Fieldbus System/ Industrial IoT Cybersecurity

In recent years, factories have introduced industrial IoT, building up complex networks of production machines. These systems maybe subject to a new threat, cyberattack. To protect the industrial IoT from cyberattacks, it is important to take multiple measures (multi-layer protection) for IoT devices, networks and clouds.

For this purpose, SMC recommends that the following measures are always taken into consideration. For further details of the following measures, please see security information published by your local country security agencies.

1. **Do not connect the devices via a public network.**
   - If you unavoidably need to access the device or cloud via a public network, ensure to use a secure, private network such as VPN.
   - Do not connect an office IT network and factory IoT network.
2. **Build a firewall to prevent a threat from entering the device and system.**
   - Set up a router or firewall at network boundaries to allow minimum required communications.
   - Disconnect from the network or turn off the device, if no continuous connection is required.
3. **Physically block an access to unused communication ports or disable them.**
   - Inspect regularly each port if any unnecessary device is connected to the network system.
   - Operate necessary services (SSH, FTP, SFTP, etc.) only.
   - Set a transmission range of the device using a wireless LAN or other radio system to the minimum required and use only devices approved according to the radio act in the country concerned.
   - Install a device generating radio waves in such place as there is no interference from indoor or outdoor.
4. **Set up a secure communication method such as data encryption.**
   - Encrypt data in every environment, including IoT networks, secure gate-way connections, for secure communications.
5. **Grant access permissions by user accounts and limit the number of users.**
   - Regularly review accounts and delete all unused accounts or permissions.
   - Establish an account lockout system to block an access to the account for a certain period if log-in fails more than the given threshold.
6. **Protect passwords.**
   - Change the default password when you first use the device or system.
   - Choose a long password (minimum 8 characters) using a mix of different letters and characters to make the password more secure and harder to hack.
7. **Use the latest security software.**
   - Install antivirus software on all computers to detect and remove viruses.
   - Keep the antivirus software up to date.
8. **Use the latest version of the device and system software.**
   - Apply patches to keep the OS and applications up to date.
9. **Monitor and detect abnormalities in the network.**
   - Keep monitoring the network for any abnormalities to take a prompt measure and issue an alert if any abnormality is detected. Install an intrusion detection system (IDS) and intrusion prevention system (IPS).
10. **Delete data from devices when disposed of.**
    - Before disposing of any IoT devices, delete stored data or physically destruct media to prevent any misuse of the data.