ICS Asia Pacific Summit 2020

ICS Attack Concepts and Demonstrations

Tim Conway

– SANS Institute

– Instructor

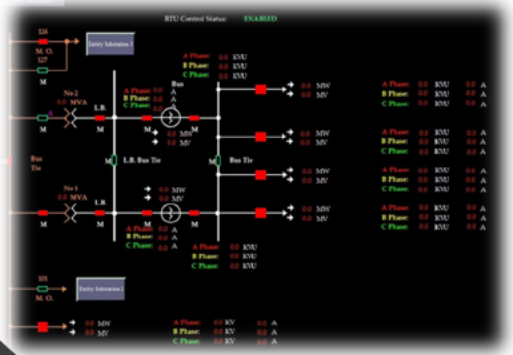
Jeff Shearer

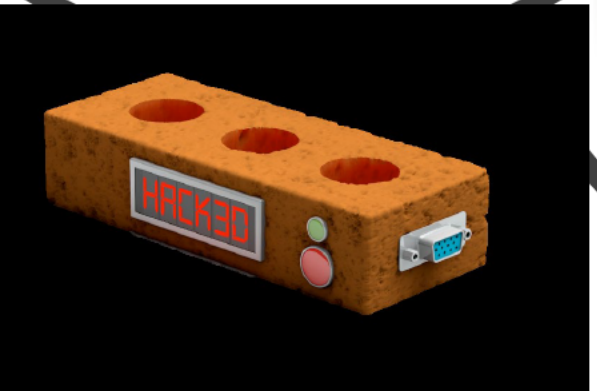
– SANS Institute

– Instructor

Agenda

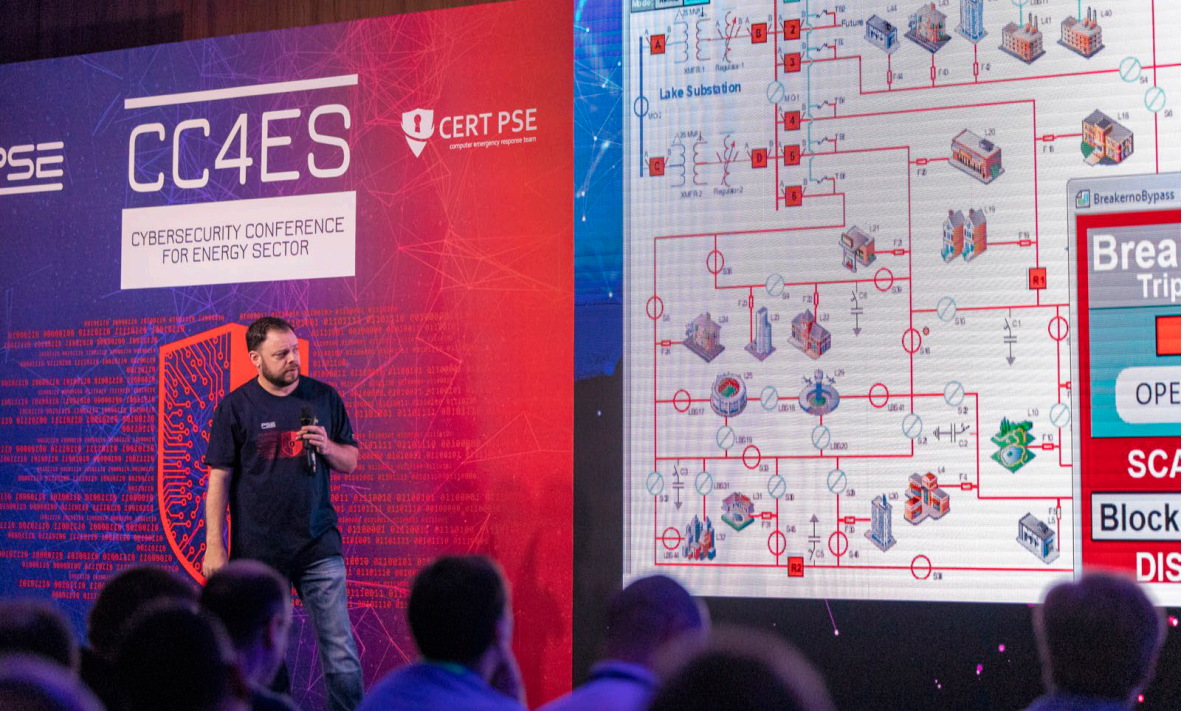

Learning Objectives
Assumed Breach
Network based attacks
Controller attacks
Now what?





GRID NETWARS

sans.org/netwars/grid


CC4ES
CYBERSECURITY CONFERENCE
FOR ENERGY SECTOR
CERT PSE
computer emergency response team
Lake Substation
BreakernoBypass


GRID
NETWARS

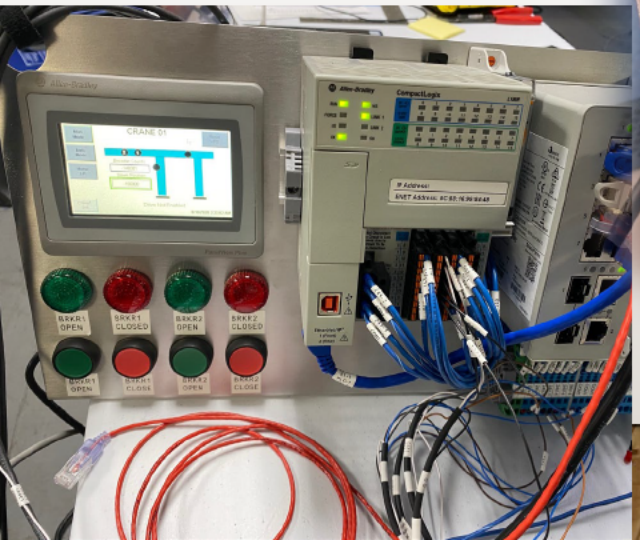

Individual Players

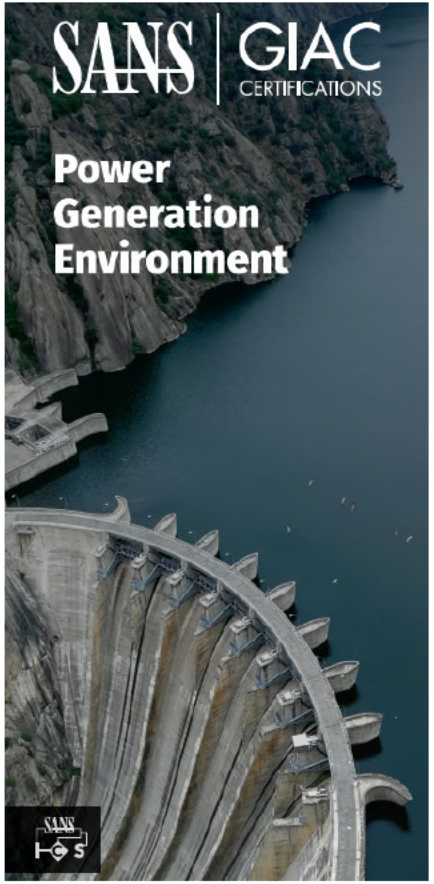
SANS | GIAC CERTIFICATIONS

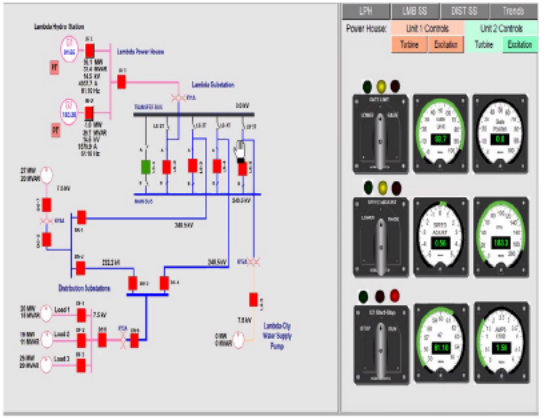
Manufacturing Environment


Positions
Run Trolley To Pos 1
On
Run Trolley To Pos 2
On
Operations Have Been Ransomed
Pay Our Demands
Cancel Exit
Main
WARNING
marathon
Motors
SyMAX


Port and Shipping Environment

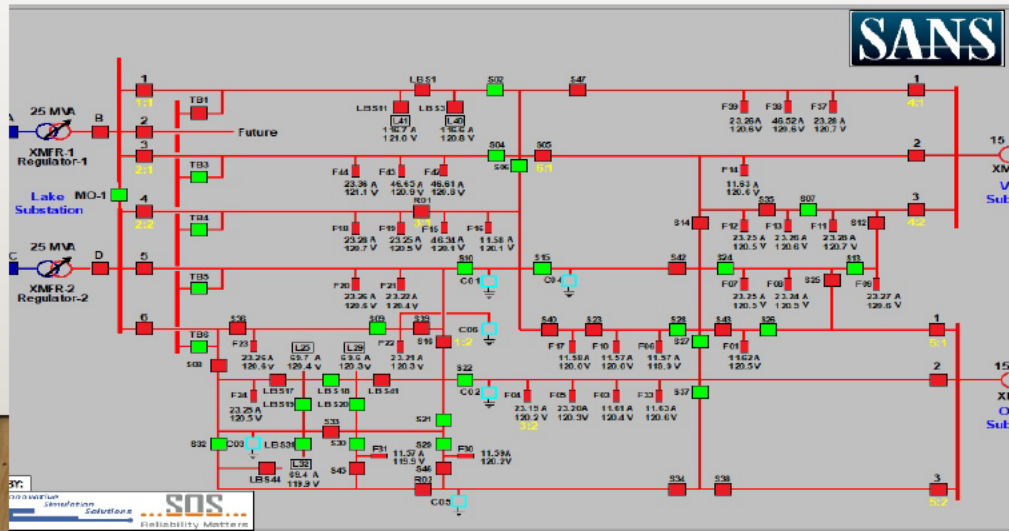



SANS
GIAC
CERTIFICATIONS
Power
Generation
Environment



SANS | GIAC CERTIFICATIONS

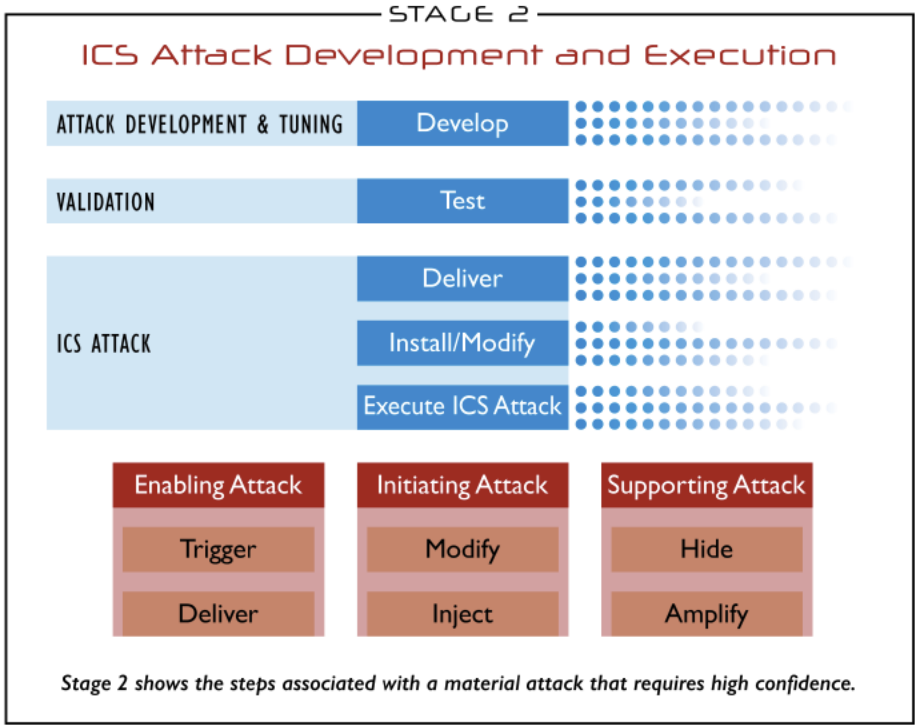
Power Distribution Environment



Agenda


Learning Objectives
Assumed Breach
Network based attacks
Controller attacks
Now what?

Killing the Kill Chain

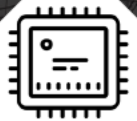


Agenda

Learning Objectives

Assumed Breach

Network based attacks



Controller attacks

Now what?

Agenda

Learning Objectives

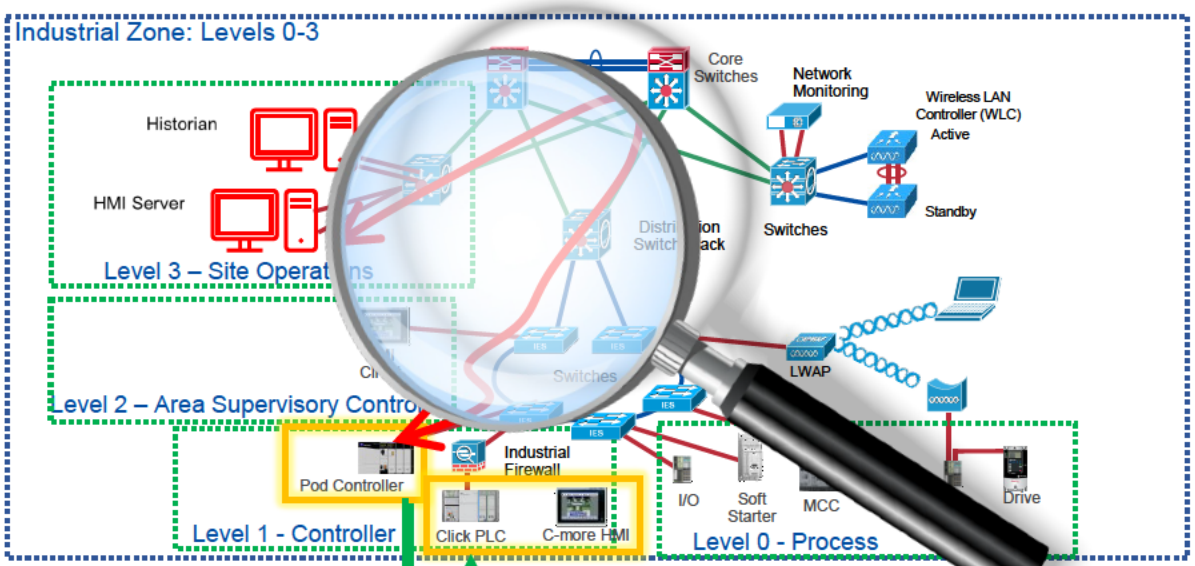
Network based attacks

Now what?

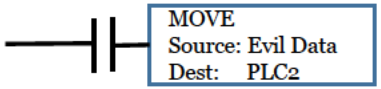
Assumed Breach

Controller attacks

We Focus on Computer to PLC & I/O For Calibration, But Not a Weaponized PLC



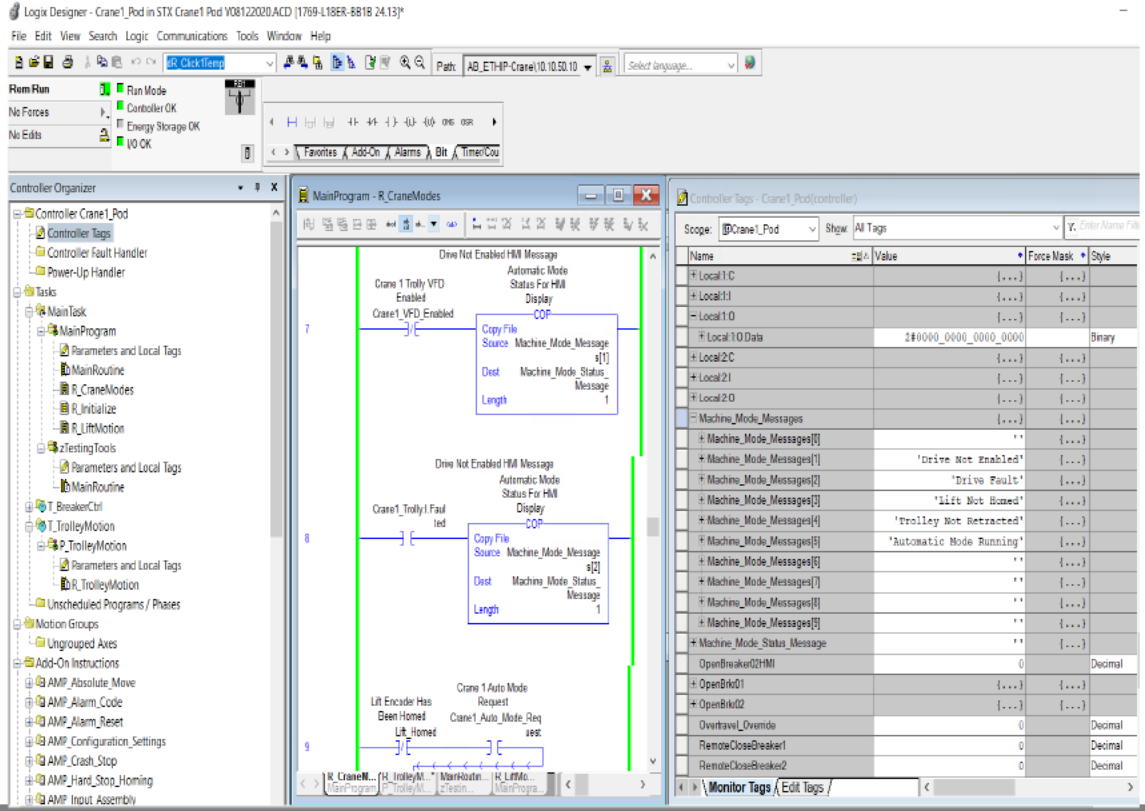
PLC1



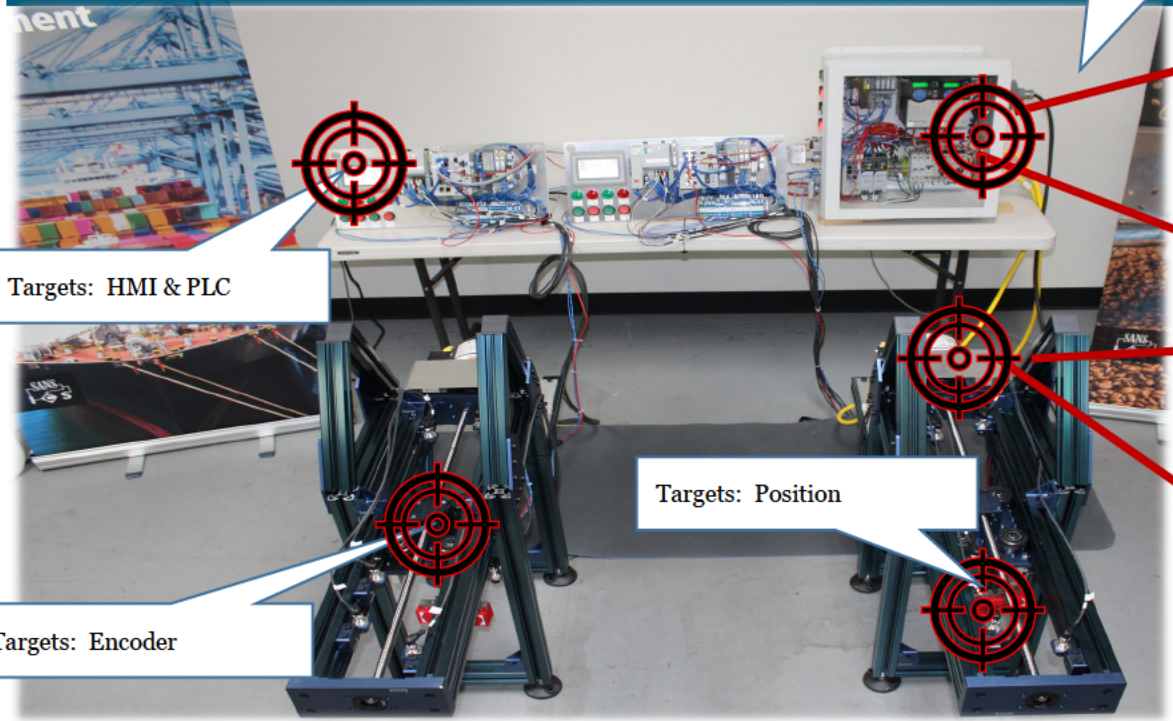
PLC2

It's Challenging to Harden a PLC

- Deep Packet Inspection (DPI) for real time communications not understood and inline processing isn't fast enough
- Understand critical parameters that are targets
- Boundary Check the data before use
  - Usually done in the HMI to trust a passed value is withing range

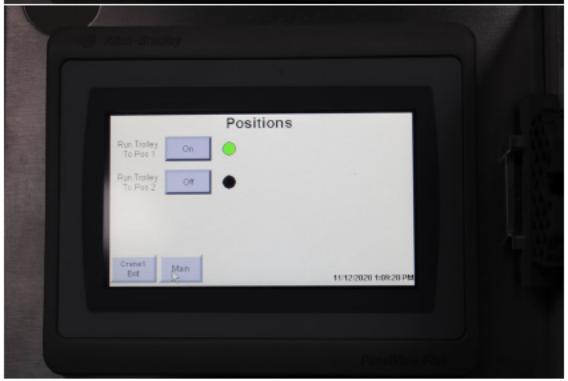


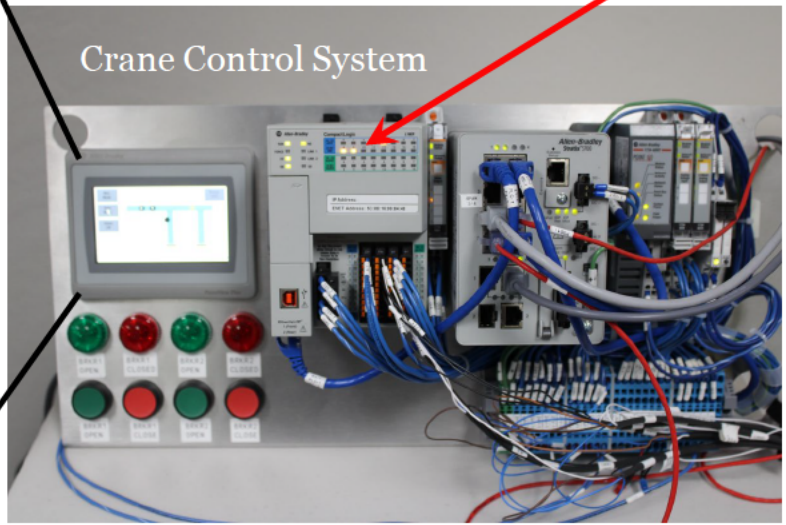
The Ship to Shore Crane Environment



Controller Delivers the Attack(s)

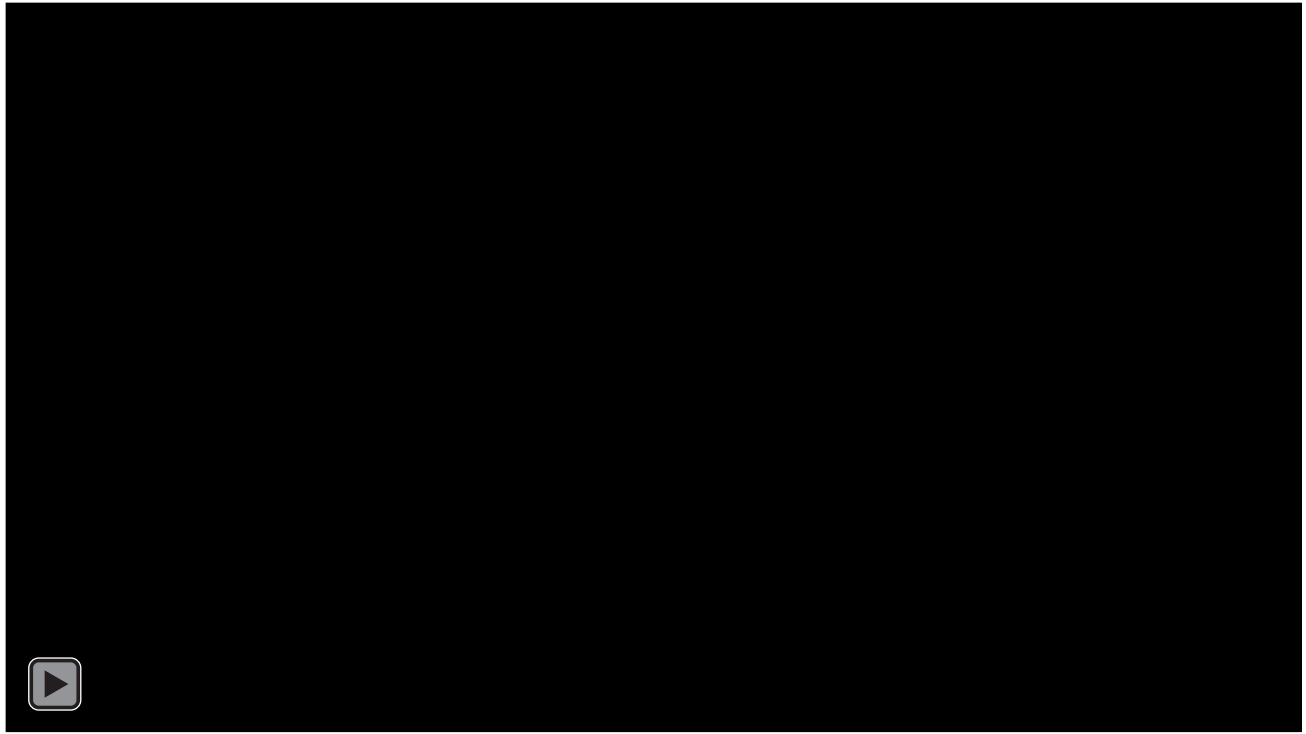
Rogue Control System





Ship To Shore Crane – Normal Operation

- Two Programmable Trolley Ship Positions
- One Trolley Shore Position
- Programmable Up and Down Positions

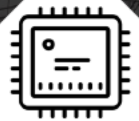


Agenda

Learning Objectives

Assumed Breach

Network based attacks

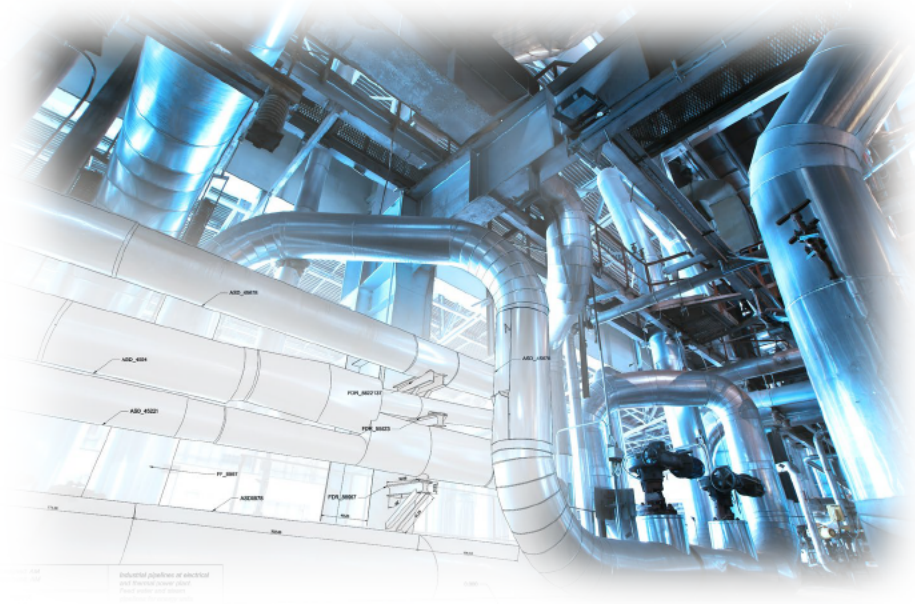


Controller attacks

Now what?

Now What?

- Gain visibility inside your ICS environments
- Develop an understanding of what normal looks like
- Look for bad and operationalize a response approach
- Ensure capabilities exist to validate logic and recover known good logic
- Engineering driven boundary checking within the logic



RESOURCES AND CONTACT INFORMATION

CONTACT
Tim Conway
tconway@sans.org

CONTACT
Jeff Shearer
jshearer@sans.org

ICS RESOURCES
https://ics.sans.org
https://ics-community.sans.org/
Twitter: @sansics

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
PRESS/PR: press@sans.org