Practical Industrial Control Systems(ICS) Cybersecurity
Lecture 1 - the single device attack

Phil Maker

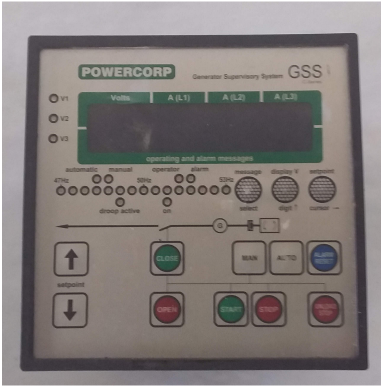
EDS: <https://eds.power.on.net/EDS>

August 2020

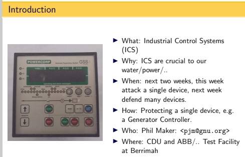
Abstract

A chat about Cyber Security for Industrial Control systems focussing on the single device and attacks upon it.

Introduction



- What: Industrial Control Systems (ICS)
- Why: ICS are crucial to our water/power/..
- When: next two weeks, this week attack a single device, next week defend many devices.
- How: Protecting a single device, e.g. a Generator Controller.
- Who: Phil Maker: `<pjm@gnu.org>`
- Where: CDU and ABB/.. Test Facility at Berrimah



Introduction

- What: Industrial Control Systems (ICS)
- Why: ICS are crucial to our water/power/..
- When: next two weeks, this week attack a single device, next week defend many devices.
- How: Protecting a single device, e.g. a Generator Controller.
- Who: Phil Maker: `<pjm@gnu.org>`
- Where: CDU and ABB/.. Test Facility at Berrimah

1:50 Model of a power system

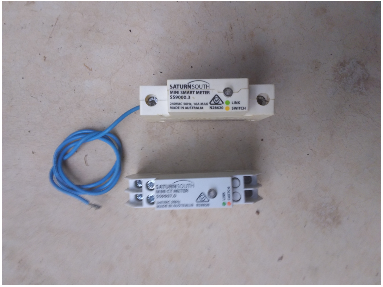
What do I expect from you?

- Listen but please interrupt at any time with questions (both ways).
- You should know about:
  - TCP/IP, UDP, nmap, zenmap, wireshark, nc, MODBUS, IETF, CVE*
  - Kali and its basic installation/use.
  - CVE* for Codesys
  - Understand what an Advanced Persistent Threat (APT) is in this setting.
  - Stuxnet, MODBUS, Aurora Generator Attack and Shammon.
- Little simulated exercise for you taking 30-60m.

The targets

- A mixture of PLC, micros, meters, protection relays, ...
- A variety of protocols including MODBUS, https, DNP3, ...
- A variety of programming languages including C, IEC61131-3, Ladder Logic, Function Blocks, ...
- Controlling a variety of physical processes.
- They have an expected lifetime of 10-20 years.

The vulnerabilities



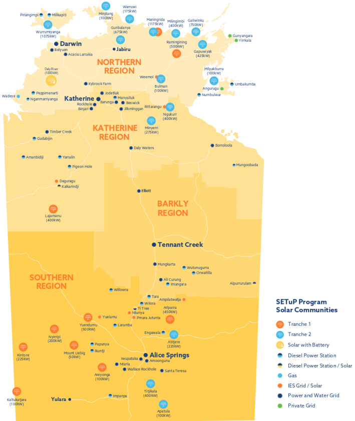
- Operators need remote access but:
  - Good passwords :-).
  - Air gaps don't work, why?
  - 2FA doesn't solve it, why?
  - VPN helps a bit?
- Locally protocols may be unprotected/open (almost always).
- Workstations may be 12 years old running Windoze??
- **The company make does not support it any more?**
- **Software reliability!!**

The attacks

I'm sure your using other words but:

- IT based.
- Industrial Protocol based.
- Network attacks via backdoors.
- Physical process attacks: Stuxnet.
- Physical attacks: Aurora
- Social attacks
- Hardware stack attacks, by management software (e.g. IMP).

The defences



- Firewalls
- Honeypots
- Network monitoring, e.g. snort, wireshark
- Network security
- Password/access security
- Physical security.
- Social attack preventation.
- The Essential 8 from the Australian Security Manual

Conclusion/Exercise

In summary:

- It is not easy securing ICS.
- It is however important.
- A shopping list like the AU Security Manual "Essential 8" is just the beginning.

Questions? Break? Next the exercise? Thanks?