

# Industrial Networking Solutions Security - PLC, SCADA



## ...by Business Industrial Network

Industrial networks are considered the best solution for industrial applications and automation systems for its superior benefits like increasing response time, distance covered and higher interoperability.

However, with such a complex system, security measurements becomes essential, and any dereliction of it could cause a serious threat to the whole system and sometime, to the personnel involved in it, in fact, production machines networks without proper security can cause physical damage to man and machine, check the educational

video [here...](http://www.youtube.com/watch?v=V4qg10yfp-s) <http://www.youtube.com/watch?v=V4qg10yfp-s>

Now let's discuss some practical advices on security recommendations within the following lines....

## Security Recommendations:

**1 - ANSI/ISA-99.02.01 security standard:** Or the [American National Standards Institute](http://www.nist.gov) according to the International Society of Automation has approved the second standard in the ISA99 series for security of industrial automation. It guides user

to establish a cyber security management system showing all details about policies, procedures, practices and personnel.... No step should be taking without full understanding of this standard.

**2 - Infrastructure:** (access points, routers, switches, hubs...etc) are the frames that hold the whole system parts together... You must consider the harsh industrial conditions in which these devices will operate in and the difference between them and their commercial counterparts as they may cost more money and convince some companies to purchase the commercial ones. The saying "You get what you pay" may apply here, as the industrial network components are environmentally tough equipments and well prepared for such conditions ... Also, when choosing and installing some parts like for an example the switches, experts should discuss some important technical details like applying the SNMP protocol and to determine whether they should be fully managed or just lightly managed or even web managed.

**3 - Power Security:** All industrial equipments should operate under wide variety of power conditions to ensure minimizing the downtime and preventing power loss, automation Ethernet is not an exception... You must install sufficient power supplies with adequate fuses and breakers that can give a very short response time and with the prospect of providing a redundant system in case needed.

**4 - Firewalls and antivirus programs:** like any other software system, your network requires protection against viruses, worms, hacking and all other forms of software preaching and interfering, put in mind to install some suitable programs for this task and update them continuously to ensure maximum protection for your system, it's recommended to check this little research article about Hacking The Industrial Network that show some statistics about security threats [here](#).

**5 - Isolation:** Sometimes, companies mix their Industrial Ethernet network with the office network or the BAS - Building Automation System- network and even make the industrial network connected to the internet .... In fact, the office networks and internet data transfer consumes significant bandwidth which causes a negative effect on industrial network response time and efficiency, not mentioning that exposing it to direct internet connection can present a serious security threat..... That's why VLANS are the ultimate solution to divide this system into several parts, tagged VLANS can isolate and secure each network, accommodates with managed switches and even manage the bandwidth traffic to prohibit delays inside the critical parts of the network. Wifi and mobile applications increase security risk and small mobile SCADA screens increase risk of operator error.

**6 - Surveillance:** The most important rule of any security system is to keep a watchful eye over every single part of it... Surveillance is more than just monitoring the network, but also, guarantees a fast intrusion to handle errors and malfunctions before they spread and cause damages and hazards to the whole operation process... Video surveillance or remote video monitoring is a very practical solution in this case as the revolutionary IP cameras can manage sending and receiving data with high traffic rate and many switches now on the market supports the expansion of this monitoring IP technology, this mechanism provides bigger flexibility to the surveillance process.

**7 - Technical Support:** It's much recommended to have a support provider to aid your system twenty four seven... Having a professional, well prepared team to back you up around the clock is a very cost effective solution. You'll save time and money by providing such service... Many bugs and problems in the system or the equipments can be handled by the technical support specialists and sometimes they can fix it remotely with no need to send a technician on site. But also keep in mind, someone working with network system remotely can greatly increase risk to man and machines as well as downtime. Also within your industrial security procedures, include corporate protocol for outside support. Insure vendors and OEMs can only access to your production equipment when the proper authority physically located in the plant, allows them access, on a case by case bases. Also remember to unplug modem phone lines connecting machines to OEM, after each remote support instance is done.

**NOTE:** With traditional computer networks, mistakes may result in communication failures and/or computer crashes. With an Industrial Network, the crash may be a live machine and could cause physical harm to humans working in a facility! Not to mention thousands in downtime cost.

## SCADA security risks:

SCADA is considered to be an HMI –Human Machine Interface- software system which is just a software program on a PC capable of accessing a PLC systems to send and receive data, this is why it has security concerns like any other software system, it can be hacked, bugged or infected by software viruses... PLCs can be indirectly effected too if the SCADA system attached to it is not properly secured.

One of the most intimidating security Breaches was the Stuxnet worm which targeted industrial software and equipments, it struck the Iranian uranium enrichment infrastructure in 2010, the Stuxnet hit [Step-7](#) software application that is used to reprogram PLC devices.

Nevertheless, Stuxnet is a windows computer worm not a PLC virus. That's why the most secured industrial system is one that only uses PLCs and local HMIs with no computer software involved.

## Current Network Status:

These are some articles and surveys about the current industrial network status in different fields showing analysis and recommendations for the security systems. The major players for 2011 in industrial network protocols are Ethernet/IP, PROFINet, Modbus TCP, ISA SP-100.11a and Wireless HART.

**1 -** The following article is about security for critical infrastructures like power plants, substations, electric utility control centers, and water systems, and describes some positive and negative points. The article shows an overview of the latest cyber security in industrial networking. <http://www.controlglobal.com/articles/2009/CyberSecurity0903.html?page=1>

**2 -** If you'd like to make a full evaluation of your current network security status, you should take a look at this detailed article that shows how to assess your security level: <http://www.controlglobal.com/articles/2005/371.html>

**3 -** Also below, is a survey from CISCO showing some articles about security and quality of service for industrial environments. <http://www.mendeley.com/research/cisco-secure-wireless-plant-security-quality-service-industrial-environments/>

4 - CISCO has also been working with Rockwell Automation to insure AB / FactoryTalk are secure, so be sure to read the material AB / Rockwell has put together at <http://www.ab.com/networks/architectures.html> for a complete industrial networking solution.

## Security Checklist:



- [ ] Review ANSI/ISA-99.02.01 security standard to map all PLCs/Machines on the network.
- [ ] Check and install all the infrastructure from network components to power equipments and make sure to test their configurations.
- [ ] Insure firewalls are in place and updated.
- [ ] Insure machine network is not connected to BAS network.
- [ ] Insure PCs with SCADA have antivirus software running on them.
- [ ] Isolate PCS with SCADA from direct internet access.
- [ ] Connect your system to an efficient surveillance and monitor system.
- [ ] Provide your system with qualified technical support provider vendor.
- [ ] Insure all personnel are trained to face emergency situations. (Including [PLC Training - http://www.bin95.com/plc\\_training.htm](http://www.bin95.com/plc_training.htm))
- [ ] Run several test operations before launching your system online.
- [ ] Have current backup copies of PLC programs and HMI/SCADA programs.
- [ ] Have industrial network policies and procedures in place and enforce them as the safety issue they are.
- [ ] Unplug phone modems attached to equipment, when remote support is finished.
- [ ] Limit and keep record of those who have wifi and mobile access to your industrial system.
- [ ] Survey your system at regular intervals to maintain maximum security.

Going further with you Industrial Network Security ...

[Securing Manufacturing Computing and Controller Assets](#)

[Achieving Secure, Remote Access to Plant-Floor Applications and Data](#)

Hope this helps.

Don Fitchett - [Business Industrial Network](#) (BIN) - BIN95.com

*About the Author:* Don Fitchett founded the activity based costing system called "True Downtime Cost" (TDC), authored books and speaks at conventions on the topic and is president of BIN. Don has been in the industrial training sector for over two decades, setting up training programs around the world, and still conducts training seminars to this day.

Business Industrial Network delivers instructor based industrial training as well as training software and on-line industrial training.

*(You may copy and distribute this article as long as all credits, including this paragraph are included and all links are active and distribution is not for profit. You may reference portions of this article as long as active link back to original article webpage at <http://www.bin95.com> is present. Otherwise this material is copyright protected.)*