Cybersecurity Considerations – for Defense Manufacturers

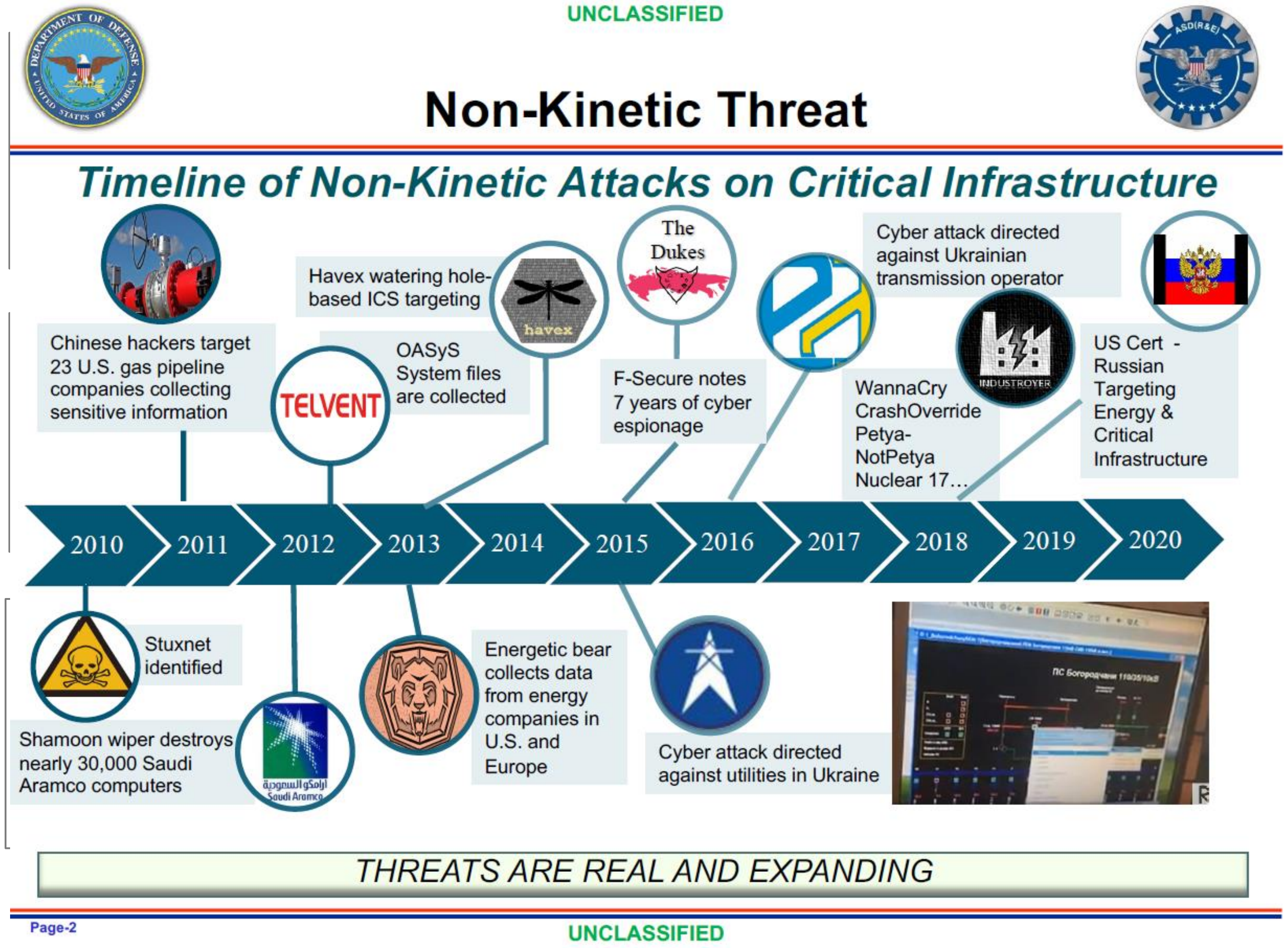
NDIA - Manufacturing Division February Meeting

16FEB2022

Richard Robinson/CEO Founder
Cynalytica Inc.

Approved for Public Release

Existential Problem: Critical Infrastructure Attacks on the Rise



UNCLASSIFIED

Non-Kinetic Threat

Timeline of Non-Kinetic Attacks on Critical Infrastructure

- 2010: Stuxnet identified
- 2011: Chinese hackers target 23 U.S. gas pipeline companies collecting sensitive information
- 2012: Shamoon wiper destroys nearly 30,000 Saudi Aramco computers
- 2012: OASyS System files are collected
- 2013: Havex watering hole-based ICS targeting
- 2013: Energetic bear collects data from energy companies in U.S. and Europe
- 2015: F-Secure notes 7 years of cyber espionage
- 2015: Cyber attack directed against utilities in Ukraine
- 2016: Cyber attack directed against Ukrainian transmission operator
- 2018: WannaCry CrashOverride Petya-NotPetya Nuclear 17…
- 2019: US Cert - Russian Targeting Energy & Critical Infrastructure

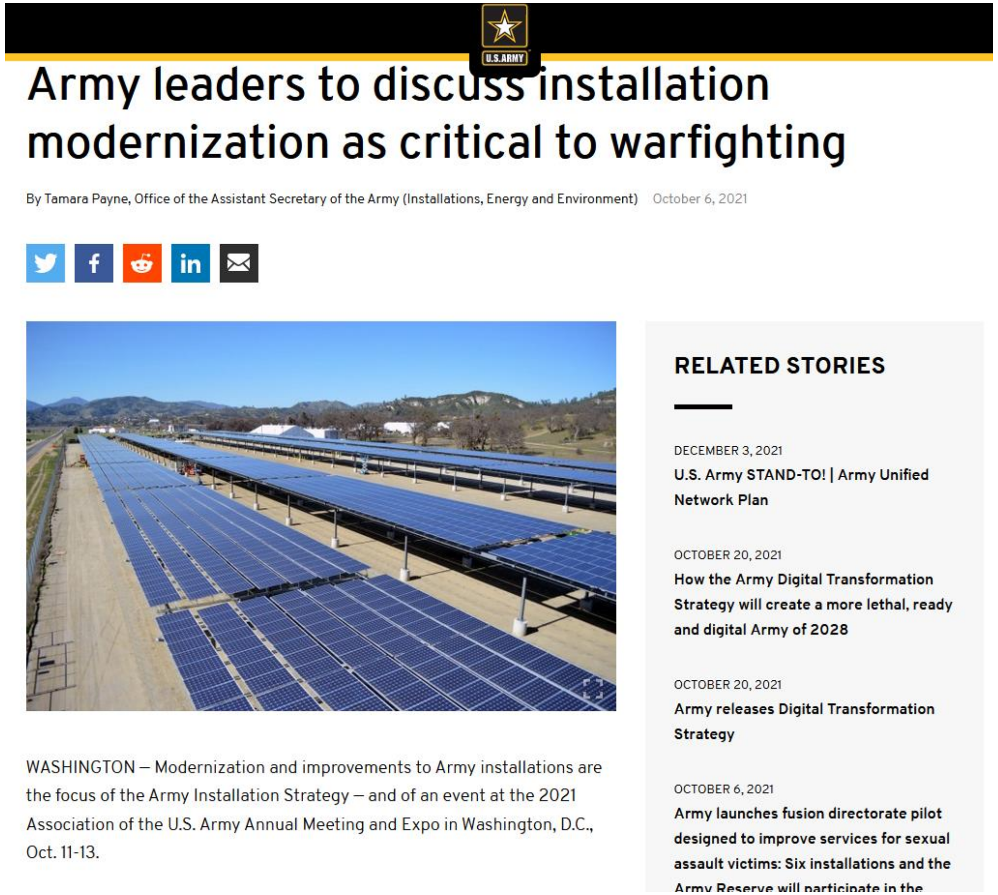
THREATS ARE REAL AND EXPANDING

Page-2

UNCLASSIFIED

- Nation-states increasingly target defense critical infrastructure with high degree of sophistication and evasion.
- Forces rely on services from communications, electric, natural gas, and water/wastewater utilities etc.
- A significant number of weapons systems and manufacturing environments rely on legacy serial communications
- Adversaries can leverage capabilities to specifically disrupt missions or harm soldiers

The Problem:
Focused Attacks on Defense Infrastructure & DIB



U.S. ARMY

Army leaders to discuss installation modernization as critical to warfighting

By Tamara Payne, Office of the Assistant Secretary of the Army (Installations, Energy and Environment) October 6, 2021

WASHINGTON – Modernization and improvements to Army installations are the focus of the Army Installation Strategy – and of an event at the 2021 Association of the U.S. Army Annual Meeting and Expo in Washington, D.C., Oct. 11-13.

RELATED STORIES

DECEMBER 3, 2021
U.S. Army STAND-TO! | Army Unified Network Plan

OCTOBER 20, 2021
How the Army Digital Transformation Strategy will create a more lethal, ready and digital Army of 2028

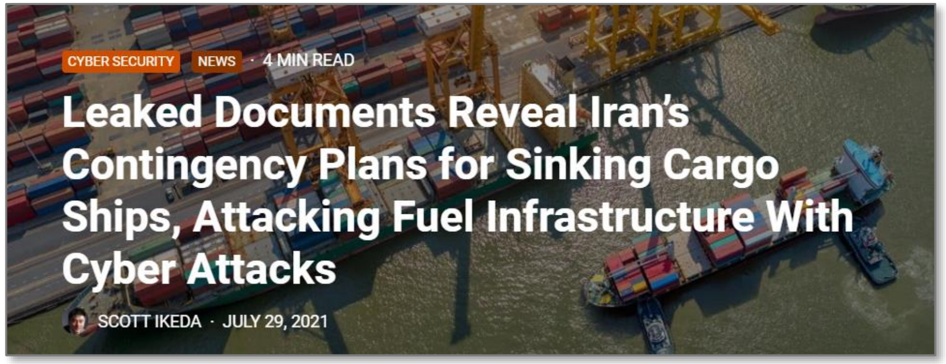
OCTOBER 20, 2021
Army releases Digital Transformation Strategy

OCTOBER 6, 2021
Army launches fusion directorate pilot designed to improve services for sexual assault victims: Six installations and the Army Reserve will participate in the

" the Army is at a pivotal point in its history: one that sees the battlefield move from beyond our borders to ***within the walls of our installations, in a domain that is multifaceted and often invisible***." October 06, 2021

https://www.army.mil/article/250963

Increasing and Unaddressed Risk



CYBER SECURITY NEWS · 4 MIN READ

Leaked Documents Reveal Iran's Contingency Plans for Sinking Cargo Ships, Attacking Fuel Infrastructure With Cyber Attacks

SCOTT IKEDA · JULY 29, 2021

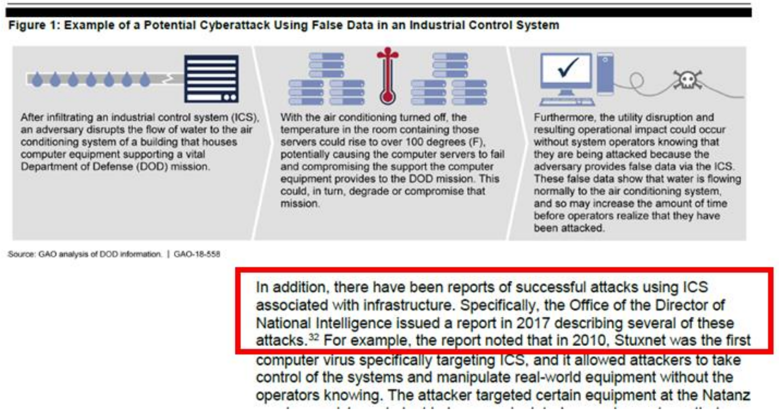


Figure 1: Example of a Potential Cyberattack Using False Data in an Industrial Control System

After infiltrating an industrial control system (ICS), an adversary disrupts the flow of water to the air conditioning system of a building that houses computer equipment supporting a vital Department of Defense (DOD) mission.

With the air conditioning turned off, the temperature in the room containing those servers could rise to over 100 degrees (F), potentially causing the computer servers to fail and compromising the support the computer equipment provides to the DOD mission. This could, in turn, degrade or compromise that mission.

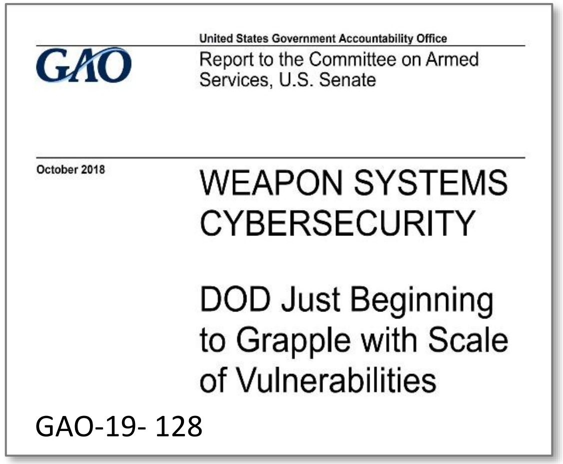
Furthermore, the utility disruption and resulting operational impact could occur without system operators knowing that they are being attacked because the adversary provides false data via the ICS. These false data show that water is flowing normally to the air conditioning system, and so may increase the amount of time before operators realize that they have been attacked.

Source: GAO analysis of DOD information. | GAO-18-558

In addition, there have been reports of successful attacks using ICS associated with infrastructure. Specifically, the Office of the Director of National Intelligence issued a report in 2017 describing several of these attacks.[32] For example, the report noted that in 2010, Stuxnet was the first computer virus specifically targeting ICS, and it allowed attackers to take control of the systems and manipulate real-world equipment without the operators knowing. The attacker targeted certain equipment at the Natanz

Microsoft Accepts it was Affected by SolarWinds Hack

#DailyCybesecurityNews



United States Government Accountability Office

GAO

Report to the Committee on Armed Services, U.S. Senate

October 2018

WEAPON SYSTEMS CYBERSECURITY

DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19- 128

"In addition, there have been reports of successful attacks using ICS associated with infrastructure.

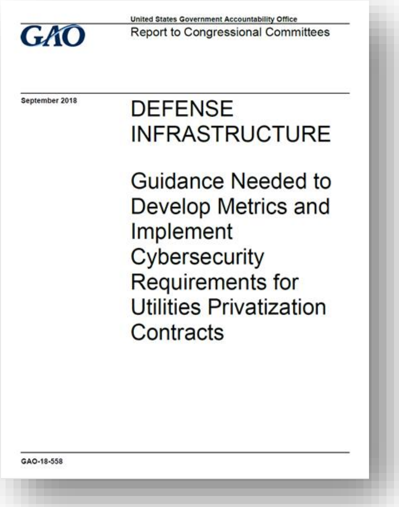
Specifically, the Office of the Director of National Intelligence issued a report in 2017 describing several of these attacks."

House of Lords
House of Commons

Joint Committee on the National Security Strategy

Cyber Security of the UK's Critical National Infrastructure

Third Report of Session 2017–19



United States Government Accountability Office

GAO

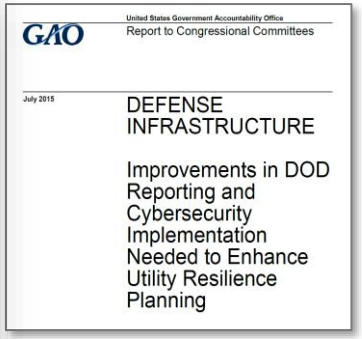
Report to Congressional Committees

September 2018

DEFENSE INFRASTRUCTURE

Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts

GAO-18-558



United States Government Accountability Office

GAO

Report to Congressional Committees

July 2015

DEFENSE INFRASTRUCTURE

Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning

GAO-15-749

Internal Problem:
Operational Complexity and Scale Complicates Effective Solutions

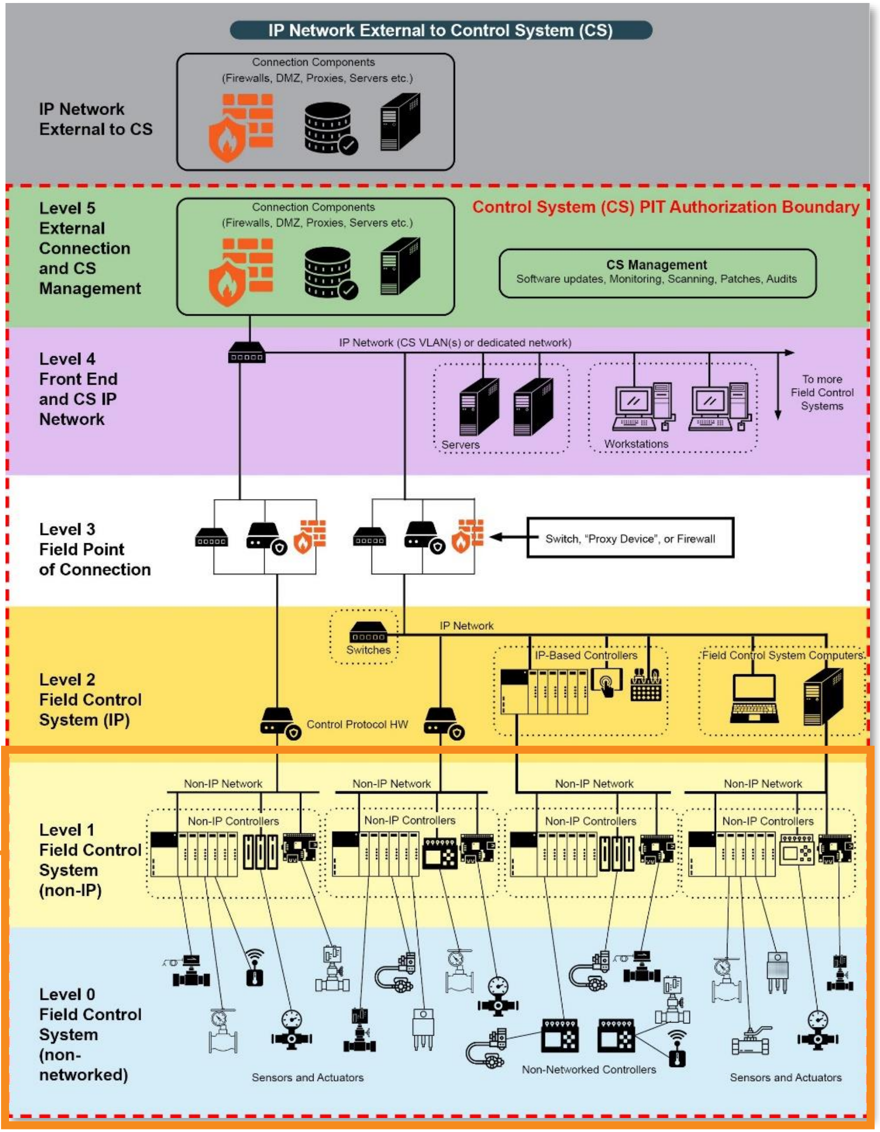
Cyber Operator – strong knowledge of the data, but may be overwhelmed with alerts

Control Systems Engineer – understands the systems but not the cyber data

Incident Response Team – deep cyber experts, but not system experts

Manufacturing ICS/SCADA's Blind Spot

- Legacy ICS communicate using insecure protocols (serial)
- Prevalent in Level 0/1 of OT Network (control cyber-physical processes)
- If adversaries bypass, evade or alter TCP/IP based intrusion detection tools, they can enact cyber-physical damage – potentially without being detected
  - Capabilities gap in current ICS cybersecurity solutions.

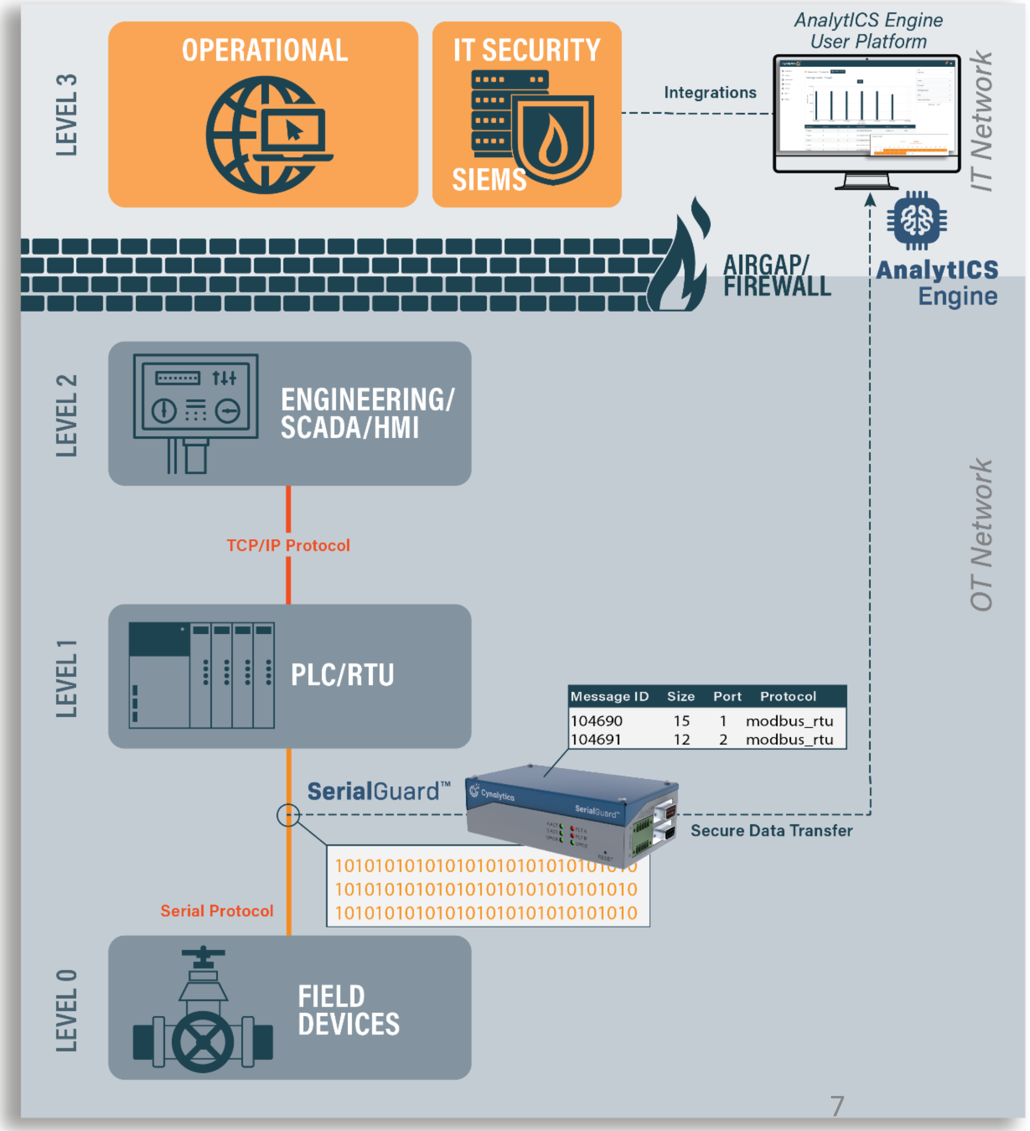

IP Network External to Control System (CS)
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc.)
Level 5 External Connection and CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc.)
Control System (CS) PIT Authorization Boundary
CS Management
Software updates, Monitoring, Scanning, Patches, Audits
Level 4 Front End and CS IP Network
IP Network (CS VLAN(s) or dedicated network)
Servers
Workstations
To more Field Control Systems
Level 3 Field Point of Connection
Switch, "Proxy Device", or Firewall
Level 2 Field Control System (IP)
IP Network
Switches
IP-Based Controllers
Field Control System Computers
Control Protocol HW
Level 1 Field Control System (non-IP)
Non-IP Network
Non-IP Network
Non-IP Network
Non-IP Network
Non-IP Controllers
Non-IP Controllers
Non-IP Controllers
Non-IP Controllers
Level 0 Field Control System (non-networked)
Sensors and Actuators
Non-Networked Controllers
Sensors and Actuators

Purdue Enterprise Reference Architecture

Cyber Analytics Use Case

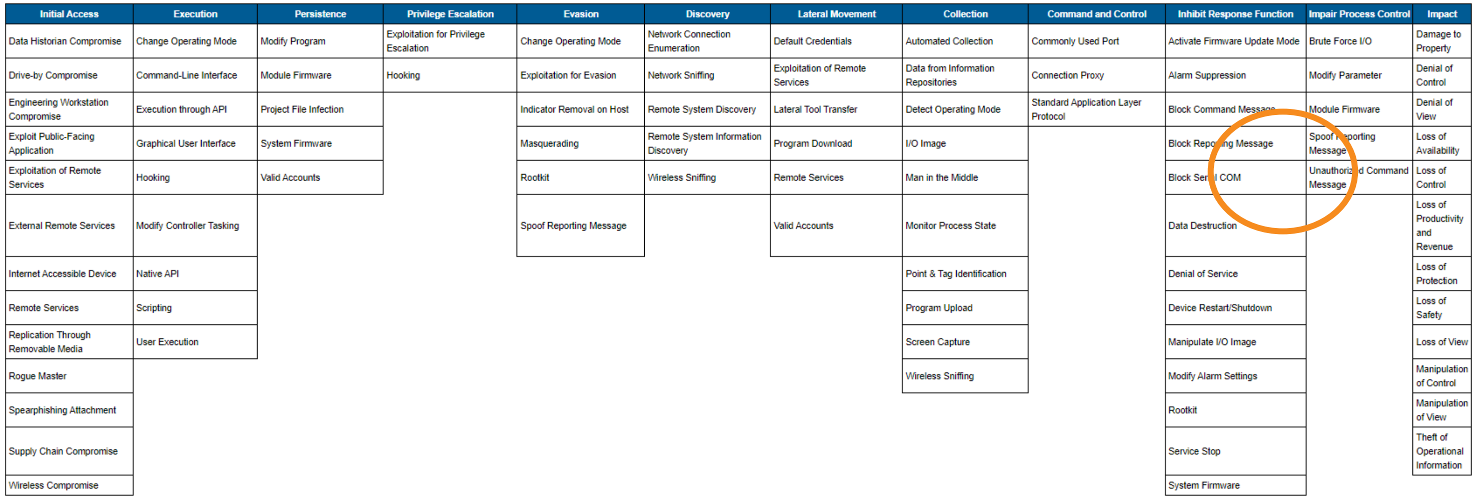
Example: Stuxnet - like

- Adversary compromises PLC (level 1)
- Adversary sends malicious commands to centrifuges (level 0)
- Adversary sends false data to HMI (level 2) to show normal operations
- Platform is tapping the data between the PLC and VFD controlling the centrifuges (level 0/1), enabling it to detect malicious commands which would go otherwise undetected.



Message ID	Size	Port	Protocol
104690	15	1	modbus_rtu
104691	12	2	modbus_rtu

Mapping to MITRE ATT&CK for ICS



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

IMPAIR PROCESS CONTROL

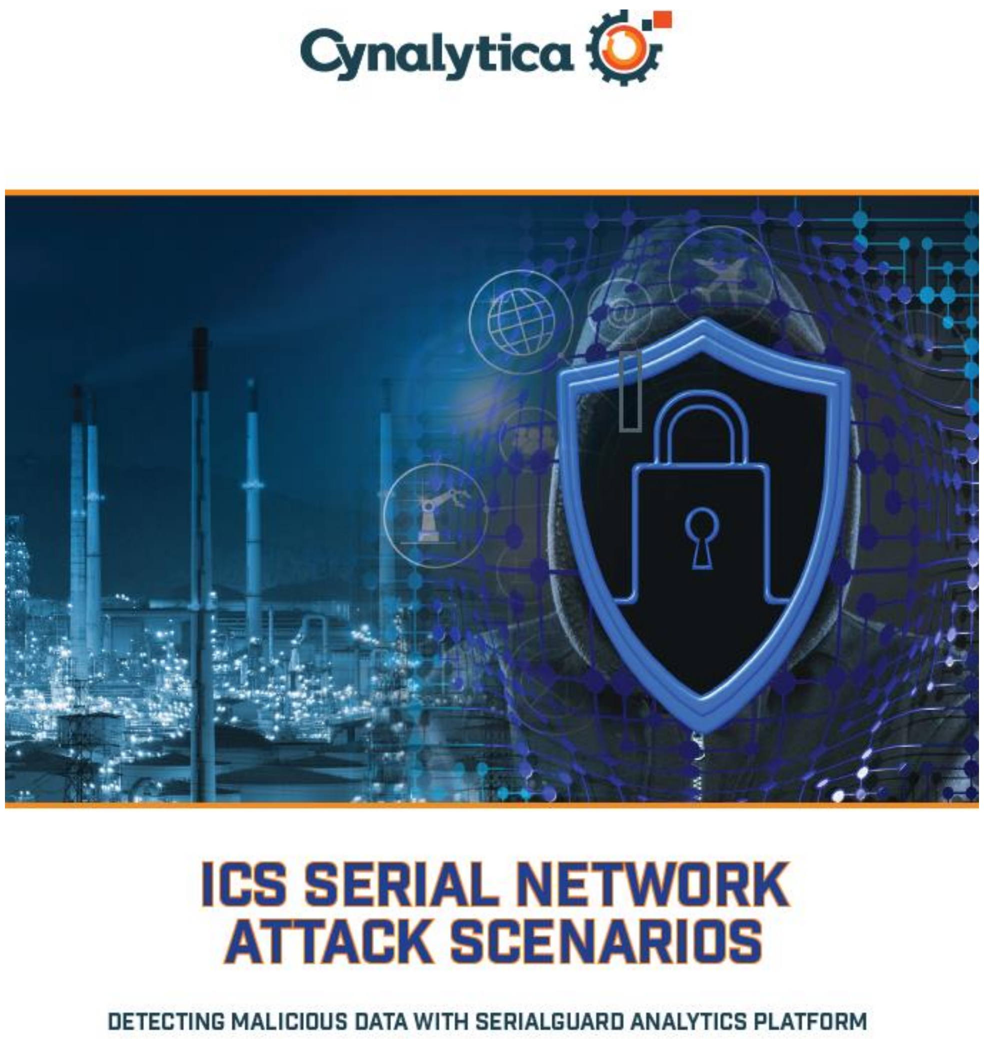
SPOOF REPORTING MESSAGE

UNAUTHORIZED COMMAND MESSAGE

In states 3 and 4 ***Stuxnet*** *sends two network bursts (done through the DP_SEND primitive). The data in the frames are instructions for the frequency converter drives.*

Source: https://collaborate.mitre.org/attackics/index.php/Technique/T0855

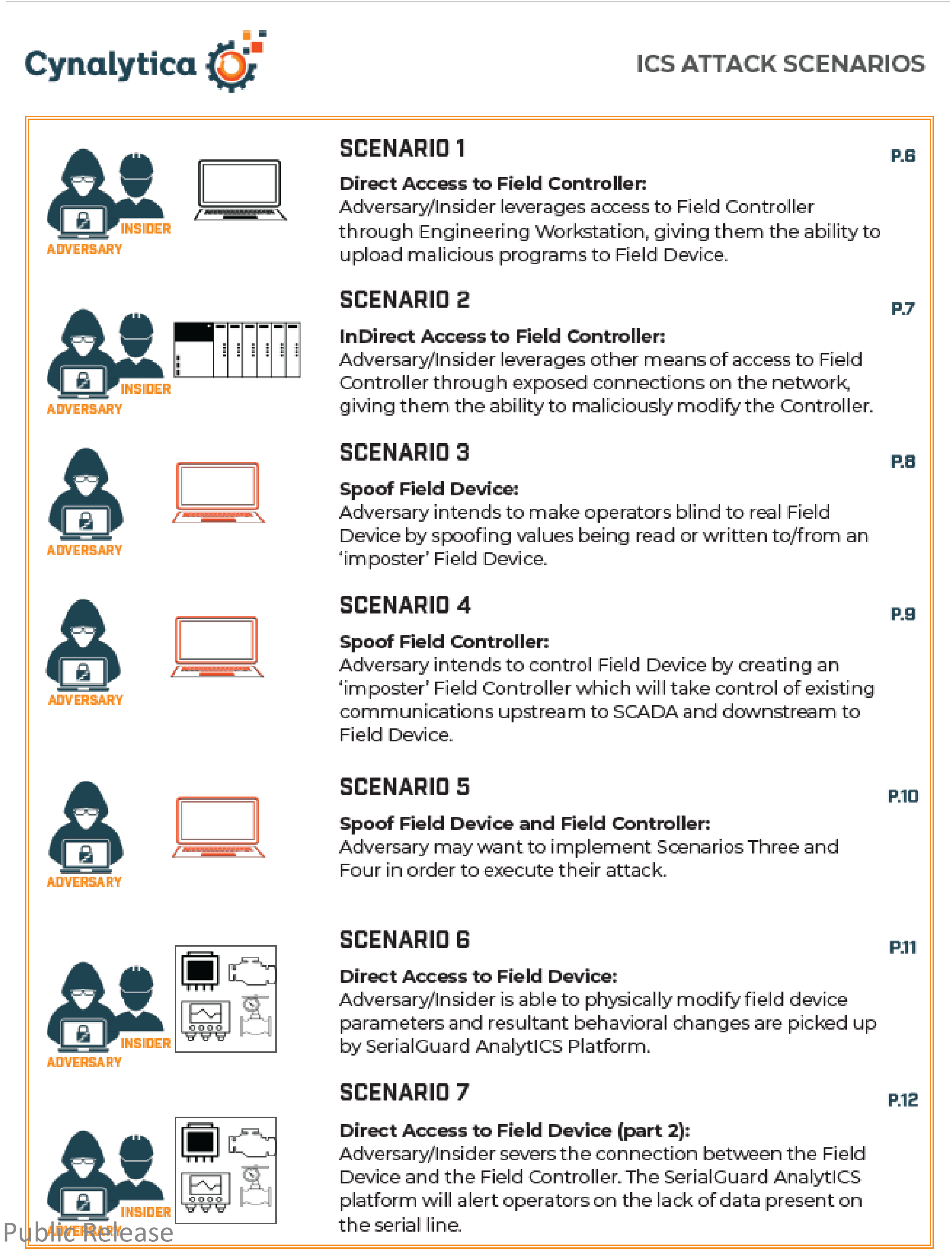
Legacy Infrastructure: Misunderstood



Cynalytica

ICS SERIAL NETWORK ATTACK SCENARIOS

DETECTING MALICIOUS DATA WITH SERIALGUARD ANALYTICS PLATFORM



Cynalytica

ICS ATTACK SCENARIOS

SCENARIO 1 P.6

Direct Access to Field Controller:
Adversary/Insider leverages access to Field Controller through Engineering Workstation, giving them the ability to upload malicious programs to Field Device.

SCENARIO 2 P.7

InDirect Access to Field Controller:
Adversary/Insider leverages other means of access to Field Controller through exposed connections on the network, giving them the ability to maliciously modify the Controller.

SCENARIO 3 P.8

Spoof Field Device:
Adversary intends to make operators blind to real Field Device by spoofing values being read or written to/from an 'imposter' Field Device.

SCENARIO 4 P.9

Spoof Field Controller:
Adversary intends to control Field Device by creating an 'imposter' Field Controller which will take control of existing communications upstream to SCADA and downstream to Field Device.

SCENARIO 5 P.10

Spoof Field Device and Field Controller:
Adversary may want to implement Scenarios Three and Four in order to execute their attack.

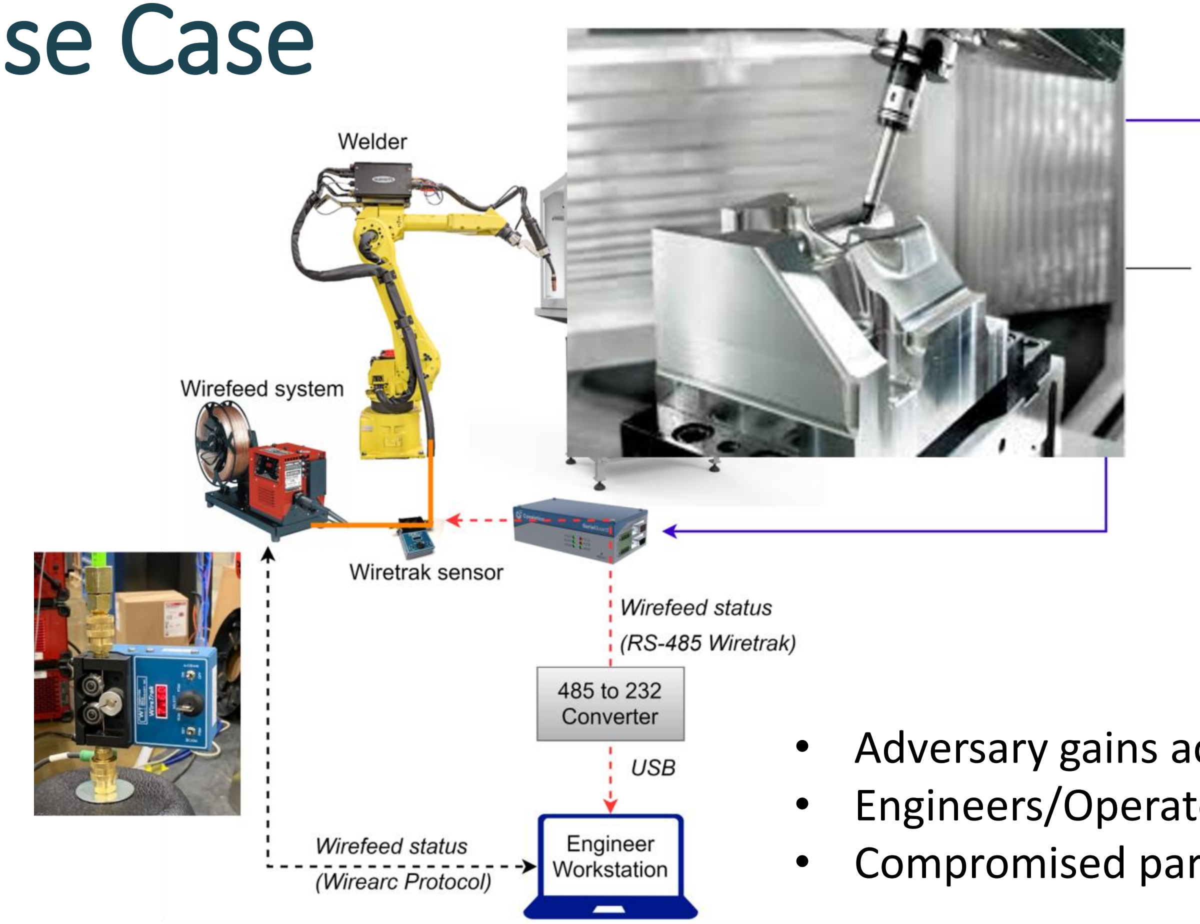
SCENARIO 6 P.11

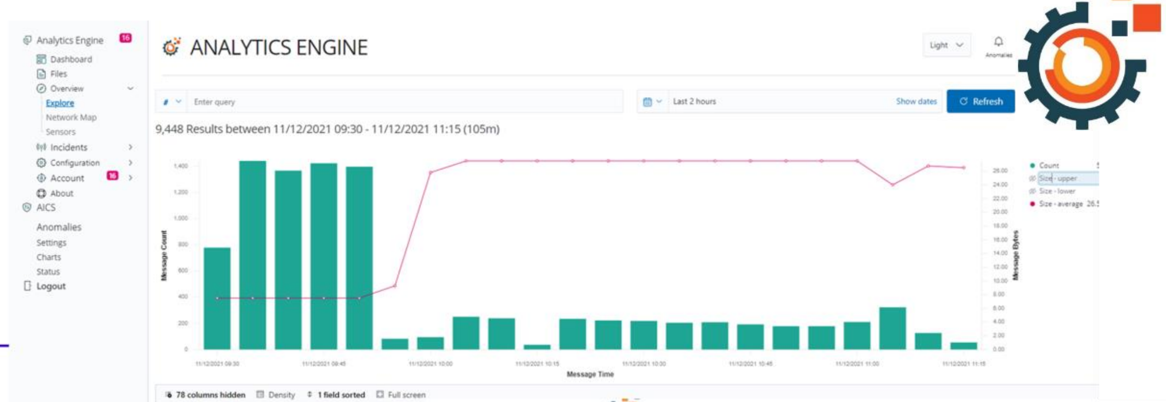
Direct Access to Field Device:
Adversary/Insider is able to physically modify field device parameters and resultant behavioral changes are picked up by SerialGuard AnalytICS Platform.

SCENARIO 7 P.12

Direct Access to Field Device (part 2):
Adversary/Insider severs the connection between the Field Device and the Field Controller. The SerialGuard AnalytICS platform will alert operators on the lack of data present on the serial line.

Additive Manufacturing Use Case

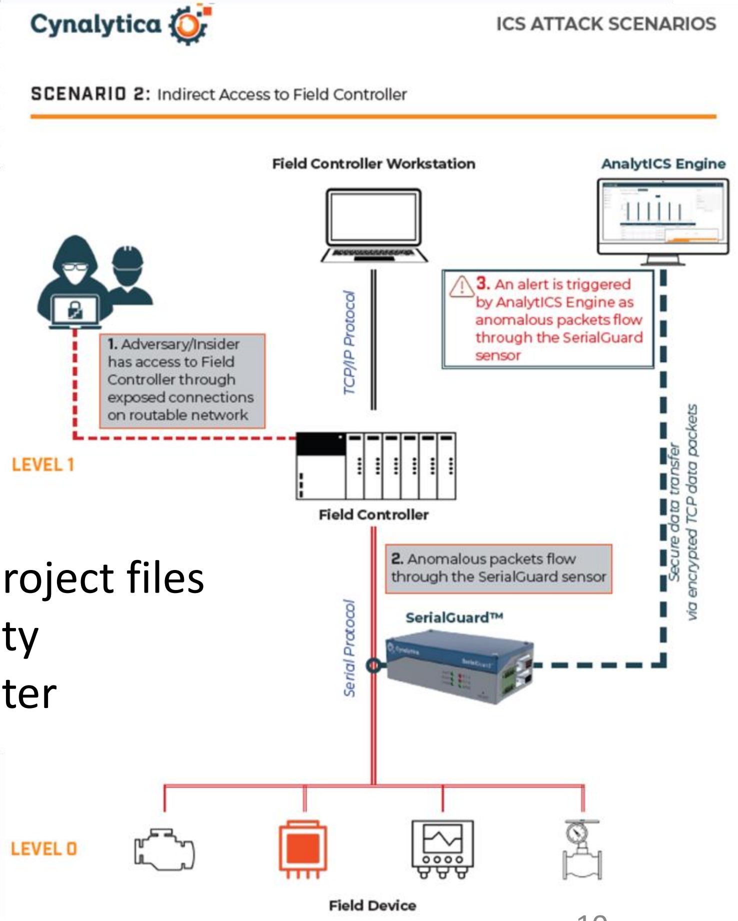




9,448 Results between 11/12/2021 09:30 - 11/12/2021 11:15 (105m)

78 columns hidden · Density · 1 field sorted · Full screen

Message Time	Register Value 40021
12-11-2021 11:17:08.0890	0
12-11-2021 11:17:08.0880	
12-11-2021 11:17:03.0880	0
12-11-2021 11:17:03.0870	
12-11-2021 11:16:58.0860	0
12-11-2021 11:16:58.0850	
12-11-2021 11:16:56.0820	0



1. Adversary/Insider has access to Field Controller through exposed connections on routable network

2. Anomalous packets flow through the SerialGuard sensor

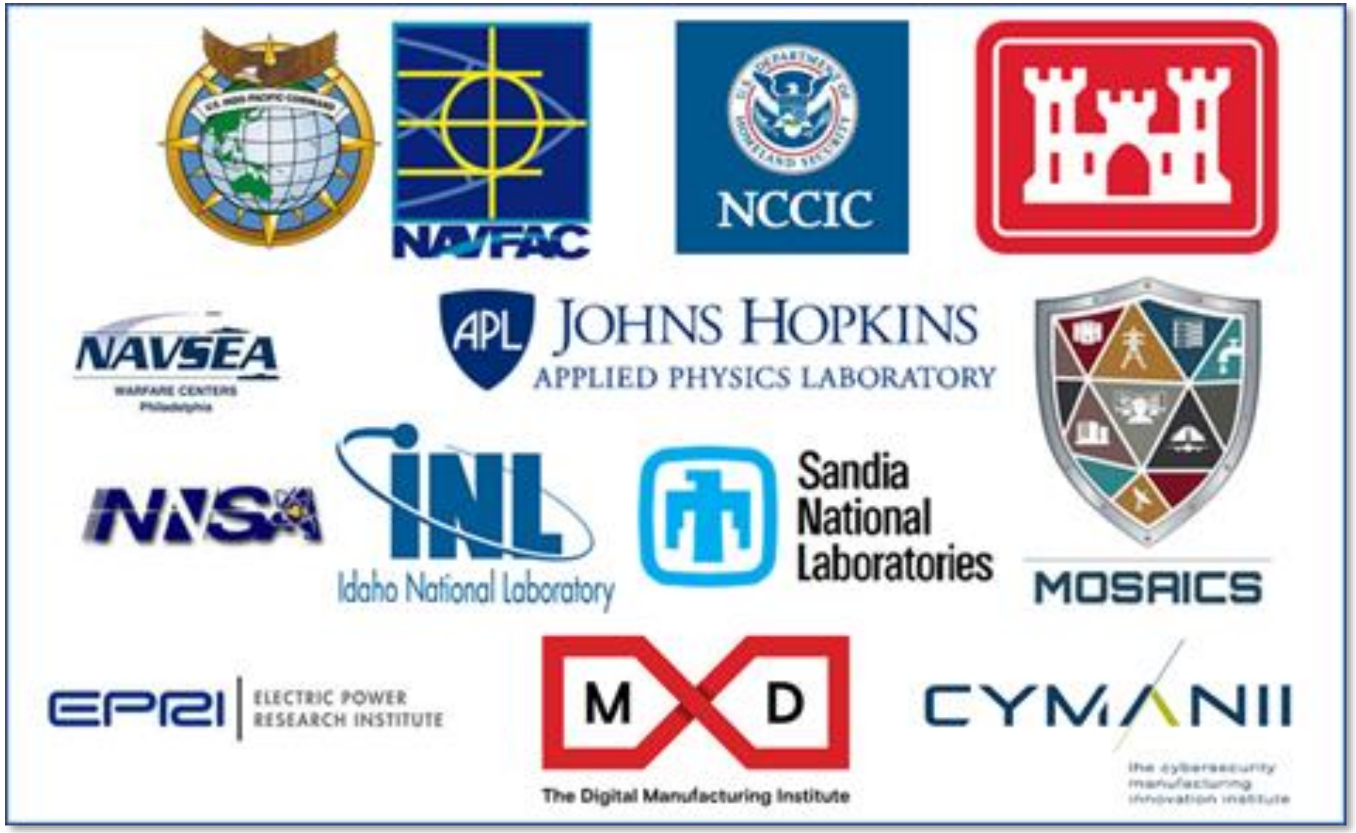
3. An alert is triggered by AnalytICS Engine as anomalous packets flow through the SerialGuard sensor

- Adversary gains access alters product/project files
- Engineers/Operators lack system visibility
- Compromised part delivered to warfighter

Approved for Public Release

Other Challenges/Scenarios:

- Ransomware
- “Digital Transformation/Industry 4.0”
- Staffing/Expertise/Resourcing
- Platform Debates
  - Cyber Tool Debate – Cost Center
  - Operational Efficiencies – Return on Investment
    - Asset Management
    - Configuration Optimization
    - Anomaly Detection (Cyber and Operational)
    - Prescriptive Maintenance
    - Predictive Failures
- Monitoring & Situational Awareness


NAVFAC
NCCIC
NAVSEA
WARFARE CENTERS
Philadelphia
APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY
NNSA
INL
Idaho National Laboratory
Sandia
National
Laboratories
MOSAICS
EPRI
ELECTRIC POWER
RESEARCH INSTITUTE
M
D
The Digital Manufacturing Institute
CYMANII
the cybersecurity
manufacturing
innovation institute

Questions & Answers

- Richard Robinson / CEO
- richard@cynalytica.com
- https://www.Cynalytica.com

Cynalytica