IIoT and the security of THINGS

As many organisations are discovering, the Industrial Internet has become a huge opportunity for growth and efficiency. To realise this value, operational technology environments need to be connected. With production systems becoming more interconnected, the exposure to cyber incidents increases. Attacks and disruptions on critical infrastructure put reputation, production, people and profits at risk.

The Industrial Internet of Things (IIoT) has some great attributes with emerging technologies, however the rapid adoption by users and vendors is potentially opening up installations to cyber attack.

Whilst a lot of IIoT devices being spruiked are "Vapour Ware" there are some devices already available that have functions and features which have some wonderful attributes and are enabling smarts and information to send/receive data to cloud based platforms - see figure 1a & 1b.

Figure 1a

GE Field Agents enables users to connect to and utilise GE's Predix Platform to easily collect and analyse industrial data to uncover insights that improve operations and asset performance. A range of communication protocols, tag capacity and connectivity options makes GE's Field Agent a great choice for almost any application, even across disparate systems.

Figure 1b

Red Lion RAM products lead the market in the greatest number of platform integrations, providing greater flexibility to quickly connect to your choice of leading IIoT cloud platforms. The combination of industrial protocol support such as DNP3 and Modbus TCP/IP, reliable cellular communication and easy-to-connect cloud support provides users with a seamless IIoT solution.

With the rapid adoption of these technologies and the media/connection methods they use, many fundamental security risks are being overlooked or fundamental protection not employed. Users need to ensure the IIoT does not become the entry point for an intrusion attempt or potentially a desired outcome that ends up being the downfall of greater function.

Ethernet and Cellular technologies along with many IT based standards have been adapted, refined and updated to keep up with threat, however deployment is largely different to that of an IT roll out. Instead of mitigating potential risk we must consider a complete lock down and only omit securely proven and robust methodologies, protocols and media to achieve the task without allowing for intrusion.

> *"The rapid adoption by users and vendors is potentially opening up installations to cyber attack."*

Some of the greatest risks we have are usually easiest to eliminate. Getting into a routine, by establishing a change management process on a regular basis can potentially stop most of these risks before they happen. For example, most devices have a default password that should be changed, as well as individual user passwords that should be updated with every employee change and periodically. Additionally the methods or means on how employees enter a system such as VPN, should be regularly maintained and updated.

With commercial communication methods adopted, 'Attack Vector' (hacker gaining access to a computer/network server to deliver a payload or malicious outcome) or an 'Attack Surface' (software environment is the sum of different points where an unauthorised user can try to enter/extract data from an environment) is growing exponentially where risks are numerous and growing.

By understanding your devices, systems, employees and methods will assist in preventing any potential cyber attack. The following checklist over the next page may help you prepare!

1. Is the device you have FIRMWARE based?

If so how do you update it (and why) and what is in play from that vendor to ensure it is not corrupted.

2. Is the IT network connected to the Process system?

If so you will need to consider locking it down so only the essential connections can be made (Historian Servers / Engineering work stations) and all others are broken. Think of BASS statement time or IT doing a SNMP network scan slowing down a process system.

3. Is there a Virtual Private Network in place?

If so the certificates must be unique, updated, managed and changed out upon employee change.

4. Is there a Process Wireless Network in place?

If so what has been done to lock it down? What processes are in place to keep or review security.

5. Are you using standard IT Protocols to connect out of the Industrial?

If so you should ask yourself why. Will it provide the security you need? Consider if another one way protocol may be suitable instead.

Simple methods of locking down

The following are just a few examples:

1. Staff are the first and last line of defence

Staff need to be factored into the Security Risk Assessment process along with policies and procedures that are part of the ICS (Industrial Control System) communications system Change Management process.

2. Know your vulnerabilities

Most ICS vendors publish known vulnerabilities. These need to be examined and routinely factored into the entire system design and usage.

3. Employing what is known as a "Honey Pot" is not a bad thing to do

Use a monitored unsecured device with naming conventions in addition to large or vast files of no value. If data is moving from this location, then you have a problem - refer figure 2.

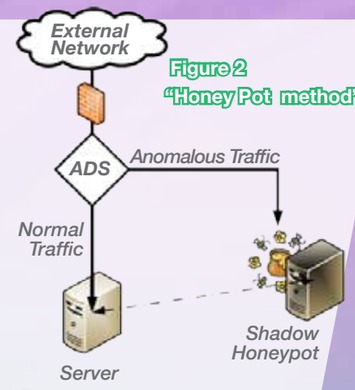

Figure 2
"Honey Pot method"

Figure 4

GE OpShield is an OT cyber security solution that delivers visibility across complex networks, enforcing policy at the protocol command level on the OPTILINX switch

4. Wireless systems

It needs to be private and heavily encrypted with limited to no transmission beyond the needed workable area. By hiding your network, using the most up-to-date encryption along with smart antenna deployment will require only having to keep up with necessary encryption changes. Don't forget to update when there are staff changes, especially with direct access to the network - refer figure 3.

Figure 3

ORing IAP-420+
Wifi Access Point

5. Employ a smart switch system

A smart switch system that has protocol monitoring on board looks at the configured transactions, its installed devices, as well as into the protocol itself. These secured protocol switches are few and far between and a level on process security stemming to the IIoT which will be the notification and stopping point for any intrusion, such as a man-in-the-middle (MIM) attack right through to a device/ data substitution attack. Refer figure 4.

6. The good old AIR GAP method

Do you really need to connect your control system to it? What would be best to put into the system. For example a device that has hard firewall and produces data as a slave for collection with intrusion detection may be ideal. It would have no detrimental impact if it was to be removed from the running system.

7. Lock the cabinet/door

An exposed USB port or network connection may seem harmless enough but this openness can be a major entry or corruption point.

8. Patching and Firmware

With the adoption of modern platforms and methods of communication the firmware and the patching (just like in Windows/ Android/Apple) will need to be kept up-to-date. Not doing so will leave an older device exposed over time. Consider a routine maintenance schedule to ensure the firmware is current as well as how the update of a particular device may require adjustment of another. Consider how this firmware is gathered, and ensure your firmware is secured from source such as a secured log-in site. Double check it's also embedded within the OEM's software itself.

"Some of the greatest risks we have are usually the easiest to eliminate."

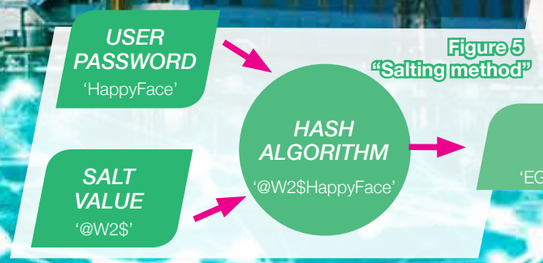

Figure 5
"Salting method"

9. Protocols and Encryption

With Ethernet being a standard networking protocol, hard coded protocols such as ProfiNet allow for IPV6 locking and encryption. This will give a base level of security. Beyond that, a simple encryption method can be adopted to ensure data integrity such as "SALTING" the data with itself - refer figure 5.

To find out more or if you need assistance with this topic, contact Control Logic on 1800 557 705 or email sales@control-logic.com.au.