

Technical Bulletin

Bulletin No: TB-0048-22-159-FS

Effective Date: 06-8-2022

Type: Informational

Subject: Trusted Suppliers

Scope

This technical bulletin discusses manufacturer viability and security issues with low-cost components.

Background

When purchasing components for use within a SCADA monitoring system, low-cost parts may have questionable aspects hidden within construction or software requirements that the integrator must be aware of. The accuracy and reliability of a quality part typically come at a premium and the lure of low prices can be tempting, however there are other factors to consider when purchasing low-cost equipment. What level of responsiveness and support does the supplier provide? Does the supplier have a sustainable business model? What benefit does a warranty provide if the manufacturer is no longer in business? In today's political environment, most importantly is the item manufactured by a hostile, foreign power?

As Stuxnet revealed to the world in 2010, even air gapped SCADA systems are not immune from attack <https://www.sciencedirect.com/topics/computer-science/stuxnet> .

Many modern systems need an internet connection to be practical, which opens up additional attack vectors. System integrators must exercise all due diligence and provide a sufficient level of control to ensure they are not contributing to the problem.

For example, while an RS485 to Ethernet adapter has a specific function, in reality this device is a mini computer with a web server capable of running numerous types of code. Because of this risk, the integrator must ensure the adapter is purchased from a trusted supplier.

Suspiciously low-priced products are a red flag that the component in question may be suspect and that additional research of the supplier must be conducted prior to purchase. Even if an item is made in a trusted country, informed purchasers must also consider where the item's parts were made. This is true for all components within a fully integrated system.

The use of suspect parts can have a negative effect across all aspects of the system. Research the supplier of every system component utilized, while verifying security certificates place of manufacture, and other technical documentation that provides evidence of a safe, supported component.

Products from FlexSCADA are clearly labeled as being manufactured in Canada utilizing only North American sourced components. Additional components provided are from trusted sources within North America and Europe, and clearly marked as such.

For more information please contact Mission Critical Energy at (716) 276-8465 or visit us at www.flexscadafusion.com .