LABS

INDUSTRIAL IOT SECURITY AND PRIVACY GUIDE

How to evaluation and assess technology and solutions prior to purchase or deployment.

Release: April 2017

This guide exists as a result of the Public Safety Canada Cyber Security Cooperation Program (CSCP). TwelveDot Labs was engaged to research the impact of using insecure IoT products and services on the risks to Canadian consumers and business using our proprietary testing techniques.

This guide presents the findings and recommendations of this research. We hope that you will find the content helpful and easy to understand and implement. However, if you find that you do have questions on the content you can reach out to us on the following channels.

E-mail	Twitter	LinkedIn
Security@twelvedotlabs.com	TwelveDotSecurity	TwelveDot

This guide serves as an overview of the issues and resolutions in the area of Industrial IoT (IIoT). This area is quite broad and encompasses many aspects such as safety that are not such a critical factor in other IoT sectors.

Due to this critical aspect of safety in IIoT, purchasers of systems must be keenly aware of both the attack surface and risks related to each component and system being deployed as part of the Industrial Control System.

From a purchasers point of view you must ensure you have implemented a risk framework to evaluate and quantify risk for your organization. This is typical split between Information Technology (IT) and Operational Technology (OT). OT represents the higher risk to most companies due to the potential for components such as sensor or actuators to either fail in operation or become a hazardous situation. Attacks can result in loss of revenue, damage to facilities or equipment, damage to reputation, potential liability, and safety impacts due to damages processes.

While cyber risks take several forms, it is important to point out that security and privacy in IIot is a balancing acting to ensure operational efficiency and cost of security controls to be deployed. Having a security program as part of an Information Security Management System (ISMS) or Cyber Security Management System (CSMS) should serve as the basis for how security is managed from the company perspective. The specific OT security aspects will have to be risk managed using combination of business processes via a Threat and Risk Assessment (TRA) methodology to quantify risks for new systems and build-outs, and then implementation of controls for identified risks. System designers must be keenly aware of these this combined approach to IIoT systems and must ensure to balance the needs of each.

As part of an ISMS and Secure Development Lifecycle (SDLC) security practitioners must work with OT staff to ensure that threat modeling has been conducted. This will provide a good understanding of the specific vectors that can be targeted for IIoT system.

System integrators need to ensure the IoT Systems they are designing meet requirements for security and privacy. Recent breaches have shown the failure to identify the risk and implement mitigation controls as well as having a breach plan will constitute negligence in many jurisdictions.

For sectors such as energy, smart buildings and smart cities the system integrators need to work with customer security teams to quantify the risks for implementations. These engagements should be formalized to ensure that TRA's and PIA's are conducted to show audit documents of risk being mitigated. Integrators for OT systems would be well advised to adhere to standards such IEC 62443 to ensure they have identified the necessary system controls.

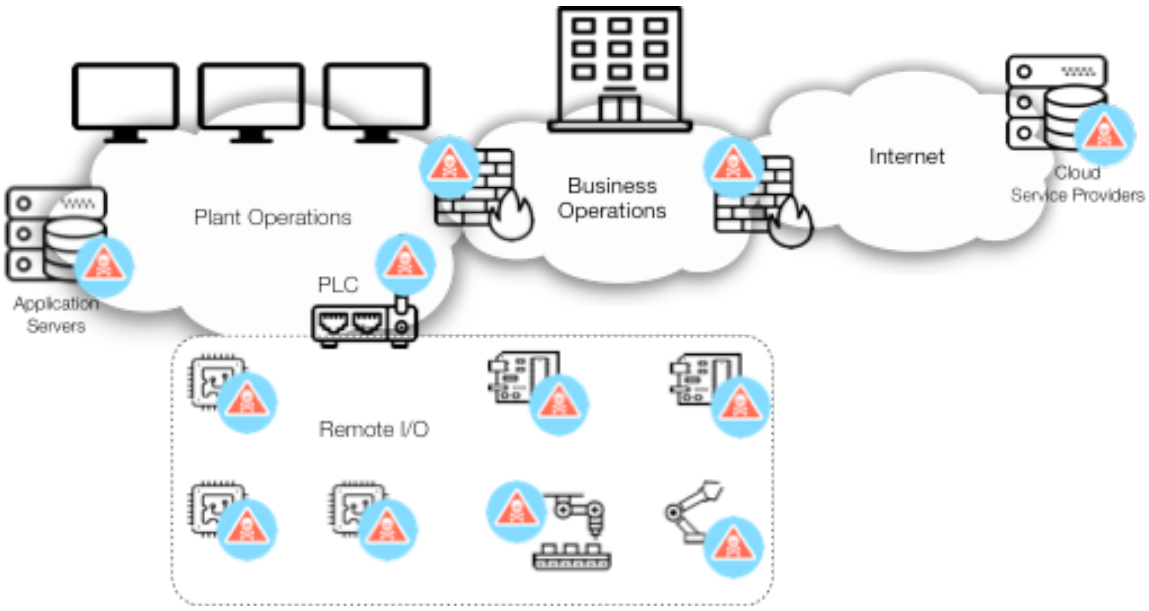

Figure 1: IIoT Attack Vectors

Risks

When considering risks specific to IIoT you have to consider what the possible outcomes could be for a specific device, network or factory under attack.

1. When conducting a TRA the asset under assessment needs to be considered as an attack vector. As such it needs to further consider the attacks against the following elements as a minimum:
    a. Physical
    b. Network
    c. Software and/or firmware
    d. Operations and monitoring systems
    e. Supply chain for all the components of these systems
2. Physical security for components, networks, and deployments. In many instances, these devices can be easily compromised once physical access has been obtained.
3. Violation of trusted relationships between components and/or systems. Depending on the deployment scenario or architecture many deployments use a trust model that permit communication and command and control to take place between operational control systems and sensor, actuators, PLCs, RTU, etc in a build-out.
4. Brown Field deployments need to threat model the current solution and products and determine the additional risks and threats that would exist with the new proposed technology to be implemented. This would include products where remote network access is permitted and become the initial attack point of the device.

5. Green Field deployments allow for all security risks and threats to be identified and mitigated prior to build out. It is best scenario to mitigate cyber risks. It is advised that TRA's and threat modeling is conducted when the plant or facilities are being designed. This will greatly reduce the costs related to retrofitting or design changes after the fact.
6. Identity of network system elements including authentication of these elements at runtime. System operators need to ensure that devices and network elements are communicating correctly and that anomalies are identified. Rogue devices and network access attempts should be quickly identified and mitigated.
7. Access controls both physical and logical need to considered as well as mechanisms that could be used to by-pass them. Users should only be provided access to complete their job function and all access attempts need to logged and catalogued.
8. Runtime Integrity should exist for higher risk asset to ensure that unauthorized changes have been made to the system during run-time. If a vendor has a secure SDLC they should provide proof of this as well as formal certification of the product.
9. Boot time Integrity will ensure that in the event of outage or physical access the firmware cannot be replaced with one that is vulnerable or compromised. If a vendor has a secure SDLC they should provide proof of this as well as formal certification of the product.
10. Data can be attacked during multiple phases of processing and handling. All of these phases need to be considered. Data phases can be considered as follows:
    a. What is the risk to Data-at-Rest (DAR), this is data that stored on a physical or logical medium such as SSD or removal media.
    b. What is the risk to Data-in-Motion (DIM), this is data that being transferred between two or more system components
    c. What is the risk to Data-in-Use (DIU), this is data that currently being processed by a volatile memory and a CPU or microcontroller.
11. Ensure your systems integrator is building OT based system to IEC 62443 control requirements at a minimum. They should also be recommending products and solutions that have been certified to this standard.
12. Ensure your devices resilience capability is evaluated through communication robustness testing (CRT). The CRT ensures the device adequately maintains essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks.

Questions for your vendor or solutions integrator

In many sectors such as energy and oil and gas many other regulatory requirements exist. This includes the reality that more vendors are considering

cyber security important and having their products being tested to IEC 62443 to provide a higher level of assurance. While this is a great stride for purchasers of these solutions you should also consider the following aspects to reduce risk and increase your level of assurance.

1. Has the product and/or solution been formally evaluated to IEC 62443? If not, why?
2. Does the vendor have a formal secure SDLC process? Can they prove it?
3. What 3rd party security evaluations have been conducted against the product or solution such as secure code analysis, penetration testing, and other product certification that would indicate the product has undergone some level of security testing?
4. What technology features does the vendor have in their IoT product/solution that addresses the following:
    a. Trust in their operational infrastructure this includes the additional aspects of:
        i. Secure run-time of code on micro-controller and components
        ii. Secure remote updating from authorized servers
        iii. Secure boot loading of system code for sensor, actuators and other elements that comprise the solution
        iv. Secure monitoring from authorized operations systems
    b. If PII is collected, has privacy has been considered for PII data collected this may include de-identification techniques for data that is stored in a data warehouse. Are users required to sign a declaration to collect or store their data? What countries is the data stored and processed and what privacy laws apply?
    c. Identity and Access Management (IAM) this covers many aspects but should include:
        i. Identifying the user who is accessing the system and components
        ii. Identifying the components in-field and while being deployed
        iii. Identifying and network and service layers to authentication communications
    d. Scalability needs to be considered not only for the deployment considered today but in the future. If the IoT component and service cannot be
5. Specific to IIoT companies and organizations need to consider the following aspects at minimum:
    a. Functional Safety
    b. Interoperability
    c. Resiliency
    d. Availability

What can you to do to greatly reduce your exposure

The quickest way to reduce your risk to cyber attacks to IIoT is understand your threat vectors and have situational awareness of threats to the Industrial Control System (ICS). This includes implementing the necessary incident management framework to quickly contain data and/or system breaches and return to normal operating state.

1. Ensure you have either a Cyber Security Management System (CSMS) or Information Security Management System (ISMS) that clearly outlines the assets to be protected and risk requirements. Typically, these systems will have associated polices and procedures as well as awareness training for all staff levels.
2. Ensure your change management process has the following elements:
    a. Asset inventory
    b. Approval process
    c. Documenting of changes and back out procedures in each change ticket created, approved and processed.
    d. Ensure only authorized personnel are assigned to change tickets
3. Understand your data at risk at collection, processing and storage for all critical systems. The following aspects need to be considered at a minimum:
    a. What risks exist if the data was compromised?
    b. What is the potential safety risks if the system was compromised?
4. Prepare for the day a breach happens with a Breach Plan and an incident handling process. This will ensure that staff in these events are well trained to react, quarantine and restore systems to normal functionality.
5. Formally evaluate all vendors and systems integrators to understand their level of competence of cyber security, this will include aspect such as:
    a. Using products/services certified to IEC 62443
    b. Conducting a TRA and threat modeling against the proposed solution
    c. Having mechanisms for determining when a component has been compromised?
    d. Having a secure SDLC process for products and solutions being developed
    e. How do they ensure that electronic components have not been compromised?
6. What is the trust model of the components being deployed? How are they authenticated at initial setup, when being monitored and performing updates? How could someone compromise this trust level?
7. Have conducted security background checks on staff?
8. Read and implement controls listed NIST 800-82 Guide to Industrial Control System Security and NIST Framework for Cyber Physical Systems

Further supporting information on security and privacy risks can be found at the following sites:

1. ISA99 – Details to IEC 62443 including the evaluation and certification process
2. NIST - NIST 800-82 Guide to Industrial Control System Security
3. Public Safety Canada - Fundamentals of Cyber Security for Canada's CI Community

Glossary

CRT	Communication Robustness Testing
CSMS	Cyber Security Management System
DAR	Data at Rest
DIM	Data in Motion
DIU	Data in Use
IAM	Identity and Access Management
IoT	Internet of Things
ISMS	Information Security Management System
TRA	Threat and Risk Assessment