Safeguarding and Securing Automotive Manufacturing Systems

Jeff Smith
jeffrey.smith@dynics.com
How much did we want to spend on ICS Security?

Nada...Zip...Nothing...Zilch.
How much industrial control system security was/is enough?

Whatever security was/is necessary to mitigate the risk that we/you are not willing to live with.
How did we decide what is important when it comes to securing our manufacturing floor?

There is no single answer. Each organization will have objectives and goals that are different from the others.
5 Attitudes towards ICS Security

1. **Prophet or Evocator** and in some cases Alarmist  
   Definition: One who calls to arms

2. **Naysayer or Defeatist**  
   Definition: An advocate or follower of defeatism as policy

3. **Apathetic**  
   Definition: Not interested or concerned, indifferent or unresponsive

4. **Purposefully Negligent** (self-preserving)  
   Definition: Unconscionable behavior / attitude

5. **Proactive** (synonym for fanatical or anxious)  
   Definition: Tending to initiate change rather than reacting to events
Step #1 - Assess

Where are you today and where do you want to be?

Remember that the last 20% is exponentially more expensive than the first 80%.
Choose the most actionable and beneficial items to the organization and get started.

Perhaps a grand plan isn’t right for the organization today, maybe “low hanging fruit is the catalyst”.

“Maybe” Create ICS Security Policy first. It would a novel idea to create policy first, and then enact it...
Step #3 – Execute

Set a pace...ANY PACE..just don’t stop!
Automotive Use Case

Tier 1 Automotive Supplier – Multiple Global Locations
Why?

- Protect our Associate’s Safety
- Protect our Equipment Safety
- Protect our Intellectual Property
- Protect our Customers’ Intellectual Property
- Protect our Delivery Schedule
We weren’t launching rockets....

Which meant the idea of “lock it all down” didn’t really fit our organizational needs.
We recognized this philosophical difference...

IT Security needs to allow everything except known badness.

ICS Security needs to prohibit everything except what is explicitly needed.
After assessing our posture, we came up with 5 initial objectives.
Key objective #1

• Protect the controls network from the enterprise network and the enterprise network from the controls network.
Key objective #2

• Secure and Safe Remote Support Capability from inside and outside the enterprise
Key objective #3

- Control & track supplier access to control systems when onsite or remote.
Key objective #4

- Protect manufacturing systems from malware attack by removing PC(s) from or isolating them on the controls network.
Teardown PC uses OpenVPN Certificate based Connection to ICS-Defender

NIC #1 to Enterprise Network

NIC #2 To PoE Injector and Scanner

PoE Injector if PoE Scanner is Used

NO PHYSICAL CONNECTION OF THIS EQUIPMENT TO THE EIP FIELDBUS
Key objective #5

• Implement an asset management system which provides audit trail and backup / recovery for critical controls assets.

We will never stop every attack, therefore our strategy must include detection and recovery.
Final Thought #1

**Manufacturing Control Systems should be designed for security.**

We have an advantage over traditional Cybersecurity in our ability to monitor and prevent catastrophe with hardwired safety. It’s our “Cockpit Door.”

When was the last time you reviewed your standard electrical drawings with an eye towards inherent security?
After significant investigation, research, testing we determined that most ICS appliances in the industrial space do not address all, or even most, of the needs of more than a basic implementation. We were fortunate to find one that did.
The majority of suppliers developing security products for manufacturing don’t understand lifecycle and implementation differences between IT space and the plant floor.
Final Thought #4

We avoided signature based appliances as we believe they are difficult and risky to manage on a plant floor.

1. Supplier identifies a new threat.

2. Supplier delivers the signature to end users for testing, they SHALL NOT simply deploy it to plant floor security devices globally in any automatic way. PERIOD.

3. In their free time, Controls Engineering will begin to vet the update and once complete, quickly deploy it to hundreds of security devices when that equipment is not running production.

4. By the time this process is done (months), the supplier will have released a couple more updates.
Necessary Features

- Stateful Firewall
- State Table
- Deep Packet Inspection (DPI)
- NAT (1:1, Outbound, etc.)
- High Availability (failover)
- Virtual Private Networking (Both IPSec and SSL)
- Captive Portal
- Reporting & Monitoring
- Easy replication of configurations (by people without degrees in security/firewall)
- Fast throughput (with full DPI), low latency
- LDAP/AD Integration
- Syslog Integration
- Local or remote Certificate Management
Questions?

Jeff Smith
Chief Technology Officer
jeffrey.smith@dynics.com

DYNICS Inc.
620 Technology Drive
Ann Arbor, MI 48108 USA