Security Rules

Securing Saia PCD®

Saia PCD® are networked products and as such must have its security correctly configured to reduce the risk of unauthorized access. For general information about securing SBC products see the «General Security Best Practice for SBC IP Based Products Information Sheet».
In addition to the actions described in the «General Security Best Practice for SBC IP Based Products Information Sheet» the advice described in the following sections must be followed.
Adopting normal installation and security best practice guidelines can mitigate the risk of a malicious IT attack from a skilled and equipped IT individual.

Security Checklist

- ☐ All related Saia PG5® projects including all depending libraries are included in the disaster recovery plan.
- ☐ Physical access to Saia PCD® is restricted.
- ☐ Physical access to networks connected to Saia PCD® is restricted.
- ☐ All SBC PCDs are running latest release of firmware.
- ☐ Ethernet network secured – see «Network Planning and Security».
- ☐ All unused services, ports and communication channels are deactivated.
- ☐ Non-guessable user names and strong passwords are set.
- ☐ Users on Saia PCD® are only given the least required privileges.

Developing a Security Program
Refer to the «General Security Best Practice for SBC IP Based Products Information Sheet».

Disaster Recovery Planning
When developing the disaster recovery plan you must ensure that all relevant Saia PG5® project files and all libraries to rebuild the project are include.

Physical and Environmental Consideration
Saia PCD® must be installed within a locked environment e.g. located in a secured plant room, or a locked cabinet.
Note: Ensure adequate ventilation.

Security Updates and Service Packs
Ensure all Saia PCD® are running the latest release of firmware especially on internet facing systems.

Virus Protection
Not applicable to Saia PCD®.

Network Planning and Security

Ethernet Network
It is recommended that the Ethernet network used by Saia PCD® is separated from the normal office network using an air gap, or virtual private network.
Physical access to the Ethernet network infrastructure must be restricted.
You must also ensure that the installation complies with your company's IT policy.
Saia PCD® must not be connected directly to the Internet. The devices shall be deployed securely behind a firewall or in a virtual private network with strong password protection and cyber security protocols to minimize the risk of unauthorized access.

MS/TP Network
Physical access to the MS/TP network infrastructure must be restricted.

RS-485 Network
Physical access to RS-485 network infrastructure must be restricted.

Profi-S-Bus Network
Physical access to Profi-S-Bus network infrastructure must be restricted.

CAN Network
Physical access to CAN network infrastructure must be restricted.

USB
Physical access to Saia PCD® USB port must be restricted.

RS-232 (PGU)
Physical access to Saia PCD® RS-232 (PGU) port must be restricted.

I/O Bus
Physical access to the Saia PCD® I/O bus must be restricted.

I/O Extension Port
Physical access to the Saia PCD® I/O extension port must be restricted.

Services
Disable all services which are not used. This reduces the attack surface and may increase the performance of a Saia PCD® system.

Web Server
Some Saia PCD® provide a HTTP web server which may listen on up to two TCP ports. It is recommend that both listening ports are disabled. If a web server is required then the make sure that the web server is protected by a strong password and that firewall rules are in place to protect against unwanted access.
Note that it is possible to access the file system of a Saia PCD® using HTTP using FTP credentials. If the HTTP server is active ensure that FTP user have non-guessable user names and strong passwords.

FTP Server
Some Saia PCD® provide an FTP file server. It is recommend to disable the FTP server. If a FTP server is required then the make sure that the FTP server is protected by using non-guessable user names and strong passwords.

BACnet IP
Due to the insecure nature of the BACnet protocol Saia PCD® that support BACnet IP MUST not be connected to the Internet under any circumstance. The Saia PCD® security system does not protect against BACnet writes. Physical access to the BACnet IP network infrastructure must be restricted. If BACnet IP communications are not required the BACnet IP Network configuration in the Saia PG5 Device Configurator must be disabled.

SNMP Server
Some Saia PCD® provide an SNMP server. The access to the SNMP server is without authentification. It is recommended to disable the SNMP server. If a SNMP server is required then the Saia PCD® device MUST not be connected to the Internet under any circumstance. In addition the SNMP configuration in Saia PG5 Device Configurator must be done to allow only limited access.

IP Filtering
Saia PCD® allow white- and blacklisting of IP addresses to grant and deny access to the system. It is recommended that this service is enabled to provide an additional layer of security.

Virtual Environments
Not applicable to Saia PCD®.

Securing Wireless Devices
If a wireless network is being used it must be secured according to your company's IT policy.

System Monitoring
Not applicable to Saia PCD®.

Windows Domains
Not applicable to Saia PCD®.

General security Best Practice for SBC IP based products

The following guidelines are in order of increasing mitigation. The exact requirements of each site should be assessed on a case by case basis. The vast majority of installations implementing all the mitigation levels described below will be far in excess of that required for satisfactory system security. Incorporating the first four items relating to Local Area Networks will generally meet the requirements for most automation control network installations.

Local Area Networks (LAN) incorporating Saia-Burgess Controls AG components
Ensure the systems operates on an appropriate password policy for user access to all services this guideline would include, but not limited to:
- The use of strong passwords
- A recommended password cycle time
- Unique user names and passwords for each user of the system
- Password disclosure rules

Prevent unauthorized access to the network equipment that is used in conjunction with systems provided by Saia-Burgess Controls AG. With any system, preventing physical access to the network and equipment reduces the risk of unauthorized interference. Security best practice with IT installations would ensure that the server rooms, patch panels and IT equipment are in locked rooms. Saia PCD® equipment should be installed within locked control cabinets, themselves located in secured plant rooms.

When completing commissioning of the following:
- Saia PCD® – ensure the device is password protected. Ensure appropriate user levels are assigned for the site users.
- Visi.Plus – ensure the system is password protected. Ensure appropriate user levels are assigned for the site users, from an administrator user, through to general user. It is best practice to disable the access rights for the guest user account.

Adopt an appropriate update policy for the infrastructure installed at the site as part of a service level agreement. This policy should include, but is not limited to, updating the following system components to the latest release:
- Devices firmware for controller, RIO, HMI, etc.
- Supervisor software, such as Visi.Plus software
- PC/Server operating systems
- Network infrastructure and any remote access systems

Configure separate IT networks for the automation control systems and the customer's corporate IT Network. This may be achieved by configuring VLAN's (Virtual LAN's) within the customer's IT infrastructure or by installing an air-gapped separate network infrastructure dedicated to the automation control systems.

Once the system has been commissioned, restrict IP traffic on the automation control network (for example using access lists) to the types of protocols required for normal operation, i.e. S-Bus, BACnet, etc…
Further information regarding the communications traffic required for normal operation can be found in the product documentation.

When interfacing with Saia PCD® using a centralized system supervisor (e.g. Visi.Plus) and where the system does not require direct access to the individual devices web server, the network infrastructure should be configured to restrict web server access.

Dynamic VLANs using MAC address allocation can protect against the un-authorized connection of a device into the system and can reduce the risk associated with an individual monitoring information on the network.

For Remote Access to IT based Building Control systems
- If remote access is required into Saia PCD® systems, use VPN (Virtual Private Network) technology to reduce the risk of data interception and protect the controls devices from being directly placed on the internet.
- The SBC.Connectivity product is a managed connectivity solution, which facilitates mobile communications such as GPRS, 3G, etc. and wired communication to remotely connect to Saia PCD®. The service provides a secure network that provides simple VPN access to the devices.

Customers adopting normal installation and security best practice guidelines can mitigate the risk of a malicious IT attack from a skilled and equipped IT individual. Further information can be found in the specific product documentation.

Saia-Burgess Controls AG
Bahnhofstrasse 18 | 3280 Murten | Switzerland | www.saia-pcd.com
T +41 26 580 30 00 | F +41 26 580 34 99
support@saia-pcd.com | www.sbc-support.com

International Represetatives & SBC Sales Companies:
www.saia-pcd.com/contact
PP26-620 11.2015 ENG01