auto_Configuration	Input	BOOL	FALSE
True	Level_1_Password	Input	STRING(32)	
True	Level_2_Password	Input	STRING(32)	
False	Poll_CA_BRKW	Input	BOOL	FALSE
False	Poll_CA_BRKW_Period	Input	TIME	T#0MS

Figure 6 Enabling the ASCII SER Logging Service in the SEL Client POU Pins

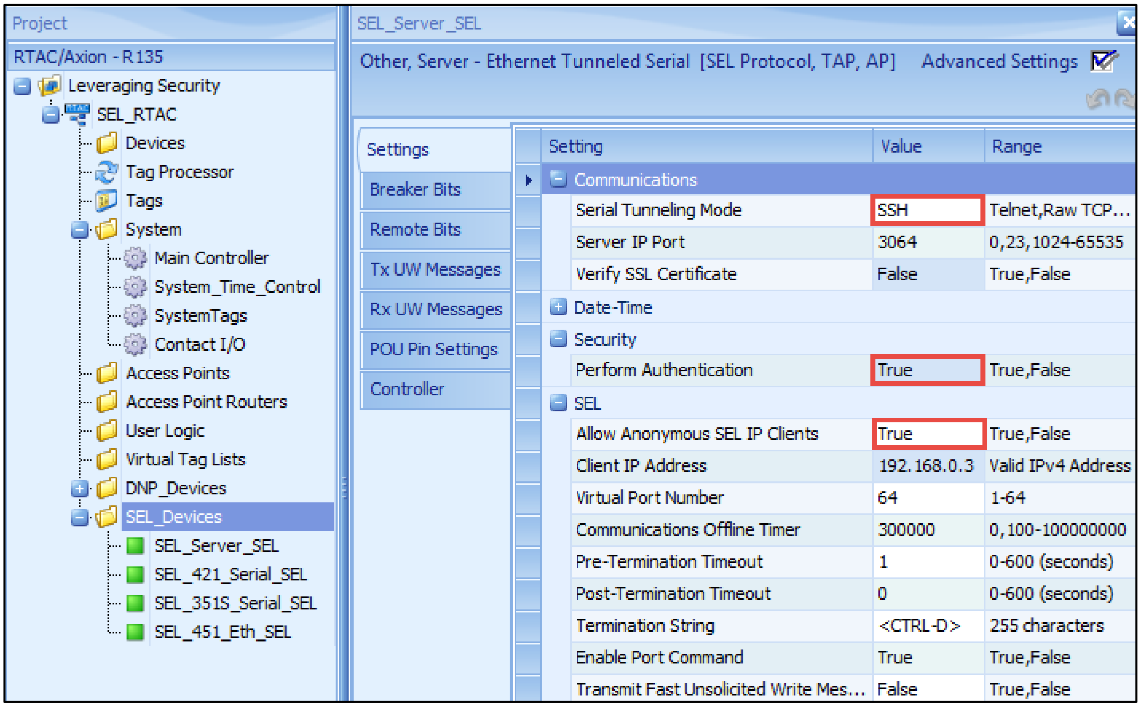
Section 5: Securing Engineering Access – Restricting IED Access

Establishing a secure engineering Access Point (AP) is essential to maintaining the integrity of less security-aware IEDs. In the topology shown in Figure 1, the SEL RTAC is the AP to a secured wide-area network (WAN). It provides data concentration for all the connected IEDs and also allows engineering access to devices that support that feature. Secure engineering access into the SEL RTAC requires encrypting the user session so that valuable information is not readable via plain text.

There are two general methods for engineering access: 1) through the SEL server or 2) using APs and AP routers (APRs). Either method accomplishes the goal. The advantage of using the SEL server is that it does not require manually configuring individual APRs for each IED. The disadvantage is that this method is only applicable to IEDs communicating with SEL protocol.

This section describes configuring the SEL server for secure access. This discussion is equally applicable to the second method described above (for more information about APs and APRs see [1]). Secure Shell (SSH) is a widely used cryptographic network protocol that provides terminal access to remote devices. The SSH tunnel method is used in this example because it is widely used and is supported by many free terminal applications. A TLS tunnel is another option for securing engineering access and is described in Section 6 (Securing SCADA – Encrypting Server Communications); however, the SSH tunnel method is equally applicable to that section as well.

As mentioned previously, the SEL server requires very little configuration for securing engineering access. Figure 7 shows a project configuration with three IEDs communicating to an RTAC via SEL protocol. The SEL server is configured for SSH and allows any IP address to connect. Alternatively, the user can disable **Allow Anonymous SEL IP Clients** and then specify a **Client IP Address** that is allowed to connect. This is useful if personnel accessing the IEDs have a known, fixed IP address. In firmware Version R136 and above, this is a separate settings field that supports a comma-separated list for multiple IP addresses. File transfer is also supported through the SEL server in firmware Version R136 and above. In firmware prior to Version R136, a separate AP and APR configured for direct connection are required for settings transfer.



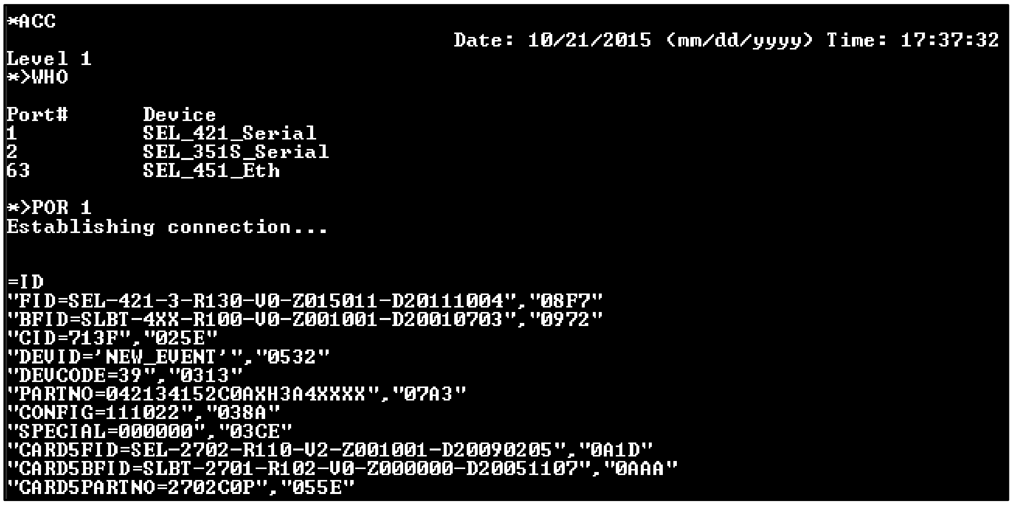
Other, Server - Ethernet Tunneled Serial [SEL Protocol, TAP, AP]

Setting	Value	Range
Communications		
Serial Tunneling Mode	SSH	Telnet,Raw TCP…
Server IP Port	3064	0,23,1024-65535
Verify SSL Certificate	False	True,False
Date-Time		
Security		
Perform Authentication	True	True,False
SEL		
Allow Anonymous SEL IP Clients	True	True,False
Client IP Address	192.168.0.3	Valid IPv4 Address
Virtual Port Number	64	1-64
Communications Offline Timer	300000	0,100-100000000
Pre-Termination Timeout	1	0-600 (seconds)
Post-Termination Timeout	0	0-600 (seconds)
Termination String	<CTRL-D>	255 characters
Enable Port Command	True	True,False
Transmit Fast Unsolicited Write Mes…	False	True,False

Figure 7 An ACSELERATOR RTAC Project Configured for Secure Engineering Access to Three IEDs Communicating Via SEL Protocol

The SEL server also supports the capability to enforce authentication before granting access to the command line interface. Note that when SSH is the serial tunnel mode, then **Perform Authentication** is automatically configured to **True**. When this setting is enabled, a username is required with a password challenge. Local accounts and centrally managed accounts (i.e., those configured through Lightweight Directory Access Protocol [LDAP]) can be used to authenticate to the SEL server.

Figure 8 shows how to use the SEL server for accessing connected IEDs. If authentication is successful, then an asterisk is returned to the terminal. Users can issue the **WHO** command to see the IEDs available for engineering access. They can issue the **POR** command in conjunction with the port number to access an IED. The port number corresponds to the serial port number for serially connected IEDs and the virtual port number in IEDs connected through Ethernet.


```
*ACC
                                    Date: 10/21/2015 (mm/dd/yyyy) Time: 17:37:32
Level 1
*>WHO

Port#      Device
1          SEL_421_Serial
2          SEL_351S_Serial
63         SEL_451_Eth

*>POR 1
Establishing connection...


=ID
"FID=SEL-421-3-R130-V0-Z015011-D20111004","08F7"
"BFID=SLBT-4XX-R100-V0-Z001001-D20010703","0972"
"CID=713F","025E"
"DEVID='NEW_EVENT'","0532"
"DEVCODE=39","0313"
"PARTNO=042134152C0AXH3A4XXXX","07A3"
"CONFIG=111022","038A"
"SPECIAL=000000","03CE"
"CARD5FID=SEL-2702-R110-V2-Z001001-D20090205","0A1D"
"CARD5BFID=SLBT-2701-R102-V0-Z000000-D20051107","0AAA"
"CARD5PARTNO=2702C0P","055E"
```

Figure 8 Captured Terminal Session of Engineering Access of the SEL Server Over an SSH Connection

Another means to provide authentication is by adding SSH authorized keys. Through the web interface at **Security > SSH Keys**, a user can add preauthorized public keys for authentication. These public keys can be generated using either RSA or DSA cryptographic algorithms. DSA in this context is as described in the Digital Signature Standard (DSS) [5]. In this method, an SSH client presents its public key during the connection initiation and the user enters a valid username that is authorized to connect to the SEL RTAC. Some SSH clients also require a passphrase associated with the key to complete the authentication. In this manner, only devices that present a preauthorized key are able to connect, and this removes the need for a user to remember a password.

In SEL RTAC firmware Version R136 and above, multifactor authentication is available in the SEL server. A POU pin available in the SEL servers and clients allows users to disable remote access. This pin can be tied to an incoming SCADA point that can enable access when personnel require engineering access. Coupled with a timer, available as a function block in the logic engine, a user can specify a time frame in which engineering access is permitted. As mentioned, this is available in both SEL servers and clients, so the method can be used to restrict all engineering access by disabling the SEL server or for an individual IED by disabling the pin associated with that device.

SECTION 6: SECURING SCADA – ENCRYPTING SERVER COMMUNICATIONS

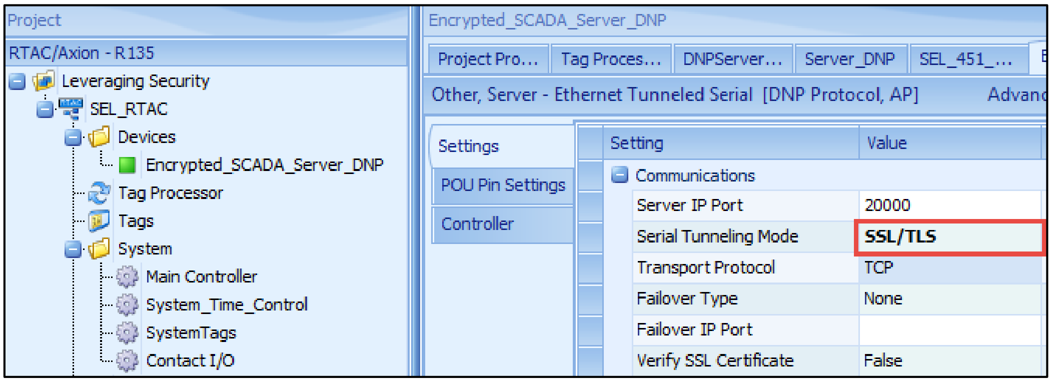
Operators maintain situational awareness with SCADA. Information about the electric power system is often transmitted in plain text and can be intercepted by any individual at a vulnerable spot in the network. Encrypting this communication provides another layer to protect the confidentiality and integrity of information critical to operating the bulk electric system.

The SEL RTAC supports Public Key Infrastructure (PKI). PKI is a formal, hierarchical system where a digital certificate is signed by a more trusted certificate. At the top of the PKI hierarchy is the most trusted certificate, the root certificate. This sequence of certificates forms the “chain of trust.” The root certificate is self-signed, highly protected, and should only be used to sign certificate authority (CA) certificates. A CA is an entity that issues, or signs, other certificates. To obtain a certificate, an entity generates a certificate signing request (CSR) that is based on a private-public key pair along with some additional information. The requester then sends the public key and credentials to a CA. The CA verifies the authenticity of the credentials and issues an X.509 certificate containing those credentials, the public key, and the CA digital signature. This is then used by the client to authenticate that the server is a known, trusted entity. Then, an encrypted communications session is negotiated by the two end points. This is the widely accepted method used in HTTPS to provide secure information exchange in the World Wide Web.

The SEL RTAC web server is only accessible through HTTPS (HTTP tunneled through a TLS connection). TLS and its predecessor, Secure Socket Layer (SSL), leverage PKI to authenticate and encrypt communications sessions. The SEL RTAC only supports TLS 1.0 and above due to security vulnerabilities discovered in SSL 3.0 and earlier. By default, all SEL RTACs have a self-signed X.509 certificate enabled. This allows any web browser to connect to the web interface securely. Web browsers, like Chrome™, Mozilla® Firefox®, and Internet Explorer® do not recognize the SEL RTAC as a trusted CA, which is why the browser displays a warning when connecting to the SEL RTAC web interface.

The PKI infrastructure also allows users to encrypt SCADA communication. Any serial protocol, with the exception of MIRRORED BITS® communications, can be tunneled through a TLS connection (serial protocols can also be tunneled through SSH; see information on SSH authorized keys in the Section 5). Using this method, a utility or process owner has a CA authority that is trusted or managed by his or her organization. In the SEL RTAC, an X.509 certificate is generated with appropriate credentials and key size, and then a CSR is generated. This CSR is then sent to the CA for verification and signing. Once the certificate has been signed, the user can import the signed X.509 certificate into the RTAC and activate it. For detailed instructions for this procedure, refer to the ACSELERATOR RTAC Instruction Manual.

After the X.509 certificate is activated, it is a simple step to encrypt the server communications. For one-way authentication where only the client (i.e., SCADA) is authenticating the certificates, all that is required is to select **SSL/TLS** as the **Serial Tunneling Mode** in ACSELERATOR RTAC (as shown in Figure 9). This allows the client to verify that the server is a trusted source of information and encrypt the communications.

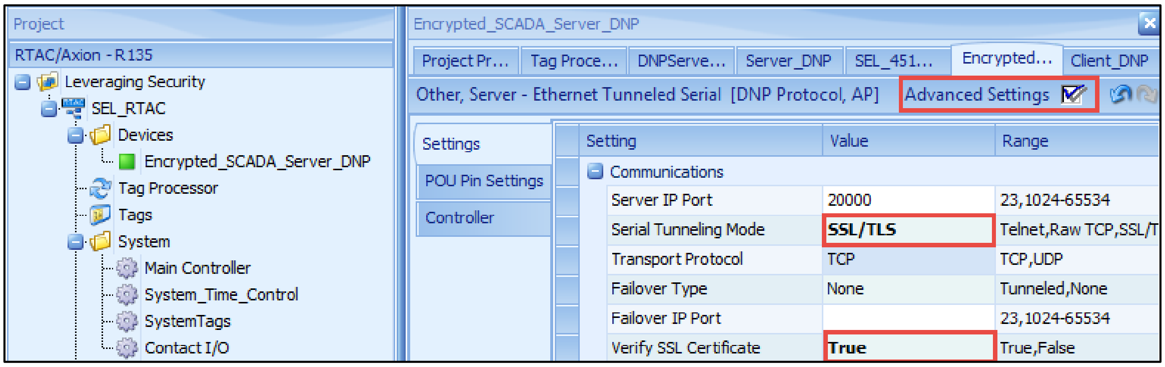


Other, Server - Ethernet Tunneled Serial [DNP Protocol, AP]

Setting	Value
Communications	
Server IP Port	20000
Serial Tunneling Mode	SSL/TLS
Transport Protocol	TCP
Failover Type	None
Failover IP Port	
Verify SSL Certificate	False

Figure 9 Configuring a DNP3 Server to Support TLS One-Way Authentication in ACSELERATOR RTAC

Alternatively, a user can enable two-way authentication. In this mode, the server also authenticates the client's (SCADA) certificate to ensure that the incoming connection originates from a trusted source. This requires the SEL RTAC to know the chain of trust for the client's certificate. This means that all the CA certificates used in the signing process for the client (SCADA) certificate must be installed in the **Security > CA Certificates** section of the SEL RTAC web interface. For example, an asset owner has a root certificate that is used to sign a CA certificate, which then, in turn, is used to sign a certificate used by the SCADA client. Both the root certificate and the CA certificate need to be installed on the SEL RTAC for the verification process to succeed. In addition, the **Verify SSL Certificate** setting in the server must be set to **True** (as shown in Figure 10). To display the **Verify SSL Certificate** setting, select the **Advanced Settings** option in the top-right corner in ACSELERATOR RTAC.



Other, Server - Ethernet Tunneled Serial [DNP Protocol, AP] Advanced Settings ☑

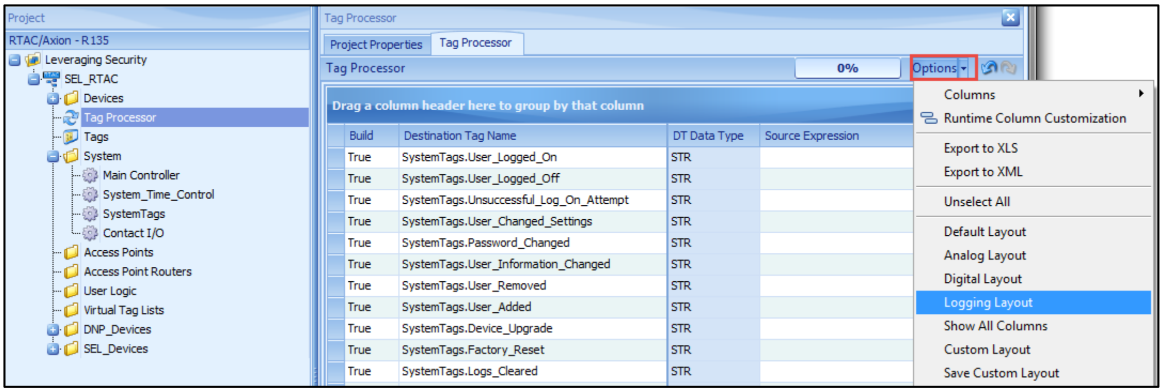
Setting	Value	Range
Communications		
Server IP Port	20000	23,1024-65534
Serial Tunneling Mode	SSL/TLS	Telnet,Raw TCP,SSL/T
Transport Protocol	TCP	TCP,UDP
Failover Type	None	Tunneled,None
Failover IP Port		23,1024-65534
Verify SSL Certificate	True	True,False

Figure 10 Configuring a DNP3 Server to Support TLS Two-Way Authentication in ACSELERATOR RTAC

SECTION 7: SECURITY AUDITING – EVENT MONITORING AND REPORTING

Tracking and archiving events is an important function provided by a data concentrator. In the event that an actual or suspected unauthorized intrusion is detected, a device's logs provide an essential piece of forensic evidence. In the SEL RTAC, the SOE log can store up to 30,000 log items. This log is accessible through the web interface or an ODBC connection and can be sent via Syslog protocol to a syslog server for archiving.

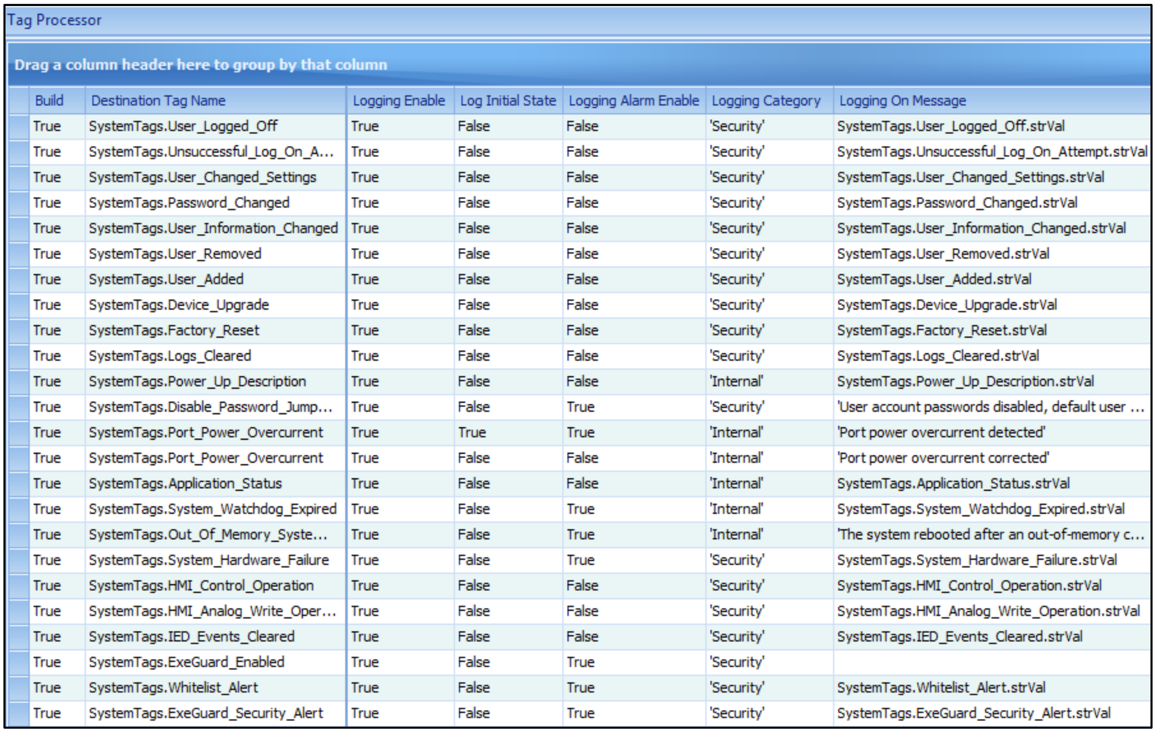
The logging configuration is transparent in the SEL RTAC, meaning that any data available to the logic engine can be logged into the SOE log. There are default logs configured in all ACSELERATOR RTAC projects; however, all default log items can be disabled or deleted. The Tag Processor in ACSELERATOR RTAC provides complete configurability for which data are logged, the messages associated with the data, and when the data are logged. To see the available logging options, navigate to the **Tag Processor > Options > Logging Layout**, as shown in Figure 11. Descriptions for each Tag Processor column are available in the ACSELERATOR RTAC Instruction Manual.



Build	Destination Tag Name	DT Data Type	Source Expression
True	SystemTags.User_Logged_On	STR	
True	SystemTags.User_Logged_Off	STR	
True	SystemTags.Unsuccessful_Log_On_Attempt	STR	
True	SystemTags.User_Changed_Settings	STR	
True	SystemTags.Password_Changed	STR	
True	SystemTags.User_Information_Changed	STR	
True	SystemTags.User_Removed	STR	
True	SystemTags.User_Added	STR	
True	SystemTags.Device_Upgrade	STR	
True	SystemTags.Factory_Reset	STR	
True	SystemTags.Logs_Cleared	STR	

Figure 11 Navigating to the Logging Layout in the Tag Processor in ACSELERATOR RTAC

In the logging layout, any tag available in the logic engine can be logged on a value change or time-stamp change. Users simply place the tag in the **Destination Tag Name** column and then enable the type of logging (status value, time change, or both) that will trigger the creation of a log entry. The message that is created for the log entry is configured in this layout. This is also the layout used to configure syslog message components. Figure 12 shows a subset of the columns for logging the layout in the Tag Processor.



Build	Destination Tag Name	Logging Enable	Log Initial State	Logging Alarm Enable	Logging Category	Logging On Message
True	SystemTags.User_Logged_Off	True	False	False	'Security'	SystemTags.User_Logged_Off.strVal
True	SystemTags.Unsuccessful_Log_On_A…	True	False	False	'Security'	SystemTags.Unsuccessful_Log_On_Attempt.strVal
True	SystemTags.User_Changed_Settings	True	False	False	'Security'	SystemTags.User_Changed_Settings.strVal
True	SystemTags.Password_Changed	True	False	False	'Security'	SystemTags.Password_Changed.strVal
True	SystemTags.User_Information_Changed	True	False	False	'Security'	SystemTags.User_Information_Changed.strVal
True	SystemTags.User_Removed	True	False	False	'Security'	SystemTags.User_Removed.strVal
True	SystemTags.User_Added	True	False	False	'Security'	SystemTags.User_Added.strVal
True	SystemTags.Device_Upgrade	True	False	False	'Security'	SystemTags.Device_Upgrade.strVal
True	SystemTags.Factory_Reset	True	False	False	'Security'	SystemTags.Factory_Reset.strVal
True	SystemTags.Logs_Cleared	True	False	False	'Security'	SystemTags.Logs_Cleared.strVal
True	SystemTags.Power_Up_Description	True	False	False	'Internal'	SystemTags.Power_Up_Description.strVal
True	SystemTags.Disable_Password_Jump…	True	False	True	'Security'	'User account passwords disabled, default user …
True	SystemTags.Port_Power_Overcurrent	True	True	True	'Internal'	'Port power overcurrent detected'
True	SystemTags.Port_Power_Overcurrent	True	False	False	'Internal'	'Port power overcurrent corrected'
True	SystemTags.Application_Status	True	False	False	'Internal'	SystemTags.Application_Status.strVal
True	SystemTags.System_Watchdog_Expired	True	False	True	'Internal'	SystemTags.System_Watchdog_Expired.strVal
True	SystemTags.Out_Of_Memory_Syste…	True	False	True	'Internal'	'The system rebooted after an out-of-memory c…
True	SystemTags.System_Hardware_Failure	True	False	True	'Security'	SystemTags.System_Hardware_Failure.strVal
True	SystemTags.HMI_Control_Operation	True	False	False	'Security'	SystemTags.HMI_Control_Operation.strVal
True	SystemTags.HMI_Analog_Write_Oper…	True	False	False	'Security'	SystemTags.HMI_Analog_Write_Operation.strVal
True	SystemTags.IED_Events_Cleared	True	False	False	'Security'	SystemTags.IED_Events_Cleared.strVal
True	SystemTags.ExeGuard_Enabled	True	False	True	'Security'	
True	SystemTags.Whitelist_Alert	True	False	True	'Security'	SystemTags.Whitelist_Alert.strVal
True	SystemTags.ExeGuard_Security_Alert	True	False	True	'Security'	SystemTags.ExeGuard_Security_Alert.strVal

Figure 12 Columns Available in the Logging Layout and the Tags Logged by Default in an ACSELERATOR RTAC Project

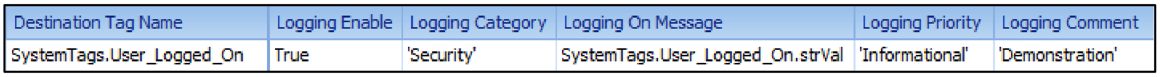
All SOE log entries are available to the SEL RTAC syslog client. To have the log entries sent via syslog, the user must configure a destination IP address and threshold through the web interface menu by selecting **Network > Syslog**. The threshold corresponds to the **Logging Priority** column in the Tag Processor. Table 3 shows how the applicable Tag Processor column maps to the syslog message components.

Table 3 Syslog Message Components Corresponding to Tag Processor Columns

Message Component	Description
Logging device	RTAC logger
Time stamp	Time stamp of the associated tag
Severity	Logging Priority: User-configured severity
Logging category	Logging Category: User-configured message
Tag name	Destination Tag Name: Tag used to trigger log
Log message	Logging On Message: Dependent on the type of trigger mechanism
Logging comment	Logging Comment: User-configured message

A sample syslog message (the corresponding Tag Processor columns are shown in Figure 13) is as follows:

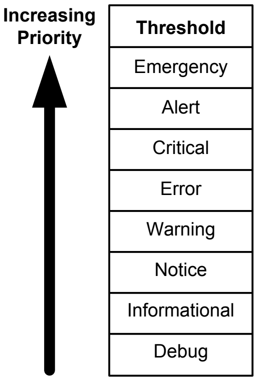
> <190>Oct 22 19:27:32 SEL-3530-0030a744574B RTAC Logger: 2015-10-22 19:27:31.918, Informational, Security, SystemTags.User_Logged_On, 'SEL logged on device via Web', 'Demonstration'



Destination Tag Name	Logging Enable	Logging Category	Logging On Message	Logging Priority	Logging Comment
SystemTags.User_Logged_On	True	'Security'	SystemTags.User_Logged_On.strVal	'Informational'	'Demonstration'

Figure 13 The Syslog Message Generated From the Configured Log in the Tag Processor

When configuring the threshold at which to send syslog messages, the categories are prioritized with Debug as the lowest priority and Emergency as the highest. All logged items that are of the threshold priority or above are sent as syslog messages to the syslog server. For example, if the threshold is set to Critical, all logs with a priority of Error, Warning, Notice, Informational, or Debug are not sent via syslog. All logs that are Critical, Alert, or Emergency are sent via syslog. The value configured in the **Logging Priority** column must match exactly the Threshold values listed in Figure 14 to work as described in this section.



Threshold
Emergency
Alert
Critical
Error
Warning
Notice
Informational
Debug

Figure 14 List of Correct Logging Priority Values That Correspond to the Syslog Threshold

CONCLUSION

Cybersecurity is often viewed as an esoteric topic. For the SEL RTAC family of products, SEL engineers have designed devices with security in mind from the beginning while still making the SEL RTAC security features easy to use and configure. It has never been more relevant to include cybersecurity principles when designing and operating critical infrastructure. Whether the goal is peace of mind or meeting regulatory compliance, the SEL RTAC has the tools necessary for securing critical infrastructure.

REFERENCES

[1] ACSELERATOR RTAC SEL-5033 Software Instruction Manual. Available: https://www.selinc.com.

[2] U.S. Department of Homeland Security, “Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).” Available: https://ics-cert.us-cert.gov/.

[3] National Institute of Standards and Technology, “National Vulnerability Database.” Available: https://nvd.nist.gov/.

[4] Schweitzer Engineering Laboratories, Inc., “The SEL Process for Disclosing Security Vulnerabilities,” February 2015. Available: https://tesla.selinc.com/security_notifications/security.php.

[5] U.S. Department of Commerce and the National Institute of Standards and Technology, “Digital Signature Standard (DSS),” FIPS PUB 186-4, July 2013. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

BIOGRAPHY

Darrin Kite received his Bachelor of Science in Renewable Energy Engineering from the Oregon Institute of Technology in 2012. Before joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2012, he worked as an engineering intern at Bonneville Power Administration. He is presently working as an automation engineer in SEL research and development.

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

LWP0018-01