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 UniStream® series controllers.

1. Equipment level

Basics

a. **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.

b. Release Notes documents: updated at each version release, these documents may contain security information relevant to a specific release. **Unitronics recommends updating controllers and development tools to version 1.32 and above.**

c. **Access Permissions and Passwords**

- Strictly control access permissions to the controller and associated equipment.
- Change the PLC default passwords and store them according to accepted practice. Changing the default password and setting a new access password for the controller **will prevent a casual user** from connecting to the controller via UniLogic.

d. UniStream products support multiple layers of security and protection. The developer and user must implement the following functionalities according to system requirements:

- Set passwords for VNC via VNC Server Management.
- Set permissions for UniApps via Password Management.
- Set users and permissions for user screens via User Access Control.
- Set users and permissions for Web Server screens.

  For systems where downloading the user application is done using Flash Drive or SD Card, care must be taken to set the various passwords in their designated places.

2. Network level

Secure Communication

a. **Controller as Internet Client:** If the controller must communicate with components or servers on the Internet, ensure that the controller acts as a client, initiating the 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 implement network-level protection quickly and easily, it is recommended to use the UCR products, Unitronics' industrial router series that includes built-in Firewall and VPN functionality. For a quick connection, refer to Setting up VPN on UCR products in four 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