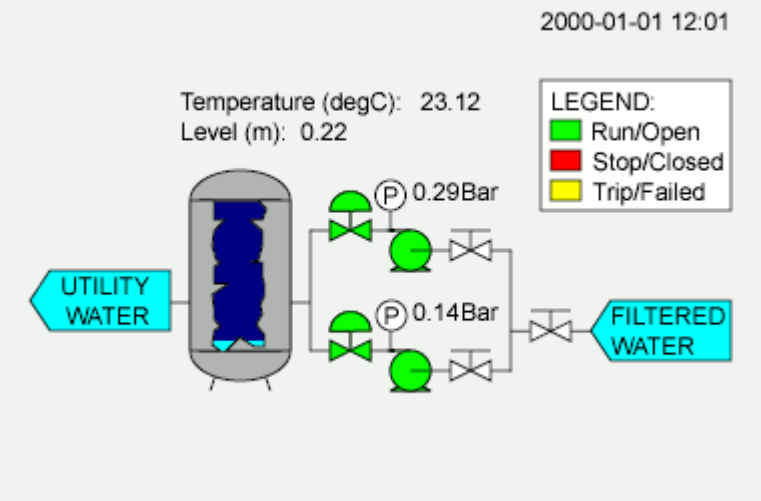

CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
Queen's University
Belfast
Industrial Control System Security Overview
Peter Maynard, PhD Researcher
# ??
@CSIT_QUB

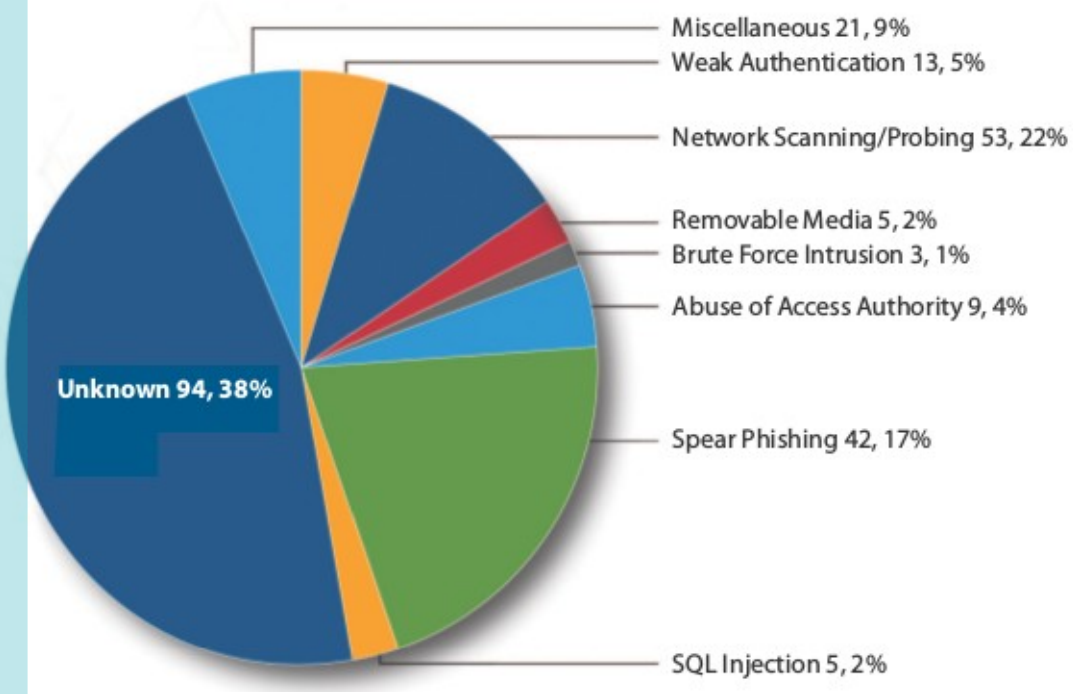
# What is ICS and SCADA

- Industrial Control Systems (ICS):
  - Chemical, water,  gas processing.
  - Transportation, electricity, nuclear systems.
- Supervisory Control And Data Acquisition (SCADA):
  - SCADA provides remote telemetry control for ICS.



# Security Threats to ICS

- ICS systems have a 40 year life span.
- Used to use firewall air-gapping to separate the networks.
- Systems often left un-patched due to system maintainability concerns.
- SCADA protocols developed in the 70s-80s still widely in use.
- Provide no form of encryption or authenticity.
  - Not implemented in industry.

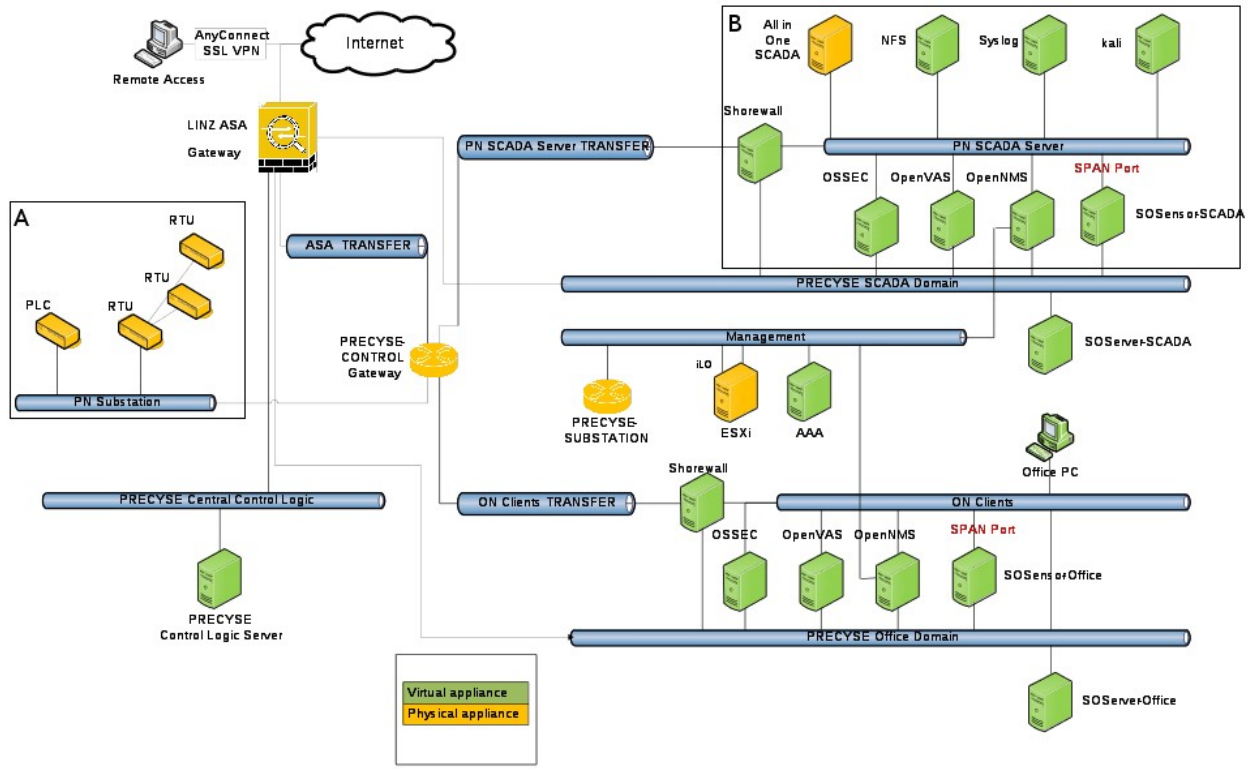


# What we have been working on

- European FP7 Project.
- Worked with Linz Strom GmbH.
  - Austrian Electrical Distribution Operator.
- Access to real world testbed.

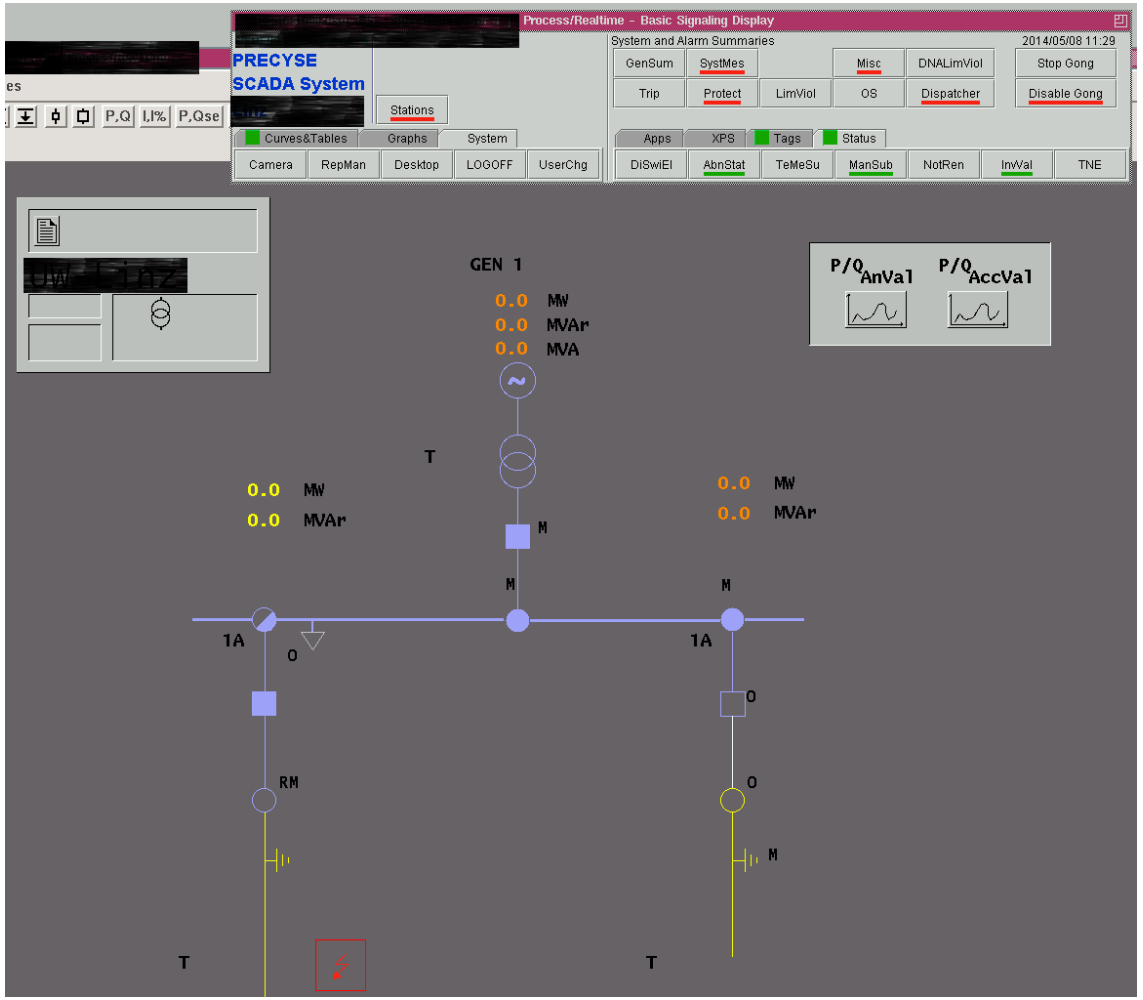
Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE



# Man-In-The-Middle Attack

- Using our custom Ettercap plugin we’re able to hide an earth fault from the operator.
- Using ARP Spoofing.
- Packet manipulation.



# Detection of attacks on ICS

- Current signature based systems, SNORT, Bro.
  - Unable to detect Zero day.
  - Unable to identify suspicious traffic. e.g. malware, backdoors
- Anomaly Detection using Machine Learning.
  - ICS networks are fairly consistent and predictable.

# Questions ?