QUANTUM COMPUTING

July 2021, Edition 1

Quantum Leap

A QUARTERLY NEWSLETTER BY
QUANTUM COMPUTING SDN BHD

Chairman's Note

CYBERSECURITY VULNERABILITIES EXISTS FOR INDUSTRIAL OPERATING SYSTEMS

Welcome to the first e-newsletter from Quantum Computing. In the last 2 years, the way we do business has changed drastically and the importance of automation in the field of manufacturing has become more crucial.

In the course of our business interactions and innovations in R&D, we have gained valuable insights into our industry that we would like to share with all our customers and acquaintances. In our first edition, we are looking at cybersecurity for operational technology (OT).

Awareness of the importance of securing the core of automated manufacturing is relatively low in Malaysia. In the feature piece, we will discuss the impact of cyber intrusions on your business.

We will also be sharing a few helpful tips on managing your cybersecurity. Cybersecurity efforts for your automated and connected plant should be dynamic and updated to ensure that your systems can keep up with the growing number of creative attack methods.

In a further effort to educate on cybersecurity for OT, we will also be hosting a 2-day training session titled “Taming Cyber Enemies in a Manufacturing Environment” in August 2021. We hope to see you in this digital training session which would include lectures, case study sharing, and interactive assessments after each module.

We hope this newsletter is a valuable read to you and we look forward to keeping producing it every quarter with a topic that benefits our manufacturing partners.

Sincerely,
Sakthivel Narayanasamy

Upcoming Event

Virtual Training
Taming Cyber Enemies in a Manufacturing Environment

25th & 26th August 2021

9.00 a.m. to 5.00 p.m. via ZOOM

Early Bird Registration (register by 15th August 2021) : RM1,200 per pax/ 2 days

Group Rate (register 3 pax or more under company): RM1,000 per pax/ 2 days

Email to enquiry@quantumcompute.io to REGISTER NOW!

Feature

Impact of Cyber Intrusions on a Production Plant

The benefits of industrial automation continue to grow and support manufacturers in reducing downtime, wastage and increase efficiency.

However, web-based connectivity and remote management capabilities also create vulnerabilities for a plant in the form of cyber risks and intrusions.

Most manufacturers either overlook or simplify the idea of securing their operating network (OT). Due to the lack of education and awareness on specific security applications and best cybersecurity practices for OT, many factories try to adopt the same security measures utilized by IT.

OT is a cyber-physical environment that involves machines, networks, remote management, and cloud deployments. Cybersecurity for this environment has to be more dynamic and controlled in its implementation as infiltration will cause safety risks, downtime, and financial losses to the manufacturer with the potential for the whole industrial control systems to be affected.

What are the possible impacts of cyber intrusions on a manufacturing facility?

Data breach/ leak
Valuable intellectual property data like patented design, formulas, or more can be accessed by third parties via security breaches in an OT system. Even if the attack is resolved and the machines resume operations, the loss of the data can send legal departments on a blind hunt to find the perpetrator and discover illegal use of the patented materials.
On another note, confidential client specifications or order details can also be stolen from the system if the right security measures are not taken to protect the networked machines. This will not only affect the plant but also the customer's trust in the company.

Production Downtime
In the cases of ransomware, administrators of the plant can be locked out of the system controls. Cybercriminals can shut down machines remotely and force a ransom demand in return for an encryption key. These incidents are on the rise especially in the times of the pandemic and despite ransoms being paid, the system recovery is not 100% to its original capacity and much mitigation work needs to be done.

Downtime can also occur in the event of malware entering the system due to human error e.g. clicking on unknown files or unverified links.

Product Damage / Machine Damage
Mid-production forced shutdowns in the form of cyber intrusions can cause extensive product damages and delays to customer order timelines. In worst-case scenarios, machines can be damaged as well e.g. foil mills could catch fire due to sudden forced production stop or furnace loss of control due to control system lockout, causing more financial losses to the manufacturers.

Loss of Reputation
Most manufacturing facilities that get affected by cyber intrusions have to face the mammoth task of recovering their reputation. They remain answerable to their customers and stakeholders while working hard to recover the operations. Following recovery, they need to constantly provide reassurance that the incident will not occur again and will face a possible loss of business depending on the scale of the intrusion and its effect on the customer.

Financial Losses - This is the bottom line!
Financial losses will be borne by the manufacturer in the form of work delay, damaged orders, damaged machines, loss of data, and more. The time element for recovery also costs money as this period will mean lower or no productivity.

The damages are numerous and the only way to secure an OT network is by deploying proactive security measures that are custom built for a manufacturing environment. A production floor must have an instantaneous and continuous protection system that can provide live detection of abnormal activities, intrusion attempts, and quick blocking capabilities. Protect the OT network to protect the business.

Get in touch with us to chat more on this.

Quick Tips for Cyber Security for OT

1. Continuous monitoring

2. Advocate good user habits

3. Proactive and quick response

Quick Assessment

Evaluate based on the indications provided on your answer options:

1. How many times has your vendor accessed your OT systems remotely in the past year (e.g. machine makers from overseas)?

If it was logged in with an unsecured connection even once then there is a chance of breach or a gateway available for an attack.

2. Is your organization's firewall active?

Yes: You are somewhat secured.

No: You are susceptible to ransomware or other cyber-attacks.

3. If yes, how are the restrictions set up?

A) IF the restrictions are based on a clearly defined security policy then you are secured, but you need to review the policy and restrictions regularly.

B) Restrictions are based on incidents as they occur. You are still susceptible to ransomware or other cyber-attacks as you have not covered possible scenarios.

4. Are you aware of the inherited vulnerabilities (CVEs) of your OT devices?

Yes: Ensure your devices' CVEs are managed and monitored.

No: A security assessment for your OT is imperative.

5. Is your OT network topology defined (or Known)?

Yes: You can define your security boundary, and you have network visibility

No: A network security implementation is necessary and must include network topology as the first step.

Our people are our most important asset. Since our inception, we have believed in building lasting careers for our teammates. Today, we are home to many exploring minds who innovate and build actionable solutions in the form of intuitive solutions like GENiE, SAM, SMITH, and SCOTS. This edition, allows us to introduce one of our core innovators

Kumaran Sukumaran, Chief Executive Officer

Kumaran is the CEO of Quantum Computing. He has been customizing machines and automation solutions for the manufacturing industry for the last 14 years. He has led projects for multiple industries including palm oil, power plants, government bodies, cement, and more. In the last 6 years, his focus has been primarily on automation projects and he has been involved from the consultation stage to planning, installation, testing, and commissioning. He has been instrumental in introducing Quantum Computing's solutions in trade fairs both locally and internationally by sharing his project experiences.

You can connect with Kumaran via LinkedIn, just look up, Kumaran Sukumaran.

Contact us: Quantum Computing Sdn Bhd ; +6012 663 1920 ; enquiry@quantumcompute.io