Unitronics Cybersecurity for Vision and Samba PLC Series

IIn today's interconnected world, cybersecurity is more important than ever, especially in industrial control systems (ICS). ICS environments are increasingly targeted by cyberattacks, which can have significant consequences, including production disruptions, safety hazards, and financial losses.

Unitronics has developed a comprehensive approach to protecting its controllers. This page outlines Unitronics' main tools and recommendations intended to raise the level of cyber protection of automation projects and machines based on Unitronics Vision and Samba Series controllers.

New! VisiLogic version 9.9.00 has built-in security enhancements.
To download the latest version Click Here.

1. Equipment level

Basics:

1. Stay Updated via http://www.unitronicsplc.com – Unitronics develops and improves its products throughout their life cycle. The company website contains the most up-to-date versions of both software and operating systems, which may include advances in Cyber protection.

2. Access Permissions and Passwords: Strictly control local and network access permissions to the controller and associated equipment.

3. Remote access permissions- Manage and define the remote access permissions according to system's and user needs in order to minimize unnecessary exposure.
For example, the PCOM protocol (a built-in communication protocol for development and management) allows protection at various levels:

- Blocked Access: Ensure that controllers do not allow connection to this protocol until there is a need for viewing only.
- Operator: Viewing and updating data.
- Technician: Troubleshooting, changing controller settings, and updating versions

4. Communication Design:

- Design the communication to reduce the usage of "SERVER" mode configured sockets
- Configure unused sockets in "Client" mode

5. Multifactor Authentication: Use SB 314 and SDW 10 to configure multifactor authentication to your Vision / Samba device. Follow the software help section for detailed instructions.

An example application can be found at:
https://downloads.unitronicsplc.com/Sites/plc/support-tools-and-applications/V570_PCOM_MFA.vlp

2. Network level

Secure Communication

1. Controller as Internet Client: If the controller must communicate with components or servers on the Internet, ensure that the controller is the client initiating the communication.

2. Connecting automation equipment to the Internet:

- Ensure that all equipment is behind a Firewall and that there are no Firewall Rules exposing the LAN network to entry from the WAN network.
  (whether it is a cellular router or a wired network).
- Verify that there are no Port Forwarding settings exposing automation equipment directly to the public network.To quickly and easily implement network-level protection, it is recommended to use UCR products, Unitronics' industrial router series that includes built-in Firewall and VPN functionality. For quick connection, refer to: Defining VPN in UCR products in 4 steps.

3. Modbus Protection: Limit the Modbus master accessible address space by enabling SB 305 and setting SI 165-168 values according to the required address space. Follow the VisiLogic help section for more details.

3. Complete Solution

Secure Connection – UniCloud-based

Unitronics' UniCloud IIoT platform allows secure connection **without the need for fixed or public Internet IP addresses**—no prior knowledge in cyber or IT is needed for implementation.
The platform contains multiple layers of advanced encryption and protection, that together provide a complete, secure solution that allows access to be restricted by permission level and tracking actual connections.