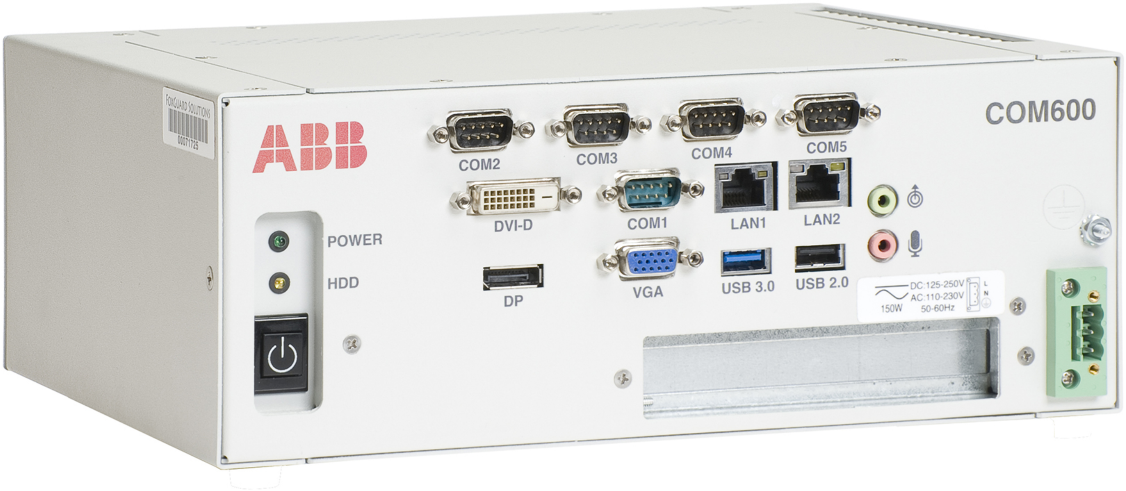
COM600 series 5.1

CAL and SEV OPC Server Users Manual



Contents:

1. About this manual

1.1. Copyright

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

http://www.abb.com/substationautomation

1.2. Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/ or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product is designed to be connected and to communicate information and data via a network interface, which should be connected to a secure network. It is sole responsibility of person or entity responsible for network administration to ensure a secure connection to the network and to establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

1.3. Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2004/108/EC) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2006/95/EC). This conformity is the result of tests conducted by ABB in accordance with the product standards EN 50263 and EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.

1.4. Trademarks

ABB is a registered trademark of ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

1.5. General information

CAL and SEV OPC servers are security related servers within COM600. They generate security-related events caused by user activity on COM600 and other software. They also capture security-related events in downstream devices, forward security-related events to upstream control systems and store security events that are sent and received between various devices.

The security violations regarding authorization, access control, service privileges and inactive associations are monitored within SEV OPC server, available in its child GSAL logical node.

SEV OPC server generates security events on real-time basis. It then transforms the security events into a prescribed ABB message format,which is then forwarded to CAL server within COM600.

The CAL Server receives security events in the form of either internally or externally generated Syslog messages. The received events are stored in an internal CAL server operation database. They can also be forwarded to external entities for additional reporting.

This manual gives an overview of the servers and their functions. The Configuration section guides you through the configuration tasks required before using the servers. The Operation section describes the basic operation procedures that can be done after the configuration. In the end you will find the Technical reference section.

1.6. Document conventions

The following conventions are used for the presentation of material:

- The words in names of screen elements (for example, the title in the title bar of a window, the label for a field of a dialog box) are initially capitalized.
- Capital letters are used for the name of a keyboard key if it is labeled on the keyboard. For example, press the ENTER key.
- Lowercase letters are used for the name of a keyboard key that is not labeled on the keyboard. For example, the space bar, comma key, and so on.
- Press CTRL+C indicates that you must hold down the CTRL key while pressing the C key (to copy a selected object in this case).
- Press ESC E C indicates that you press and release each key in sequence (to copy a selected object in this case).
- The names of push and toggle buttons are boldfaced. For example, click **OK**.
- The names of menus and menu items are boldfaced. For example, the **File** menu.
  - The following convention is used for menu operations: **MenuName** > **MenuItem** > **CascadedMenuItem**. For example: select **File** > **New** > **Type**.
  - The **Start** menu name always refers to the **Start** menu on the Windows taskbar.
- System prompts/messages and user responses/input are shown in the Courier font. For example, if you enter a value out of range, the following message is displayed:

```
Entered value is not valid. The value must be 0 - 30  .
```

- You can be asked to enter the string MIF349 in a field. The string is shown as follows in the procedure:

  MIF349
- Variables are shown using lowercase letters:

sequence name

1.7. Use of symbols

This publication includes warning, caution, and information icons that point out safety-related conditions or other important information. It also includes tip icons to point out useful information to the reader. The corresponding icons should be interpreted as follows.

⚡ The electrical warning icon indicates the presence of a hazard which could result in electrical shock.

⚠ The warning icon indicates the presence of a hazard which could result in personal injury.

The caution icon indicates important information or warning related to the concept discussed in the text. It may indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.

The information icon alerts the reader to relevant facts and conditions.

The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

1.8. Terminology

Term	Description
Alarm	An abnormal state of a condition.
Alarms and Events; AE	An OPC service for providing information about alarms and events to OPC clients.
COM600 Series; COM600	COM600 as a generic name for COM600S IEC and COM600F ANSI products
Data Access; DA	An OPC service for providing information about process data to OPC clients.
Data Object; DO	Part of a logical node object representing specific information, for example, status, or measurement. From an object-oriented point of view, a data object is an instance of a class data object. DOs are normally used as transaction objects; that is, they are data structures.
Data Set	The data set is the content basis for reporting and logging. The data set contains references to the data and data attribute values.
Device	A physical device that behaves as its own communication node in the network, for example, protection relay.
Event	Change of process data or an OPC internal value. Normally, an event consists of value, quality, and timestamp.
Intelligent Electronic Device	A physical IEC 61850 device that behaves as its own communication node in the IEC 61850 protocol.
Logical Device; LD	Representation of a group of functions. Each function is defined as a logical node. A physical device consists of one or several LDs.

Term	Description
Logical Node; LN	The smallest part of a function that exchanges data. An LN is an object defined by its data and methods.
OPC	Series of standards specifications aiming at open connectivity in industrial automation and the enterprise systems that support industry.
OPC item	Representation of a connection to the data source within the OPC server. An OPC item is identified by a string <object path>:<property name>. Associated with each OPC item are Value, Quality, and Time Stamp.
Property	Named data item.
Report Control Block	The report control block controls the reporting processes for event data as they occur. The reporting process continues as long as the communication is available.

1.9. Abbreviations

Abbreviation	Description
CAL	Centralized user Activity Logging
CDC	Common Data Class
CSV	Comma Separated Values
DO	Data Object
GAPC	Generic automatic process control
GGIO	Generic process I/O
GSAL	Generic Security AppLication
IED	Intelligent Electronic Device
OPC	OLE for Process Control
SEC	Security violation counting
SEV	Security EVent
UAL	User Activity Logging

1.10. Related documents

Name of the manual	MRS number
COM600 User’s Manual	1MRS756125
COM600 Operator's Manual	1MRS756705
COM600 HMI Configuration Manual	1MRS756740

Name of the manual	MRS number
COM600 Data Historian Operator's Manual	1MRS756739
COM600 Sequence Control Configuration Manual	1MRS755001
Master Protocols (Ethernet based) Configuration and Operation Manual	1MRS758689
Master Protocols (Ethernet based) Technical Reference Manual	1MRS758690
Slave Protocols (Ethernet based) Configuration and Operation Manual	1MRS758691
Slave Protocols (Ethernet based) Technical Reference Manual	1MRS758692
DNP 3.0 Serial Master (OPC) User's Manual	1MRS756567
DNP 3.0 Serial Slave (OPC) User's Manual	1MRS755495
IEC 60870-5-101 Slave (OPC) User's Manual	1MRS755382
IEC 60870-5-101 Master (OPC) User's Manual	1MRS756703
IEC 60870-5-103 Master (OPC) User's Manual	1MRS752278
COM600 Logic Processor User's Manual	1MRS756738
Modbus Serial Master (OPC) User's Manual	1MRS756126
Modbus Serial Slave (OPC) User's Manual	1MRS756913

1.11. Document revisions

Document version/date	Product revision	History
A/13.3.2015	4.1	Document created
B/24.5.2017	5.0	Document revised
C/6.3.2018	5.1	Document revised

2. Introduction

2.1. General information about the COM600 series

The COM600 product series are versatile Substation Management Units that help realize smart substation and grid automation solutions in industrial and utility distribution networks.

They get deployed together with protection and control IEDs, substation devices such as RTUs, meters and PLCs in dedicated cabinets and switchgear.

The COM600 product is an all-in-one unit that functions as:

- Communication gateway
- Web Human Machine Interface (WebHMI)
- Automation controller
- Real-time and historical data management unit

The COM600 product series use process information and device data, acquired over Ethernet or serial communication protocol interfaces to execute specific substation functions and applications. Thus, they are critical building blocks to realize substation secondary system solutions and in the process solving diverse customer needs.

2.2. COM600 product series variants and rationale

To facilitate substation and grid automation solutions in IEC and ANSI market areas, a variant-based system similar to Relion® 615 and 620 series is being followed from COM600 5.0 release.

The main reasons for such an approach are the following:

- To ensure all COM600 product series features are advantageously used in end-customer projects in the medium voltage substation automation domain.
- To ensure an optimum feature set to be bundled together to realize specific applications required in IEC and ANSI market areas.
- To ensure a future-proof product approach.

This release then comprises of two variants, based on the primary intent or application are defined as follows:

- COM600S IEC – COM600 for substation automation, analysis and data management (for IEC markets)
  - COM600S IEC is a substation automation, analyzer and data management unit that integrates devices, facilitates operations, manages communication and runs analysis applications pertinent to equipment or operations in utility or industrial distribution substations.
- COM600F ANSI – COM600 as distribution automation controller (for ANSI markets)

- COM600F is a dedicated distribution automation controller unit that runs distributed grid and feeder applications for ANSI power networks and inherits all core features of the COM600 series.

2.3. Functional overview

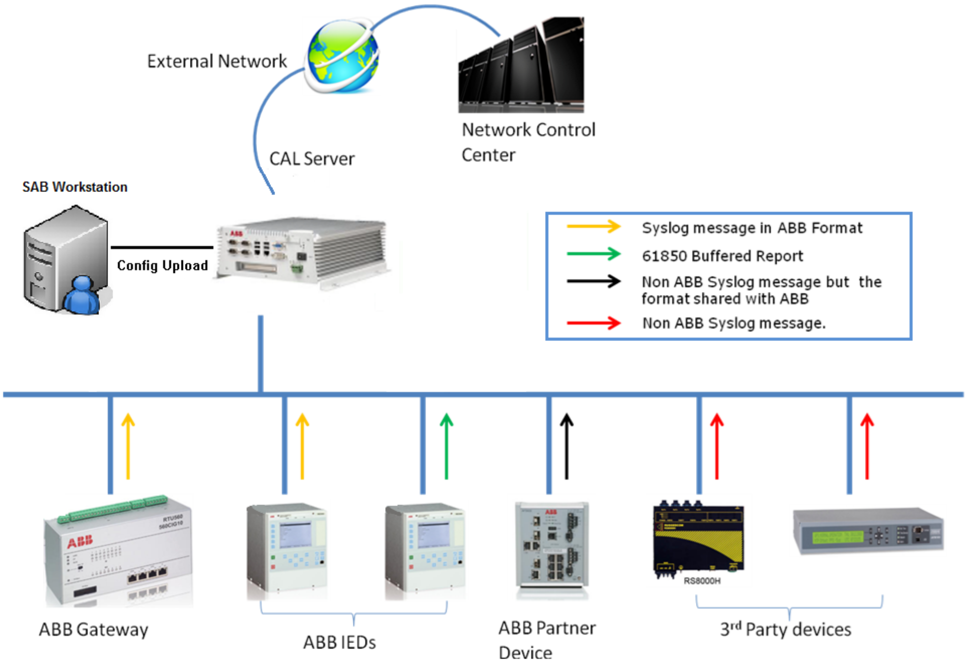
There are security related servers available within COM600.

The security-related servers are capable of

- Generating security-related events caused by user activity on COM600 and other software operation
- Capturing security-related events occurring in downstream devices, which COM600 is connected to
- Forwarding security-related events that are generated from COM600 and other downstream devices (like IED, RTU) to upstream control systems like DMS, or to other station computers
- Storing security events to an internal database for future auditing purposes.

The security events are sent and received between various devices using standard communication protocols like Syslog/ IEC 61850. These messages follow a prescribed format when forwarded using Syslog.

Additional details on the syslog message format used can be found in Table 5.2-1.



System_Overview.png

Figure 2.3-1 System overview

The security events that are generated in COM600 will always follow the ABB-prescribed format when forwarded to an upstream external device using Syslog, or to the CAL server functioning within COM600.

The security events that are received by COM600 and generated in downstream devices will always follow the format used in the source/downstream device when forwarded to upstream devices by COM600.

2.4. Security Event OPC Server

The primary purpose of the SEV OPC Server is to generate security events on real-time basis. The software components that underlie in the operating system and are available in COM600, like WebHMI, communication OPC Servers, (including IEC 61850, DNP, IEC101-104 and Modbus etc.), will interface with this server instance to deliver the security events in real time.

The SEV OPC Server then transforms these security events into a prescribed ABB message format. It is sent across the network, using standard Syslog protocol on a TCP/UDP communication link. Each of the security events is also accounted within a suitable IEC 61850 GSAL data object.

The GSAL logical node, specified by IEC 61850 data modeling approach, is typically used to monitor security violations regarding authorization, access control, service privileges and inactive associations. The data objects defined within a GSAL logical node are counters representing the security access/violations as they happen within a supporting device.

For additional details on the mapping between a security event and its corresponding GSAL logical node, see 5.2, COM600 Security Events.

By default, the security event OPC Server is set up to forward the security events generated in the COM600 CAL Server available locally within the same box.

2.5. CAL Server

The CAL (Centralized Account Logging) Server can receive security events in the form of Syslog messages. The received messages can be security events generated either internally within COM600 or externally from a downstream device like IED, RTU etc.

The received security events are then stored in a database internal to CAL server operation. The CAL Server also performs a security event cleanup from this database after a configurable time period.

The received security events can also be forwarded to external entities using a corresponding TCP/UDP link for additional reporting. The CAL Server can support up to six connections when forwarding security events through Syslog messages.

2.6. Security alarms over other protocols

In addition to the Syslog communication supported by Security Events OPC Server, also traditional communication protocols like DNP, IEC 101-104 and Modbus can be used when forwarding the security events generated within COM600.

To accomplish this, the data objects available within the Security Event OPC Server can be cross-referenced to a slave OPC Server instance. The master implementation available in an upstream control system/device can then connect to the slave instance available within COM600 and scan for these specific security-oriented data objects to retrieve the relevant information.

COM600 supports slave instances like DNP slave (on both serial/TCP IP link), IEC 101-104 slave and Modbus slave (on both serial/TCP IP link).

3. Configuration

3.1. About this section

This section guides you in the configuration tasks required before you can start using the CAL Server and SEV OPC Server. For information on the IEC 61850 data modeling, refer to the COM600 User's Manual.

To start

1. Select **File** > **Open/Manage Project**
2. In the **Open/Manage Project** dialog, select the required location for the project, either:
   - Projects on My computer
   - Project on Network
3. Select **New Project** on the left.
   - Enter a project name. The description is optional.
4. Click **Create**.
5. Click **Open Project**.

3.2. Overview of configuration

Before you can start using the CAL Server or the SEV OPC Server, you need to build and configure an object tree in SAB600. The object tree is used to define the communication structure.

The possible objects for CAL Server are:

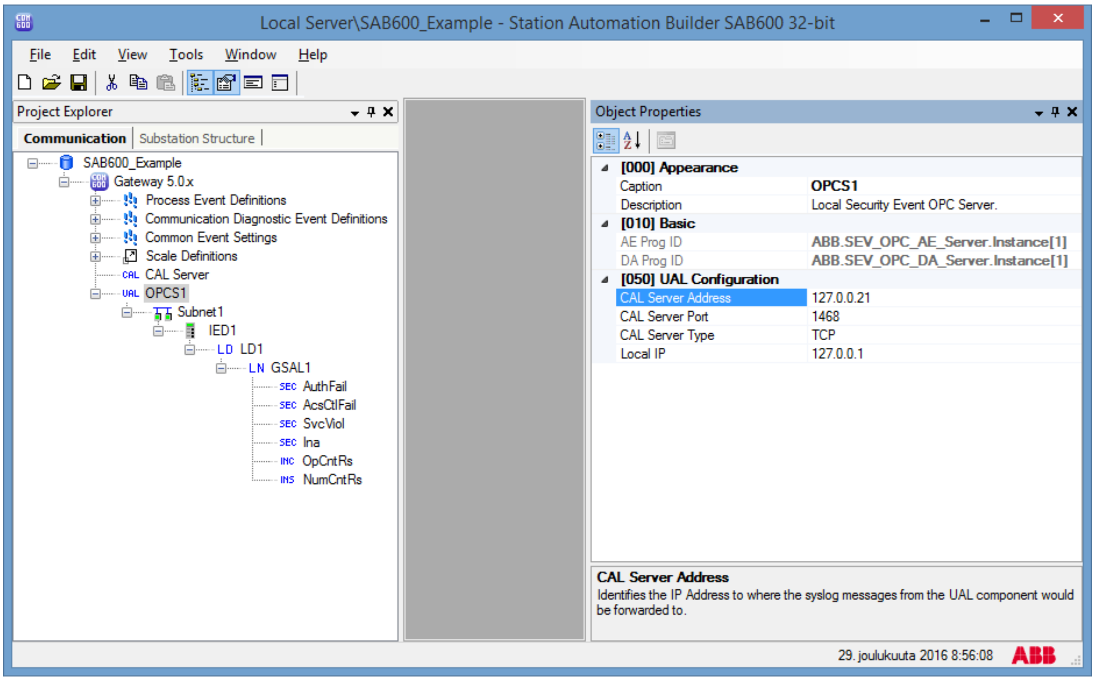
- Gateway
- CAL Server

The possible objects for SEV OPC Server are:

- Gateway
- SEV OPC Server
- SEV OPC Subnetwork
- SEV OPC IED
- SEV Logical Device objects
- SEV Logical Node objects
- SEV Data objects

Figure 3.2-1 shows an example view of SAB600, including an object tree in the communication structure on the left, and an object properties window displaying the object properties on the right.

When configuring OPC Servers the following characters cannot be used in object names: \ ` ' " #


Local Server\SAB600_Example - Station Automation Builder SAB600 32-bit
File
Edit
View
Tools
Window
Help
Project Explorer
Communication
Substation Structure
Object Properties
29. joulukuuta 2016 8:56:08

```
SAB600_Example
  Gateway 5.0.x
    Process Event Definitions
    Communication Diagnostic Event Definitions
    Common Event Settings
    Scale Definitions
    CAL CAL Server
    UAL OPCS1
      Subnet1
        IED1
          LD LD1
            LN GSAL1
              SEC AuthFail
              SEC AcsCtlFail
              SEC SvcViol
              SEC Ina
              INC OpCntRs
              INS NumCntRs
```

[000] Appearance	
Caption	OPCS1
Description	Local Security Event OPC Server.
[010] Basic	
AE Prog ID	ABB.SEV_OPC_AE_Server.Instance[1]
DA Prog ID	ABB.SEV_OPC_DA_Server.Instance[1]
[050] UAL Configuration	
CAL Server Address	127.0.0.21
CAL Server Port	1468
CAL Server Type	TCP
Local IP	127.0.0.1

CAL Server Address
Identifies the IP Address to where the syslog messages from the UAL component would be forwarded to.

SAB600_CAL_SEV_Example_View.png

Figure 3.2-1 Example view of SAB600

Configuration can be divided into two separate tasks:

1. Building an object tree, and
2. Configuring object properties.

First, build an object tree by adding objects to it. See 3.3, Building an object tree for additional details.

Figure 3.2-1 shows how an object tree may look like. In the example tree you can see a CAL Server and SEV OPC Server objects as well as the child objects of SEV_OPC_SERVER, like subnetwork, devices and data objects. Indentation indicates the parent-child relationship between the objects.

When you have added all the necessary objects to the object tree communication structure, you can configure the objects. See 3.4, Configuring objects for additional details.

3.3. Building an object tree

3.3.1. General information about building object tree

The object tree is built in the communication structure of SAB600. For details, see Figure 3.2-1.

When building an object tree, start from the Gateway and continue by adding objects in logical order.

You have several possible ways to add objects to the object tree in the communication structure.

You can add objects in three different ways:

- Right-click on the object to which you want to add a child object.
  Then select **New** > **Object type group** > **Object name**.
- Right-click on the object type and select **New** > **New**.
  A New object window appears. Select the object type you want to add and click **OK** or double-click it.
- You can copy the object.

Add the objects in the following order:

1. Gateway
2. CAL Server
3. SEV OPC Server
4. SEV OPC Subnetwork
5. SEV OPC IED
6. SEV OPC Logical device objects
7. SEV OPC Logical node objects
8. SEV Data objects

Each of the above objects can be renamed, if needed.

To rename an object:

1. Right-click on the object, and select **Rename**.
2. Select the object and change the value of the **Caption** property in the object properties view.
3. Double-click on the object to change its name.

3.3.2. Adding a Gateway object

To start building the object tree, add a Gateway object in the communication structure.

To add a Gateway object:

1. Select the project name.
2. Right-click on the selected name.
3. Select **New** > **Communication** > **Gateway**.

3.3.3. Adding a CAL Server object

When you have added the Gateway, continue building the object tree by adding a CAL Server object.

To add a CAL Server object:

1. Select the Gateway object in the communication structure and right-click on it.
2. Select **New** > **Security** > **CAL Server**.

Gateway object can have only one CAL server object as its child object.

3.3.4. Adding a SEV OPC Server object

When you have added the Gateway object, continue building the object tree by adding a SEV OPC Server object.

To add a SEV OPC Server object:

1. Select the Gateway object in the communication structure and right-click it.
2. Select **New** > **Security** > **SEV OPC Server**.

Gateway object can have only one SEV OPC Server object as its child object.

3.3.5. Adding a SEV OPC Subnetwork object

When you have added the SEV OPC Server object, continue building the object tree by adding a SEV OPC Subnetwork object.

To add a SEV OPC Subnetwork object:

1. Select a SEV OPC Server object and right-click on it.
2. Select **New** > **Subnetwork** > **SEV OPC Subnetwork** to add a SEV OPC Subnetwork object.

SEV OPC Server object can have only one SEV OPC Subnetwork object as a child object.

3.3.6. Adding a SEV OPC IED object

When you have added a SEV OPC Subnetwork object, continue building the object tree by adding a SEV OPC IED object.

To add a SEV OPC IED object:

1. Select a SEV OPC Subnetwork object and right-click on it.
2. ASelect **New** > **Security IED** > **SEV OPC IED** to add a SEV OPC IED object.

SEV OPC Subnetwork object can have only one SEV OPC IED object as a child object.

3.3.7. Adding a SEV OPC Logical Device objects

When you have added a SEV OPC IED object, continue building the object tree by adding a SEV OPC LD (Logical Device) object.

To add a SEV OPC LD object:

1. Select a SEV OPC IED object and right-click on it.
2. Select **New** > **Communication** > **SEV OPC LD** to add a SEV OPC LD object.
3. Rename the new object. The names of the Logical Device objects have to be unique.

3.3.8. Adding SEV OPC Logical Node objects

When you have added a SEV OPC LD object, continue building the object tree by adding a SEV OPC LN (Logical Node) object.

To add a SEV OPC LN object:

1. Select a SEV OPC LD object and right-click on it.
2. Select **New** > **Communication** > **SEV OPC LN** to add a SEV OPC LN object.
3. Rename the new object.
   The names of the Logical Node objects within a Logical Device have to be unique. To rename a logical node object, use its properties Logical Node Class/ Logical Node Instance/ Logical Node Prefix in the object properties view.

A logical device object can have only one logical Node 0 (LLN0) as a child object.

3.3.9. Adding data objects

To add a data object:

1. Select a Logical Node object and right-click on it.
2. Add a data object.
3. Rename the new object. The names of the data objects have to be unique.

3.4. Configuring objects

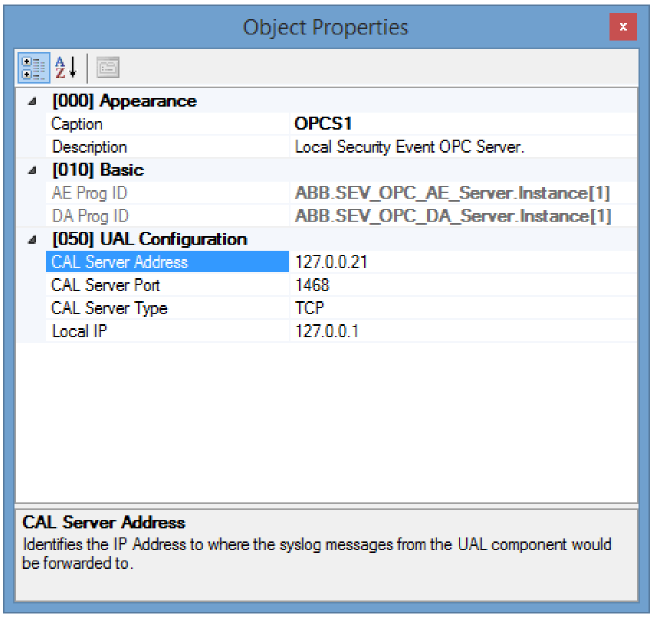
3.4.1. General information about configuring objects

When you have added the objects, continue by configuring the object properties.

The figure below shows an example of how to use SAB600 to configure the object properties for SEV OPC Server.

To configure an object:

1. Select an object in the object tree of the communication structure.
   • The object properties appear now in the **Object Properties** window. You can view the properties and their values as shown in the picture below.



[000] Appearance	
Caption	**OPCS1**
Description	Local Security Event OPC Server.
[010] Basic	
AE Prog ID	ABB.SEV_OPC_AE_Server.Instance[1]
DA Prog ID	ABB.SEV_OPC_DA_Server.Instance[1]
[050] UAL Configuration	
CAL Server Address	127.0.0.21
CAL Server Port	1468
CAL Server Type	TCP
Local IP	127.0.0.1

CAL Server Address
Identifies the IP Address to where the syslog messages from the UAL component would be forwarded to.

SAB600_CAL_SEV_Object_Properties_Example.png

Figure 3.4.1-1 Example of object properties in the Object Properties window

2. Select the property you want to configure. Depending on the property value type, you can configure either by
   • selecting a predefined value from a drop-down menu, or
   • entering a text string or a numerical value in a text field.
   The available properties for different objects are listed in the following subsections.

3.4.2. Configuring CAL Server properties

Table 3.4.2-1 CAL Server properties

Property/Parameter	Value or Value range/ Default	Description
Basic		

Property/Parameter	Value or Value range/ Default	Description
In Use	In Use / Not In Use Default: In Use	Specifies if the CAL Server is in use or not.
CAL UAL Receiver Configuration		
UAL Exact Library File	Default:exact_library.txt	Specifies the name of the configuration file containing parsing rules. These rules are used when parsing the incoming syslog messages to figure out an equivalent ABB UAL event ID, based on its contents.
UAL Fuzzy Library File	Default: fuzzy_library.txt	Specifies the name of the configuration file containing fuzzy parsing rules to be used while parsing incoming syslog messages
UAL Local IP	Default: 127.0.0.1	Specifies the IP address of the local network interface (NIC) to be used. This is the address in where the CAL Server expects to receive syslog messages.
UAL Persistency Days	1…90 Default: 90	Specifies the number of days security events should be kept. Only relevant if UAL Persistency Type is not 0 (none).
UAL Persistency Event Size	9…3000 Default: 100	Specifies the capacity of the ring buffer, maximum number of events that can be stored. Only relevant if UAL Persistency Type is “Ring Buffer”.
UAL Persistency Type	Default: DB	Specifies the type of storage used to keep security events.
UAL Syslog TCP In use	In Use / Not In Use Default: In Use	Enable/Disable the syslog message receiver via TCP connection
UAL Syslog TCP Port	1 … 65535 Default: 1468	Specifies the port number to be used by the syslog message when receiving messages via TCP connection.
UAL Syslog UDP In use	In Use / Not In Use Default: In Use	Enable/Disable the syslog message receiver via UDP connection.
UAL Syslog UDP Port	1 … 65535 Default: 514	Specifies the port number to be used by the syslog message receiver, when receiving messages via UDP connection.

Property/Parameter	Value or Value range/ Default	Description
CAL Syslog Publisher (1…6)		
Culture (1...6)	Default: en-US	Indicates the type of internationalization to be used when forwarding syslog messages
In Use (1…6)	In Use / Not In Use Default: Not In Use	Enable/Disable the security event forwarding capability via syslog messages to an external device
IP Address (1…6)	Default: 127.0.0.1	Specifies the IP address of the external syslog server to where the security events available within COM600 would be forwarded
Port (1…6)	1…65535 Default: 514	Specifies the port number of the external syslog server to where the security events available within COM600 would be forwarded
Protocol (1…6)	TCP/UDP Default: TCP	Specifies the type of network connection to be used with the external syslog server when forwarding security events

The CAL Server is capable of forwarding security events to up to six external devices via syslog messages. The security events include both events from COM600 as well as events received from downstream devices connected to COM600.

3.4.3. Configuring SEV OPC Server properties

Table 3.4.3-1 SEV OPC Server properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
AE Prog ID		Instance identification of diagnostic OPC alarm and event server.
DA Prog ID		Instance identification of diagnostic OPC data access server.
UAL Configuration		

Property/Parameter	Value or Value range/ Default	Description
CAL Server Address	Default: 127.0.0.21	Identifies the IP address to where the security events generated within COM600 would be forwarded to Centralized security event log collection. Typically the security events would be forwarded to CAL Server available within COM600.
CAL Server Port	1…65535 Default: 1468	Specifies the port number of the centralized syslog server to where the security events generated within COM600 would be forwarded to.
CAL Server Type	TCP/UDP Default: TCP	Specifies the type of network connection to be used when forwarding the security events generated within COM600 to the centralized user activity logging server.
Local IP	Default: 127.0.0.1	Specifies the local IP address to be used by the Security Event OPC Server.

3.4.4. Configuring SEV OPC Subnetwork properties

Table 3.4.4-1 SEV OPC Subnetwork properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
In Use	In Use/ Not In Use Default: In Use	Specifies if the SEV OPC Subnetwork is in use or not.

3.4.5. Configuring SEV OPC IED properties

Table 3.4.5-1 SEV OPC IED properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Diagnostics Enabled	True/ False Default: False	Enable diagnostics on the device.

Property/Parameter	Value or Value range/ Default	Description
In Use.	In Use/ Not In Use Enable/disables the device from use.	Enable/disables the device from use.
Simulation Mode	True/False Default: False	Specifies if the device is in simulation mode or not.
Control Authorization		
Station/Remote Switch OPC Path		OPC path of the station remote switch position to be used with this IED. The format is "#ProgID For OPC Server#Channel Name\IED Name\Logical Device Name\Logical Node Name\Data Object Name."
OPC Alarm and Event		
Device Connection Status	Device Connection status	Specifies the event class object to be used for event annunciation for change in device connection state.

3.4.6. Configuring SEV OPC Logical Device properties

Table 3.4.6-1 SEV OPC Logical Device properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
SRSwitchForLogicalDevice		OPC path of the station remote switch position to be used with this Logical Device. The format is #ProgID For OPC Server#Channel Name\IED Name\Logical Device Name\Logical Node Name\Data Object Name.

3.4.7. Configuring SEV OPC Logical Node properties

Table 3.4.7-1 Configuring SEV OPC Logical Node properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
LLN0		

Property/Parameter	**Value or Value range/ Default**	**Description**
Logical Node Class	LLN0	Logical node class
GGIO1		
Logical Node Class	Default: GGIO	Logical Node Class
Logical Node Instance	1…2147483647	Logical node instance number
	Default: 1	
Logical Node Prefix	Default: None	Prefix for logical node

3.4.8. Configuring data objects for internal OPC data

3.4.8.1. General information

Internal OPC data objects are used to extract the internal information an OPC Server needs for an external entity.

This information includes:
- runtime status to indicate if the device is in use
- its connection status
- message transmission characteristics for a connection

The SEV OPC Server supports three internal data object types that provide this status information:
- Integer status (INS)
- Controllable single point (SPC)
- Single point status (SPS)

3.4.8.2. Integer Status (INS)

Table 3.4.8.2-1 Internal INS properties

Property/Parameter	**Value or Value range/ Default**	**Description**
Basic		
Common Data Class	INS	IEC 61850 Data Object type, Common Data Class.
Addresses		

Property/Parameter	Value or Value range/ Default	Description
Item Tag Path	Default: none	Item tag path for the internal status information. The internal server tags that can be used are located in the Attributes nodes that are located under the opc server, channel and IED nodes. When an attribute tag is referred to in the internal item definitions below, it is possible to use either the whole tag path or just the path relative to the IED (the internal tags are configured per IED); for example, Attributes\Diagnostic counters\Transmitted data messages. When the whole path is used, it must be preceded by slash (/) character, for example, /Channel Name\Attributes\Diagnostic counters\Transmitted data messages.
OPC Alarm and Event		
Indication Event	Default: none	Indication event used with this data object.

3.4.8.3. Controllable single point (SPC)

Table 3.4.8.3-1 Internal SPC properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Common Data Class	SPC	IEC 61850 Data Object type, Common Data Class.
Addresses		

Property/Parameter	Value or Value range/ Default	Description
Item Tag Path	Default: none	Item tag path for the internal status information. The internal server tags that can be used are located in the Attributes nodes that are located under the OPC Server, channel and IED nodes. When an attribute tag is referred to in the internal item definitions below, it is possible to use either the whole tag path or just the path relative to the IED (the internal tags are configured per IED); for example, Attributes\Diagnostic counters\Transmitted data messages. When the whole path is used, it must be preceded by slash (/) character, for example, /Channel Name\Attributes\Diagnostic counters\Transmitted data messages
OPC Alarm and Event		
Command Tracking Event	Default: none	Control event class to be used with this data object.
Indication Event	Default: none	Indication event used with this data object.

3.4.8.4. Single point status (SPS)

Table 3.4.8.4-1 Internal SPS properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Common Data Class	SPS	IEC 61850 Data Object type, Common Data Class.
Addresses		

Property/Parameter	Value or Value range/ Default	Description
Item Tag Path	Default: none	Item tag path for the internal status information. You can find the the internal server tags that can be used in the Attributes nodes that are located under the OPC Server, channel and IED nodes. When an attribute tag is referred to in the internal item definitions below, it is possible to use either the whole tag path or just the path relative to the IED (the internal tags are configured per IED); for example, Attributes\Diagnostic counters\Transmitted data messages. When the whole path is used, it must be preceded by slash (/) character, for example, /Channel Name\Attributes\Diagnostic counters\Transmitted data messages.
OPC Alarm and Event		
Indication Event	Default: none	Indication event used with this data object.

3.4.9. Configuring data objects

3.4.9.1. Security Violation Counter (SEC)

Table 3.4.9.1-1 SEC DO properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Common Data Class	SEC	IEC 61850 Data Object type, Common Data Class.
OPC Alarm and Event		
Indication Event	Default: none	Indication event used with this data object.

3.4.9.2. Controllable Integer Status (INC)

Table 3.4.9.2-1 INC DO properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Common Data Class	INC	IEC 61850 Data Object type, Common Data Class.
Addresses		
UAL Event IDs		Comma separated values of UAL Event IDs, listing out selective security events to be attributed within this data object. Additional details on the list of available UAL event IDs that can be used are available in Table 5.2-1
OPC Alarm and Event		
Command Tracking Event	Default: none	Control event class to be used with this data object.
Indication Event	Default: none	Indication event used with this data object.

3.4.9.3. Integer Status (INS)

Table 3.4.9.3-1 INS DO properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Common Data Class	INS	IEC 61850 Data Object type, Common Data Class.
Addresses		
UAL Event IDs		Comma separated values of UAL Event IDs, listing out selective security events to be attributed within this data object. Additional details on the list of available UAL event IDs that can be used are available in Table 5.2-1.
OPC Alarm and Event		
Indication Event	Default: none	Indication event used with this data object.

3.4.9.4. Controllable single point (SPC)

Table 3.4.9.4-1 SPC DO properties

Property/Parameter	Value or Value range/ Default	Description
Basic		
Common Data Class	SPC	IEC 61850 Data Object type, Common Data Class.
Addresses		
UAL Event IDs		Comma separated values of UAL Event IDs, listing out selective security events to be attributed within this data object. Additional details on the list of available UAL event IDs that can be used are available in Table 5.2-1.
OPC Alarm and Event		
Command Tracking Event	Default: none	Control event class to be used with this data object.
Indication Event	Default: none	Indication event used with this data object.

4. Operation

4.1. About this section

This section describes the basic operation procedures you can do when you have configured the CAL and SEV OPC Server.

4.2. Activating COM600 with the new configurations

For information about activating COM600 with new configuration, see the COM600 User’s Manual.

4.3. Security event counters

4.3.1. Default Counters

When you have added the SEV OPC IED object to the SAB600 communication structure, a **GSAL 1** logical node automatically appears under an “LD1” logical device.

As per the IEC 61850 data modeling specification, this logical node is used to monitor security violations in the following areas:

- authorization
- access control
- service privileges
- inactive associations

Table 4.3.1-1 specifies the data object included for a GSAL logical node.

Each of the security events generated within COM600 is attributed within any one of the data object in the SEC common data class category. These data objects can then be directly used to extract the relevant security information using applicable IEC 61850 communication services.

You will find additional information on mapping between a UAL event and its corresponding IEC 61850 data object in 5.2, COM600 Security Events.

Table 4.3.1-1 Data objects specified for a GSAL logical node

Data Object Name	Common Data Class	Description
AuthFail	SEC	Authorization failures
AcsCtlFail	SEC	Access control failures detected.
SvcViol	SEC	Service privilege violations

Data Object Name	Common Data Class	Description
Ina	SEC	Inactive associations
NumCntRs	INS	Number of counter resets
OpCntRs	INC	Resettable Operation counter

4.3.2. Custom counters

In addition to the default data objects, you can create custom data objects in the GSAL logical node. The custom data objects can be used to selectively attribute a list of UAL event IDs for a more abstract count.

You can configurate a selective list of the UAL event IDs into the custom data object by editing its object properties.

You can also group custom objects under multiple general purpose logical nodes like GAPC, GGIO, etc. The custom objects should only be represented as an INC, or an INS, or a SPC common data class type.

See 3.4.9, Configuring data objects for additional information on the data objects for a SEV OPC IED and its configuration.

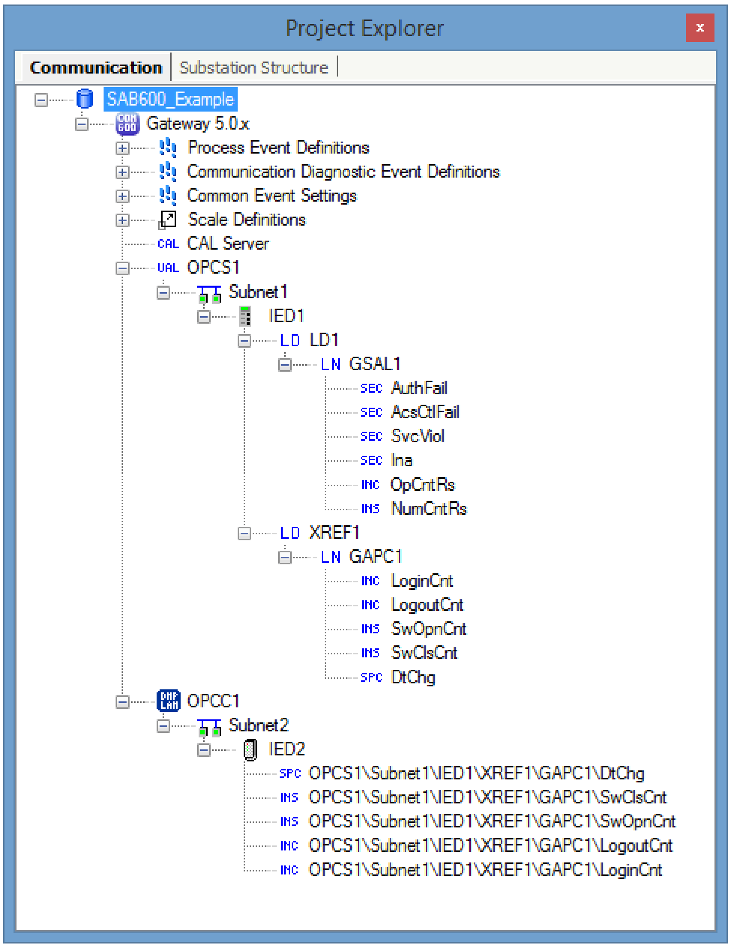
4.3.3. Cross referencing custom counters

You can cross-reference the custom data objects created for SEV OPC IED to other protocol slave IED implementations supported within COM600.

You can cross-reference to the following protocol slave implementations:

- IEC 101-104 slave
- DNP slave
- Modbus slave
- IEC 61850 Proxy Server

The master protocol implementation from the upstream device/system can then connect to the slave instances within COM600, and receive the security information. The security counters can also be published to an upstream device using other communication protocols, alongside with the syslog messaging mechanism.



Project Explorer

Communication | Substation Structure

```
SAB600_Example
  Gateway 5.0.x
    Process Event Definitions
    Communication Diagnostic Event Definitions
    Common Event Settings
    Scale Definitions
    CAL CAL Server
    UAL OPCS1
      Subnet1
        IED1
          LD LD1
            LN GSAL1
              SEC AuthFail
              SEC AcsCtlFail
              SEC SvcViol
              SEC Ina
              INC OpCntRs
              INS NumCntRs
          LD XREF1
            LN GAPC1
              INC LoginCnt
              INC LogoutCnt
              INS SwOpnCnt
              INS SwClsCnt
              SPC DtChg
    OPCC1
      Subnet2
        IED2
          SPC OPCS1\Subnet1\IED1\XREF1\GAPC1\DtChg
          INS OPCS1\Subnet1\IED1\XREF1\GAPC1\SwClsCnt
          INS OPCS1\Subnet1\IED1\XREF1\GAPC1\SwOpnCnt
          INC OPCS1\Subnet1\IED1\XREF1\GAPC1\LogoutCnt
          INC OPCS1\Subnet1\IED1\XREF1\GAPC1\LoginCnt
```

SAB600_CAL_SEV_Cross_References.png

Figure 4.3.3-1 Sample cross references

To cross-reference a security data object:

1. Start with adding a slave IED to the SAB600.
2. Launch the cross-reference tool available for the slave IED.
3. Drag and drop the selected security data object from SEV OPC IED to the cross-reference tool.
4. Finish the configuration by assigning appropriate values to the parameters in the cross-references tool.

Figure 4.3.3-1 shows a sample communication structure in SAB600 with data objects from SEV OPC IED cross referenced to a DNP Slave IED instance within COM600.

The custom data objects in GAPC logical node within the SEV OPC IED attribute to count the number of login/logoff/data change security events. These data objects are then cross-referenced to a DNP slave IED. A DNP master from an upstream device/system connecting to the slave instance can then retrieve the security count information by polling for appropriate DNP objects configured within the cross-references tool.

For more information on configuring each of the slave IED in COM600 see the following manuals:

- COM600 IEC60870-5-101 Slave (OPC) User’s Manual
- COM600 Series 5.0 Slave Protocols (Ethernet based) Configuration and Operation Manual
- COM600 DNP v3.0 Serial Slave (OPC) User’s Manual
- COM600 Modbus Serial Slave (OPC) User’s Manual

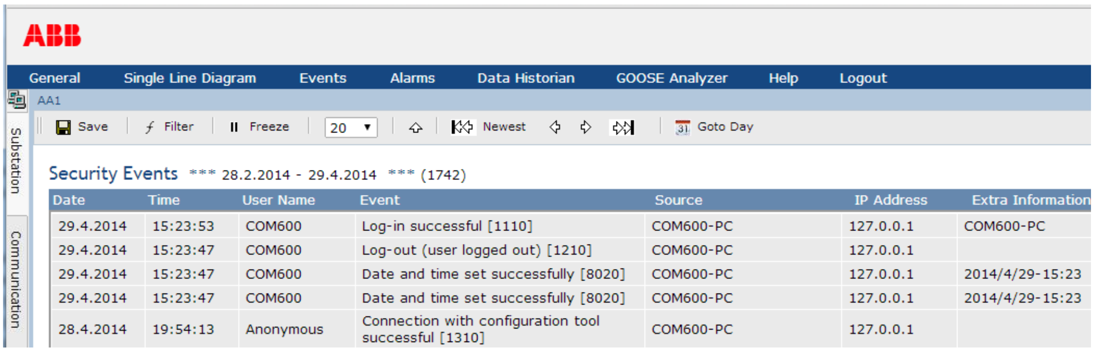
4.4. Viewing Security Events

The COM600 WebHMI **Security Events** web page displays all the security events received by COM600 as syslog messages. These messages include both security events generated within COM600 and security events generated from downstream devices.

Please note that the “Security Events” page is available only to users with COM600-Administrator access rights.

To open the **Security Events** page:

1. Access the **Events** page from COM600 WebHMI toolbar
2. Press on the **Open Security Events** button
3. Use the toolbar button, as pointed out in Figure 4.4-1, to select the filters you need for retrieving a selective set of security events from COM600 .



Security Events *** 28.2.2014 - 29.4.2014 *** (1742)

Date	Time	User Name	Event	Source	IP Address	Extra Information
29.4.2014	15:23:53	COM600	Log-in successful [1110]	COM600-PC	127.0.0.1	COM600-PC
29.4.2014	15:23:47	COM600	Log-out (user logged out) [1210]	COM600-PC	127.0.0.1	
29.4.2014	15:23:47	COM600	Date and time set successfully [8020]	COM600-PC	127.0.0.1	2014/4/29-15:23
29.4.2014	15:23:47	COM600	Date and time set successfully [8020]	COM600-PC	127.0.0.1	2014/4/29-15:23
28.4.2014	19:54:13	Anonymous	Connection with configuration tool successful [1310]	COM600-PC	127.0.0.1	

WHMI_Security_Events_page.png

Figure 4.4-1 COM600 WebHMI Security Events page

5. Technical Reference

5.1. Security Event

A Security Event in COM600 is an event that occurs due to a user or a software action and that changes the environment in which the product functions.

This environment includes both internal and external actions to perform a predefined function. Internal refers to the underlying system where the product functions and external refers to the various interfaces with which the product connects to other external products/systems.

5.2. COM600 Security Events

The following table provides a list with an indication of all the events as applicable to COM600.

The table includes a description of

- Event number - Specific ID assigned within ABB devices to identify a security event.
- 61850 severities to be used when publishing security events using IEC 61850.
- 61850 mapping, defining the data object to be used when publishing security events using IEC 61850.
- Description of the security event.

Table 5.2-1 COM600 Security Events

Event Number	61850 severity	61850 mapping	Description
1110	GSAL_SEV_UNKNOWN	GSAL.Ina	Log-in successful
1130	GSAL_SEV_WARNING	GSAL.AuthFail	Log-in failed - Wrong credentials
1170	GSAL_SEV_CRITICAL	GSAL.AuthFail	Log-in failed 3 times
1210	GSAL_SEV_UNKNOWN	GSAL.Ina	Log-out (user logged out)
1310	GSAL_SEV_UNKNOWN	GSAL.Ina	Connection with configuration tool successful
2110	GSAL_SEV_UNKNOWN	GSAL.Ina	User account created successfully
2115	GSAL_SEV_UNKNOWN	GSAL.Ina	User account enabled successfully
2117	GSAL_SEV_UNKNOWN	GSAL.Ina	User account disabled successfully

Event Number	61850 severity	61850 mapping	Description
2120	GSAL_SEV_UNKNOWN	GSAL.Ina	User account deleted successfully
2160	GSAL_SEV_UNKNOWN	GSAL.Ina	New role assigned to user successfully
2162	GSAL_SEV_UNKNOWN	GSAL.Ina	Permission added successfully
2172	GSAL_SEV_UNKNOWN	GSAL.Ina	User permission removed successfully
2210	GSAL_SEV_MINOR	GSAL.SvcViol	User password changed successfully
2220	GSAL_SEV_MINOR	SAL.SvcViol	Change of user password failed
2230	GSAL_SEV_MINOR	GSAL.SvcViol	New user role assignment failed
2270	GSAL_SEV_MINOR	GSAL.SvcViol	Role assignment removal failed
3420	GSAL_SEV_CRITICAL	GSAL.Ina	Security log file deleted by user
4310	GSAL_SEV_UNKNOWN	GSAL.Ina	VPN Connection successful
4350	GSAL_SEV_CRITICAL	AuthFail	VPN Connection failed - Negotiation failed
4360	GSAL_SEV_CRITICAL	GSAL.AuthFail	VPN Connection failed - IKE failed
5160	GSAL_SEV_MINOR	GSAL.Ina	Gateway/RTU restarted
5270	GSAL_SEV_UNKNOWN	GSAL.Ina	System startup
5280	GSAL_SEV_UNKNOWN	GSAL.Ina	System shutting down
6130	GSAL_SEV_WARNING	GSAL.Ina	Control operation performed successfully
6132	GSAL_SEV_WARNING	GSAL.Ina	Failed to perform a control operation
7110	GSAL_SEV_UNKNOWN	GSAL.Ina	Switching Device open
7120	GSAL_SEV_UNKNOWN	GSAL.Ina	Switching Device close
8020	GSAL_SEV_UNKNOWN	GSAL.Ina	Date and time set successfully
8040	GSAL_SEV_UNKNOWN	GSAL.Ina	Communication system startup successful
8220	GSAL_SEV_UNKNOWN	GSAL.Ina	Date and time setting failed

Event Number	61850 severity	61850 mapping	Description
8240	GSAL_SEV_UNKNOWN	GSAL.Ina	Communication system startup failed
9010	GSAL_SEV_CRITICAL	GSAL.Ina	Flooding attack detected
9110	GSAL_SEV_CRITICAL	GSAL.Ina	Firewall blocked incoming connection
9150	GSAL_SEV_CRITICAL	GSAL.Ina	Firewall settings/rules changed successfully
9210	GSAL_SEV_CRITICAL	GSAL.Ina	IPS blocked incoming packet
9510	GSAL_SEV_CRITICAL	GSAL.Ina	CSR approved and certificate issued successfully
9520	GSAL_SEV_CRITICAL	GSAL.Ina	Certificate Signing request failed
9610	GSAL_SEV_CRITICAL	GSAL.Ina	Certificate validation succeeded
9620	GSAL_SEV_CRITICAL	GSAL.Ina	Certificate validation failed - Certificate expired
9630	GSAL_SEV_CRITICAL	GSAL.Ina	Certificate validation failed - Certificate revoked
9640	GSAL_SEV_CRITICAL	GSAL.Ina	Certificate validation failed - Certificate signature check failed
9995	GSAL_SEV_CRITICAL	GSAL.Ina	UAL Syslog FIFO receiver overflow, message overwritten
13200	GSAL_SEV_UNKNOWN	GSAL.Ina	Configuration transferred to the device successfully
13210	GSAL_SEV_UNKNOWN	GSAL.Ina	Configuration transfer to the device started
13300	GSAL_SEV_UNKNOWN	GSAL.Ina	Configuration files read/exported from the device successfully
13310	GSAL_SEV_UNKNOWN	GSAL.Ina	Configuration exporting from the device started successfully
13570	GSAL_SEV_UNKNOWN	GSAL.Ina	Exported/read diagnosis file from the device successfully

Event Number	61850 severity	61850 mapping	Description
14200	GSAL_SEV_WARNING	GSAL.SvcViol	Failed to transfer configuration to the device
14210	GSAL_SEV_UNKNOWN	GSAL.Ina	Failed to start transfer of configuration to the device
14300	GSAL_SEV_UNKNOWN	GSAL.Ina	Failed to read configuration files from the device
14310	GSAL_SEV_UNKNOWN	GSAL.Ina	Failed to start export of configuration from the device
14570	GSAL_SEV_UNKNOWN	GSAL.Ina	Failed to read diagnosis file from the device

Index

—

ABB Distribution Solutions
Distribution Automation
P.O. Box 699
FI-65101 Vaasa, Finland
Phone: +358 10 22 11

ABB Distribution Automation
4300 Coral Ridge Drive
Coral Springs, Florida 33065
Phone: +1 954 752 6700

www.abb.com/mediumvoltage
www.abb.com/substationautomation