ARC VIEW

AUGUST 7, 2020

Practical Industrial Cybersecurity Solutions Enable Security for All Facilities

By Sid Snitkin

Summary

The prevalence of small, unprotected industrial control systems is undermining the security of our critical infrastructure. Many companies underestimate the risks and overestimate the costs of managing these systems.

Loss of control system integrity is a serious matter, regardless of system size. People can be hurt, equipment damaged, product quality degraded, and operations interrupted. Industrial companies invest in comprehensive cybersecurity programs to mitigate these risks in large facilities, but small systems are often ignored. Managers don't think the risks justify the high costs of a cybersecurity program. They also ignore the fact that digital transformation efforts can make small systems ideal launchpads for attacks on larger, more critical systems.

Many small industrial control systems are operating with the risks of serious compromises. There is no reason to accept this situation. As ARC learned in a recent briefing with Bayshore Networks, effective cybersecurity doesn't have to be complex or expensive.

There is no reason for companies to accept these risks. An effective cybersecurity strategy doesn't have to be complex or expensive. Cost-effective, low maintenance approaches can significantly reduce the risks of threats and unauthorized changes.

Recently, ARC Advisory Group discussed the challenge of extending security to smaller systems with executives from Bayshore Networks. This company offers a range of practical, cost-effective industrial network security solutions for industrial and critical infrastructure control systems.

Small Systems Can Represent Big Risks

Industrial control systems (ICS) typically range in size from small, isolated systems for HVAC in buildings and data centers to very large, integrated plant control systems. Malfunctions in small systems can be just as

damaging as those in large systems. Data centers and buildings can't operate without trustworthy HVAC and power management systems. Small systems can also provide pathways for attackers to pivot into larger, more critical OT and IT systems. Target suffered $18.3 million in losses when attackers gained access to 41 million customer accounts through an insecure HVAC system. And these kinds of pivoting risks are growing as digital transformation demands more connectivity with small systems.

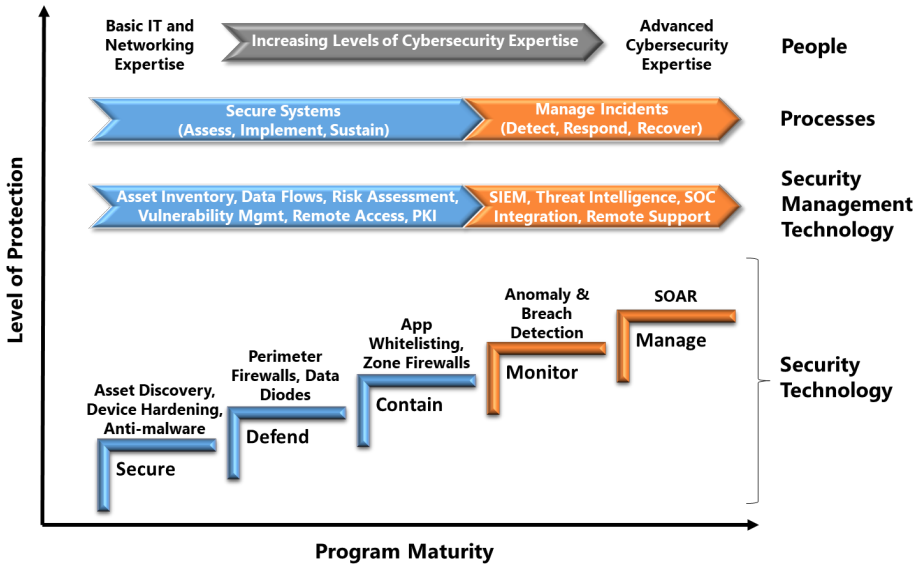
Small, unprotected systems are easy targets for attackers as many use products with known vulnerabilities. Surveys by security researchers also show that many have open internet connections that can be discovered through common, open source tools. These ports often provide VPN access for equipment suppliers, with simple passwords for security. Even new systems can be delivered with security risks, as many suppliers lack secure development practices.

At a minimum, organizations need to recognize these security risks and implement basic security policies and defenses that block attacker access to small systems and their links to more critical systems.

Building a Cybersecurity Program for Small Systems

ARC's Industrial/OT Cybersecurity Maturity Model can help industrial companies balance cyber risk reduction with financial and resource capabilities. This model aligns with the NIST Cybersecurity Framework recommendations and provides a recommended sequence of security layers that reduce cyber risks incrementally. Each layer addresses a specific, easily understandable security issue such as **securing** individual devices, **defending** systems from external attacks, **containing** malware spread, **monitoring** for signs of latent compromises, and **managing** active attacks and cyber incidents.

Each layer has an associated set of technologies that can be used to accomplish its goals. Blue and orange colors in the model distinguish basic defensive technologies from advanced technologies to support active defenders.



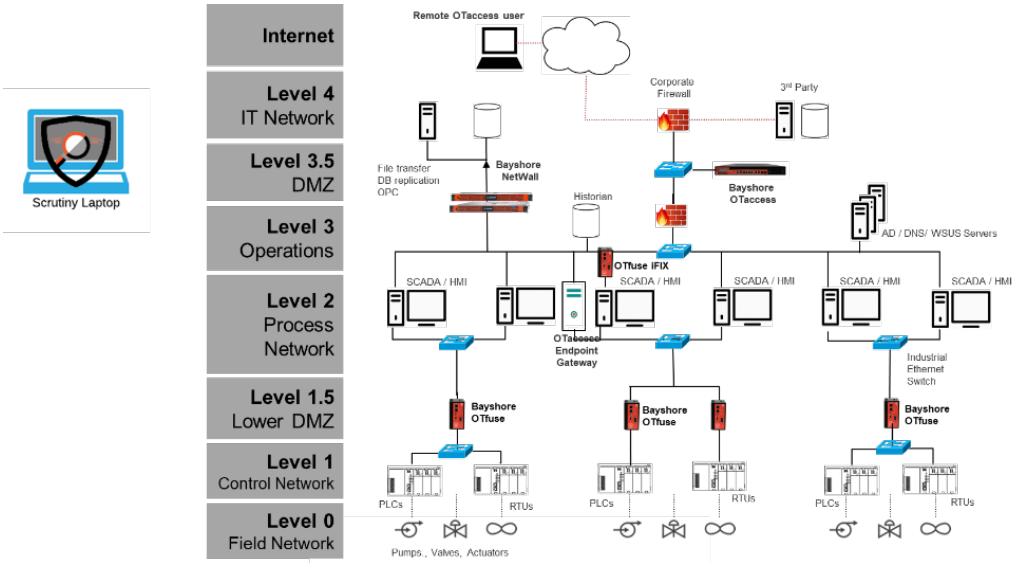
ARC Industrial/OT Cybersecurity Model

Resource requirements grow as programs add layers. Security technologies need periodic updates, alerts need to be analyzed, and compromises need to be addressed. Maintenance personnel can often maintain basic defenses with inexpensive vulnerability management tools. But to derive value from advanced security solutions, companies require cybersecurity professionals and sophisticated tools for forensics and remediation. Costs for cybersecurity include security technologies, security management technologies, and resources. These costs increase rapidly when companies implement advanced cybersecurity programs.

The additional costs for advanced security may be justifiable for large and critical control systems. But for most small systems, the basic defenses described in the first three steps of ARC's model are often sufficient to reduce local safety and operational risks as well as the risks of an attacker using the system as a launchpad for attacks on more critical systems. Focusing cyber investments on these layers can also minimize or eliminate the need for costly cybersecurity resources.

Bayshore Networks Solutions Address Small System Needs

Bayshore Networks, a supplier of network security solutions for industrial/OT systems, recognizes the importance of securing small industrial control systems. The company also understands the challenges in justifying security investments. Bayshore designed its portfolio of cost-effective, practical security solutions to enable companies to secure all of their control systems, regardless of size.



Bayshore Networks Security Solutions

Defend and Contain Products

Bayshore Networks offers two products that can help companies achieve ARC's *defend* and *contain* goals. These products protect assets against network-based cyber attacks and other dangerous events. These events include configuration changes, logic programming modifications, and device resets that might jeopardize process control and operational performance. The products also prevent unauthorized access to critical, proprietary data.

OTfuse, the company's flagship product, is an industrial deep packet inspection (DPI) network security solution. The device provides OSI layer 7 message parsing for a wide range of industrial protocols and granular validity checking based upon the Pallaton Policy Enforcement Engine. OTfuse includes a learning mode that automates the generation of message whitelisting policies for normal operational exchanges between assets. Messages that violate these policies can be blocked and/or alerted so the device can

also be used for basic anomaly and breach detection. OTfuse can be used to protect a single device, a small network segment, or an entire group of control systems.

NetWall is the company's offering to help companies secure and isolate critical IT and OT systems and trusted domains without the added cost, time, and complexity of typical network segmentation projects. It allows assets within a protected network segment to send messages to external systems but blocks external messages from entering the protected domain. This isolation is accomplished with a high-speed, software-based, data diode that ensures non-routable, unidirectional file transfers, database sharing, and server replication. The device supports guaranteed delivery of unidirectional communications for TCP, UDP, file transfer, OPC, and Modbus/TCP messages. NetWall can be used in IT and OT systems, at perimeters to isolate an entire group of systems, or to create trusted domain isolation of small network segments.

Security Management Products

Bayshore Networks offers two products that can help companies establish and maintain security within all system assets.

Scrutiny is Bayshore Network's OT asset discovery and flow visualization tool that companies can use to secure OT systems. This Windows-based application collects a snapshot of OT network traffic data through a local network interface or switch span/mirror port. Collected data is analyzed to identify all system assets and data flows and a report is generated that identifies all devices and the related information needed to develop security defenses. This includes operating system, IP address, MAC address and vendor, as well as country and public DNS, if available. The product understands industrial and IT protocols and can identify what equipment, protocols and ports are in use as well as the source and destinations of all message flows. The product can also be used to analyze packet capture (PCAP) data files. Bayshore offers Scrutiny as a free download for users.

OTaccess

OTaccess, a flexible, remote access solution, provides granular, controlled access to designated OT assets and services. The product provides far more security than conventional VPN connectivity, as it manages end-to-end, encrypted access according to protocol, port, and user. Before any access is

permitted, users need to explicitly expose the endpoint and service and give users permission to access specific endpoint/service combinations. This approach allows remote employees and third-party vendors to access specific OT system assets without exposing the rest of the system to threats. It also enables user policies that prohibit actions on OT assets and networks without line of sight support.

Conclusion

Clearly, securing small industrial control systems is a serious matter. A cyber compromise or unauthorized change can impact the health and safety of people, damage costly equipment, and disrupt operations for extended periods. Ongoing digital transformation efforts also increase the likelihood that small systems will be used to launch attacks on critical corporate systems. Unfortunately, many companies still don't appreciate these risks. Those that do still struggle to justify security investments because they assume they need costly, advanced cybersecurity programs.

As ARC learned, companies don't need expensive solutions and costly cybersecurity experts for every small industrial control system. In many cases, they can reduce risk significantly using basic security practices and technologies. Bayshore Networks offers practical, cost-effective solutions to meet these needs. Prudent companies will review their small system risks and make the appropriate investments in basic cybersecurity defenses.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.