Arctic

Cyber Security Deployment Guideline

Document ID: 1MRS758860
Issued: 2021-12-20
Revision: F

Copyright

Trademarks

Warranty

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

abb.com/mediumvoltage

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

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. In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

Table of contents

Table of contents

Section 1 Introduction

1.1 This manual

The cyber security deployment guideline describes the process for handling cyber security when communicating with the device. The cyber security deployment guideline provides information on how to secure the system on which the device is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

1.2 Intended audience

This guideline is intended for the system engineering, commissioning, operation and maintenance personnel handling cybersecurity during the product lifecycle.

The personnel is expected to have general knowledge about topics related to cybersecurity.

- Protection and control devices, gateways and workstations
- Networking, including Ethernet and TCP/IP with its concept of ports and services
- Security policies
- Firewalls
- Antivirus protection
- Application whitelisting
- Secure remote communication

1.3 Product documentation

1.3.1 Product documentation set

Product series- and product-specific manuals can be downloaded from the ABB Web site abb.com/mediumvoltage.

1.3.2 Document revision history

Document revision/date	Product versions	History
A/2017-09-28	Arctic 600 devices Ver.3.4 ARM600 Ver.4.3	First release
B/2018-06-29	Arctic 600 devices Ver.3.4.5 ARM600 Ver.4.4.1	Content updated to correspond to the product versions
C/2019-04-24	Arctic 600 devices Ver.3.4.7 ARM600 Ver.4.5.1	Content updated to correspond to the product versions
D/2020-11-03	Arctic 600 devices Ver.3.4.9 ARM600 Ver.4.5.3	Content updated to correspond to the product version
E/2021-06-28	Arctic 600 devices Ver.3.4.9 ARM600 Ver.5.0.1	Content updated to correspond to the product version
F/2021-12-20	Arctic 600 devices Ver.3.4.9 ARM600 Ver.5.0.1	Content updated

1.3.3 Related documentation

Name of the document	Description	Document ID
Wireless Controller M2M solution security guide		1MRS758448
Configuring Arctic Wireless Gateways/ Controllers and ARM600		1MRS758449
3G/LTE configuration guide Technical Note	Configuring Wireless Gateways, Controllers and M2M Gateway	1MRS758449

Product series- and product-specific manuals can be downloaded from the ABB Web site abb.com/mediumvoltage.

1.4 Symbols and conventions

1.4.1 Symbols

The caution icon indicates important information or warning related to the concept discussed in the text. It might 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 of important facts and conditions.

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

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

1.4.2 Document conventions

A particular convention may not be used in this manual.

- Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.
- Menu paths are presented in bold.
  Select **Main menu/Settings**.
- Parameter names are shown in italics.
  The function can be enabled and disabled with the *Operation* setting.
- Parameter values are indicated with quotation marks.
  The corresponding parameter values are "On" and "Off".

Section 2 Security in distribution automation

2.1 General security in distribution automation

Technological advancements and breakthroughs have caused a significant evolution in the electric power grid. As a result, the emerging “smart grid” and “Internet of Things” are quickly becoming a reality. At the heart of these intelligent advancements are specialized IT systems – various control and automation solutions such as distribution automation systems. To provide end users with comprehensive real-time information, enabling higher reliability and greater control, automation systems have become ever more interconnected. To combat the increased risks associated with these interconnections, ABB offers a wide range of cyber security products and solutions for automation systems and critical infrastructure.

The new generation of automation systems uses open standards such as IEC 60870-5-104, DNP3 and IEC 61850 and commercial technologies, in particular Ethernet and TCP/IP based communication protocols. They also enable connectivity to external networks, such as office intranet systems and the Internet. These changes in technology, including the adoption of open IT standards, have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only to office or enterprise IT systems.

To counter cyber security risks, open IT standards are equipped with cyber security mechanisms. These mechanisms, developed in a large number of enterprise environments, are proven technologies. They enable the design, development and continual improvement of cyber security solutions also for control systems, including distribution automation applications.

ABB understands the importance of cyber security and its role in advancing the security of distribution networks. A customer investing in new ABB technologies can rely on system solutions where reliability and security have the highest priority.

Reporting of vulnerability or cyber security issues related to any ABB product can be done via cybersecurity@ch.abb.com.

2.2 Reference documents

Information security in critical infrastructure like electrical distribution and transmission networks has been in high focus for both vendors and utilities. This

together with developing technology, for example, appliance of Ethernet and IP based communication networks in substations, power plants and network control centers creates a need of specifying systems with cyber security.

ABB is involved in the standardization and definition of several cyber standards, the most applicable and referred ones are ISO 2700x, IEC 62443, IEEE P1686 and IEC 62351. Besides standardization efforts there are also several governments initiated requirements and practices like NERC CIP and BDEW. ABB fully understands the importance of cyber security for substation automation systems and is committed to support users in efforts to achieve or maintain compliance to these.

Section 3 Secure system setup

3.1 Basic system hardening rules

Today's distribution automation systems are basically specialized IT systems. Therefore, several rules of hardening an automation system apply to these systems, too. Protection and control relays are from the automation system perspective on the lowest level and closest to the actual primary process. It is important to apply defense-in-depth information assurance concept where each layer in the system is capable of protecting the automation system and therefore protection and control relays are also part of this concept. The following should be taken into consideration when planning the system protection.

- Recognizing and familiarizing all parts of the system and the system's communication links
- Removing all unnecessary communication links in the system
- Rating the security level of remaining connections and improving with applicable methods
- Hardening the system by removing or deactivating all unused processes, communication ports and services
- Checking that the whole system has backups available from all applicable parts
- Collecting and storing backups of the system components and keeping those up-to-date
- Removing all unnecessary user accounts
- Defining password policies
- Changing default passwords and using strong passwords
- Checking that the link from substation to upper level system uses strong encryption and authentication
- Segregating public network (untrusted) from automation networks (trusted)
- Segmenting traffic and networks
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using malware protection in workstations and keeping those up-to-date

It is important to utilize the defence-in-depth concept when designing automation system security. It is not recommended to connect a device directly to the Internet without adequate additional security components. The different layers and interfaces in the system should use security controls. Robust security means, besides product features, enabling and using the available features and also enforcing their use by company policies. Adequate training is also needed for the personnel accessing and using the system.

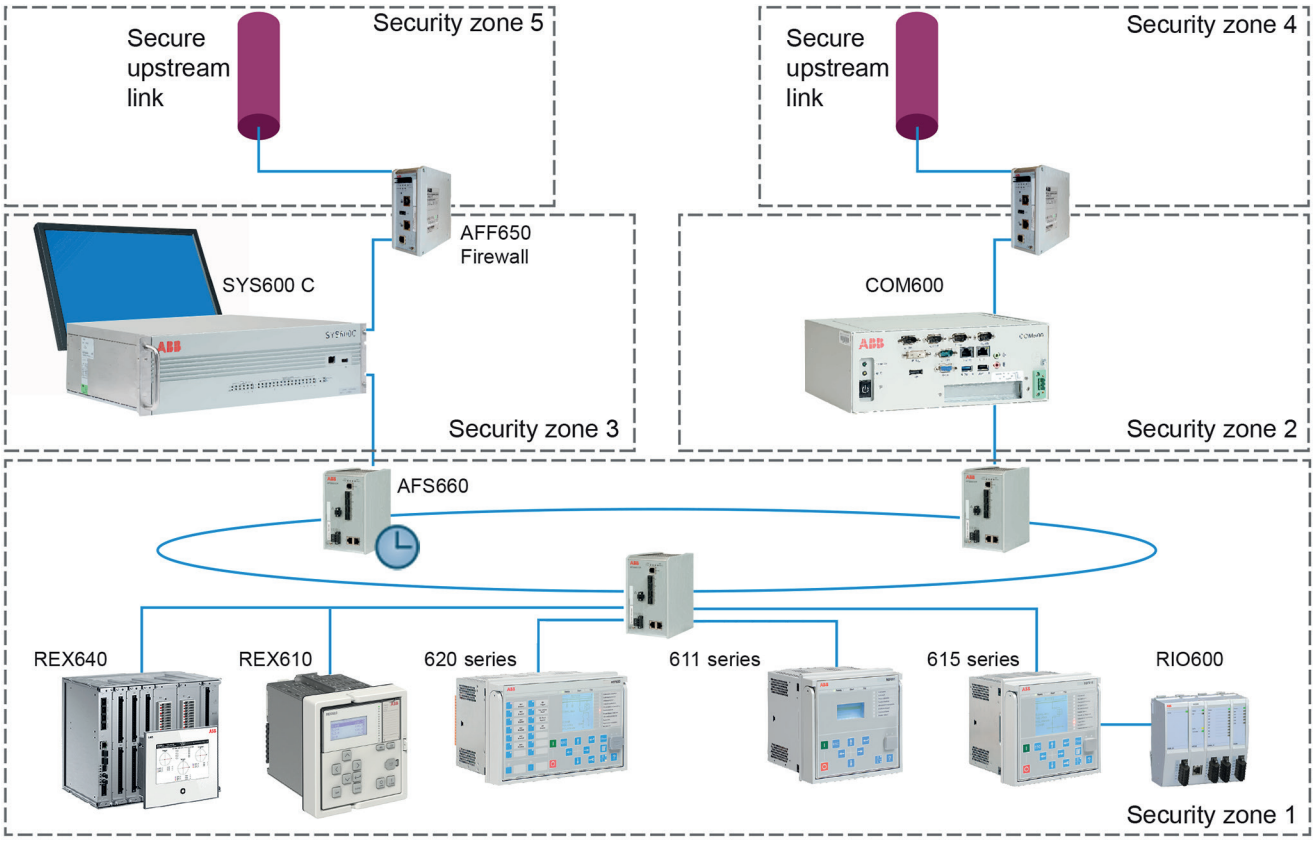

Figure 1: Distribution substation example

3.2 System overview

M2M Gateway ARM600 is a member of ABB's Arctic product family. ARM600 is a communication server, a VPN concentrator and firewall, and is typically placed within the same location as the central control and monitoring system, such as SCADA. ARM600 manages all Arctic 600 series wireless gateway connections and is the main interface between the field devices and the central control and monitoring system. Connection between Arctic and ARM600 is typically established via cellular network and VPN.

ARM600SW is a software-only version of ARM600 with additional features such as a faster update cycle via a dedicated software repository and capability to be run in virtual machine environment.

Arctic 600 series provides wireless connection of field devices via cellular network from a central site or control center. The devices offer industrial quality connectivity for TCP/IP based protocols. Wireless Gateway ARG600 exhibits integrated communication capability and seamless integration to SCADA systems using ARM600 VPN and management services.

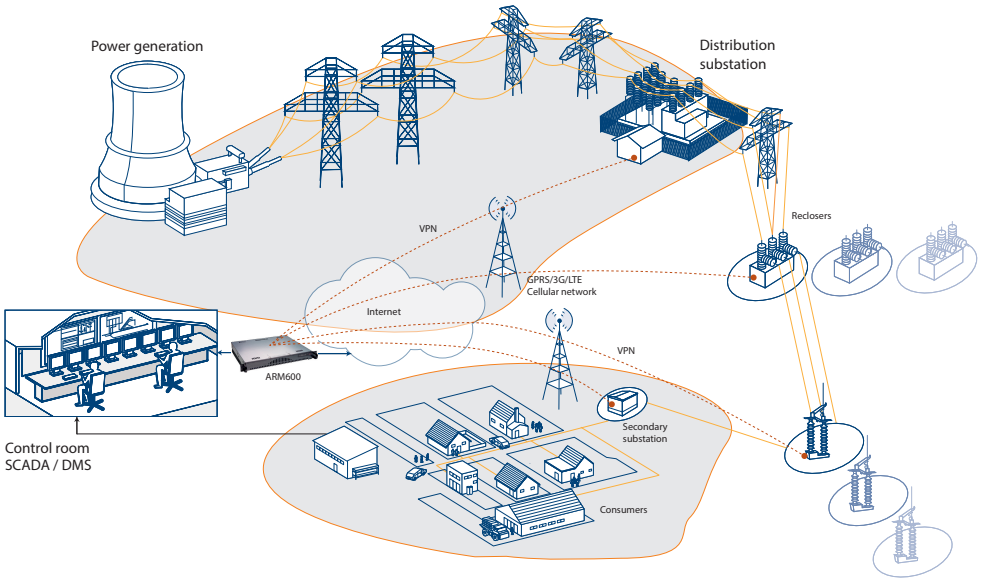

Figure 2: Communication solution in distribution automation

Section 4 Arctic 600 series

4.1 Communication interfaces

Arctic devices have three communication ports that can be disabled from configuration.

- LAN (Ethernet) port
- Cellular
- Serial ports

The dual SIM models have two additional ports.

- Console port
- WAN port

4.2 Serial port based protocols

The physical Console port on the Arctic wireless devices provides authenticated terminal login to Linux shell.

The physical Serial ports have individually configurable applications (Serial Gateway, SMS Modem, IEC-104 Gateway and Modbus Gateway). In the gateway applications, the serial data is tunnelled or relayed to the remote TCP/UDP connection endpoint.

If SMS Modem is enabled as an application on one of the serial ports, it allows unauthenticated access to the Arctic device’s internal modem.

4.3 TCP/IP based protocols and used IP ports

IP port security depends on specific installation, requirements and existing infrastructure. The required external equipment can be separate devices or devices that combine firewall, router and secure VPN functionality. When the network is divided into security zones, it is done using either substation devices with firewall functionality or dedicated firewall products. Security zone boundaries are inside the substation or between the substation and the outside world.

Table 1: Available IP ports

Port number	Type	Default state	IPv4	IPv6	Description
22	TCP	Open	Yes	Yes	SSH
443	TCP	Open	Yes	Yes	Web HTTPS (WHMI)
53	TCP/UDP	Open	Yes	No	DNS Proxy
2404	TCP	Open	Yes	No	IEC-104 (model dependant)
7001	TCP	Open	Yes	No	Serial GW
7003	TCP	Open	Yes	No	Serial GW
5355	UDP	Open	No	Yes	LLMNR
5353, 32768...61000	UDP	Open	Yes	Yes	mDNS

4.4 Secure communication

Arctic devices support encrypted communication to user configuration via HTTPS (WHMI) and SSH protocols. All other communications into the device are recommended to be used via a VPN tunnel.

4.4.1 Certificate handling

For encryption and secure identification of WHMI (HTTPS protocol) the device uses public key certificates that bind together a public key with an identity, that is, information such as the name of an organization, their address and so on. The server certificate used by the device is generated by the device itself as a self-signed certificate and not issued by any certification authority (CA).

Certificates use encryption to provide secure communication over the network. A self-signed X.509 certificate is generated by the device.

The certificate is used to verify that a public key belongs to an identity. In case of HTTPS, the WHMI server in the device presents the certificate to the Web client giving the client the public key and the identity of the server. The public key is one part of an asymmetric key algorithm in which one key is used to encrypt a message and another key is used to decrypt it. The public private key pair (asymmetric key) is used to exchange the symmetric key, which is used to encrypt and decrypt the data that is exchanged between server and client.

For WHMI use, the certificate signed by the device must be accepted in the Web browser when opening the connection to WHMI. The Web browser displays a warning because the WHMI uses self-signed certificates.

4.4.2 Virtual private networks

The virtual private networks are used, for example, in extending or routing the company's local area network to the remote site using publicly available media such as the Internet. The Arctic system VPN tunnel implementations are SSH-VPN, L2TP-VPN and OpenVPN. The first two are proprietary implementations providing a link between the M2M gateway and the cellular gateways, while the third can be used for connecting also third-party devices, such as computers, to the M2M gateway for administration or control purposes.

The implementation of the VPN defines certain security characteristics. Thus, they can be listed in order from strongest to weakest security in M2M solution:

- OpenVPN
- SSH-VPN
- L2TP-VPN

L2TP-VPN does not offer encryption of traffic. When connected to public networks, it is recommended to use OpenVPN.

OpenVPN is the only recommended option.

4.4.3 SNMPv3

SNMP agent does not force encryption. Although encryption is enabled in the SNMP agent settings, a client can still connect without encryption.

4.5 Web HMI

WHMI is one of the available user access services in the device. The service is enabled by default and the HTTPS TCP port is open for connections.

For the HTTPS access, the Web client must support HTTPS via TLS 1.1/1.2. The WHMI is verified with Internet Explorer 8.0, 9.0, 10.0 and 11.0. The recommend connection setting is TLS 1.2.

4.6 Security

Certain measures should be taken to enhance operator and subscription security.

- Network subscription and SIM card must be stored safely and configured to prevent misuse of services.
  - Unused services should be disabled from SIM cards.
    - Voice calls
    - SMS
    - Paid services
    - Roaming
  - Pin code should be used in SIM cards.
- A private APN service from the operator should be preferred.
- M2M subscription SIM cards from the operator should be preferred.
- Private IP addressing from the operator for cellular network based communications should be used.
- If connected to a public IP network, plain text protocols such as http, SNMP and telnet should not be used. Instead, VPN should always be used to connect to the device.

4.7 Firewall

The Arctic wireless devices have internal firewalls. By default the Arctic firewall is enabled and the default rules for standard traffic are applicable. For optimal security, the recommended approach is to limit the allowed packets, if possible. The firewall should be set to drop all packets via the WHMI path **Firewall/ Generic/Default Actions** and then to allow the needed packets, the most frequent packets appearing first in the list. User-defined filtering tables are available for the Filter Incoming, Filter Forwarded and Filter Outgoing packets under **Network/ Firewall**. Generic rules are applied before the user-defined filtering tables.

The current firewall status can be monitored via **System/Status/Firewall**. More detailed information on the firewall rules can be obtained from **Tools/Support log**.

All the firewall rules under **Firewall/General** are applied before the user-defined rules in Filter Incoming, Filter Forwarded and Filter Outgoing. If the generic rules are used to allow traffic, the user-applied rules cannot block the same traffic allowed by the generic rules.

4.7.1 Configuring firewall

With firmware version 3.4.9 or older and a certain ABB Arctic wireless gateway configuration, the Ethernet-connected devices in

the Arctic wireless gateway's LAN may access the Internet even though the VPN routing is set to "Default route".

The default route via a VPN tunnel is only active while the VPN tunnel is up. While the VPN tunnel is down, the LAN clients have access to the Internet with the default firewall settings of Arctic wireless gateway. If this behavior is unwanted, configure the firewall using the WHMI.

1. In the left pane, under **Firewall**, click **General**.
2. Ensure that the firewall's default action for forwarded packets is "Drop" (default setting). If not, check the necessary firewall rules for allowing the forwarded traffic before changing the default action to "Drop".
3. Set the *LAN-Out accepted* rule to "No".

The *LAN-Out accepted rule* ("Yes"/"No") under **Firewall/General** is ineffective when the firewall's forward table default action is set to "Pass".

4. Submit the changes and reboot the device.

The "Yes"/"No" rules under **Firewall/General** depend on the firewall's default drop actions in the input and forward tables. Set the firewall's default actions for incoming and forwarded packets to "Drop", and check the firewall rules for allowing the necessary incoming and forwarded traffic.

4.8 User management

Arctic devices have three user accounts. The credentials for arctic-adm user and the password for root user can be changed via **WHMI Tool/User Config**. The restricted shell credentials can be changed via **WHMI Tool/Restricted Shell**.

Table 2: Arctic user accounts

Username	Password	Interface	Enabled by default
root	arct1cemt0em	Console, su	Yes
arctic-adm	arcticm2m	Console, WHMI, SSH	Yes
arctic-user	arcticm2m	SSH (restricted shell)	No

4.9 Backup files

Backup of the current Arctic device configuration can be downloaded via **Tools/ Configuration Profiles/Export** by selecting the active profile.

If Arctic Patrol is used and the *Backup active configuration to server* parameter, found via menu path **Services/Patrol**, is enabled, the device automatically transfers the configuration to the patrol server located in ARM600.

4.10 Restoring administrator password

If authentication is enabled in the device and the administrator password is lost, it is no longer possible to change passwords or operate the device with full access rights.

- Contact ABB technical customer support to retrieve back the administrator level access to the device.

Section 5 ARM600

5.1 Communication interfaces (only for ARM600 hardware variants)

ARM600 has two or four Ethernet communication ports that can be disabled from configuration via WHMI path **Network /Network Configuration**.

- LAN (Ethernet) ports Gb1 and Gb2 in the standard edition
- LAN (Ethernet) ports Ethernet 1, Ethernet 2, Ethernet 3 and Ethernet 4 in the enterprise edition

ARM600 can be accessed also locally via the VGA display and USB keyboard.

5.2 TCP/IP based protocols and used IP ports

IP port security depends on specific installation, requirements and existing infrastructure. The required external equipment can be separate devices or devices that combine firewall, router and secure VPN functionality. When the network is divided into security zones, it is done using either substation devices with firewall functionality or dedicated firewall products. Security zone boundaries are inside the substation or between the substation and the outside world.

Table 3: Available IP ports

Port number	Type	Default state	IPv4	IPv6	Description
22	TCP	Open	Yes	No	SSH-VPN, Patrol Server
10022	TCP	Open	Yes	No	SSH
10000	TCP	Open	Yes	Yes	Web HTTPS (WHMI), Patrol Server
443	TCP	Open	Yes	No	Web Server HTTPS
1701	UDP	Closed	Yes	No	L2TP-VPN
1194...1200	UDP/TCP	Closed	Yes	No	OpenVPN

5.3 Secure communication

Arctic devices support encrypted communication to user configuration via HTTPS (WHMI) and SSH protocols. All other communications into the device are recommended to be used via a VPN tunnel.

5.3.1 Certificate handling

For encryption and secure identification of WHMI (HTTPS protocol) the device uses public key certificates that bind together a public key with an identity, that is, information such as the name of an organization, their address and so on. The server certificate used by the device is generated by the device itself as a self-signed certificate and not issued by any certification authority (CA).

Certificates use encryption to provide secure communication over the network. A self-signed X.509 certificate generated by the device.

The certificate is used to verify that a public key belongs to an identity. In case of HTTPS, the WHMI server in the device presents the certificate to the Web client giving the client the public key and the identity of the server. The public key is one part of an asymmetric key algorithm in which one key is used to encrypt a message and another key is used to decrypt it. The public private key pair (asymmetric key) is used to exchange the symmetric key, which is used to encrypt and decrypt the data that is exchanged between server and client.

For WHMI use, the certificate signed by the device must be accepted in the Web browser when opening the connection to WHMI. The Web browser displays a warning because WHMI uses self-signed certificates.

5.3.2 Virtual private networks

The virtual private networks are used, for example, in extending or routing the company’s local area network to the remote site using publicly available media, such as the Internet. ARM600 offers VPN tunnel server implementations SSH-VPN, L2TP-VPN and OpenVPN. The first two are proprietary implementations providing a link between ARM600 and the Arctic cellular gateways, while the third can be used also for connecting third-party devices, such as computers, to the M2M gateway for administration or control purposes.

The implementation of the VPN defines certain security characteristics. Thus, they can be listed in order from strongest to weakest security in M2M solution:

- OpenVPN
- SSH-VPN
- L2TP-VPN

L2TP-VPN does not offer encryption of traffic. When connected to public networks, it is recommended to use OpenVPN.

OpenVPN is the only recommended option.

5.3.3 OpenVPN server

OpenVPN is the most recommended VPN type between the Arctic and ARM600 devices. ARM600 supports OpenVPN in two different modes.

- Normal (Layer 3, IP)
- Bridge (Layer 2)

Normal (Layer 3, IP) is the most common mode. In this mode the IP routing is used to communicate with OpenVPN clients that are typically Arctic devices. By default, the OpenVPN clients connected to the same server are allowed to communicate with each other. This can be limited by changing the OpenVPN server and firewall configurations.

In the default configuration, the ARM600 firewall cannot limit the IP connections between OpenVPN peers connected to the same OpenVPN server.

When a new ARM600 OpenVPN server is created, it uses self-signed certicates, with an expiry time of 10 years, for authentication. It is recommended to use certificates with RSA 2048-bit with SHA-2 digital signature algorithm for all the devices using OpenVPN server.

When the OpenVPN client or server certificates have expired, the remote Arctic devices cannot establish an OpenVPN connection. Check the certificate expiry dates and renew the certificates from **VPN/OpenVPN**. OpenVPN certificates can be renewed in ARM600 Ver.4.4.1 or later.

5.3.4 Time synchronization

By default ARM600 synchronizes the clock via NTP from centos.pool.ntp.org. It is recommended to set the NTP synchronization to local stratum 1 clock.

5.3.5 Patrol server

Patrol server is used remotely for the updating and managing of a large group of Arctic devices (batch updates). The Arctic Patrol Client connects to ARM600 either using the SSH protocol running in port 22 or the HTTPS protocol running in port 10000. It is recommended to limit access to these ports with a firewall, for example, by introducing allowed IP address ranges.

5.3.6 SSH-VPN server

By default the ARM600 SSH-VPN server is enabled in port 22. This port is shared with Arctic Patrol if SSH is used as a Patrol protocol. It is recommended to allow only SSH Protocol version 2 and to limit access to these ports with a firewall, for example, by introducing allowed IP address ranges.

In ARM600 Ver.4.4.1 or later support for SSHv1 has been disabled. The SSH legacy mode might be activated automatically on backup restore or when the update installer is used. A notification is shown at the top of the screen if legacy mode is activated.

The SSH legacy mode is enabled only if SSHv1 support was previously activated (SSH-VPN settings) and at least one active SSH-VPN client or Patrol connection uses SSHv1 keys.

5.3.7 SSH server (admin)

By default the ARM600 SSH for administration server is enabled in port 10022. It is recommended to limit access to port 10022 with a firewall, for example, by introducing allowed IP address ranges. The SSH service can be disabled by issuing command `systemctl disable sshd-admin`.

5.3.8 IPv6

ARM600 uses a link-local address (IPv6 unicast address) that is automatically configured using the link-local prefix FE80::/10. By default the IPv6 firewall blocks the incoming connections, except for ICMP. The IPv6 firewall rules can be issued with the `ip6tables-save` command.

The default rules for IPv6 firewall are:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [7:460]
-A INPUT -i lo -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -p tcp -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
COMMIT
```

Contact ABB's technical support to disable the IPv6.

5.4 Web HMI

WHMI is one of the available user access services in the device. The service is enabled by default and the HTTPS TCP port 10000 is open for connections.

For the HTTPS access, the Web client must support HTTPS via TLS 1.1/1.2. The WHMI is verified with Internet Explorer 8.0, 9.0, 10.0 and 11.0. The recommend connection setting is TLS 1.2.

5.5 Security

To ensure the highest security, ARM600 should be installed behind a firewall, for example, in company DMZ zone.

ARM600 in the company's DMZ

The DMZ is a safe subnet, separated by firewalls from the company LAN and from the Internet. The servers requiring accessibility from the Internet are placed in the DMZ. The company's border router/firewall forwards the VPN port from the public IP to ARM600, which has a private IP address and uses the border router as a default gateway.

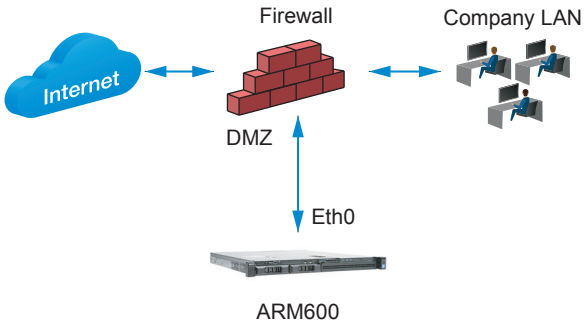

Figure 3: DMZ installation

ARM600 has an internal firewall (iptables) which should be enabled also when the external firewall is used. For the highest security, customized firewall (iptables) rules should be applied according to the network setup. The ARM600 custom firewall rules are available in the ARM600 WHMI via **Firewall /Custom rules**. All access to ports should be limited as much as possible by allowing access only

from known remote network IP or interface and by allowing incoming connections only to the available ports.

5.6 User management

The first user must be created immediately after connecting the system to the network. The first created user gets admin privileges by default. For information on how to create users for ARM600, see the user manual.

5.7 Backup and Auto backup

During the system backup and restore or update it is possible that the user home directories are deleted and recreated. Any information stored in the user home directories is erased during the process.

Backup of the current ARM600 configuration can be generated via **Tools/Backup/Create Backup**.

Backup is used to create and restore backups and upload/download them from/to a PC. ARM600 contains a factory backup that can be used for reverting to the factory configuration. However, the IP addresses of network interfaces are not reverted to factory defaults. Both standard backup and full backup are configuration backups and they cannot be used for full disaster recovery.

Auto backup is used to configure ARM600 to back up the configuration to an additional standby ARM600. The data transfer method is rsync over SSH.

Starting from version 5.0.1, backups use a dedicated service user account for improved cybersecurity.

Table 4: Compatibility between source and target systems in auto backups

Source system	Target system	Compatibility
4.5.3 or older	Fresh installation of 5.0.1	Incompatible Starting from 5.0.1, there is no default user anymore, which prevents using older auto backup targets.
4.5.3 or older	4.5.3 first updated to 5.0.1 with the “update installer” script	Incompatible Starting from 5.0.1, there is no default user anymore, which prevents using older auto backup targets.
5.0.1	4.5.3	Compatible Target address for the auto backup requires the username, for example, "arctic-adm@10.10.10.10".

Section 6 Glossary

APN	Access Point Name
BDEW	Bundesverband der Energie- und Wasserwirtschaft
CA	Certification authority
DMZ	De-militarized zone
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DNS	Domain Name System
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEC 60870-5-104	Network access for IEC 60870-5-101
IEC 61850	International standard for substation communication and modeling
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet protocol
IP address	A set of four numbers between 0 and 255, separated by periods. Each server connected to the Internet is assigned a unique IP address that specifies the location for the TCP/IP protocol.
IPv6	Internet protocol version 6
ISO	International Standard Organization
LAN	Local area network
M2M	Machine to machine
NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection
NTP	Network time protocol
SCADA	Supervision, control and data acquisition
SIM	Subscriber identity module
SMS	1. Short Message Service

	2. Station monitoring system
SNMP	Simple Network Management Protocol
SSH	Secure shell
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	An Internet protocol that allows logging on to a remote computer using a user name and password
TLS	Transport layer security
UDP	User datagram protocol
VPN	Virtual Private Network
WHMI	Web human-machine interface

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

abb.com/mediumvoltage

1MRS758860 F