

Automation Systems: Identifying Threats and Implementing Security Measures

Prepared by:
Loras Even
Managing Director
Technology Risk Management Services
RSM McGladrey, Inc.
loras.even@rsmi.com
319.274.8541

Industry in general has experienced a technology revolution. General network standards have replaced proprietary industrial systems, making the security of automation systems more important.

The 2009 RSM McGladrey Manufacturing and Wholesale Distribution (MWD) National Survey provided insight into the growing importance of information technology (IT) to industry in general. IT is considered a critical component of business operations by almost 90 percent of the companies surveyed and the importance of IT to manufacturing is further highlighted by the fact that 78 percent of the surveyed companies plan on expanding IT investment during a weak economy.

Not long ago, automated manufacturing and inventory systems (industrial systems) were often comprised of various proprietary pieces of equipment that did not support general networking standards. While the proprietary industrial systems were often difficult to interface into other business systems and processes, it also meant that various security attacks that attempted to wreak havoc in the office areas could not affect these systems. In essence, the industrial systems spoke a different language and simply didn't understand the attack language; therefore they were immune.

Industrial systems often did not comply with information standards as they were developed in a different environment where reliability, survivability, unique processes and environmental requirements were more important than standards support.

Over time, general networking standards have found their way into the industrial systems world. Examples of this include Microsoft Windows, TCP/IP, Web interfaces and even Java, a virtual machine standard supported in most browsers in use today. Examples of industrial system devices that now support or work with general networking standards include:

- HMI/SCADA
- PLCs
- CNCs
- Single Loop Control
- Process Control
- Motion Control

Allen Bradley and other industrial systems manufacturers often even include an embedded WEB server on many of their controllers. The WEB server in turn runs on an open source operating system which is most commonly UNIX.

A very common example of a wide-spread industrial system is the traditional phone system. The old phone system (Mountain Bell, Illinois Bell, Northwestern Bell, GTE, etc.) was a specialized

system that used to be impervious to common network and computer viruses. In the past, special equipment was needed to interface with the phone system and specialized signaling (SS7); protocols and even terminating devices (the phone you picked up at the telephone company) were needed. Now, the PDA or cell phone you carry is likely to run a version of Microsoft Windows or Mac OS, therefore making them susceptible to network attacks. Even the phone companies have migrated some of their production systems to standards based computing models (voice over IP for example).

Identify threats to industrial system security

A lot of the security concepts from office systems can be adapted to industrial systems; one of these concepts includes the identification of threats to security. It is generally best to start first with the concept of identifying common threats to industrial systems. Some of these examples may seem obvious but are often missed. Examples of common threats to industrial systems include at minimum the following:

Office systems – The enterprises own office systems are a source of many attacks. Several attacks often come from workstations that have become infected with worms that then they scan the networks including your industrial systems. Once they have identified a target they then begin to attack it.

Customer (WEB) access portals – Opening your systems to customer access is fairly common these days and for competitive reasons a necessity for most. Web services invite significant amounts of unwanted activity and often because of the portal or application many more vulnerabilities are created such as SQL injecting, Cross-site scripting and others. For example, in 2009, the Center for Internet Security identified that WEB attacks account for a large amount of data theft (tied for number two with hacking).

The only way to identify whether your company's customer (WEB) access portal is secure is by performing an application test. Application testing of these portals should be performed whenever a change is made to the program or annually at minimum.

Supplier personnel – Often maintenance personnel from vendors (sometimes the manufacturing reps themselves) are in possession of laptops that are themselves infected from having been connected to a previously infected network. These same laptops may contain your sensitive information which is lost and potentially misused if the supplier laptops are stolen.

Dual-purpose industrial workstations – As more of the "floor" workstations have become multipurpose units, they have become exposed to more threats, which in turn threaten the industrial

applications and systems. An example of this includes data collection workstations which are used to browse the Web during "down" times.

Wireless networks – Wireless networking and the flexibility of movement and other benefits have led to their widespread use in the implementation of industrial systems. Too often, they are not configured securely and expose the industrial network itself to additional threats that may lie outside of the building (wireless propagates well beyond a buildings walls in many cases).

Many readers of this document will probably identify additional threats not listed. Some threats may even be unique to your business due to several circumstances, such as proprietary processes.

Security in layers and segments (divide and conquer)

The most common approach today when implementing security is to follow a layered approach. Even the Transportation Security Administration (TSA) uses a layered approach when identifying terrorist paths; the TSA creates "layers" for the terrorist to traverse. Similarly, we must utilize a layered approach when implementing security measures and will also have to divide the network (segment).

First, we should be able to identify which components of our industrial systems are connected to the enterprise network. This may seem like a needless task, but we've found that when clients go through this exercise one member or another will bring up a system or two that are connected to the network that came about during a installation, repair or renovation of one of the production systems.

Once we have identified the industrial systems inventory, we need to identify connection points to the office network. Sometimes this may be a single connection point and sometimes it may be many points. We've found that many industrial networks, especially cabling, have developed over the course of time through convenience (proximity or distance of cable pull) rather than following a structured cable plan.

When you have identified the connection points you have then identified the point or points at which you need to create an access-control point or firewall. Most will recognize the purpose of a firewall is normally to protect our enterprise network from an untrusted network (Internet for example) but many have not thought of using one to protect various segments of the network from itself. Often, an internal firewall equivalent can be layer 3 switches or routers. A detailed discussion of the selection, configuration and implementation of the "firewall" is beyond the scope of this document. There are myriad of steps including

identifying and documenting permitted services, trusted hosts and network devices, etc.)

Now we've identified our industrial systems and segmenting the industrial network from other networks we need to work with each of the identified systems to determine whether they have been hardened to some standard (NIST, for example) and configured securely. Often, industrial systems are still installed with the primary goal being to make them work, while securing them is an afterthought. Too often they are left with shared or default userids and system admin passwords. This is often a slow and orderly process as unfortunately, the applications may not permit the same level of system standards as the regular enterprise systems.

Proactive security tools such as virus/malware, intrusion detection/prevention and other items should also be installed on the industrial systems that will permit them. Normally, the vendor of the system should be contacted prior to installation to verify that it will work with the security tool being implemented.

After the network assessment and secure re-design and deployment of the production systems and networks have been performed, a network security audit should be performed to test the systems. The security audit will verify the effectiveness of the security controls implemented and also identify where further security controls may be needed. Unfortunately, in the 2009 RSM McGladrey MWD Survey, it was discovered that that only 47 percent of companies perform security tests of their IT systems annually.

Conclusion

Industrial systems have transitioned from proprietary architecture to industry standards based architecture. While this transition has brought many benefits with it, it has also increased the potential security risks from various threats. What this means is that we must take proper steps to protect our industrial systems.

Those steps include:

- Network assessment and secure re-design and deployment as needed
- Industrial/Production Network systems security audit
- Application testing of customer portals

Loras Even is a managing director in RSM McGladrey's information technology practice. He can be reached at loras.even@rsmi.com.

RSM McGladrey, Inc. and McGladrey & Pullen LLP have an alternative practice structure. Though separate and independent legal entities, the two firms work together to serve clients' business needs. RSM McGladrey, Inc. is not a licensed CPA firm.

RSM McGladrey and McGladrey & Pullen serve clients' global business needs through their membership in RSM International, the seventh-largest worldwide organization of independent accounting and consulting firms (source: *International Accounting Bulletin*), with 680 offices and 27,000 professionals in 65 countries.

To learn more, call 800.274.3978 or visit www.rsmmcgladrey.com.

RSM! McGladrey
Accounting | Tax | Business Consulting