TETRA TECH

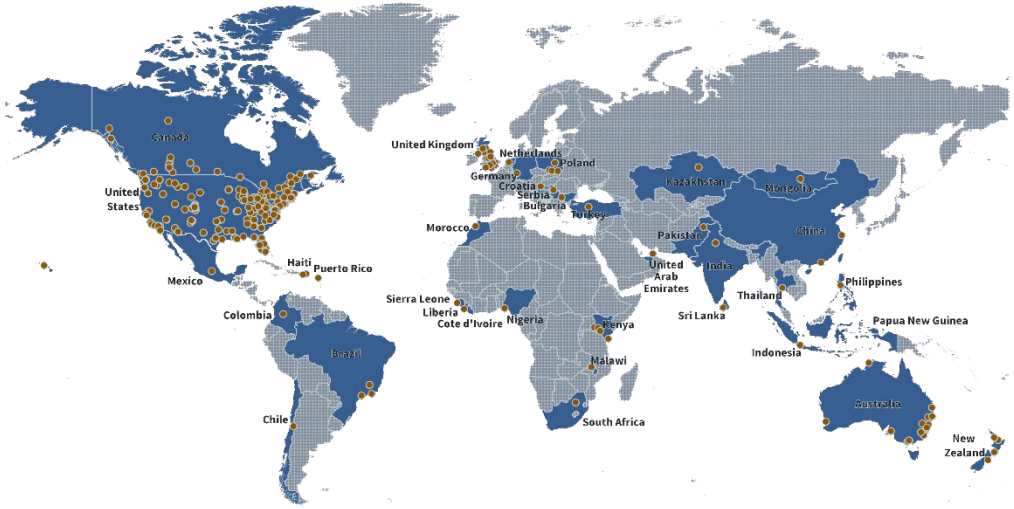
Cyber-Hardened, Resilient Industrial Infrastructure -- Systems Platform (CRIISP)

Start Secure. Stay Secure. Restore Secure!

TETRA TECH

Leading with Science®

- Strong understanding of AF. USSF. and DoD utility and facility control infrastructure, risk, and vulnerabilities
- Advanced machine-learning appliances developed by Frontline Cyber Solutions accelerate development of automated cybersecurity solutions
- First-of-kind Operational Control network installed for AF at Cheyenne Mountain Space Force Station



With 470 offices worldwide, we can quickly respond to our clients' needs.

TETRA TECH SNAPSHOT

WORKS IN **125** COUNTRIES

7 CONTINENTS

Publicly traded on NASDAQ as TTEK NASDAQ GLOBAL SELECT

$3.5 billion ANNUAL REVENUE

WORKS ON **80,000** PROJECTS ANNUALLY

470 OFFICES WORLDWIDE

22,000 ASSOCIATES

***ENR* RANKINGS**

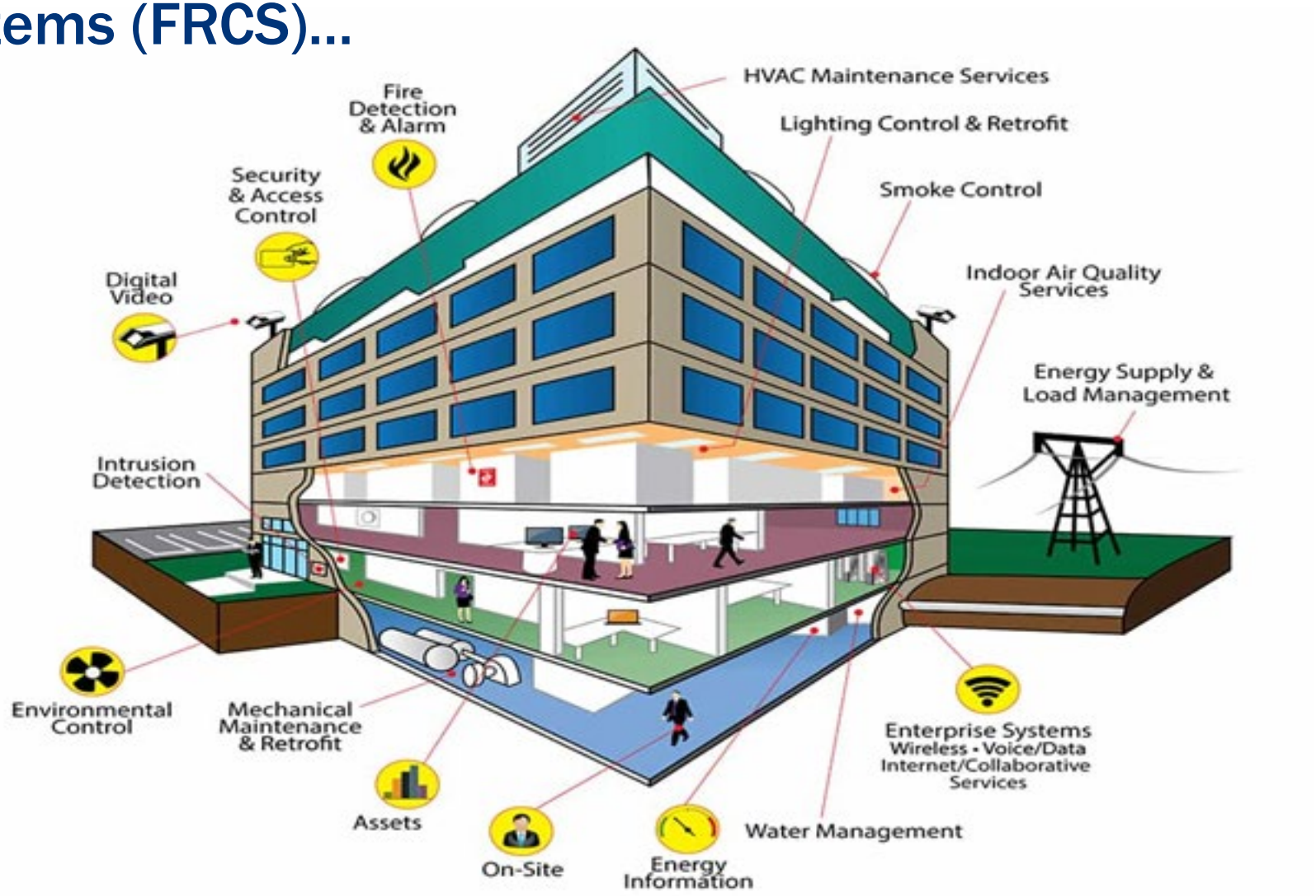
- #1 Environmental Management
- #1 Hydro Plants
- #1 Water
- #1 Water Treatment/Desalination

20,000 CLIENTS

Problem Space

- **Cyber protection of critical Operational technology (OT) across DoD installations has national attention…**
- **Resilient operation of national defense infrastructure (power generation/distribution, fuel, water, wastewater, facility automation, HVAC, etc.) relies on OT.**
- **OT is vulnerable!**
- **Advanced, persistent OT cyber threats are a reality!!**
- **Standardized, cyber-hardened, resilient solution is required to:**
  - ✓Overcome pervasive, disparate problems
  - ✓Assure reliable mission critical operations during crisis
  - ✓Establish, maintain and restore trust in systems
  - ✓*Start Secure. Stay Secure. Restore Secure*

Operational Technology includes Facility Related Control Systems (FRCS)…



Why cyber-harden ***critical*** systems?

- February 5, 2021 – Cyber actors gain unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility.
- Actors manipulated system to increase concentration of sodium hydroxide in the water treatment process.
- **Personnel** noticed the change **before** the system's software alarmed.
- The cyber actors likely exploited poor password security and an outdated operating system.

Anatomy of OT Cyber Attacks

Software

Step 1 A software vulnerability goes undetected

Step 2 Attackers discover the vulnerability and target exposed OT

Step 3 Malware is installed, allowing attackers to tamper with system controls

Social Engineering

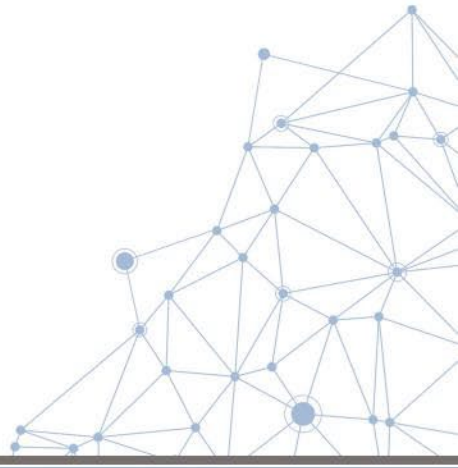
Step 1 Attackers spear-phish employee and gain a foothold in the target system

Step 2 Attackers exploit IT network and create a 'bridge' into OT network

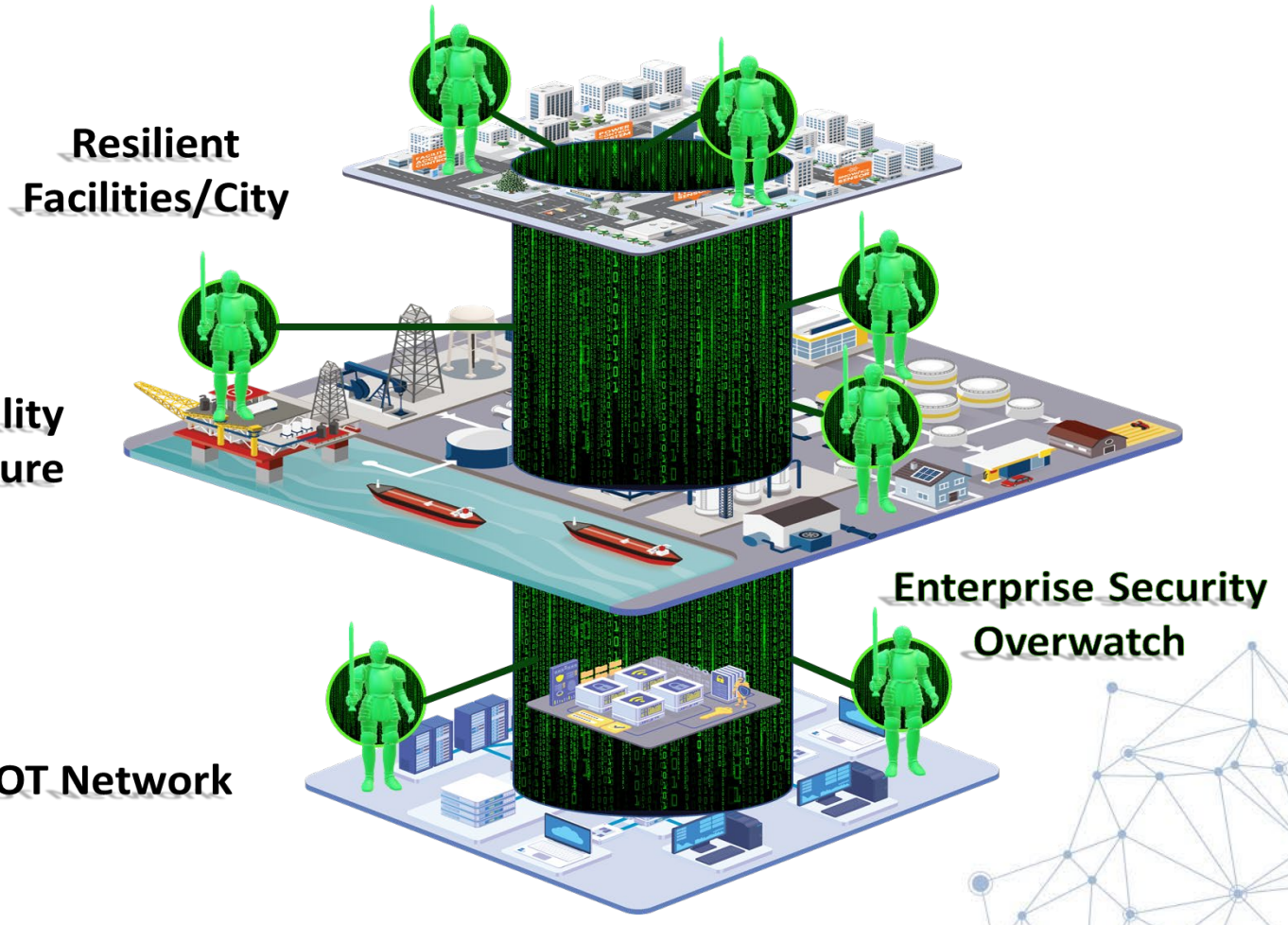
Step 3 Attackers deploy malware to alter data, equipment operation, or cause outages

Case Study: Design/Install New OT Network - Cheyenne Mountain AFS, CO

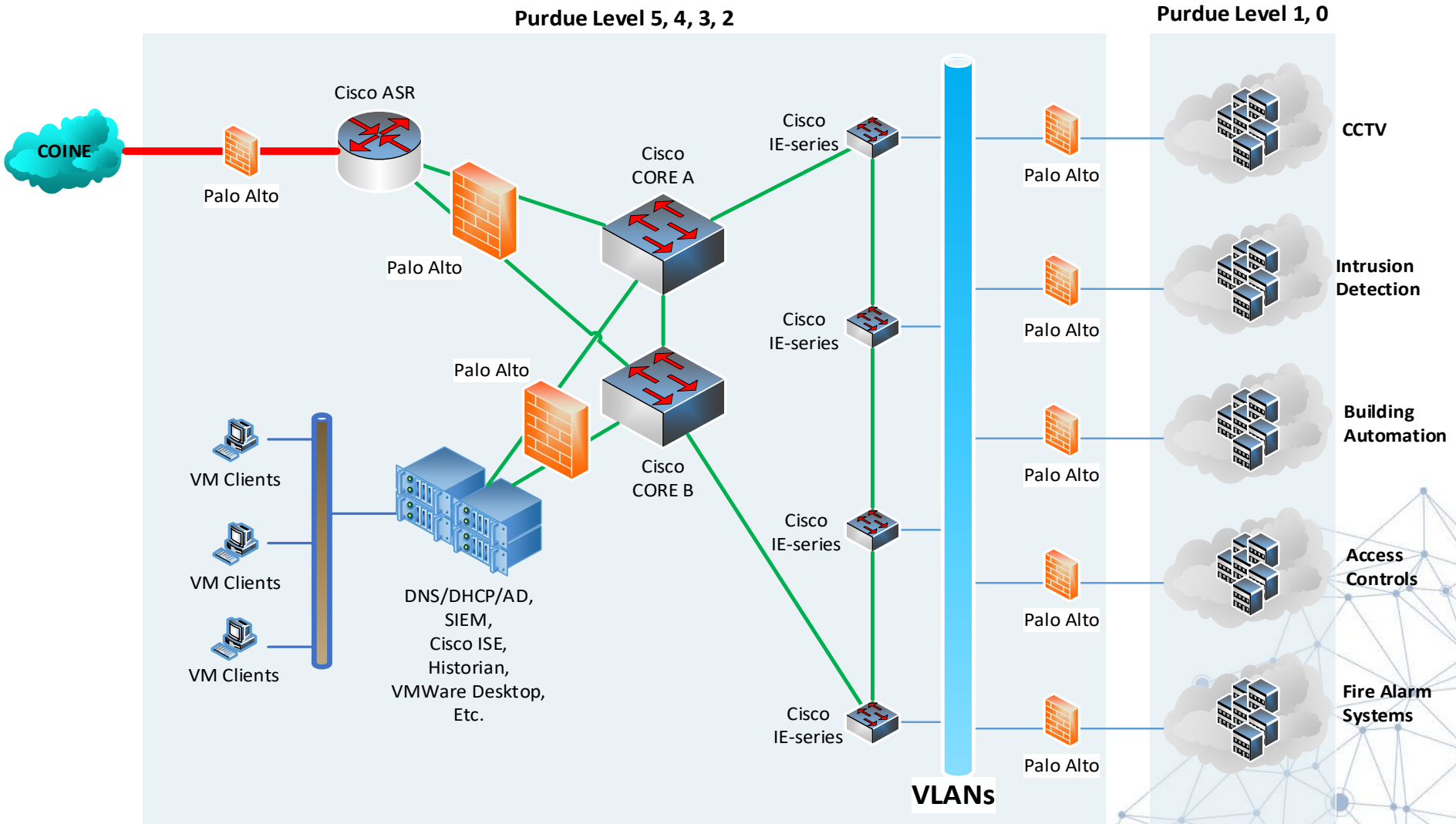
- **High-level, mission resiliency requirements drove need for a next-generation, cyber-hardened control system network architecture:**
  - Resilient, survivable, secure, defensible, and recoverable
  - Where feasible, make it autonomous (to reduce man-hours required to perform monitoring/defense)
  - End-to-end physical and cyber security with layered-defense/defense-in-depth methodologies
  - Strong segmentation between networks, enclaves, zones



Operational View (OV-1)

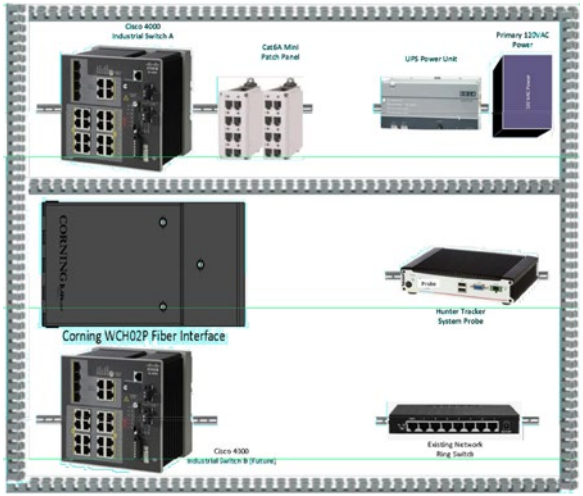


Design - CRIISP Topology



Project Breakdown

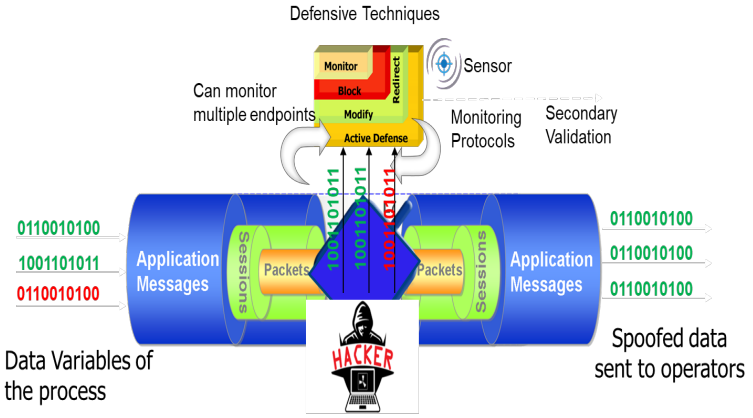
- **Team: Tribal One | Tetra Tech | Frontline Cyber Solutions**
- **PoP: 2 years**
  - Design - 6 months
  - Install - 18 months
    - COVID
    - Access delays to classified work centers



- **Lessons Learned**
  - Decide on equipment and materials early.
  - Design team understand equipment and operating environment specifications **prior** to site visit.
  - Customer accompany team on site visits quickly get answers to questions instead of waiting on RFIs.
  - Ask lots of questions -- Communicate!

CRIISP – Design Best Practices

- **Embodies NIST, UFC/UFGS, and DoD standards**
- **Scalable architecture; build as much or as little as needed**
- **Layered defense; zero-trust**
  - Assumes exploitation (i.e. enemy has compromised network)
  - Out-of-band, Real-time monitoring, anomaly detection, and logging
  - Assure safe and reliable operation of critical functions during attack



- **Exports predictive maintenance and infrastructure performance data for use in enterprise/building analysis**

Questions?

Project Contacts:

Tribal 1 (Prime/GC) :

Doug Wells, DougWells@tribal.one

Sr. Executive Director, Business Development, 719.352.6409

Tetra Tech (DOR):

Jeff Robertson, Jeff.Robertson1@tetratech.com

Sr. Manager/Solution OT Cybersecurity Engineer, 719.367.7926

Frontline Cyber Solutions (Technology Implementor):

Sam Becker, sbecker@frontlinecyber.us

Director, Federal Cyber Solutions, 303.521.7017

Additional Cyber Exploits:

- Discovered in 2020, Ripple20 represents a series of critical vulnerabilities affecting the Treck TCP/IP communication stack used in hundreds of millions of IoT devices across industrial, power grids, medical devices, oil and gas, aviation, transportation, and retail.[2]
- Israeli water facilities attacks in April 2020 were reportedly due to SCADA control systems that were outdated with weak access configurations and/or exposed to the Internet.[3]
- Ransomware infected the aluminium producer Norsk Hydro's plants causing operators to resort to manual processes while systems were out.[4]
- Attackers in the Shamoon [5], BlackEnergy [6], German steel mill [7], and Triton/Trisis [8] incidents all infiltrated OT networks via targeted phishing emails sent to employees that gained them initial corporate network access.
- 2009 NightDragon attacks against companies in the energy sector [9], and attacks on US gas pipelines.[10]