MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

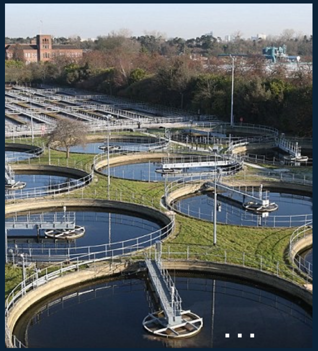
Threat-informed Defenses using ATT&CK for ICS

Adam Hahn

Attacks to ICS

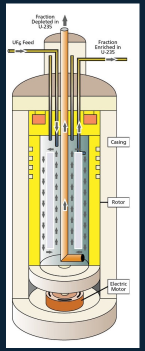
Maroochy Water Services (2000)

Malicious insider used remote access to dump raw sewage to Queensland parks/rivers



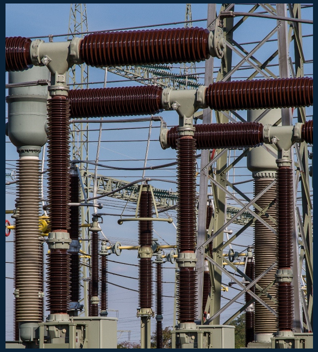
Stuxnet (2011)

Advanced malware manipulated operation of PLCs controlling Iranian uranium enrichment facility



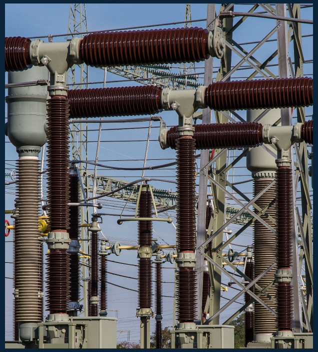
Ukraine (2015)

3 Ukrainian distribution control centers remotely compromised, disabling power to 225k customers



Industroyer (2016)

Sophisticated malware targeting Ukrainian electric power grid in December 2016

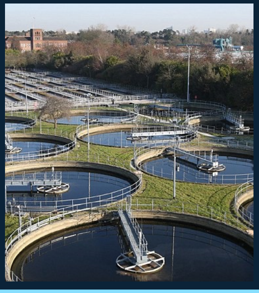


Triton (2017)

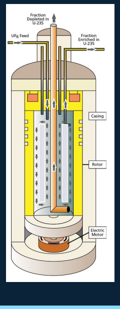
Malware infected Safety Instrumented System (SIS) at petrochemical plant in Saudi Arabia

What is ATT&CK® for ICS?

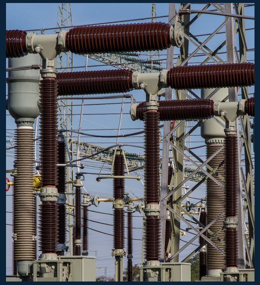
Maroochy Water Services (2000)



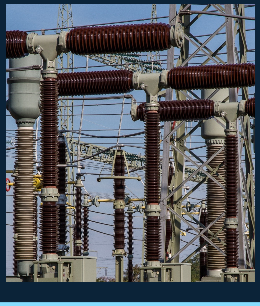
Stuxnet (2011)



BlackEnergy3 (2015)



Industroyer (2016)



Triton (2017)

A knowledge base of adversary behavior

- *Based on real-world observations*
- *Free, open, and globally accessible*
- *A common language*
- *Community-driven*

Tactics

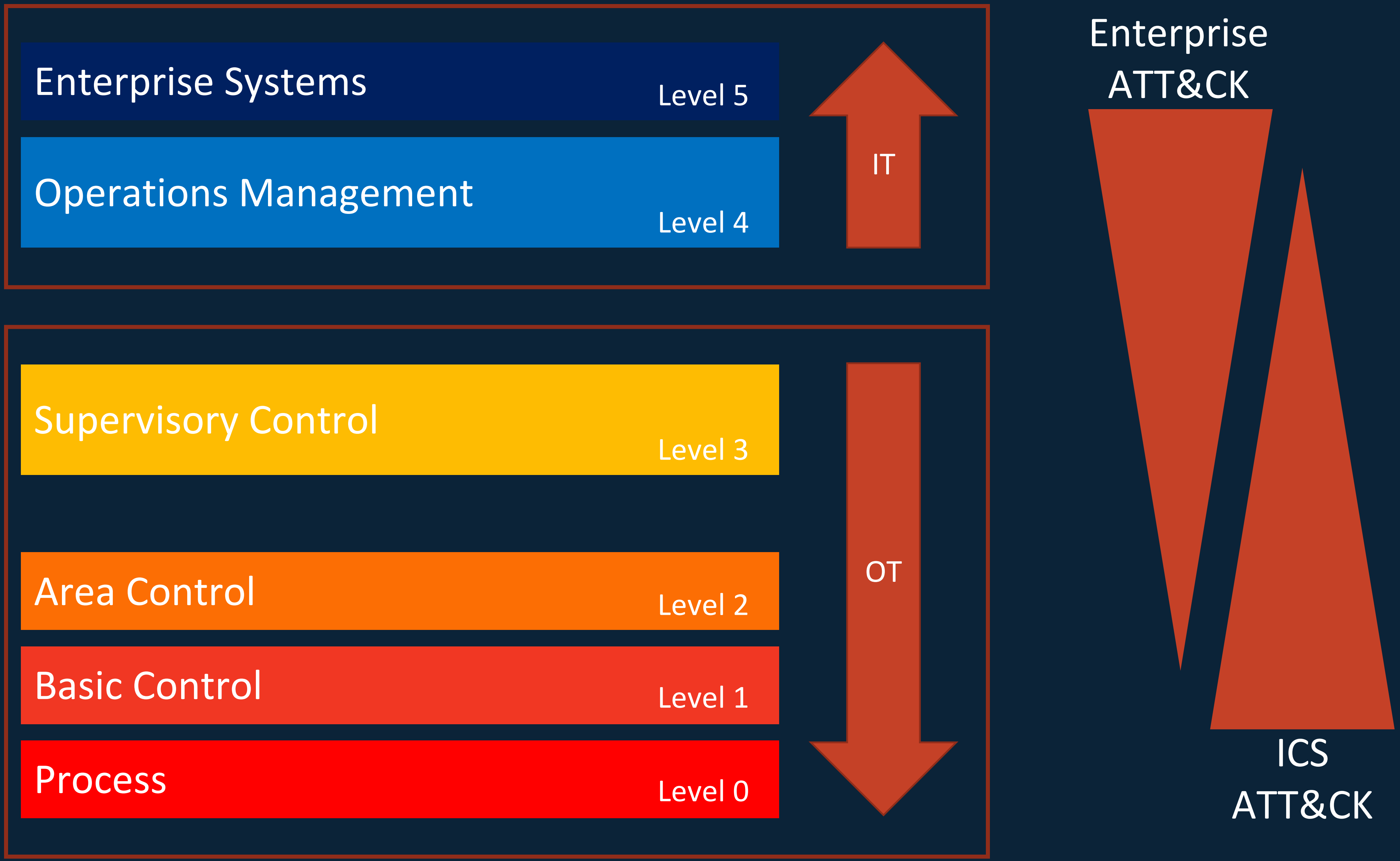
Techniques

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		

MITRE

ATT&CK for ICS: Why Different Knowledge Bases?

- Adversary motivations are different
  - Gaining access, accomplishing an objective depends on target and what the objective is
    - Enterprise and cyber physical differences
  - Different phases in the lifecycle mean different choices
    - Pre/post compromise differences
- Technologies are different
  - How an adversary interacts with systems depends on that system
    - Enterprise systems and embedded devices differences
  - Very different ways of defending them
    - Data collection
    - Mitigation tradeoffs



Enterprise Systems Level 5

Operations Management Level 4

IT

Supervisory Control Level 3

Area Control Level 2

Basic Control Level 1

Process Level 0

OT

Enterprise ATT&CK

ICS ATT&CK

ATT&CK for ICS – Technique Matrix

Tactics

Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by 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
Exploit Public-Facing Application	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
Exploitation of Remote Services	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
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

The adversary is finding targets, collecting information and ultimately staging an attack

ATT&CK for ICS – Technique Matrix

Tactics

Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by 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
Exploit Public-Facing Application	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
Exploitation of Remote Services	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
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

The adversary is directly affecting the control system

MITRE

ATT&CK for ICS – Technique Matrix

Tactics

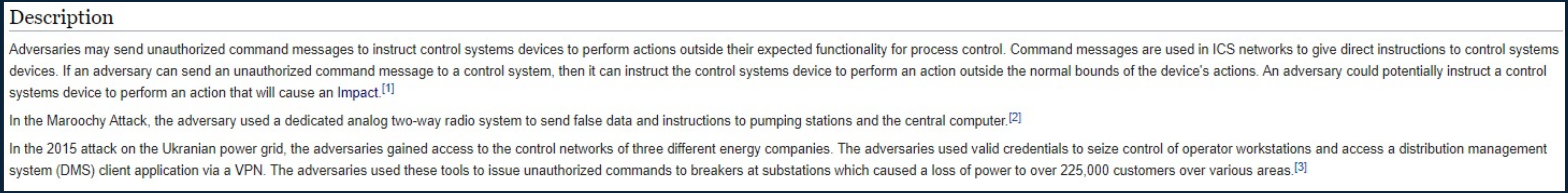
Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by 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
Exploit Public-Facing Application	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
Exploitation of Remote Services	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
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

The impacts that the adversary seeks to create

MITRE

Example Technique – Unauthorized Command Message

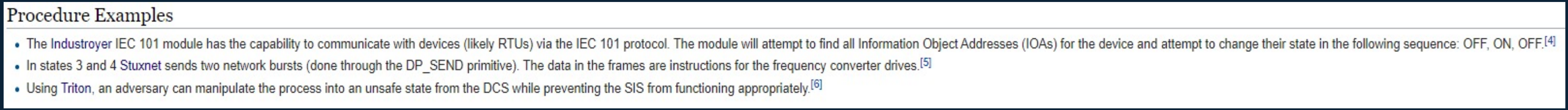


Description

Adversaries may send unauthorized command messages to instruct control systems devices to perform actions outside their expected functionality for process control. Command messages are used in ICS networks to give direct instructions to control systems devices. If an adversary can send an unauthorized command message to a control system, then it can instruct the control systems device to perform an action outside the normal bounds of the device's actions. An adversary could potentially instruct a control systems device to perform an action that will cause an Impact.[1]

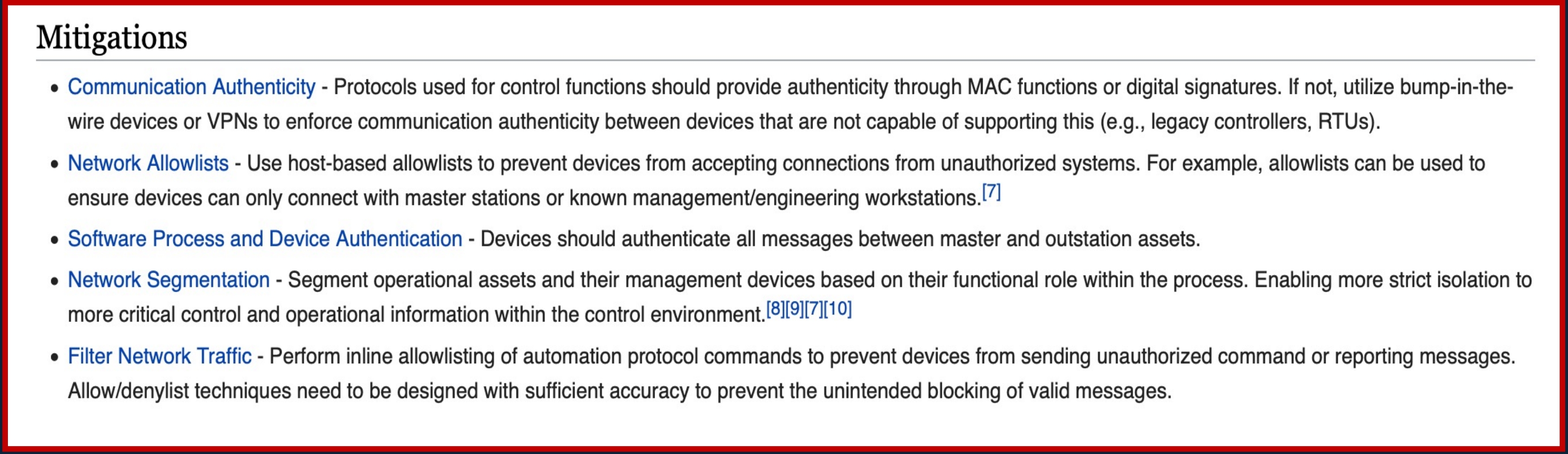
In the Maroochy Attack, the adversary used a dedicated analog two-way radio system to send false data and instructions to pumping stations and the central computer.[2]

In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries used valid credentials to seize control of operator workstations and access a distribution management system (DMS) client application via a VPN. The adversaries used these tools to issue unauthorized commands to breakers at substations which caused a loss of power to over 225,000 customers over various areas.[3]



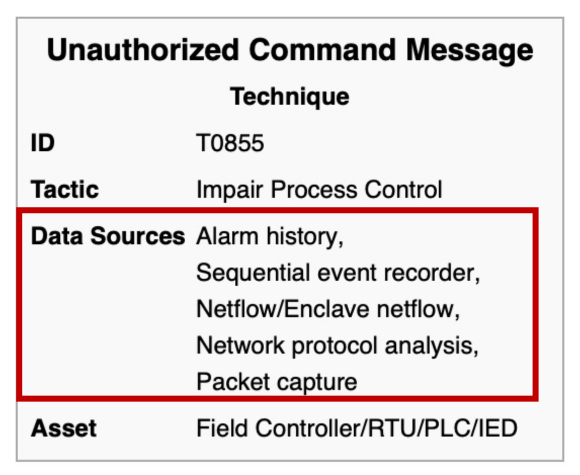
Procedure Examples

- The Industroyer IEC 101 module has the capability to communicate with devices (likely RTUs) via the IEC 101 protocol. The module will attempt to find all Information Object Addresses (IOAs) for the device and attempt to change their state in the following sequence: OFF, ON, OFF.[4]
- 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.[5]
- Using Triton, an adversary can manipulate the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately.[6]



Mitigations

- Communication Authenticity - Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).
- Network Allowlists - Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations.[7]
- Software Process and Device Authentication - Devices should authenticate all messages between master and outstation assets.
- Network Segmentation - Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment.[8][9][7][10]
- Filter Network Traffic - Perform inline allowlisting of automation protocol commands to prevent devices from sending unauthorized command or reporting messages. Allow/denylist techniques need to be designed with sufficient accuracy to prevent the unintended blocking of valid messages.



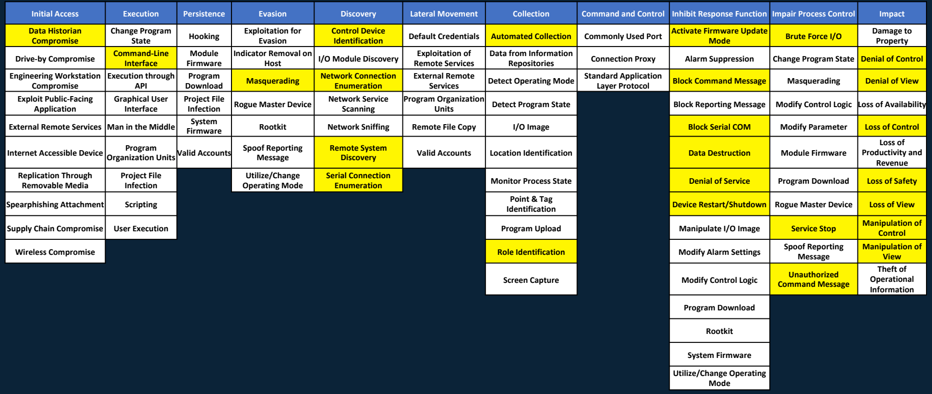
Unauthorized Command Message

Technique

ID	T0855
Tactic	Impair Process Control
Data Sources	Alarm history, Sequential event recorder, Netflow/Enclave netflow, Network protocol analysis, Packet capture
Asset	Field Controller/RTU/PLC/IED

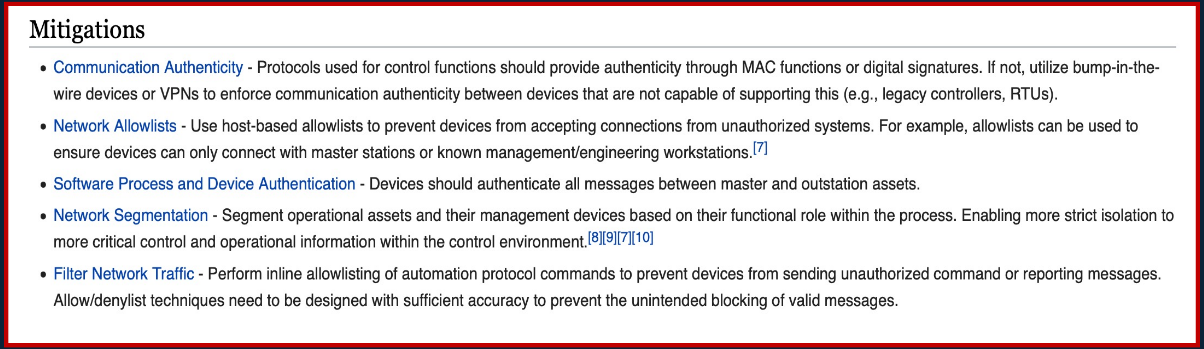
ATT&CK for ICS – Use Cases

Share information about observed threats



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

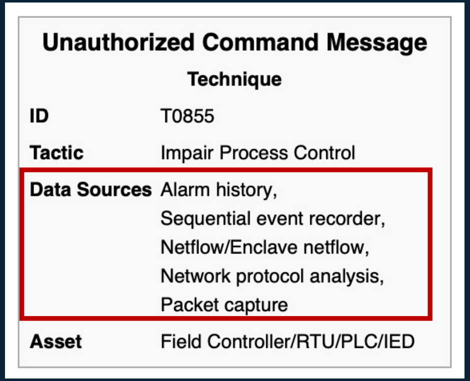
Identify mitigations for organizations and devices



Mitigations

- Communication Authenticity - Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).
- Network Allowlists - Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations.[7]
- Software Process and Device Authentication - Devices should authenticate all messages between master and outstation assets.
- Network Segmentation - Segment operational assets and their management devices based on their functional role within the process. Enabling more strict isolation to more critical control and operational information within the control environment.[8][9][7][10]
- Filter Network Traffic - Perform inline allowlisting of automation protocol commands to prevent devices from sending unauthorized command or reporting messages. Allow/denylist techniques need to be designed with sufficient accuracy to prevent the unintended blocking of valid messages.

Prioritize Investments in tools to detect threats

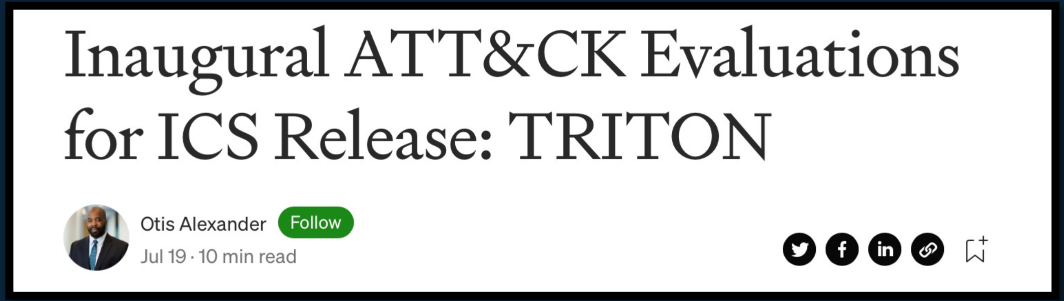


Unauthorized Command Message

Technique

ID	T0855
Tactic	Impair Process Control
Data Sources	Alarm history, Sequential event recorder, Netflow/Enclave netflow, Network protocol analysis, Packet capture
Asset	Field Controller/RTU/PLC/IED

Evaluate the effectiveness of vendor products



Inaugural ATT&CK Evaluations for ICS Release: TRITON

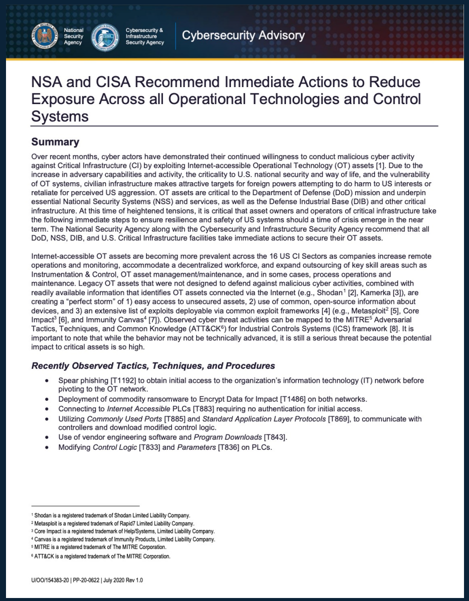
Otis Alexander

Jul 19 · 10 min read

https://medium.com/mitre-engenuity/att-ck-evaluations-for-ics-round-1-triton-results-69e39a23da3f

ATT&CK for ICS Adoption

Government



National Security Agency

Cybersecurity & Infrastructure Security Agency

Cybersecurity Advisory

NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems

Summary

Over recent months, cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against Critical Infrastructure (CI) by exploiting Internet-accessible Operational Technology (OT) assets [1]. Due to the increase in adversary capabilities and activity, the criticality to U.S. national security and way of life, and the vulnerability of OT systems, civilian infrastructure makes attractive targets for foreign powers attempting to do harm to US interests or retaliate for perceived US aggression. OT assets are critical to the Department of Defense (DoD) mission and underpin essential National Security Systems (NSS) and services, as well as the Defense Industrial Base (DIB) and other critical infrastructure. At this time of heightened tensions, it is critical that asset owners and operators of critical infrastructure take the following immediate steps to ensure resilience and safety of US systems should a time of crisis emerge in the near term. The National Security Agency along with the Cybersecurity and Infrastructure Security Agency recommend that all DoD, NSS, DIB, and U.S. Critical Infrastructure facilities take immediate actions to secure their OT assets.

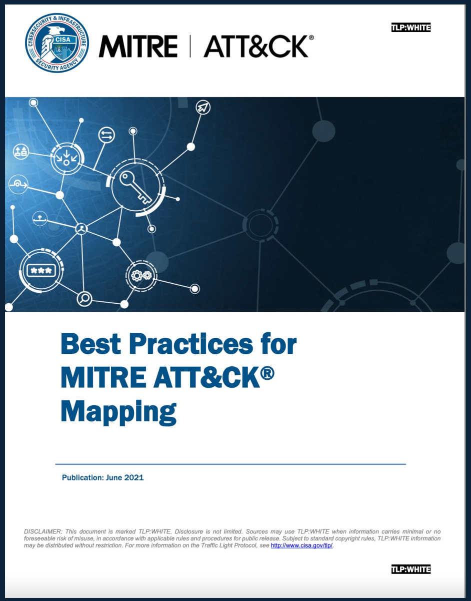
Internet-accessible OT assets are becoming more prevalent across the 16 US CI Sectors as companies increase remote operations and monitoring, accommodate a decentralized workforce, and expand outsourcing of key skill areas such as Instrumentation & Control, OT asset management/maintenance, and in some cases, process operations and maintenance. Legacy OT assets that were not designed to defend against malicious cyber activities, combined with readily available information that identifies OT assets connected via the Internet (e.g., Shodan[1] [2], Kamerka [3]), are creating a "perfect storm" of 1) easy access to unsecured assets, 2) use of common, open-source information about devices, and 3) an extensive list of exploits deployable via common exploit frameworks [4] (e.g., Metasploit[2] [5], Core Impact[3] [6], and Immunity Canvas[4] [7]). Observed cyber threat activities can be mapped to the MITRE[5] Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK[6]) for Industrial Controls Systems (ICS) framework [8]. It is important to note that while the behavior may not be technically advanced, it is still a serious threat because the potential impact to critical assets is so high.

Recently Observed Tactics, Techniques, and Procedures

- Spear phishing [T1192] to obtain initial access to the organization's information technology (IT) network before pivoting to the OT network.
- Deployment of commodity ransomware to Encrypt Data for Impact [T1486] on both networks.
- Connecting to *Internet Accessible* PLCs [T883] requiring no authentication for initial access.
- Utilizing *Commonly Used Ports* [T885] and *Standard Application Layer Protocols* [T869], to communicate with controllers and download modified control logic.
- Use of vendor engineering software and *Program Downloads* [T843].
- Modifying *Control Logic* [T833] and *Parameters* [T836] on PLCs.

[1] Shodan is a registered trademark of Shodan Limited Liability Company.
[2] Metasploit is a registered trademark of Rapid7 Limited Liability Company.
[3] Core Impact is a registered trademark of Help/Systems, Limited Liability Company.
[4] Canvas is a registered trademark of Immunity Products, Limited Liability Company.
[5] MITRE is a registered trademark of The MITRE Corporation.
[6] ATT&CK is a registered trademark of The MITRE Corporation.

U/OO/154383-20 | PP-20-0622 | July 2020 Rev 1.0



MITRE | ATT&CK®

TLP:WHITE

Best Practices for MITRE ATT&CK® Mapping

Publication: June 2021

DISCLAIMER: This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

TLP:WHITE

Industry

SANS / DRAGOS

MITRE ATT&CK for ICS Webinar

April 2, 2020

Robert M. Lee
Dragos CEO

Austin Scott
Dragos ICS Penetration Testing Principal

DRAGOS

ADDRESSING THE MITRE ATT&CK FOR ICS MATRIX

How CyberX Protects Against IoT/ICS Threats Described in

FORESCOUT

From Events to TTPs: Maturing OT Incident Response with MITRE ATT&CK® for ICS

INDUSTRIAL DEFENDER

MITRE ATT&CK for ICS Detection Methods

CyberSecurity

FILLING THE GAP WITH MITRE ATT&CK FOR ICS

FELIX ROIDER, SECURITY ANALYST

ARMIS

HOW ARMIS SUPPORTS THE MITRE ATT&CK™ FOR ICS MATRIX

Grantek and ThreatGEN Cybersecurity Webinar: ICS ATT&CK

Creating a More Cost-Effective Risk Mitigation Strategy

March 5, 2020

GRANTEK

THREATGEN

Isaac Guevara
ICS Network/Cybersecurity Specialist, Grantek

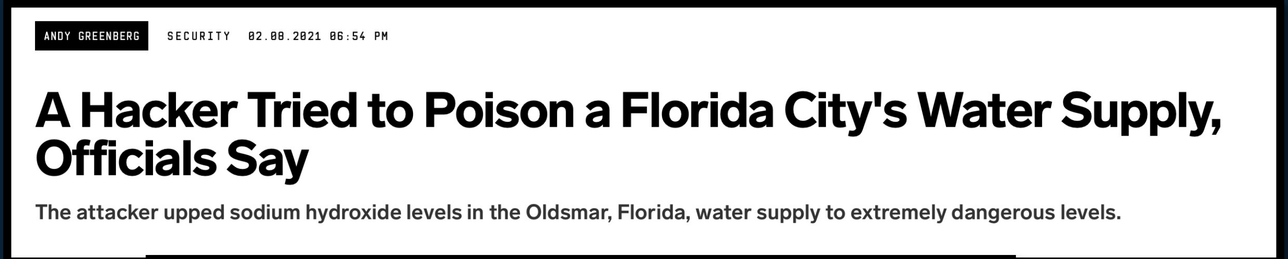
Clint Bodungen
Founder & CEO, ThreatGEN

MITRE

ATT&CK for ICS Challenges

Mapping adversarial techniques depends on accurate threat intelligence:

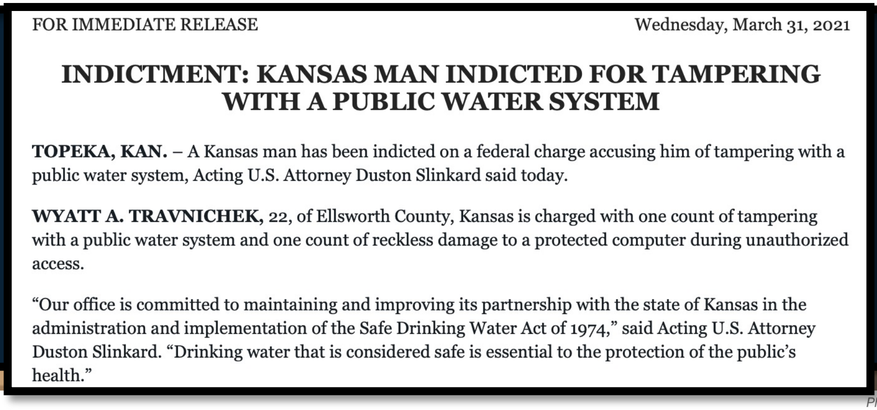
- Organizations lack security monitoring capabilities to detect attacks
- Private organizations may choose not to share threat information due to concerns that it reflects negatively on their organization/industry



ANDY GREENBERG SECURITY 02.08.2021 06:54 PM

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



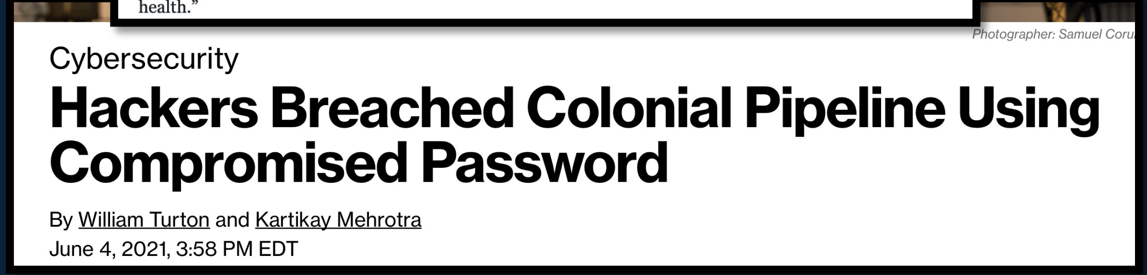
FOR IMMEDIATE RELEASE Wednesday, March 31, 2021

INDICTMENT: KANSAS MAN INDICTED FOR TAMPERING WITH A PUBLIC WATER SYSTEM

TOPEKA, KAN. – A Kansas man has been indicted on a federal charge accusing him of tampering with a public water system, Acting U.S. Attorney Duston Slinkard said today.

WYATT A. TRAVNICHEK, 22, of Ellsworth County, Kansas is charged with one count of tampering with a public water system and one count of reckless damage to a protected computer during unauthorized access.

"Our office is committed to maintaining and improving its partnership with the state of Kansas in the administration and implementation of the Safe Drinking Water Act of 1974," said Acting U.S. Attorney Duston Slinkard. "Drinking water that is considered safe is essential to the protection of the public's health."



Photographer: Samuel Coru

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 3:58 PM EDT

https://www.wired.com/story/oldsmar-florida-water-utility-hack/
https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system
https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

MITRE

Using Failure & Attack Scenarios

Failure Scenarios

Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,
- Human error,
- Interference with the equipment lifecycle, and
- Natural disasters that impact cyber security posture.

Useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing

Example sources of data:

- Subject Matter Experts (Operators, Researchers, etc.)
- Incident Repositories (NTSB, PHMSA, etc.)
- Scenario Repositories (EPRI NESCOR failure scenarios)

Example Failure Scenarios

Scenario 1: Transformer Overloading

- Objective: Rapidly deteriorate transformer insulation
- Technique: Modify trip settings of overcurrent and thermal protection relays, block communications (alarms, etc.) and open a breaker to force one transformer to bear load. Transformer will rapidly heat up and degrade insulation.

Scenario 2: Disrupting Switching Executions for Circuit Breaker and Isolators

- Objective: Cause dielectric breakdown of a breaker and isolator
- Technique: Execute continuous switching actions to take one or more pieces of equipment out of service. Block communications (alarms, etc.)

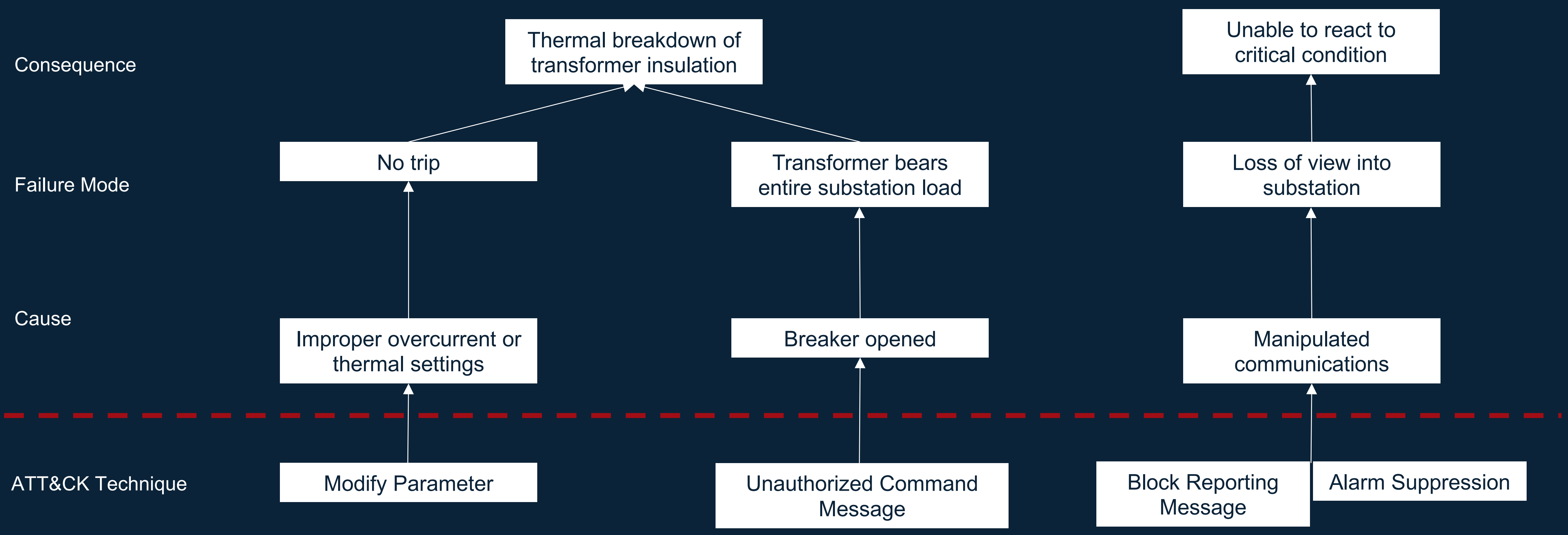
Scenario 3: Entire Substation Outage

- Objective: Cause entire substage outage and contingencies
- Technique: Execute command to open one or more breakers

Ten, Chee-Wooi, Koji Yamashita, Zhiyuan Yang, Athanasios Vasilakos, and Andrew Ginter. "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems." *IEEE Transactions on Smart Grid* (2017).

MITRE

Scenario 1: Transformer Overloading



Consequence

Failure Mode

Cause

ATT&CK Technique

Thermal breakdown of transformer insulation

Unable to react to critical condition

No trip

Transformer bears entire substation load

Loss of view into substation

Improper overcurrent or thermal settings

Breaker opened

Manipulated communications

Modify Parameter

Unauthorized Command Message

Block Reporting Message

Alarm Suppression

Building an ATT&CK Scenario

- **We now know what we are trying to accomplish. What's next?**
  - What's our entry point?
    - Initial Access (Engineering Workstation Compromise, External Remote Service)
  - How do we find our target(s)?
    - Discovery (Network Sniffing, Remote System Discovery, Remote System Information Discovery)
  - How do we sustain our attack?
    - Inhibit Response Function (Block Reporting Message, Alarm Suppression)
  - How do we cause the failure?
    - Impair Process Control (Modify Parameter, Unauthorized Command Message)

MITRE

Identifying Host-based Data Sources

Understanding Data Source Collection

- **Maintaining visibility into Operational Technology (OT) networks is essential for quickly detecting and remediating cyber threats.**
- **Understanding the various data sources that are available in OT networks is key to this endeavor. Network traffic is a popular source of data in OT networks but there are other valuable sources of data that are often overlooked.**
  - Host based logs housed on embedded OT devices such as Intelligent Electronic Devices (IED)
  - Asset management data associated with equipment under control.

Data Source Collection

Configuration

- Firmware version
- System settings
- Control logic
- Parameters

Performance and Statistics

- CPU, Memory, Disk, Ethernet, etc.
- Network connection information

Process Information

- I/O values associated with tags
- Alarms and Faults (e.g., Digital Fault Recorder)
- Events (e.g., command execution)
- Process quality (e.g., Phasor Measurement Unit)

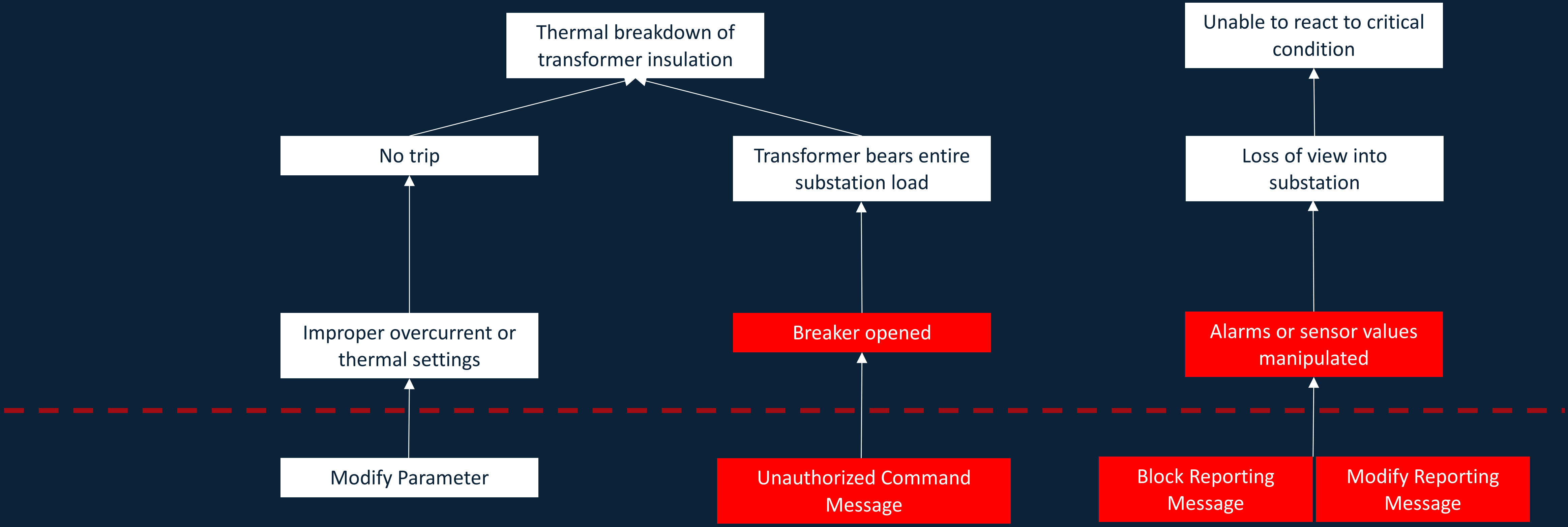
Asset Management

- Condition-Based Monitoring
- Predictive Maintenance

Physical

- Physical sensors (e.g., tamper detection)

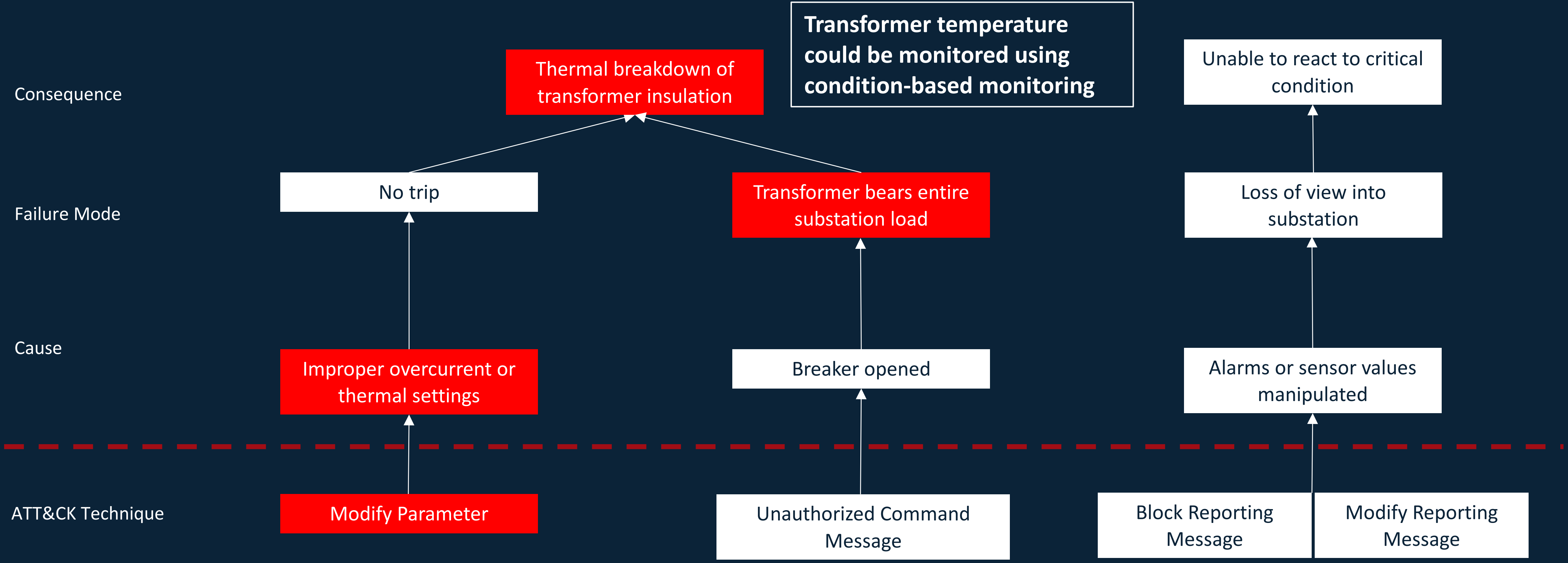
Data Sources - Attack Scenario – Network Data


Thermal breakdown of transformer insulation
No trip
Transformer bears entire substation load
Unable to react to critical condition
Loss of view into substation
Improper overcurrent or thermal settings
Breaker opened
Alarms or sensor values manipulated
Modify Parameter
Unauthorized Command Message
Block Reporting Message
Modify Reporting Message

May be detected from the network

MITRE

Data Sources - Attack Scenario – Host Data



Consequence

Failure Mode

Cause

ATT&CK Technique

Thermal breakdown of transformer insulation

No trip

Transformer bears entire substation load

Improper overcurrent or thermal settings

Breaker opened

Modify Parameter

Unauthorized Command Message

Unable to react to critical condition

Loss of view into substation

Alarms or sensor values manipulated

Block Reporting Message

Modify Reporting Message

Transformer temperature could be monitored using condition-based monitoring

Changes to the relay settings can be monitored

Identifying Data Sources - Approach

Easier

- Identify built-in collection mechanisms
- Identify vendor aggregation points

More Effort

- Access device using vendor engineering software

Explore available data that can be used for threat detection

- Collect data with engineering software

Analyze PCAPs to understand methods of access

- Communication protocol (Telnet etc. vs Industrial Protocol)
- Commands

Develop collector to replicate access

Thank You

Adam Hahn

ahahn@mitre.org

ATT&CK for ICS

https://attack.mitre.org/ics

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD