Internet Connectivity increases the risk of security breaches, but that connectivity is a mandatory requirement for many automation projects—making Cyber-Protection procedures absolutely vital.

Cloud connectivity, Remote Access, recipe update, data backup, and remote control for maintenance: the need for external connectivity creates new challenges in the field of information security, as it increases the potential exposure and risk. The responsibility for preventing security breaches lies with the operations and control personnel, who program and connect the controllers to an external network.

Unitronics offers a variety of solutions and tools that may be used to mitigate risk and prevent security breaches. This document details the main tools and recommendations intended to raise the level of cyber protection of automation projects and machines based on Unitronics Samba™ and Vision™ series controllers.

1. Equipment level

Basics

a. **Stay Updated via** 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.

b. **Access Permissions and Passwords** - Strictly control network access permissions to the controller and associated equipment.

c. 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.

2. Network Level Security

Secure Communication

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

b. **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. 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.

International Headquarters: P.O.B. 300, Ben Gurion Airport 7019900, Israel. Tel: +972 3 977 88 88, global.sales@unitronics.com