UniSAB 4
Hardening Guide

GPS0055-CE-EN
Version 1.0
Rev A
Revised 2025-04-22

Johnson Controls

Introduction

Our practices provide peace of mind for our customers with a holistic cyber mind set beginning at initial project design concept, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

This hardening document intends to provide cybersecurity requirements used in planning, deployment, and maintenance periods for the UniSAB 4 compressor control unit solution.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution’s functional operation.

This guide provides hardening requirements for configuration and maintenance, including the user accounts, and patch management.

1. Planning	2. Deployment
Define the scope, and identify security features, along with the characteristics of the associated components	Select the required hardening steps based on the products and security features of the target system components

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

1 Planning

This section helps plan for the implementation of security requirements for the UniSAB 4 Compressor Control Unit solution.

1.1 UniSAB 4 Compressor Control Unit Solution overview

The UniSAB 4 Control unit is responsible for the real time control of an industrial chiller, heat pump, or compressor unit. The purpose of the unit is to continuously monitor the active states of the machine, react to changes in the environment, machine faults, or user defined setpoints, making sure that the required thermodynamic properties are always being delivered.

<u>Main Features</u>

- Compact mechanical design, compatible with the predecessor (UniSAB III)
- I/O compatible with the predecessor (UniSAB III)
- Backward compatible industrial fieldbus support,
  making retrofitting at sites with existing SCADA/PLC applications easy
- Can be operated as a standalone controller
- The controller is equipped with 10” color touch screen, for local HMI (Human Machine Interface) interaction
- The HMI is available to all devices, with a modern browser, that is connected to the same LAN
- Can coordinate the capacity delivery, across several UniSAB III/4 controlled compressors, with the built in MultiSAB++ distributed control system, no PLC or custom code required.

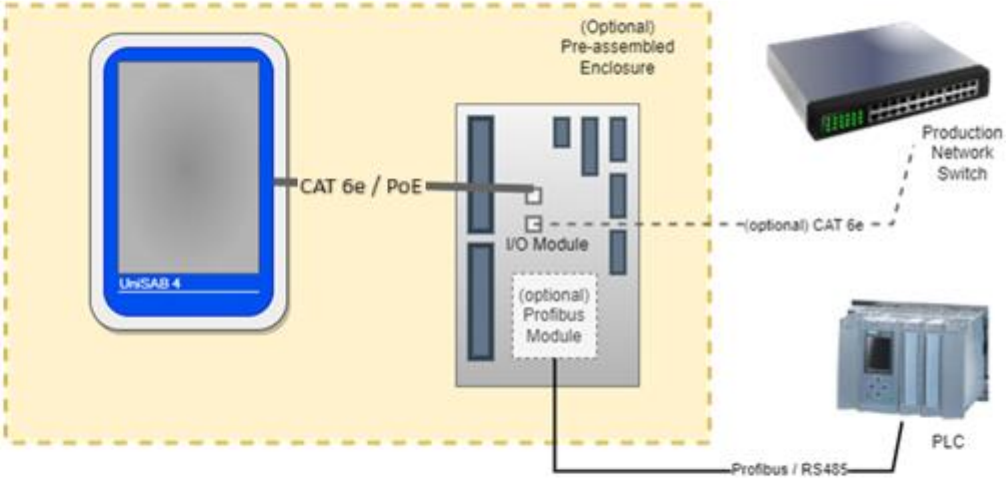
1.1.1 Deployment architecture

The UniSAB 4 Controller exists in two form factors, which includes the same base hardware.

- <u>Cassette version</u>. In this form, the UniSAB 4 is pre-assembled in an enclosure.
- <u>Panel Mount version</u>. In this form, the UniSAB 4 is shipped where each component can be installed in an electrical cabinet, requiring post-mount assembly.

The electrical connections required for deployment are the same, regardless of the form factor, as shown in figure 1.1.1.1 on the next page.

Figure 1.1.1.1 Deployment Architecture Hardware Perspective



Use Cases for the UniSAB4. The UniSAB 4 is designed to be operable as a stand-alone controller or integrated into a network. Basic operation in a stand-alone configuration does not require ethernet or fieldbus connections; only a local PoE connection to the UniSAB 4 and the I/O module. However, if the controller is to be integrated, these connections will be used and will need to be hardened. Over the next few pages, we will cover these common use cases for UniSAB 4:

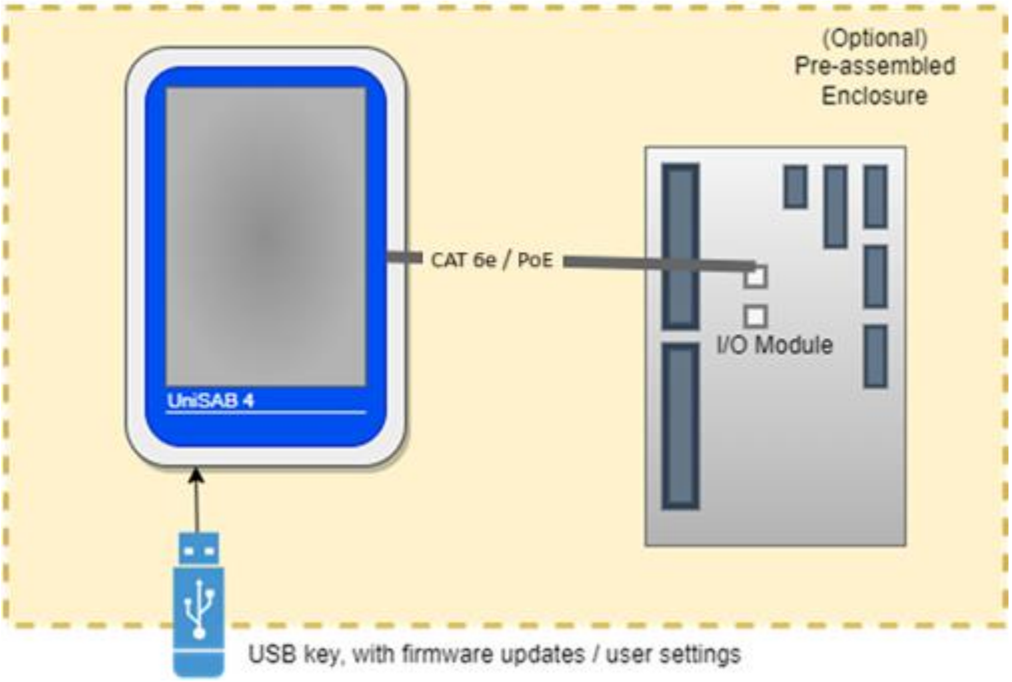
Table 1.1.1.1 Use Cases for UniSAB4

Use Case	Description	Recommended use
1	Standalone Controller maintains a Constant Reference	Touch screen (local)
2	Controller Integrated with PLC, only via Profibus	Touch screen (local)
3	Controller Integrated via Profibus and Open Blue	Production or Control system
4	Controller Integrated via Isolated Production Network	Local, Fieldbus data, Air-gapped
5	Controller Integrated via Internal Production Network	Local, Fieldbus data, Mobile
6	Controller on Production Network, with OpenBlue	Production with OpenBlue
7	Controller on Production Network	Production, Mobile
8	Controller is Online	Mobile

Note: Use case descriptions below include basic details about integration with OpenBlue where applicable. For more information on hardening OpenBlue in the above use cases, refer to the specific **OpenBlue Hardening Guide** at the following link - https://www.johnsoncontrols.com/trust-center/cybersecurity/resources.

UniSAB 4 Use Cases

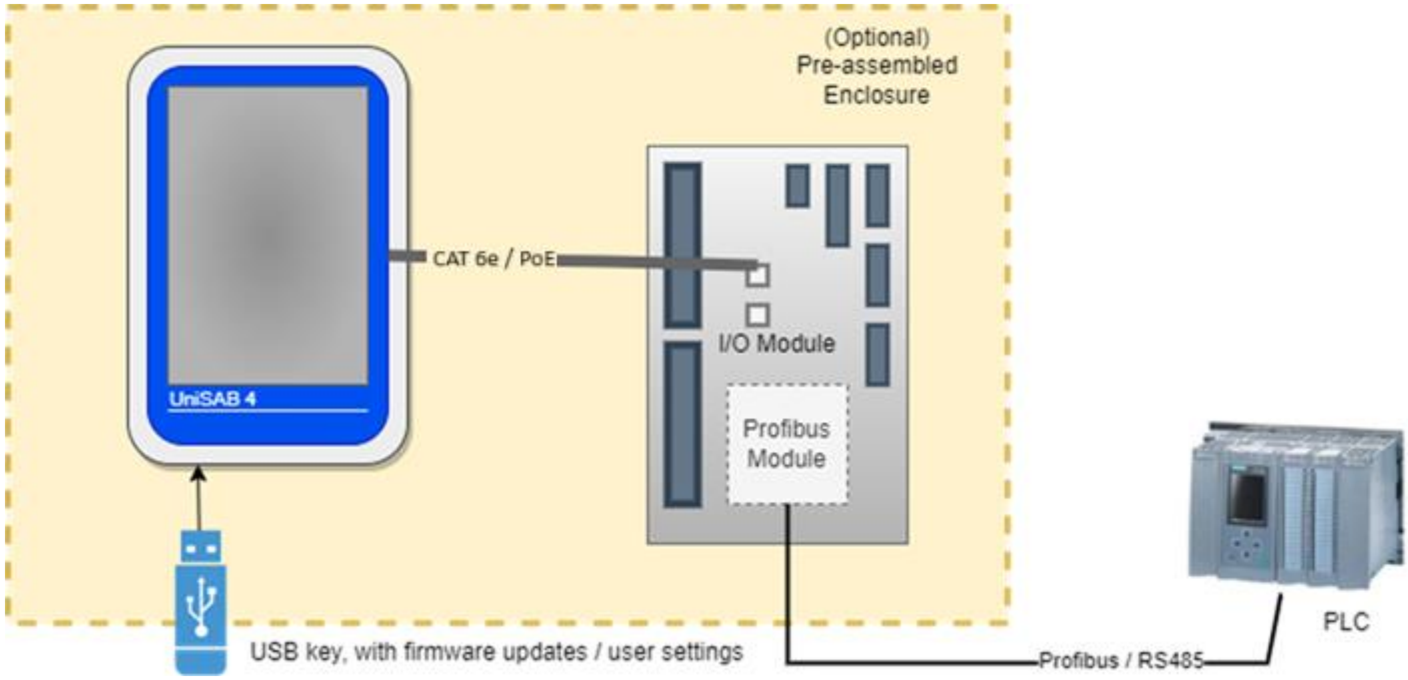
Use Case 1 – Standalone Controller Maintains a Constant Reference



Features and best uses:

- Installations where a technician operates the refrigeration system via touch screen only
- When the system is expected to maintain a constant temperature or pressure, based on the technician's reference adjustments
- Does not show nor require network connections
- Requires a USB key to backup user settings or update the firmware.
  See additional details on this process in Section 2.

Use Case 2 - Controller Integrated with PLC, only via Profibus

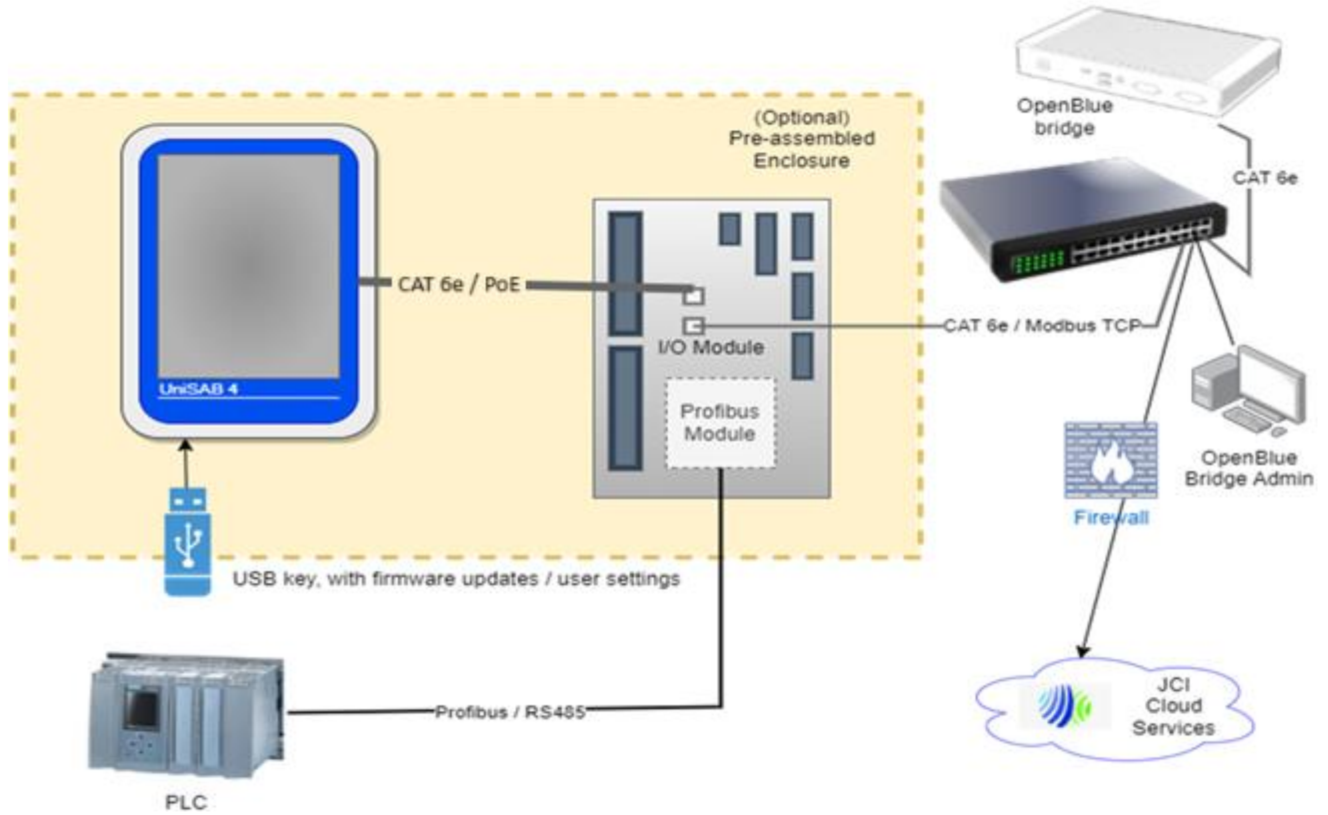


Features and best uses:

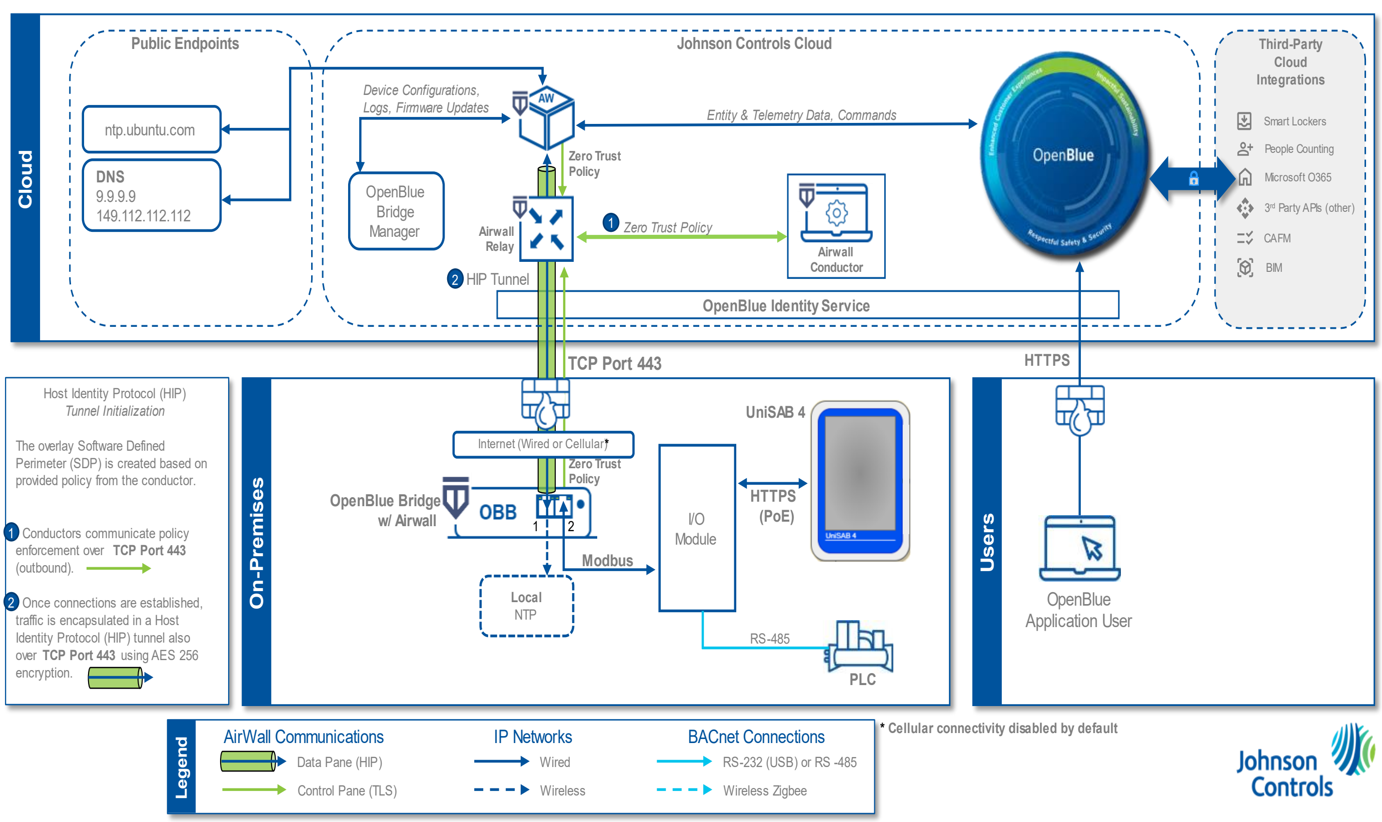
- A production system, or environmental control system, is implemented on a PLC with Profibus, and there is no other network connected to the UniSAB 4 controller
- The Profibus connection will allow the PLC to set references, change settings, and do almost anything that a supervisor user can do via the local HMI (described in section 1.1)
- Does not show nor require network connections
- Requires a USB key to backup user settings or update the firmware

Note: If more than one controller exists, consider setting up an internal production network, to avoid the need for USB keys.

Use Case 3 - Controller Integrated via Profibus and Open Blue



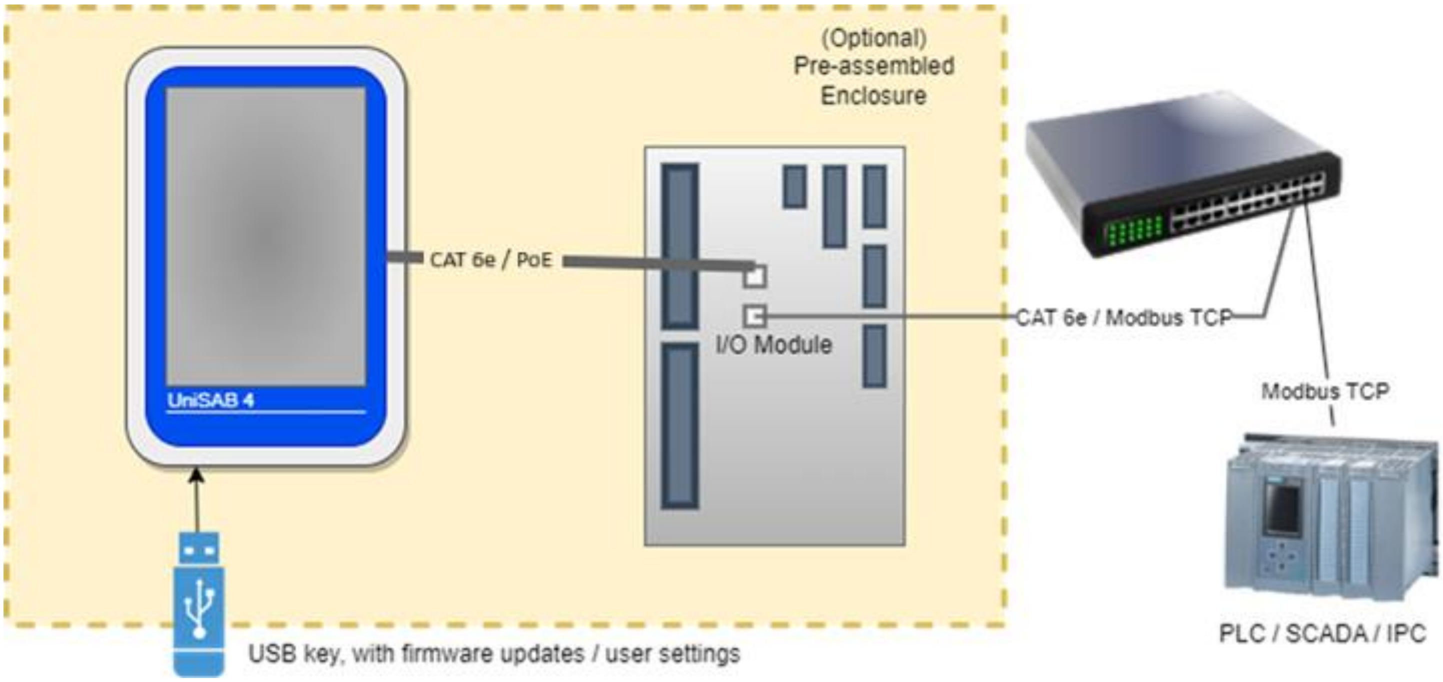
OpenBlue Architecture – IT / Security Overview



Features and best uses:

- A production system or environmental control system is implemented on a PLC with Profibus with no other *local* need for a connected network
- Network is installed to support JCI OpenBlue (Doesn't use network connections)
- Requires a USB key to backup user settings or update the firmware

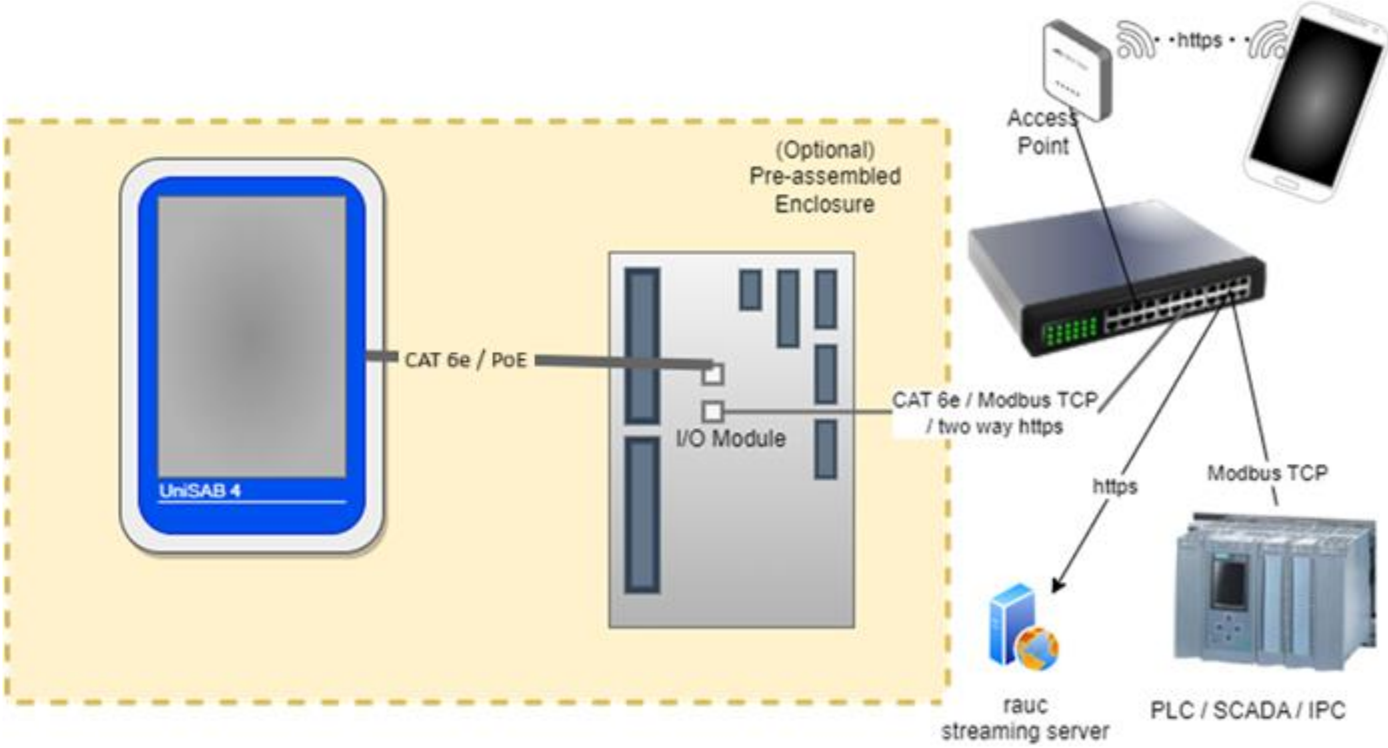
Use Case 4: Controller Integrated via Isolated Production Network



Features and best uses:

- A production system, or environmental control system, is implemented on a PLC with Modbus TCP
- A local production network is installed to support production fieldbus data. In this setup the production network is considered air-gapped from other networks.
- Network is used as a carrier for Modbus (not for TCP/IP ethernet)
- Requires a USB key to backup user settings or update the firmware

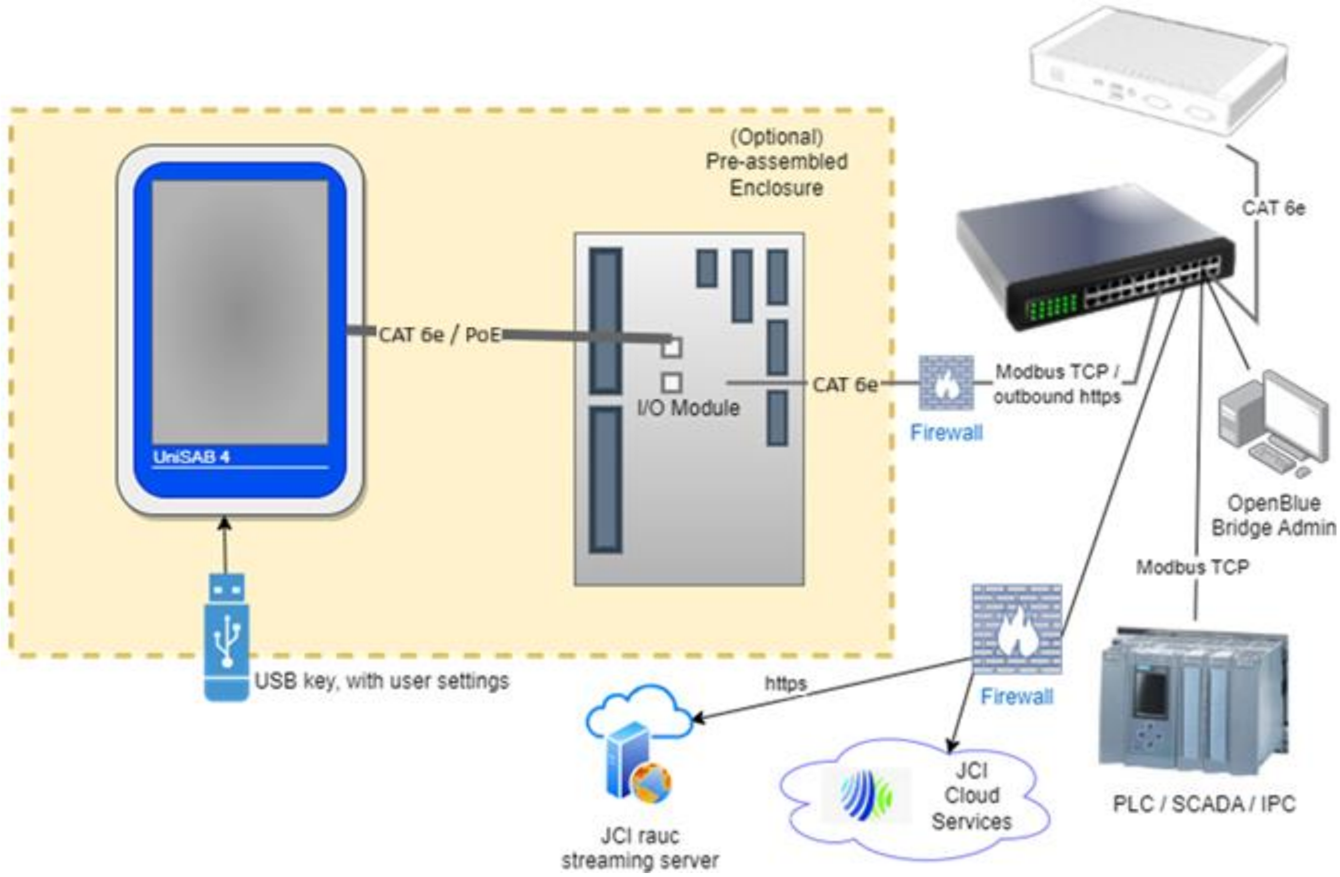
Use Case 5: Controller Integrated via Internal Production Network

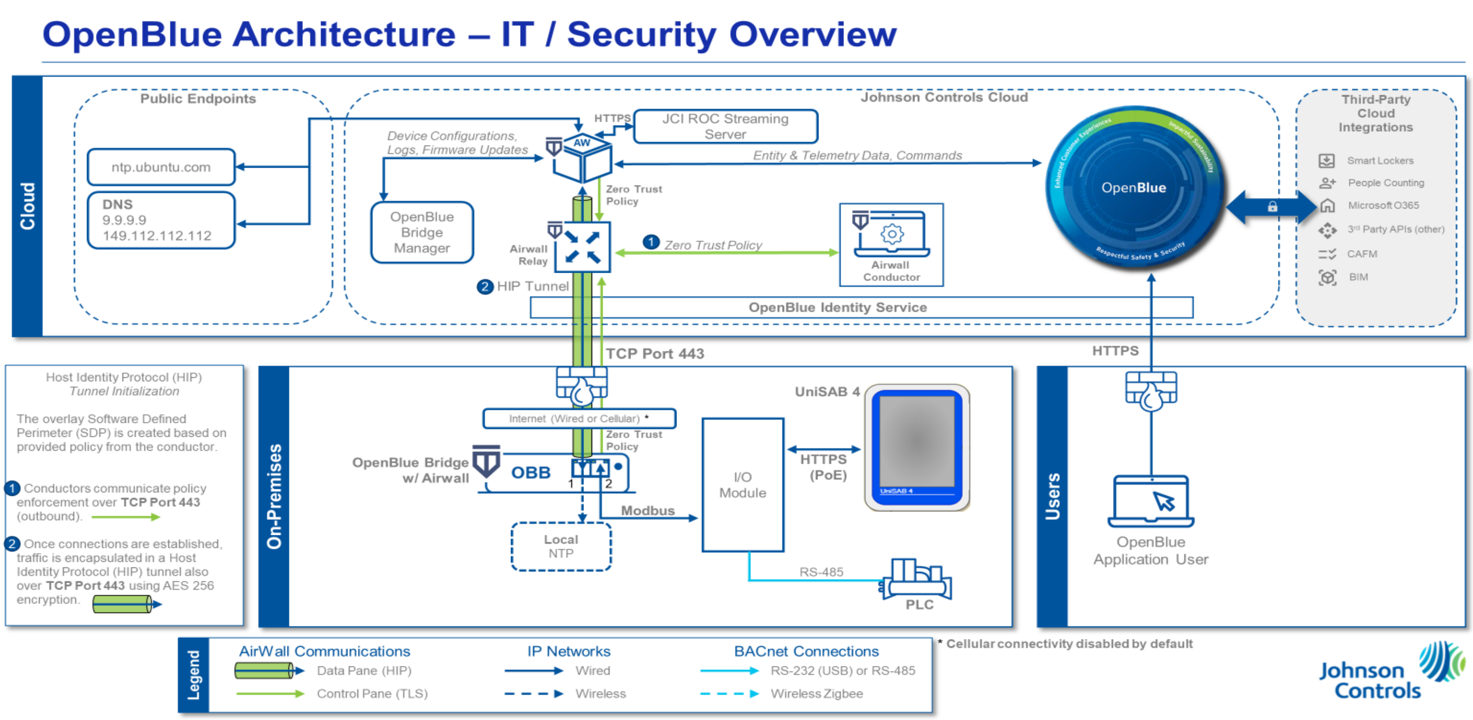


Features and best uses:

- A production system, or environmental control system, is implemented on a PLC with Modbus TCP, connected to an administration system.
- An internal production network is installed allowing technicians to access the network. In this setup the production network cannot be considered air-gapped from other networks. However, there is no online connections to the internet that the controller can utilize.
- This controller uses TLS certificates for the HMI which will expire if not updated. New certificates are shipped with the firmware updates.
- Johnson Controls recommends that an internal RAUC streaming server is installed in the production network. For additional details, see section 1.1.3 – Supporting Components, RAUC File Streaming Server
- Installing the RAUC server also means that a USB key is no longer needed, as a user can utilize the network to install updates, and backup user settings, via the sites network, using the HMI on e.g. a Wi-Fi connected mobile device, or laptop, via https.

Use Case 6: Controller on Production Network, with OpenBlue





Features and best uses:

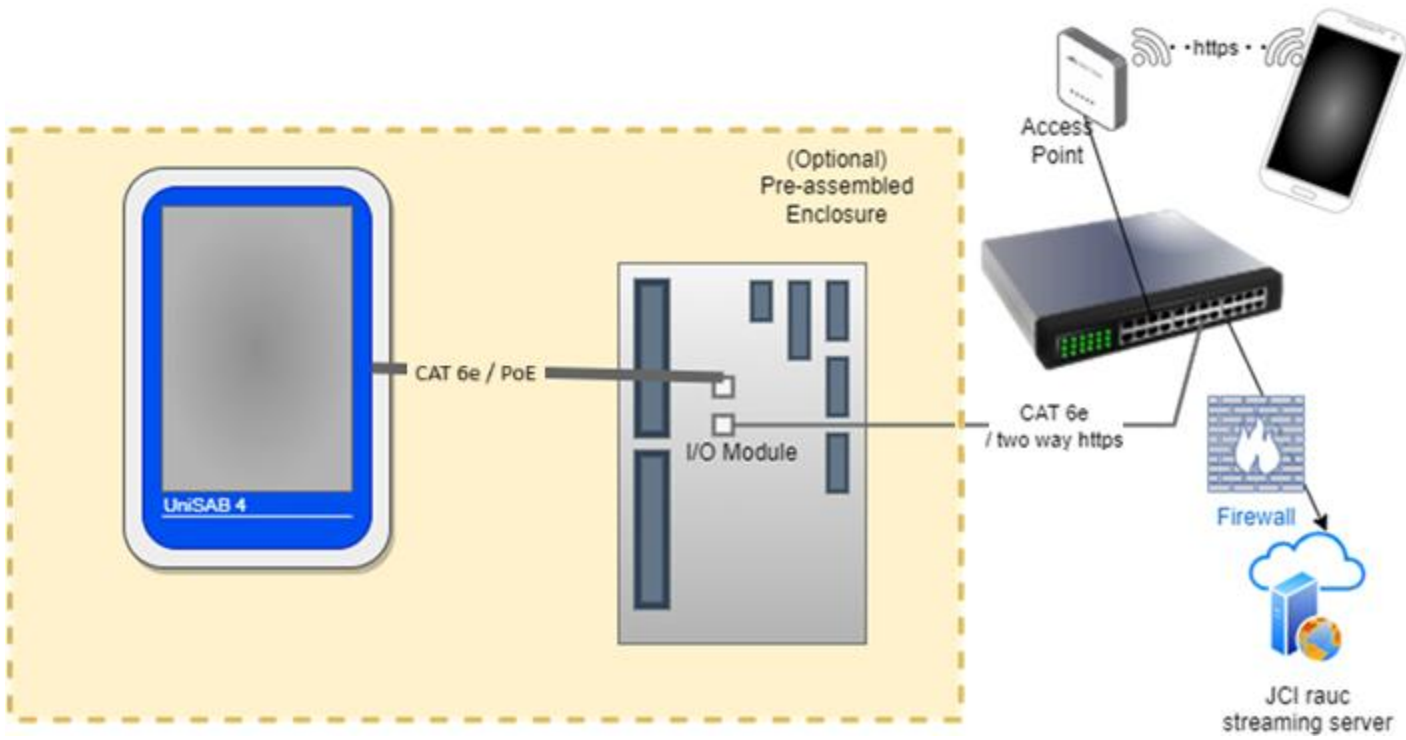
- A production system, or environmental control system is implemented on a PLC with Modbus TCP, connected to an administration system.
- An internal production network is installed allowing technicians to access the network.

Note: If there is no need to use mobile devices / laptops / control room computers to monitor the controllers HMI, we recommend isolating it with a firewall, so only the Modbus and outbound https connections are available to the controller.

This type of installation requires an internet connection for OpenBlue to work, opening ports for outbound https traffic. We recommend updating the firmware whenever we release new updates. When OpenBlue is deployed, we recommend also allowing the controllers to make outbound https connections via the firewall. With this configuration firmware updates are automatically downloaded, and ready for approval via the HMI. This reduces or eliminates the need to utilize a USB key.

User settings change infrequently and never without an initiated need from a user. It must still be backed up on USB keys when there is no inbound https ports open to the controller.

Use Case 7: Controller on Production Network

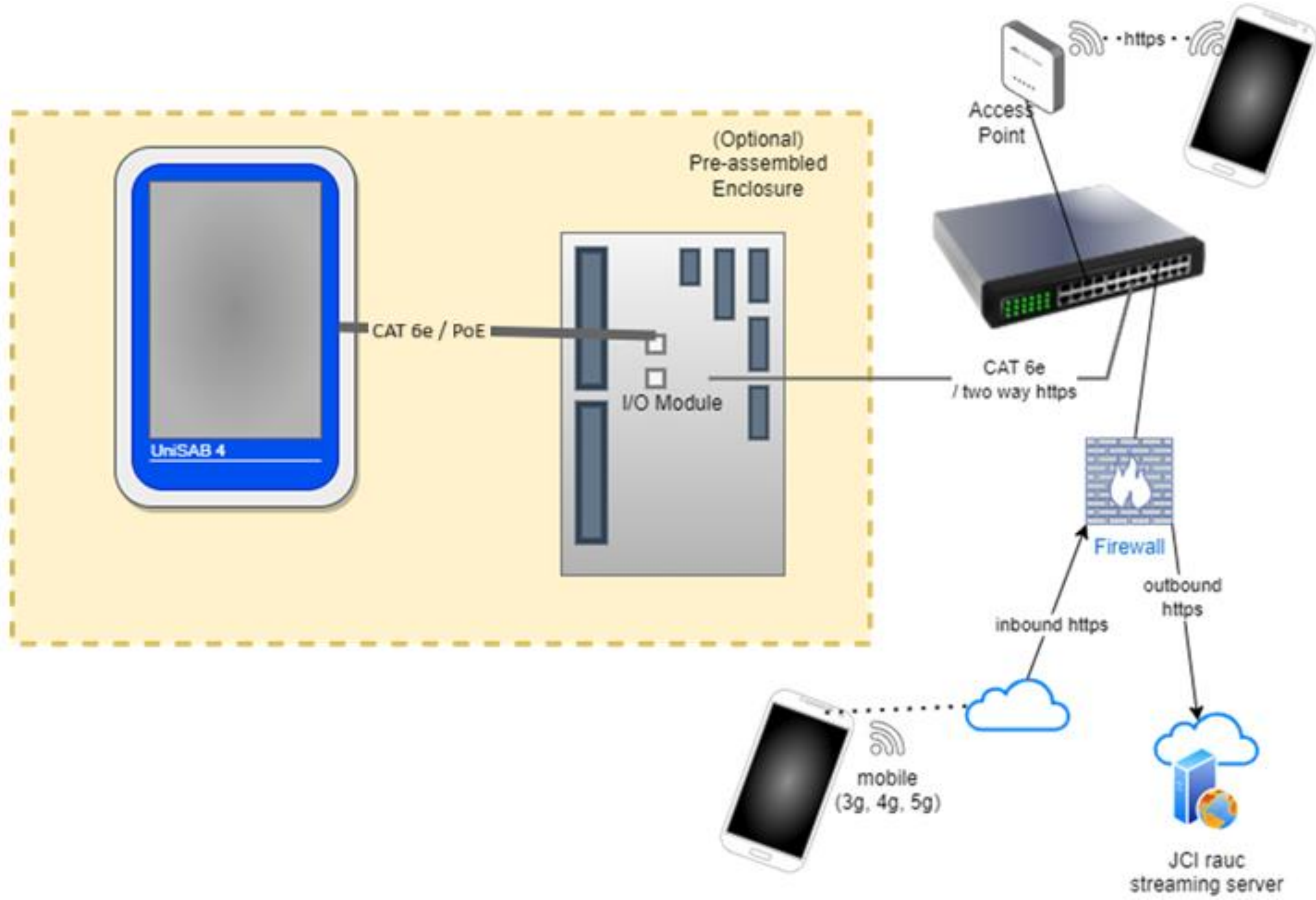


Features and best uses:

- Installations where a technician uses the system HMI only, typically located in noisy environments
- When the system is expected to maintain a constant temperature, or pressure, between the technicians' adjustments of references.

- Production network should be behind a firewall, allowing HTTPS outbound (only) connections to automatically download available updates via public RAUC streaming server (incoming traffic should not be allowed). The controller will only install an update following manual approval via the HMI.
- A USB key or local RAUC server isn't required. The HMI network is utilized to backup user settings or update firmware (via public RAUC server) using the HMI on a Wi-Fi connected mobile device, or laptop.

Use Case 8: Controller is Online



Features and best uses:

- Where the technician will operate the HMI though a remote device, such as cell phone or laptop
- When the system is expected to maintain a constant temperature, or pressure, between the technicians' adjustments of references
- Production network should be behind a firewall, allowing HTTPS outbound (only) connections to automatically download available updates via public RAUC streaming server (incoming traffic should not be allowed). The controller will only install an update following manual approval via the HMI.
- A USB key or local RAUC server isn't required. The HMI network is utilized to backup user settings or update firmware (via public RAUC server) using a browser, and the users' credentials.

1.1.2 Components

The UniSAB 4 solutions consists of the following components which require hardening on premises:

Control Unit

The control unit is the main computer module which implements the controller logic and hosts the HMI. The control unit has the following interfaces:

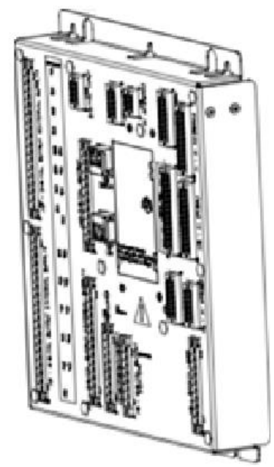
- (x40) 24Vdc External supply – *optional, if running without PoE support*
- (x41) RS485 *disabled – reserved for future use*
- (x42) Status LED light – *optional, for external status LED, Panel mount only*
- (x43) Display LAN (RJ45 *PoE*) - *connect this to I/O board*
- (x44) HDMI *disabled – reserved for future use*
- (x45) USB micro (µ B) disabled – reserved for internal use.
- (x46) USB (A) – for software updates, and backups
- (x47) SD Card *disabled – reserved for future use*

  Note: Items in light gray text are reserved

I/O Board

The I/O Board holds all plugs for the analog sensor, contactors, and actuator connections. It is also the point of contact with the surrounding networks, as it has both a connection to the Control Unit, and optionally a connection to the production network.

It has the following interfaces connecting it with the equipment it monitors and controls:



- (x1) AI Analogue Inputs (4-20mA)
- (x3) DI Digital Inputs
- (x4) AO Analogue Outputs (4-20mA)
- (x5) AI (PRESS) Analogue Inputs dedicated for Pressure Sensors
- (x6) DO Digital Outputs (Heater)
- (x8) DO Digital Outputs (Internal Supply)
- (x10) DO Digital Outputs (Internal Supply)
- (x12) DO Digital Outputs (External Supply)
- (x13) safety loop
- (x19) Analogue Inputs (PT100 temperature sensors)
- (x30) DO Digital Outputs *new in UniSAB 4*
- (x33) DI Digital Inputs *new in UniSAB 4*
- (x34) AO Analogue Outputs *new in UniSAB 4*
- (x39) Analogue Inputs (PT100 temperature sensors) *new in UniSAB 4*

It has the following interfaces connecting UniSAB 4, with itself, and external integrations, which are the elements relevant to the hardening guide.

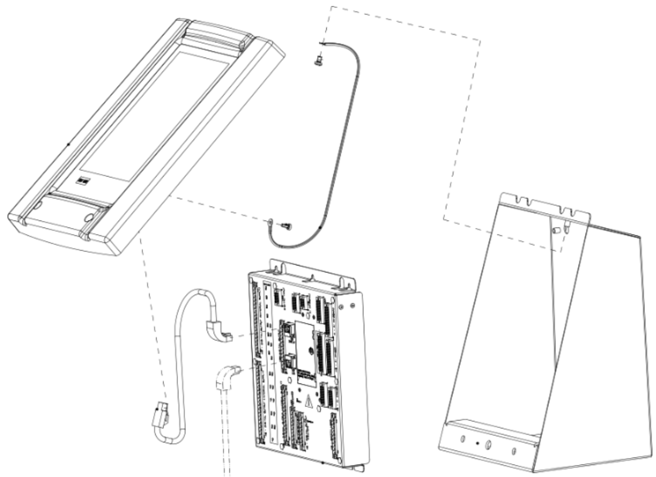
- (x20) Power – for powering the controller
- (x22) LAN *(optional) – for connecting the controller with the production network.*
- (x23) Display – for connecting the I/O Board with the controller.

Touch Screen

The 10” touch screen is a glass surface, supported by a steel backplate, with error indicating LED’s, and no physical push buttons. It acts as the local interface for operators. From here they can access the HMI, to update settings, or setpoints, and they can monitor the controller. There are no bypass mechanisms to operate the device without the HMI. If the touch screen is broken, it shall be replaced asap to ensure safe operation, if the controller is otherwise operational, the HMI must be continuously accessed remotely while waiting for the repair.

Cassette Enclosure, or Panel Mounted Mechanics

UniSAB 4 can be bought in a pre-assembled mechanical enclosure. This version, including the mechanics, is called a cassette. During commissioning and hardware maintenance, like replacing a sensor, it is necessary to open the cassette, to get access to the I/O Board, placed behind the Touch Screen.



UniSAB 4 Cassette Pre-assembly.

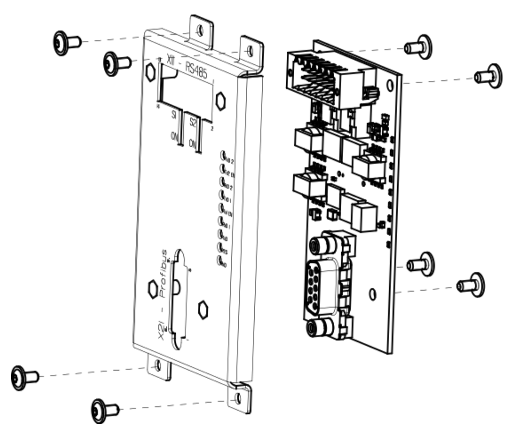
UniSAB 4 can also be purchased as a panel mount version, in which the individual components are shipped with brackets for mounting in an electrical cabinet. Assembly of cables and ground leads are required, for it to function properly.

Profibus Communication Module (optional)

The UniSAB 4 I/O Board can be expanded with a Profibus Communication Module, this is done by removing the expansion slot cover, and installing the module in its place, connecting it to the I/O Boards sockets.

The Profibus Communication module adds two ports to the I/O Board:

- (x11) RS485 *disabled – reserved for future use*
- (x21) Profibus – DSUB-9 DP connections for Profibus



Profibus Communication Module

1.1.3 Supporting components

Supporting components are those which are recommended for system operations but are not within the targeted scope of this document. This solution is supported by the following components:

Service laptops / Mobile Devices

Service laptops and mobile devices (i.e. tablets, notebooks, cellular device, etc.) which will be used to service the UniSAB 4 controller, which requires a web browser. HMI is tested using the latest Google Chrome and MS Edge browser. These scenarios are described in use cases 5, 6, 7, 8.

Service personnel can connect laptops or mobile devices to the UniSAB 4, if the UniSAB 4 is connected to a production network, and inbound https connections are allowed.

Internet Gateway / Firewall

An internet gateway is used for external communication instead of a modem. This internet gateway is to be supplied separately by the customer if required. A firewall is used to block or allow specific ports to communicate. These scenarios are described in use cases 3, 5, 6, 7 and 8

RAUC Server (Robust Auto-update Controller)

With a RAUC server, the UniSAB 4 controller can securely and automatically check for downloads. Updates will be automatically downloaded and cached on the streaming server. Updates will be shown as available via the HMI, requiring manual approval to install. This process also reduced the chances of expired certificates.

There are 2 types of RAUC servers

> *Remote - JCI RAUC streaming server*
>
> The JCI hosted RAUC Streaming Server hosts the latest firmware files, allowing the UniSAB 4 controllers with https access to download the latest firmware. This simplifies the controller update process. The JCI RAUC server is featured in use cases 3, 5, 6, 7 and 8.
>
> *Local - RAUC File Streaming Server (optional)*
>
> The RAUC File Streaming Server is a locally hosted webserver which allows automatic downloading and hosting of UniSAB 4 firmware. It is then used to distribute firmware updates to all controllers on the network from a central location under your control. This allows updating controllers without physical access, making updating firmware easier, and manageable if a site has many controllers.
>
> The URL setting that points to a locally hosted RAUC streaming server location can be changed on the HMI. The RAUC Streaming Server is featured in use case 5.
> **Note:** Downloading firmware to the locally hosted RAUC server needs to be done manually.

Switch (optional)

Connection of the UniSAB 4 to a production network will require a switch. These scenarios are described in use cases 3, 5, 6, 7 and 8.

Access point (optional)

An access point provides wireless network access (Wi-Fi) to the production network for connectivity to mobile to the UniSAB 4 HMI. These scenarios are described in use cases 6, 7, and 8.

Mobile Device (optional)

The UniSAB 4 HMI is optimized for use with touch screens and available as a webservice via https for devices on the production network. This makes operation from a tablet, etc., as optimal as using the controller’s locally mounted screen. A modern browser with HTTPS support for https is required for a mobile device.

PLC (optional)

A PLC allows integrations with other production automation solutions connecting to the UniSAB 4 via either Modbus TCP or Profibus. When using Modbus TCP, the PLC needs to be assigned a static IP, as the UniSAB 4 will only accept connections from whitelisted IP's. This is accomplished by either:

- Create a DHCP server rule to always assign the same IP
- Assign a static IP on the PLC

These scenarios are described in use cases 2, 3, 4, 5, and 6.

(optional) Open Blue Bridge / Admin

The Open Blue Bridge intercepts Modbus TCP traffic, re-packages it, and transmit it as Open Blue network packages to the Open Blue Cloud Services. As a minimum the Bridge and related Administrator servers are required for Open Blue. Hardening the Open Blue setup is covered in the OpenBlue Hardening Guide at the following link - https://www.johnsoncontrols.com/trust-center/cybersecurity/resources. These scenarios are described in use cases 3 and 6.

1.2 Security feature set

Johnson Controls products are designed with built-in cybersecurity features out of the box. Some features are included and set by default while other features need the reader to go through steps for advanced hardening.

The UniSAB 4 Controller has the following security features:

- Secure Boot
    - Redundant Booting / Safe Updates – A redundant set of firmware is installed. If firmware fails to load within the allocated timeframe, the controller will boot from the other partition. When updating the controller, it means that only the *other (inactive)* instance can be replaced, never the running one. After the update, the controller will boot from the updated partition.
      This means that if an update fails, the update code will fail to start and automatically reboot the controller into the old (running) version again. Only after a successful update will the redundant firmware be updated.
    - Integrity Checks During Boot – Installed firmware uses hashes to check the integrity of the filesystem before booting. This ensures no changes can be made to the running system. Changes to any critical part of the filesystem will be detected during reboot, preventing the controller from loading the modified firmware version.
- Secure Firmware
    - Hardware Secured Storage – All data is encrypted using a controller specific encryption key. This prevents extracting secrets directly from the onboard memory.
    - Encrypted Firmware – the RAUC Bundles used to package the firmware, are publicly available, and encrypted. The controllers store the decryption key in the Hardware Secured Storage, hosting the equivalent to an internal HSM, making the controller able to decrypt the firmware during installation, but unable to expose the decryption key.
    - Digitally Signed Firmware – the RAUC Bundles used to package the firmware, are digitally signed in production. This means the controller must validate the identity of firmware packages author, and the integrity of it, preventing tampering with a released firmware package, or

creating false firmware packages.

(To prevent firmware tampering, an event indicating author identity theft will result in a Critical Firmware Release which will invalidate the compromised credentials. In this event, you must update immediately, to prevent fake or modified firmware to be accepted by the controller)

- HMI User Based Access Control – Data presented on the HMI is restricted by security profiles, so different user accounts have access to see specific topics and change specific parameters. Managing users is performed through the HMI.
  - Encrypted HMI Traffic – All https messages sent between a browser and the webservice providing the HMI are protected by TLS. The certificates required for TLS will need to be updated at frequent intervals, which is achieved by updating the controller's firmware.
  - MQTTs – The data for HMI elements, like parameter fields, references, form inputs, or live data, are all transmitted as TLS protected MQTT signals, in a single user bound connection. Hence accessing the HMI means establishing a MQTTs connection, per session, which always requires an initial successful user login.
  - Connection Throttling – The frequency of connection attempts are throttled, so several seconds must pass between each attempt, making brute force login attempts very slow.
  - User Login Retry Time Dropoff – The retry time before a user can login again, is increased on every failure, to make user targeted credential testing implausible.
  - Simple or Personal User Accounts **–** aka. Low and High Security Mode means you can define how many user accounts you want to manage, and if the credentials are pre-defined, or individually locally defined. We recommend using personalized credentials. See table 2.4.1 for password guidance.
  - Forced User Creation – In high security mode, there are no pre-installed user accounts, so usernames and passwords must be created on first logon. In low security mode, each must have a password defined, before the controller allows any other operation.
- Automatic Download of Updates – Secure firmware updates (see above) can automatically be pulled from firmware hosting RAUC streaming servers. This means that the controller will send a message via the HMI when an update is ready.
  - Manual Install of Updates – Firmware updates will restart the equipment, and interrupt production, and therefore it cannot be automatic, but must be scheduled by the operator. This requires a user login to the HMI, so Firmware updates interrupting production cannot be started remotely without proper credentials.
- Cassette Version Tooled PCB Access – Controllers in the cassette enclosure require removal of the screen to gain access to the PCB. This is required for downloading firmware, or user settings from a USB key to the controller. The screen is mounted with screws meaning that it cannot be removed quickly, and inconspicuously. We recommend replacing the screen mounting screws with site specific customized security screws to make tampering more difficult, while still allowing technicians access. For additional details, see Hardening step 6.   We do not recommend glueing the screws in place, as service access must be possible in case of failures.

1.3 Intended environment

Physical access and installation of devices can greatly impact cybersecurity. The UniSAB 4 is rugged and designed to be operated in industrial locations. Johnson Controls recommends a registered electrician installing this controller.

Please refer to the UniSAB 4 Safety Installation and Operating Guide (See Appendix A) for additional details.

1.3.1 Internet connectivity

Connecting any Operational Technology (OT) system to the internet always increases cybersecurity risk. Although the UniSAB 4 is designed to utilize internet connectivity (only for optional integrations), it does not need the Internet to function.

To harden your system, Johnson Controls recommends that you do not connect UniSAB 4 to the internet. If you do connect your solution to the internet, the hardening steps in section 2 must be taken to limit external access.

1.3.2 Integration with IT networks

You may integrate UniSAB 4 into standard IT deployments, but it is best practice to deploy UniSAB 4 and any supporting components to a dedicated and isolated network.

When a dedicated and isolated network is available, consider setting up a local RAUC streaming server, for synchronizing timestamp in logs, with other production system, and central control of the deployment of firmware to UniSAB 4 controllers.

1.3.3 Integration with external systems

Integration with external systems is optional, for example the JCI RAUC Firmware Streaming Server.

If RAUC Streaming is required, a default server of rauc.unisab.com is provided. This URL setting can be modified by the customer as necessary, using the HMI.

1.4 Update policy

The policy documented here sets forth the current internal operating guidelines and process regarding UniSAB 4, which may change from time to time at the sole discretion of Johnson Controls. It is best practice to apply the latest UniSAB 4 firmware to get the current security fixes for your system.

When applying updates, always refer to your company’s policies.

Note: Currently, the UniSAB 4 controller is equipped only to load firmware updates.

UniSAB 4 support is provided for the latest version of the current release. Support will also be given for 1 major version back of the prior software release for a duration of 6 months.

Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavors to address issues that arise within UniSAB 4 with the severity that they warrant.

Security Updates are provided for the UniSAB 4 via Firmware Updates. Firmware Releases are published via websites, and the JCI RAUC streaming server. Depending on the connectivity of the controller in your setup, the controller may be able to download new firmware updates automatically, it is your responsibility to install them.

The UniSAB 4 Firmware is composed of several sources, where each component has their own security update, safety update, or bugfix release strategy. The underlying Real Time Operating Systems Release Policy is to release bi-annual service updates, and if CRITICAL vulnerability issues are fixed, ad-hoc releases are delivered as fast as practically possible. The same goes for the hardware drivers, and similar device tree specific dependencies.

Johnson Controls will use commercially reasonable efforts to issue updated Firmware packages as fast as possible, in response to releases in the operating system. Firmware releases may be more frequent, as releases can also be shipped to fix machine safety critical bug-fixes to functionality, or application layer security updates as follows:

- When CRITICAL severity security vulnerabilities are discovered within the UniSAB 4 application layers, Johnson Controls will use commercially reasonable efforts to issue a critical update for the current Release of UniSAB 4.
- When non-CRITICAL vulnerabilities are discovered within the UniSAB 4, Johnson Controls will use commercially reasonable efforts to:
    - Apply fixes for HIGH severity vulnerabilities in the next immediate Release of UniSAB 4, following the regular release rules.
    - Johnson Controls will assess MEDIUM severity vulnerabilities and plan accordingly

1.5 Hardening methodology

While the UniSAB 4 product provide onboard security safeguards, including many secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, deployment.

Generally, you should aim for a defense-in-depth strategy employing standard IT hardening methods and compensating controls as needed to complement the base security features of each component.

1.6 Communication

1.6.1 Communication port configuration

Port/ Range	Protocol	Direction	Destination System	Process/ Service	Description
502	Modbus TCP	In / Out	SCADA, PLC, Other UniSAB 4	Modbus Fieldbus TCP	For making real time changes in setpoints / settings, monitoring process or software states, and required for the MultiSAB++ distributed control solution
443	https	In / Out	Server	RAUC Streaming	Out: Automatic Firmware Downloading, for scheduled updates In: Remote HMI access
22	SSH / sFTP	In		Secure Shell / Secured File Transfer	Used for field test purposes only.

1.6.2 Data flow diagram

A data flow diagram is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls and zero-trust architectures.

The use requirements of each path should be identified as:

- Required – this path must be established for the solution to function for all supported applications.
- Optional – this path is optionally required depending on the functions that will be enabled (e.g., webserver, email)
- Setup only – this path is only needed during the setup and configuration and disabling during normal operations is recommended.
- Service – this path is only needed for service. A service path is typically a temporary remote service connection which is disabled during non-service periods.

It is useful for someone who is not as familiar with the process to break the communication paths to understand the processes for the basic to the more complex applications. It is helpful to group paths by function. Communication paths should be labelled so they can be referenced within the document.

<u>UniSAB 4 (U4) Data Flows</u>

Use Case 1 - Standalone Controller Maintains a Constant Reference

U4 --- [Setup/Service] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]

Use Case 2 - Controller Integrated with PLC, only via Profibus

U4 --- [Required] – (Profibus / RS485) ---> PLC
U4 --- [Setup/Service] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]

Use Case 3 - Controller Integrated via Profibus and Open Blue

U4 --- [Required] – (Profibus / RS485) ---> PLC
U4 --- [Required] – (Modbus TCP, port:502) ---> Ethernet Switch
U4 --- [Setup/Service] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]
Ethernet Switch --- [Required] – (Modbus TCP, port:502) ---> OpenBlue bridge
Ethernet Switch --- [Required] – (https, port:443) ---> OpenBlue bridge admin
OpenBlue bridge --- [Required] – (https, port:443) ---> Ethernet Switch
Ethernet Switch --- [Required] – (https, port:443) ---> Firewall / gateway
gateway ---> JCI Cloud Services, Open Blue

Use Case 4 - Controller Integrated via Isolated Production Network

U4 <--- [Required] – (Modbus TCP, port:502) ---> Ethernet Switch
Ethernet Switch <--- [Required] – (Modbus TCP / port:502) ---> PLC
U4 --- [Setup/Service] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]

Use Case 5 - Controller Integrated via Internal Production Network

U4 <--- [Required] – (Modbus TCP, port:502) ---> Ethernet Switch
U4 <--- [Required] – (https, port:443) ---> Ethernet Switch
U4 --- [Setup] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]
Ethernet Switch <--- [Required] – (Modbus TCP / port:502) ---> PLC
Ethernet Switch --- [Required] – (https, port:443) ---> Firewall / gateway
Ethernet Switch <--- [Required] – (https, port:443) ---> Access Point

Mobile Device --- [Required] – (https, port:443) ---> Access Point
gateway ---> JCI Cloud Services, RAUC Streaming Service

Use Case 6 - Controller on Production Network, with OpenBlue

U4 <--- [Required] – (Modbus TCP, port:502) ---> Ethernet Switch
U4 <--- [Required] – (https, port:443) ---> Ethernet Switch
Ethernet Switch <--- [Required] – (Modbus TCP / port:502) ---> PLC
Ethernet Switch --- [Required] – (https, port:443) ---> Firewall / gateway
Ethernet Switch <--- [Required] – (https, port:443) ---> Access Point
Mobile Device --- [Required] – (https, port:443) ---> Access Point
gateway ---> JCI Cloud Services, RAUC Streaming Service
Ethernet Switch --- [Required] – (Modbus TCP, port:502) ---> OpenBlue bridge
Ethernet Switch --- [Required] – (https, port:443) ---> OpenBlue bridge admin
OpenBlue bridge --- [Required] – (https, port:443) ---> Ethernet Switch
Ethernet Switch --- [Required] – (https, port:443) ---> Firewall / gateway
gateway ---> JCI Cloud Services, Open Blue
U4 --- [Setup/Service] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]

Use Case 7 - Controller on Production Network

U4 --- [Setup] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]
U4 <--- [Required] – (https, port:443) ---> Ethernet Switch
Ethernet Switch --- [Required] – (https, port:443) ---> Firewall / gateway
Ethernet Switch <--- [Required] – (https, port:443) ---> Access Point
Mobile Device --- [Required] – (https, port:443) ---> Access Point
gateway ---> JCI Cloud Services, RAUC Streaming Service

Use Case 8 - Controller is Online

U4 --- [Setup] – (USB 2.0+) ---> Key, [FAT32 / NTFS / ext4]
U4 <--- [Required] – (https, port:443) ---> Ethernet Switch
Ethernet Switch --- [Required] – (https, port:443) ---> Firewall / gateway
Ethernet Switch <--- [Required] – (https, port:443) ---> Access Point
Mobile Device --- [Required] – (https, port:443) ---> Access Point
gateway ---> JCI Cloud Services, RAUC Streaming Service
Mobile Device --- [Required] – (https, port:?) ---> gateway / Firewall (port forwarded)

2 Deployment

This section is designed to help execute the deployment phase of your system. The contents within this section address how to initiate secure deployment for new installations, how to harden your attack surface and additional steps after commissioning required before the new or upgraded system is turned over to runtime operations.

2.1 Deployment overview

Security hardening begins prior to deployment with careful planning as outlined in section 1 of this guide. It is good practice to review sections prior to deployment to fully understand the security feature set, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Resetting factory defaults
- Considerations for commissioning
- Recommended knowledge level

Before you start the installation of your solution, consider the guidance in the following sections.

2.1.1 Physical installation considerations

Install hardware using the instructions provided in the UniSAB 4 Safety Installation and Operating Guide (See Appendix A) for additional details. Keep in mind that physical access to the device and physical installation of the device can impact cybersecurity.

The distance from the I/O module to the sensors and actuators installed on the compressor must be limited to the minimum required, to reduce signal noise.

The cassette version of the controller includes both the UniSAB 4 and the I/O board. In this form factor, the cassette is typically mounted directly on the compressor frame, usually located in a production area, with restricted access.

The panel version, of the UniSAB 4 controller can be placed within PoE Distance (up to 90 meters from the I/O board). However, the ethernet cable connecting the controller to the I/O module is part of the control loop and must remain unbroken for the equipment to operate properly. If this cable is exposed outside electrical cabinets, it is recommended to mechanically shield it from rodent, and malicious attackers by running it inside steel piping.

Depending on your selected use cases (see 1, 2,3, 4, 5b), you may need to physically access the controller to update firmware or use the touch screen to locally interact with the controller and change setpoints, or other settings. For all cases where this access type is not needed, we recommend placing the controller in an out of reach location.

2.1.2 Default Security Behavior

On the initial startup, limited functions are available facilitating only the most common commissioning tasks

- Security Mode Selection
  (example: high *(default)* / low)
- User Account Settings
  (example: create administrator user on first login, create other users, change passwords)
- Enhanced password validation
  (depending on the chosen security level, the users' passwords must follow specific validation rules)

2.1.3 Resetting factory defaults

The controllers' configurations, aka. User settings, refrigerant and compressor type choice, controller parameters etc. can be reset to factory defaults, via the HMI. The feature is available to Supervisor and Administrator Account types only.

The users are not removed when factory resetting, they must be removed manually. Managing User accounts is available to the Administrator Account and can be done via the HMI.

Details on how to navigate the HMI and accomplish the factory reset, and user account removals, ca be found in the UniSAB 4 Safety, Installation and Operating Guide (See Appendix A for link).

2.1.4 Considerations for commission

The controller may be a spare part, which can be on storage for some uncontrolled amount of time, or it has been mounted on equipment prior to shipping. Commissioning of the controller can sometimes occur a long time after the construction of the equipment. Hence, we recommend downloading the latest version of the firmware to a USB stick, and as soon as an administrator account is created, the firmware should be updated before the controller is connected to any production network.

While the controller's user settings, defining compressor control parameters, have defaults provided by JCI, for each of JCI's compressor models, it will most likely not be sufficient to fully commission the system. Parameters are expected to need a few adjustments on site, to account for local conditions.
You can change the parameters, and dial in the controller via the HMI, or upload a settings file from an old controller.

When user settings are adjusted satisfactory, providing appropriate compressor behavior, the settings file should be backed up, for easy recovery in case of any future controller failure! This currently requires using the USB port. For additional details see the UniSAB 4 Installation and Operating Guide.

In the commissioning phase, a user login, shall also be created in the UniSAB service/support system (in case the user haven't already done so), and the controller shall be associated with this user. The association is only possible using the controllers apparent identifying markers, like MAC address and serial number. The controller can only be associated with a single user account. The controller will work fine without this registration, but it is needed for ownership identification in case of emergencies and may be used to recover access to a locked machine.

2.1.5 Recommended knowledge level

Fundamental knowledge of industrial refrigeration (IR) systems is required to install and maintain a UniSAB 4 controller. The compressor being controlled by UniSAB 4 is potentially dangerous to operate if not installed properly. Installation and maintenance should only be performed by technicians with proper local certifications in IR due to the hazards working on the equipment (Sensor removal, cause damage, etc.) specifically those which could result in refrigerant leakage.

Any cabling work done on the controller shall be carried out by an electrician certified in industrial installation, or by personnel with equivalent safe installation courses. Any work must comply with the local safety legislation for working with electrical installations within the industrial setting.

We recommend that technicians unfamiliar with Johnson Controls' products, attend the UniSAB operation and installation course, available through the knowledge and learning center at JCI Holme DK.

Connecting the controller to a production network should only be done by experienced IT personnel, that can configure switches or firewalls, to block unwanted traffic. (See Section 2.7 2.7 Configure Communication Ports)

2.2 Hardening

While many products include secure-by-default safeguards, additional hardening is usually required to meet the security requirements of the target environment. It is important to apply to the correct level of protection as warranted by the customer policies and government regulations that may govern the application security settings for this deployment.

2.2.1 Hardening checklist

While UniSAB 4 have several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment. This checklist provides an example list of hardening steps you may select to go through. The actual steps you will take is based upon the features included within your specific environment as gathered in Section 1.0.

- ☐ Hardening Step 1: Create user account(s)
- ☐ Hardening Step 2: Update user password
- ☐ Hardening Step 3: Update controller parameters
- ☐ Hardening Step 4: Backup User Settings
- ☐ Hardening Step 5: Securely mounting the Controller
- ☐ Hardening Step 6: Locking Controller Plugs with secure clips
- ☐ Hardening Step 7: Disable unused ports
- ☐ Hardening Step 8: Whitelisting Inbound Modbus TCP / MultiSAB IP's
- ☐ Hardening Step 9: Reset the UniSAB 4
- ☐ Hardening Step 10: As-built documentation

2.3 User accounts

When the UniSAB 4 is initially powered up, it has no user accounts, except an anonymous viewer account. If no accounts have been set up, the Security level must be chosen (default) **HIGH** / **LOW**, and an

Administrator account must be created. Until this is completed the controller's HMI will not allow any other operation.

When creating passwords, refer to table 2.4.1 for guidance:

Hardening Step 1: Create user account(s)

During the first powerup of the controller, you must create the administrator account. The HMI will show the **Administrator Sign-up** dialog box shown in figure 2.3.1. Here you will create the administrator account with a freely chosen username which will be used to administer the system. See table 2.4.1 for rules to create user accounts.

Figure 2.3.1

After you press the **Sign-up** button, the HMI presents a screen to select the security level. To harden the controller, set the Security level to **HIGH**.

The Administrator is now logged in to user management on the HMI and can proceed to create other users. The other users created are given Supervisor, Superuser, or User roles. This privilege is only available to the Administrator.

New users will have a random generated password assigned; shown to the administrator on account creation. This password will be used for First-time account set up. Users are forced to change their password upon first login. From the time of account creation to first login, nefarious agents should not have access to this First-Time Password, so we recommend communicating this securely (i.e. not through insecure digital methods).

Additional details on creating users is found in the UniSAB 4 Installation and Operating Guide. See appendix A for link.

Note: Do not connect UniSAB 4 to a network before the administrator account creation is completed.

2.4 User passwords

The criteria for setting a password (length, special chars. etc.) is verified by the HMI. Users must change their password at the first login. A user can then change their password whenever they feel the need to do so.
If passwords are forgotten, a random one can be created by the administrator, effectively re-activating the requirement that they must change it upon the next login.

Hardening Step 2: Update user password

All users who have existing accounts created for them, and have not yet logged in with their account, must login and change their password from the default. It is not recommended to have "dormant" accounts on the system. Johnson controls recommends the following password attributes when initially setting up user accounts and during the change password process:

Table 2.4.1 – Password guidance

Attribute	Minimum requirement	Recommended for further hardening
Password total length	8 characters	Create passwords of at least 15 characters (max 16)
Special characters	1 character such as **-**, **.**, @, #, !, ?, $, %. All other special characters are invalid, including spaces.	Include 2 or more non-succession special characters
Upper Case characters	1 character	Include 2 or more
Lower Case characters	1 character	Include 2 or more
Numbers	1 character	Include 1 or more
Blocked Words List	Must not contain dictionary words	Establish a password policy to exclude company and product names associated with project (e.g., JCI, UniSAB, OpenBlue, etc.) to the blocked words list

2.5 UniSAB 4 Controller specific settings

Update Controller Parameters

Hardening Step 3: Update controller parameters

Login as an IR technician and update all relevant (operating, monitoring, alarm, etc.) configuration settings, so the controller is expected to behave in a tolerable fashion, when the compressor is started. These settings will vary depending on the specific installation and components in use. See your specific installation manual to determine the appropriate settings for your installation.

Backup User Settings

Hardening Step 4: Backup User Settings

After the controller has been run-in, backup the controller settings to a USB drive. This allows smooth replacement of the controller in the event of failure, or recovery from a factory reset to an operational condition, using good and trusted values for all parameters.

2.6 Hardware Hardening

The Controller's PCB is exposed if the controller can be removed. Proper security is required to prevent tampering.

Hardening Step 5: Securely mounting the Controller

Secure the controller's encasing to the Touch Screen with the provided torque screws or optional safety screws (not provided). It is also recommended to glue (not provided) these screws to prevent removal and tampering with the controller.

Note: This also prevents service and maintenance of the hardware. This optional step should be completed once the controller has been successfully run-in.

Hardening Step 6: Locking Controller Plugs with secure clips

All ports are protected from short-circuiting attacks, so unused ports can securely be left unplugged.

However, the (x43) RJ45 plug which is required for PoE, and I/O board communication, should be secured with secure clips to prevent unauthorized removal. E.g. DeLock RJ45 Secure Clip 86406. As this enforces that removal requires a special tool, or key.

Note: Many of these RJ45 locks will require removing the regular built-in clip of the RJ45, effectively removing the warranty from the cable.

Note: Remember to also secure the other end of the cable to the I/O board, or if relaying switches are inserted in the path, locking all of those as well. If switches are found in the path, plug up all other ports of the switch with locked in place dummies, to prevent insertion of cables with foreign ethernet traffic, as this is required to be a real time network.

2.7 Configure Communication Ports

Hardening Step 7: Disable unused ports

To decide what ports to open refer to the Port Assignments in section 1.6.1. Block all unused ports. For example, if you no longer need SSH / sFTP, and are not using port 22 for any other use, block port 22.

Hardening Step 8: Whitelisting Inbound Modbus TCP / MultiSAB IP's

As a security feature, the UniSAB 4 is designed to ignore all Modbus TCP packets by default. If your installation requires the use of Modbus TCP, or MultiSAB IP, the IP address must be whitelisted on the controller. To Whitelist the IP Address, see your specific installation manual to determine the unique settings for your installation.

<u>Advanced note for users with a managed switch:</u> To further harden you system, add a rule to the managed switch which states the ARP must be unchanged. For additional information on managed switch settings, see the switch's operator manual or local IT department.

2.8 UniSAB 4 – Reset Functions

The UniSAB 4 has built-in functions to reset the device in the event the controller becomes inaccessible, if you are unable to log in due to lost credentials or are attempting to move the controller onto another compressor.

Hardening Step 9: Reset the UniSAB 4

The following reset functions are available on the UniSAB 4.

User Management Reset. With a **User Management Reset**, all users are removed from the device, while all other settings remain on the controller. The **User Management Reset** action can be activated only by the Administrator Account, by carrying out a specific sequence in the HMI designed to avoid accidental activations.

To authorize the **User Management Reset** process, a set of hardware interactions will be required. If these process steps do not occur within a specified time period (timeout), the process will not be carried out, and the controller remains unchanged. Follow the instructions presented on the HMI.

Factory Reset. With a **Factory Reset**, all settings are restored to factory defaults, and all user accounts are deleted. Beware that a factory reset also removes all user specific settings, including warning/alarm limits, any adjustments made to controller parameters, etc.

To perform a factory reset, ssh access is required. The ssh terminal is protected by public/private keypairs, and you should install your own key into the controller, to reduce the risk of unauthorized access.

When you have established the ssh connection, you will need to run a set of commands. Contact our support number to obtain this set of commands.

On installations where a personal key has not been installed, a default global public service key is used, where JCI owns the private key. In this case you will need to place the controller on a network connection serviceable by the support team. To authorize the factory reset process, a set of hardware interactions are required. If they do not occur within a predefined timeframe (timeout), the factory reset will not be completed.

2.9 Security audits and documentation

A well-documented deployment of the solution will be useful in security audits, and a security audit can expose errors in the system documentation and identifying gaps in protection. Each task feeds the other and it may be necessary to repeat hardening step 11, after an audit is complete and the gaps are addressed.

Hardening step 10: As-built documentation

Document deployment once hardening is sufficient for run-time operations. When updates are released, or security advisories are published this documentation will be useful. The documentation will allow for quick assessment to determine if the deployment is impacted by the issues described in a security advisory and requires a configuration change, software update or patch.

Include the following details in creating as-built security documentation:

- As-built architecture drawing of system
- For all system components record:
    - Component identification
        - Name
        - Description
        - Device Type
        - Location
        - Vendor
        - Model
        - IP address
        - MAC address
    - Support details
        - Software version
        - Hardware version
        - Licenses
        - Installation date
    - Communication configuration details
        - Enabled Ports and protocols
        - Encryption settings

Appendix A - Additional Literature

Document title	Document number
UniSAB 4 Safety, Installation, and Operating Guide	IR-SAB-USR-0001-001-en
UniSAB 4 two-pager Product Bulletin	5672

https://docs.johnsoncontrols.com/industrialrefrigeration/

The Engineering Guide is available to Johnson Controls Employees only (requires authentication) through the following link- https://docs.johnsoncontrols.com/industrialrefrigeration/v/u/Sabroe/en-US/UniSAB-4-Engineering-Guide/002/1.00

Appendix B – Acronyms

Acronym	Description
HMI	Human Machine Interface
HTTPS	(Secured) Hyper Text Transfer Protocol
HSM	Hardware Security Module
IP	Internet Protocol
IR	Industrial Refrigeration
JCI	Johnson Controls, Inc.
LAN	Local Area Network
OT	Operational Technology
PLC	Programmable Logic Controller
PoE	Power over Ethernet
RAUC	Robust Auto-Update Controller
SCADA	Supervisory Control and Data Acquisition
SFTP	(Secured) File Transfer Protocol
SSH	(Secured) Shell