Industrial Control Systems & SCADA: Risks & Solutions

Del Rodillas, MSEE | GICSP | MBA

Director, OT Industry Solutions, Palo Alto Networks

October 2020

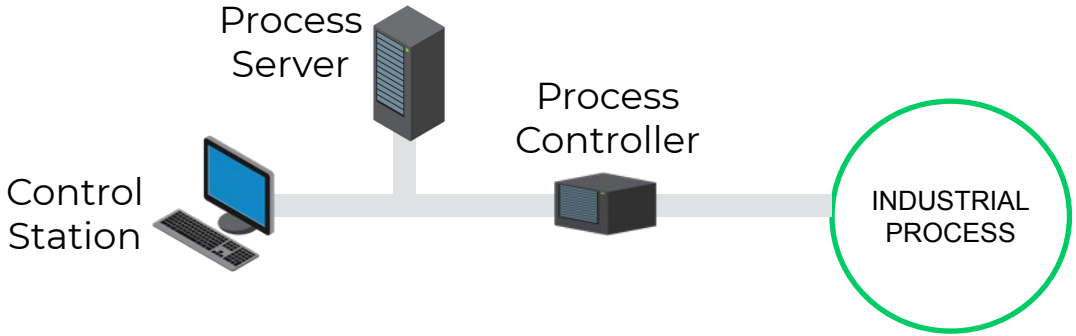
What are ICS and SCADA?

ICS = Industrial Control Systems

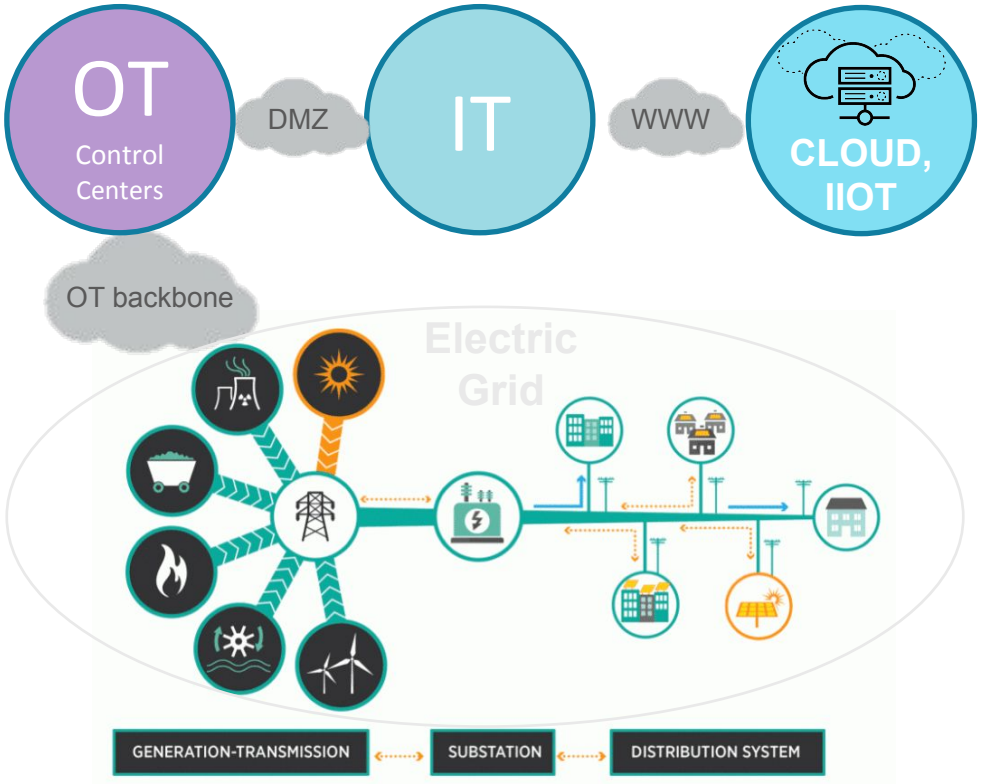
SCADA = SUPERVISORY CONTROL AND DATA ACQUISITION

Industrial networks and systems which sit behind the corporate IT networks of industrial companies (Energy, Utilities, Manufacturing, Transport)

- E.g. power plants, substations, factories, oilfields, pipelines, etc
- Part of the OPERATIONAL TECHNOLOGY (OT)
- Prioritize Availability and Safety (vs. Confidentiality in IT)
- In the past, “air-gapped” from business networks and the internet



Digital Transformation of Electric Utility IT-OT Infrastructure



- Grid Modernization
- IT-OT Integration
- Big-data Analytics
- Industrial IoT

Electric Utilities OT Assets Provide Critical Services and Information

Transmission/Distribution

- Service - Power delivery
- Assets - Switching, protection, control, transformers, etc.
- Loss of service impact - Financial and human safety /loss of life

Power Generation

- Service - Power generation
- Assets - Turbine, Fuel, generator, cooling, etc.
- Loss of service impact - Financial, human safety /loss of life, environment

Advanced Metering

- Service - End-user consumption data
- Assets - Concentrators, meters, repeaters
- Loss of service impact - Loss of key operational information (load, billing)

Threat Model

Internet

Social Engineering

IT Network

Level 4 or 5: Corporate desktop,
Remote access workstation,
domain server, webserver

Credential Theft

OT Network

Level 3: EMS, SCADA, GMS, AMI HE
Level 2: HMI, Historian, EWS
Level 1: PLC, IED, RTU, Meter

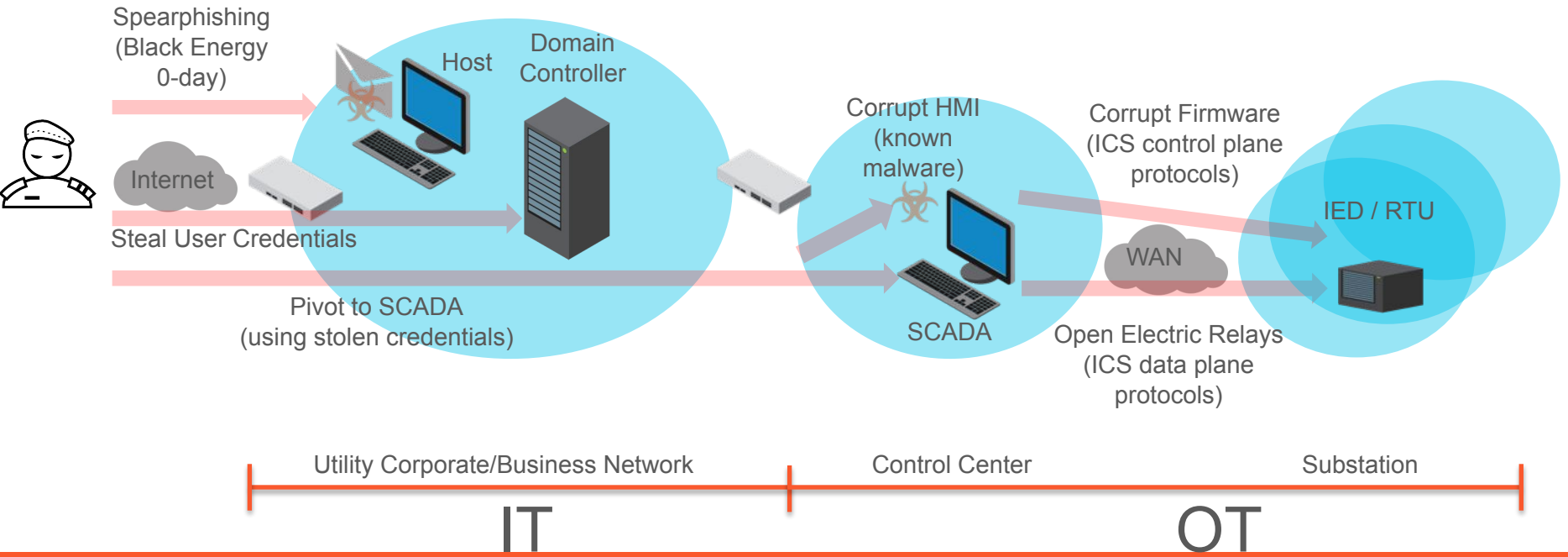
Cyberphysical Attack

OT Network (EMS, SCADA, GMS, AMI Headend

Side-channel
attack

Example Threat Model - Ukraine Grid Attack

BREACH PERIMETER → DELIVER MALWARE → ENDPOINT OPERATIONS → REACH THE TARGET → ACHIEVE OBJECTIVE



What are the risks and how real are they?

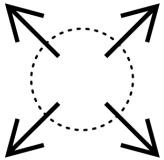
- Loss of utility services at scale
- Human health and safety
- Environmental damage
- Regulatory non-compliance
- Operational ineffeciency
- Reputational damage
- Financial loss

Cost of successful cyber-attack to London electricity networks
- Univ. of Oxford 2016

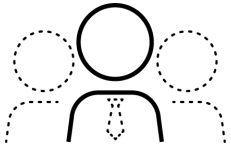
Utilities who experienced an attack involving loss of private information or OT outage in the past 12 months.
- *Siemens/Ponemon 2019*

Your Mindset is Critical - Adopt a Zero Trust Approach

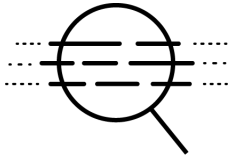
Define business outcomes



Design from the inside out



Determine who/what needs access



Inspect and log all traffic

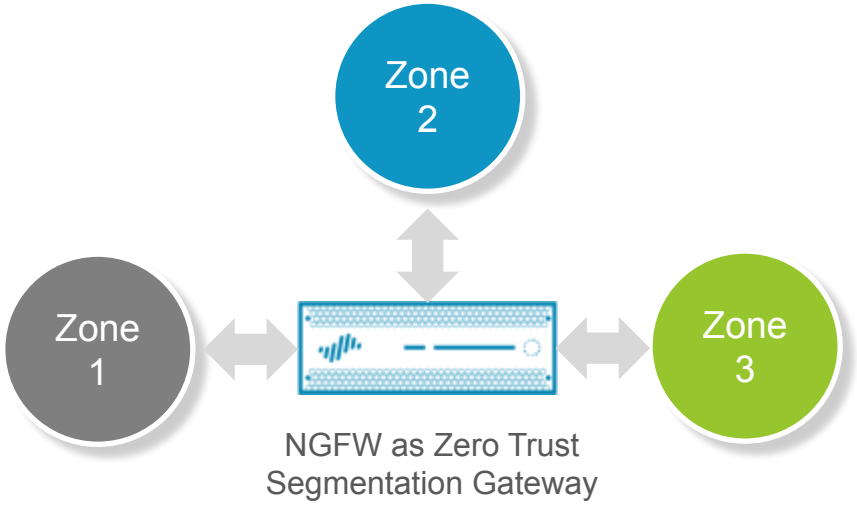
Cybersecurity Capabilities and Value for OT Security

Increasing Maturity

Cybersecurity Capability	Description	Value for OT Security
ICS Protocol Visibility/Whitelisting	Identify and control OT-specific protocols and applications	Implement a Zero Trust architecture to reduce the attack surface
Asset Identification	Identify OT and IoT devices	Minimize the risk of OT/IoT being compromised
Intrusion Detection and Prevention	Detect and protect against known threats	Protect legacy unpatched or unpatchable OT systems until scheduled downtime
Malware Sandboxing	Detect and protect against zero-day malware	Reduce the risk of successful targeted attacks using unknown threats
Threat Intelligence Management	Ingestion and sharing of utility-specific threat intelligence	Real time information on newly discovered industry threats and protections
Automated Threat Detection and Response	ML/AI based intelligence threat detection and response	Rapidly detect and respond to threats. Quickly recover from incidents.

Example Technology with Next-generation OT Security Capabilities

Next-generation Firewall (NGFW)



Services provided by a Next-generation Firewall

- ICS/OT protocol visibility and control
- Role-based access control with multi-factor authentication
- Intrusion detection and prevention
- Malware sandboxing
- OT and IoT Asset Identification and protection
- Cellular IoT security

IT-OT Collaboration Could Be the Biggest Challenge

- Utilities with weak IT-OT links struggle to progress OT security
- IT and OT often seen as having opposing goals
- In reality, both share an interest to protect the core business

- Change starts at the top with senior leadership
- Foster a collaborative culture and joint accountability
- Cross-training personnel in both disciplines helps
- Set up governance boards made up of senior leadership

Key Takeaways

High-risk Profile

Grid cybersecurity is a high-risk endeavor and action is required.

Zero Trust

A zero-trust mindset is required to increase your protection surface

Tech Investment

Yesterday's technology is inadequate for stopping new threats

IT-OT Collaboration

An organization's ability to foster IT-OT collaboration is critical

paloalto NETWORKS

Thank you