Security Risks in Manufacturing Environments and Key Points to Know. -Introduction

Controller Div., Product Business Div. HQ, Industrial Automation Company, OMRON Corporation

With the advancement of data utilization using IT/IoT technology in the manufacturing field, and the increased importance of data from factory automation (FA) equipment, we are facing a crisis of severe damage from cyber attacks targeting FA systems themselves, which lack sufficient security measures. This document discusses the common threats of cyber attacks that FA systems may encounter, the severity of such damage, and the risk mitigation strategies. Finally, I will introduce guidelines for effectively utilizing the security roles and features handled by OMRON controllers.

1. Preface

Traditionally, FA systems were not connected to external networks such as the internet and existed within a 'closed' network. However, the use of data through DX is being promoted even in manufacturing sites, and many FA devices have now become connected to the outside. This has increased the importance of security as FA systems are now exposed to cyberattack threats just like IT systems.

2. Threats

Then, what specific cyber threats exist? Figure 1 shows examples of threats faced by FA systems.

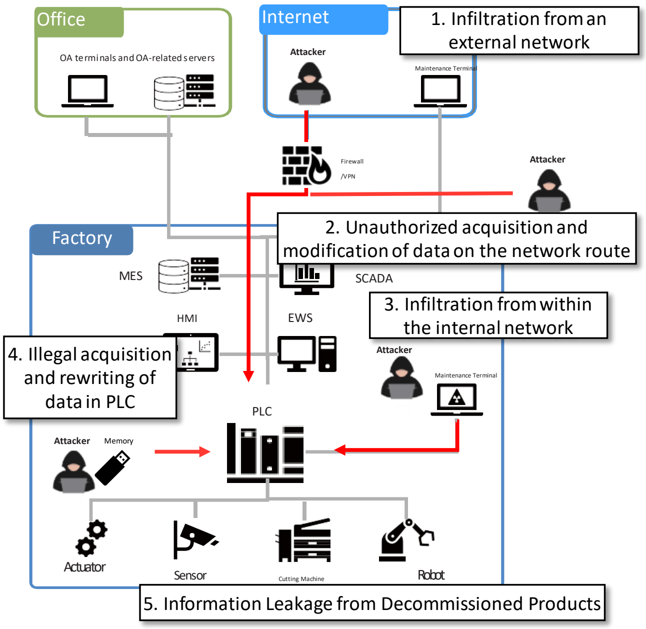

Office
OA terminals and OA-related servers
Internet
Attacker
Maintenance Terminal
1. Infiltration from an external network
Firewall /VPN
Attacker
Factory
2. Unauthorized acquisition and modification of data on the network route
MES
SCADA
HMI
EWS
3. Infiltration from within the internal network
Attacker
Maintenance Terminal
4. Illegal acquisition and rewriting of data in PLC
PLC
Attacker
Memory
Actuator
Sensor
Cutting Machine
Robot
5. Information Leakage from Decommissioned Products

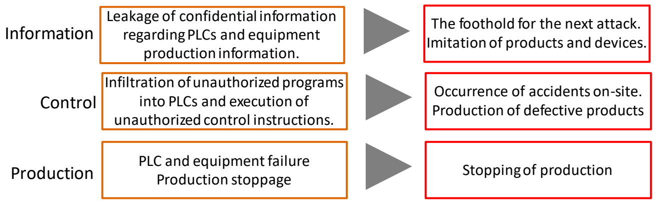
Fig.1 Examples of threats faced by FA systems.

Attacks imagined by many as being carried out by hackers are probably intrusions from the internet (1). Many manufacturers have been subjected to ransomware attacks from external. In the unlikely event that a firewall separating the IT area and the FA area is breached, there is a risk of important information being stolen or altered when using a communication method that does not consider security (2). Internal network intrusion tends to be forgotten (3). Due to its nature, maintenance terminals are connected within the firewall. These terminals may be connected to the outside for remote maintenance. There have been incidents where attackers log into maintenance terminals due to configuration errors, and launch attacks from there.

There are also attacks where attackers directly target data physically from PLCs (4). There may be cases where due to inadequacies in managing factory entry and exit, external intrusions are allowed, or there may be insiders with monetary motives. Finally, there is information leakage from the discarded devices (5). If FA devices like PLCs are discarded without proper handling, there is a risk of important information being extracted from them.

3. Damages

What kind of damage could occur if the FA system suffers a cyber attack? Figure 2 shows an example of damage.



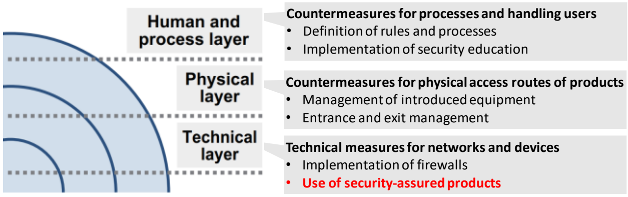
Information	Leakage of confidential information regarding PLCs and equipment production information.	▶	The foothold for the next attack. Imitation of products and devices.
Control	Infiltration of unauthorized programs into PLCs and execution of unauthorized control instructions.	▶	Occurrence of accidents on-site. Production of defective products
Production	PLC and equipment failure Production stoppage	▶	Stopping of production

Fig.2 Examples of Damage Caused by cyber attacks

Firstly, information leakage is a concern. If confidential information from PLCs, know-how is leaked, it could lead to reduced competitiveness due to product or device replication, or the privileged information obtained from PLCs or devices could be used as the basis for further attacks. Next, damages are anticipated from unauthorized program infiltration and execution of invalid control instructions within the PLC. For example, in the sealing process, insufficient heating may result in the recall of all products because the preservation condition cannot be guaranteed, or damages such as accidents where workers are injured due to improper behavior of factory robot arms are conceivable. Finally, there could be a production stoppage. The PLCs may become inoperative, potentially stopping the entire production line and causing significant damage.

4. Countermeasures

How can you prevent damage from these cyber attacks in advance? Unfortunately, there is no superhero-like solution where just one measure will suffice. It is necessary to employ a multi-layered defense approach, reducing risks by using another defensive measure if one is breached. Figure 3 shows an example of defense using multiple layers that commonly known as Defense-in-Depth.



Countermeasures for processes and handling users
- Definition of rules and processes
- Implementation of security education

Countermeasures for physical access routes of products
- Management of introduced equipment
- Entrance and exit management

Technical measures for networks and devices
- Implementation of firewalls
- Use of security-assured products

Fig.3 Example of Defense Using Multiple Layers

Generally, defense is implemented through three layers: human and process defenses, physical defenses, and technical defenses. Moreover, multiple measures are implemented within each layer. Defense within the human, process, or physical layer is a measure implemented by the end user. On the other hand, it is achieved by having the products themselves used in the devices, such as PLCs, be secure and have the necessary security functions. In other words, the security required for OMRON controllers is security measures at this technical level.

5. The Role of OMRON Controllers

Fundamentally, it is necessary for the OMRON controller itself to be secure. For that, it is important that planning, development, and manufacturing take security into consideration. To this end, the Controller Division has obtained the international standard "IEC62443-4-1", which pertains to cybersecurity for FA systems. In accordance with this standard, OMRON ensures the security of its controllers.

The OMRON controllers address the threats from a technical perspective. User authentication functions eliminate attackers and the project file protection features shield important customer information and production from many threats.

Figure 4 shows some of the security features of the OMRON controller.

1. Infiltration from an external network
- User authentication
- Packet filter
- TCP/UDP port closing

2. Unauthorized acquisition and modification of data on the network route
- Secure Communication
- Secure Socket Service
- OPC UA Server
- DB Connection Service

3. Infiltration from within the internal network
- User authentication
- Packet Filter
- TCP/UDP Port Close

4. Illegal acquisition and rewriting of data in PLC
- Project File Protection
- Data Protection
- Write Protection for the CPU Unit
- Disable Backup to SD Memory Card Setting
- Disable Firmware Update Setting

5. Information Leakage from Waste Products
- User program execution ID
- Complete erasure function

Fig.4 Security Features in OMRON Controllers

6. Guidelines

OMRON controllers are equipped with various security features. The FA system can be protected from threats by correctly using these features. OMRON provides free guidelines[1] to help you fully and correctly utilize the security features of the controllers. The guideline includes expertise and precautions for using the security features of the NJ/NX series. It is necessary for end-users to implement their own defensive measures. OMRON also offers a free FA System Security Guideline to help end-users implement security measures.

7. Conclusion

As manufacturing sites become increasingly connected to external networks, convenience has been significantly enhanced. On the other hand, they are now exposed to the risk of cyber-attacks. There is no definitive solution that can absolutely guarantee security. The aim is to perform risk assessments tailored to the environment and reduce risks to acceptable levels through multi-layered defense.

We hope this white paper will be utilized to enhance the cybersecurity of FA systems.

References

1) Product Security | OMRON FA