# If I Knew Then What I Know Now: On Reevaluating DNP3 Security using Power Substation Traffic


**Celine Irvene**

Tohid Shekari

David Formby

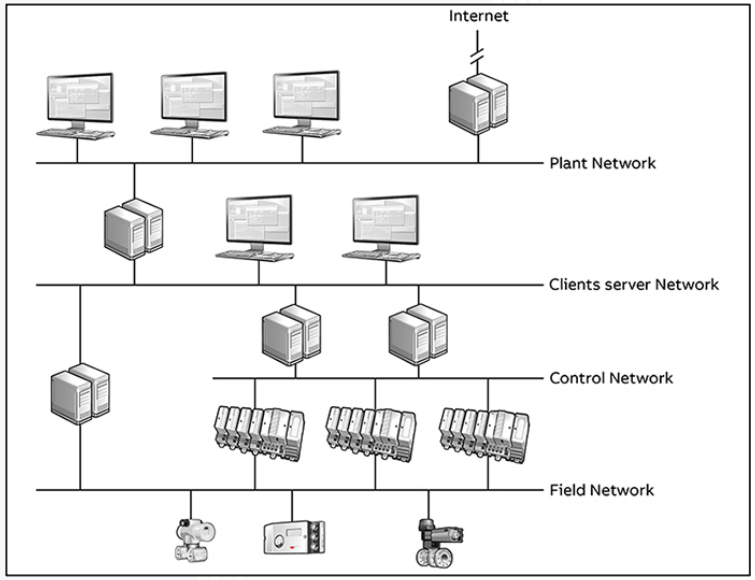
Raheem Beyah

**ICSS '19 – December 2019**

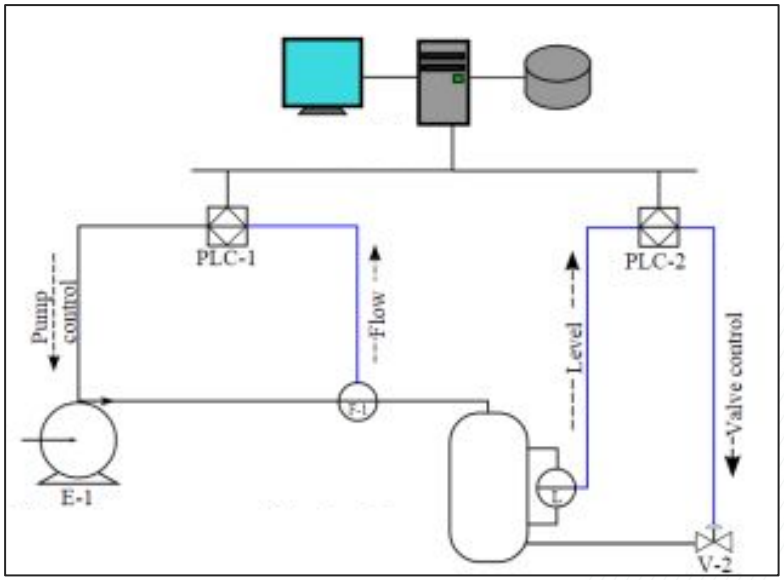
# Industrial Control Systems

Broad class of automation systems used to provide control and monitoring functionality

## System Types




DCS




SCADA

Georgia Tech
CREATING THE NEXT

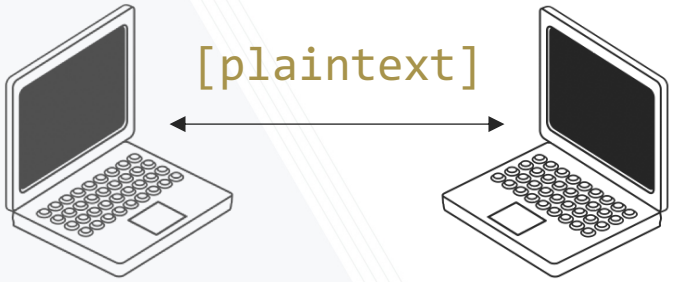
# ICS Applications

Monitor wide ranges of industrial processes and span many domains

## Span Many Domains

- Public Transportation
- Health Care and Medicine
- Manufacturing
- Building Automation
- And Many More!


Georgia Tech
CREATING THE NEXT




# I(nsecure)CS

- Plaintext Communications

- Vulnerable Legacy Devices Accessible via Internet

- Insufficient Authentication and Authorization

- Employees Untrained in Secure Methods and Techniques

# ICS Attacks

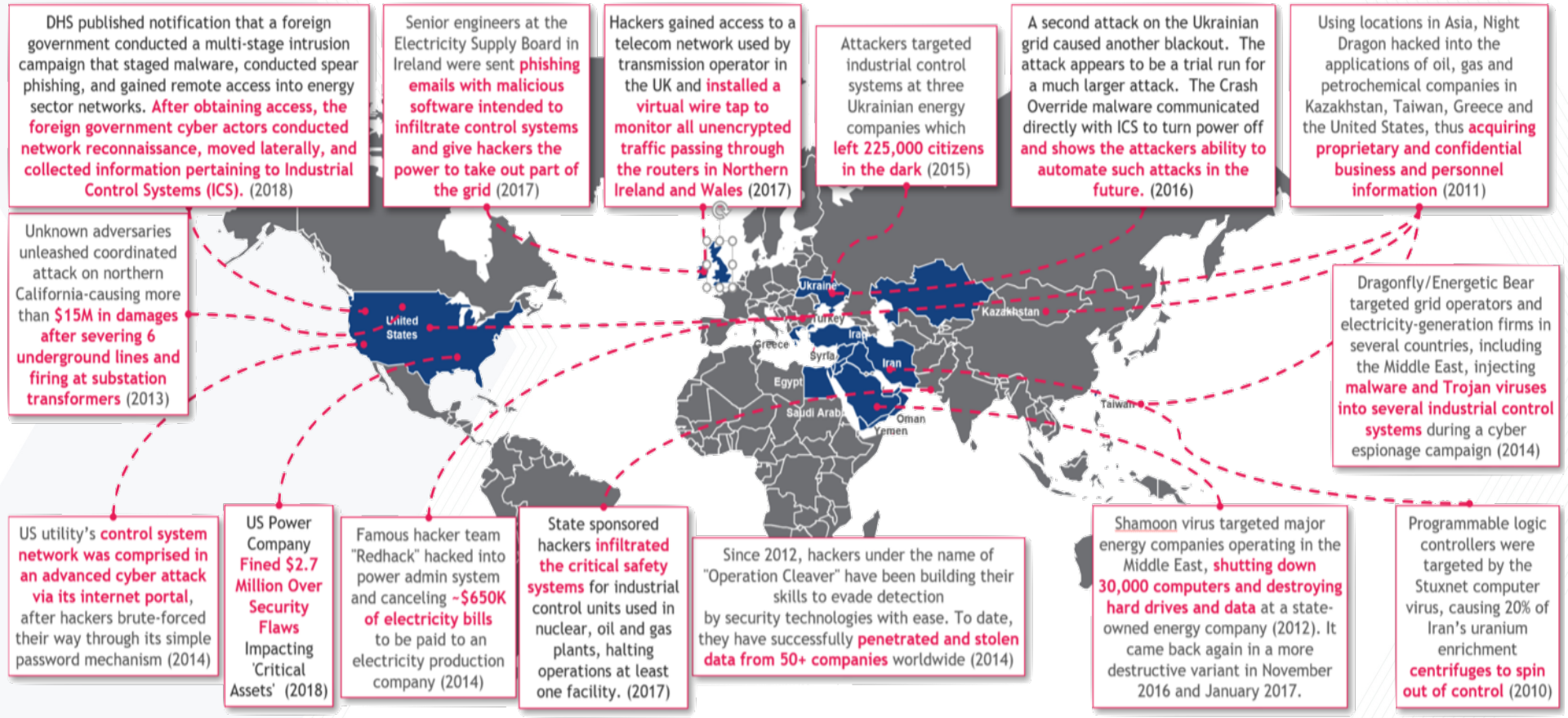
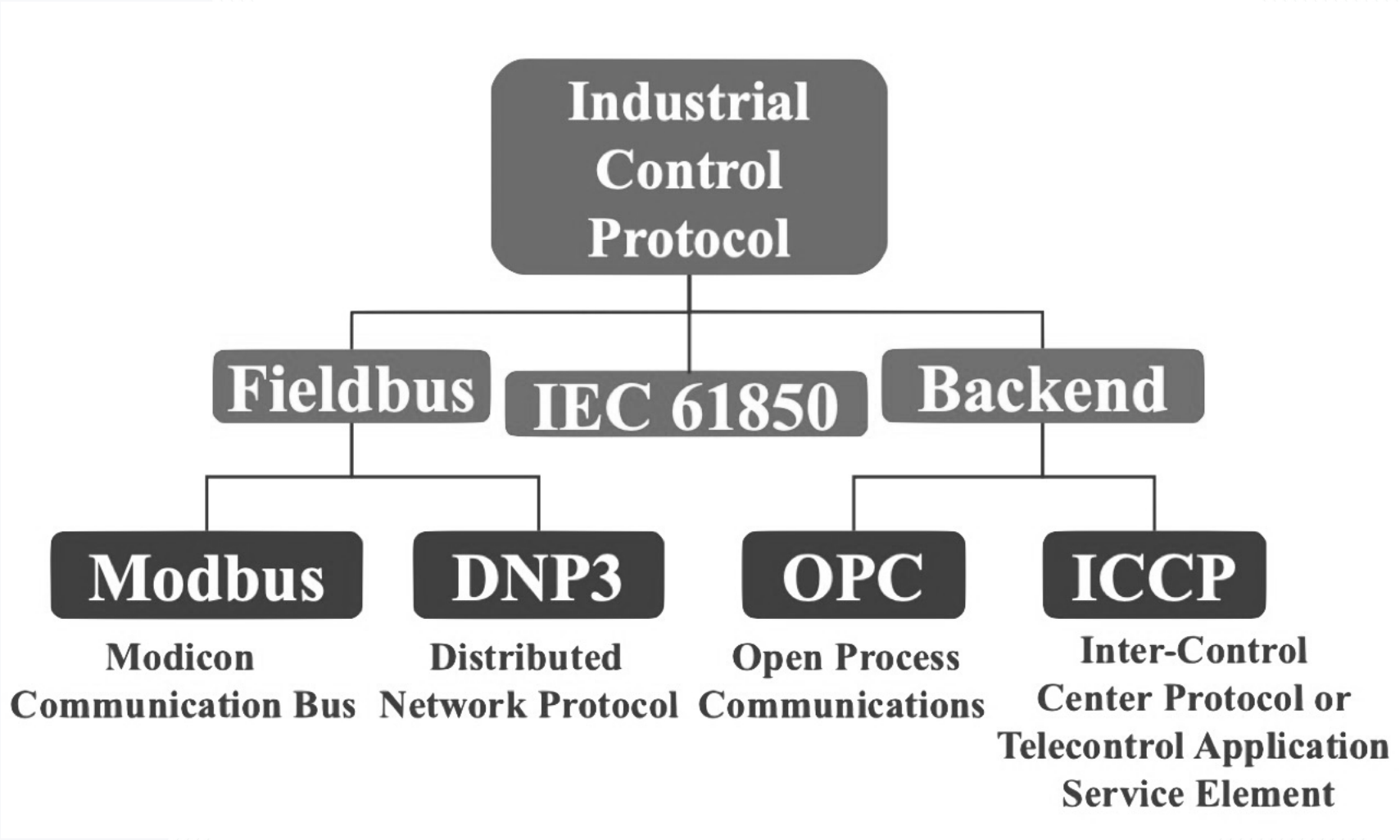


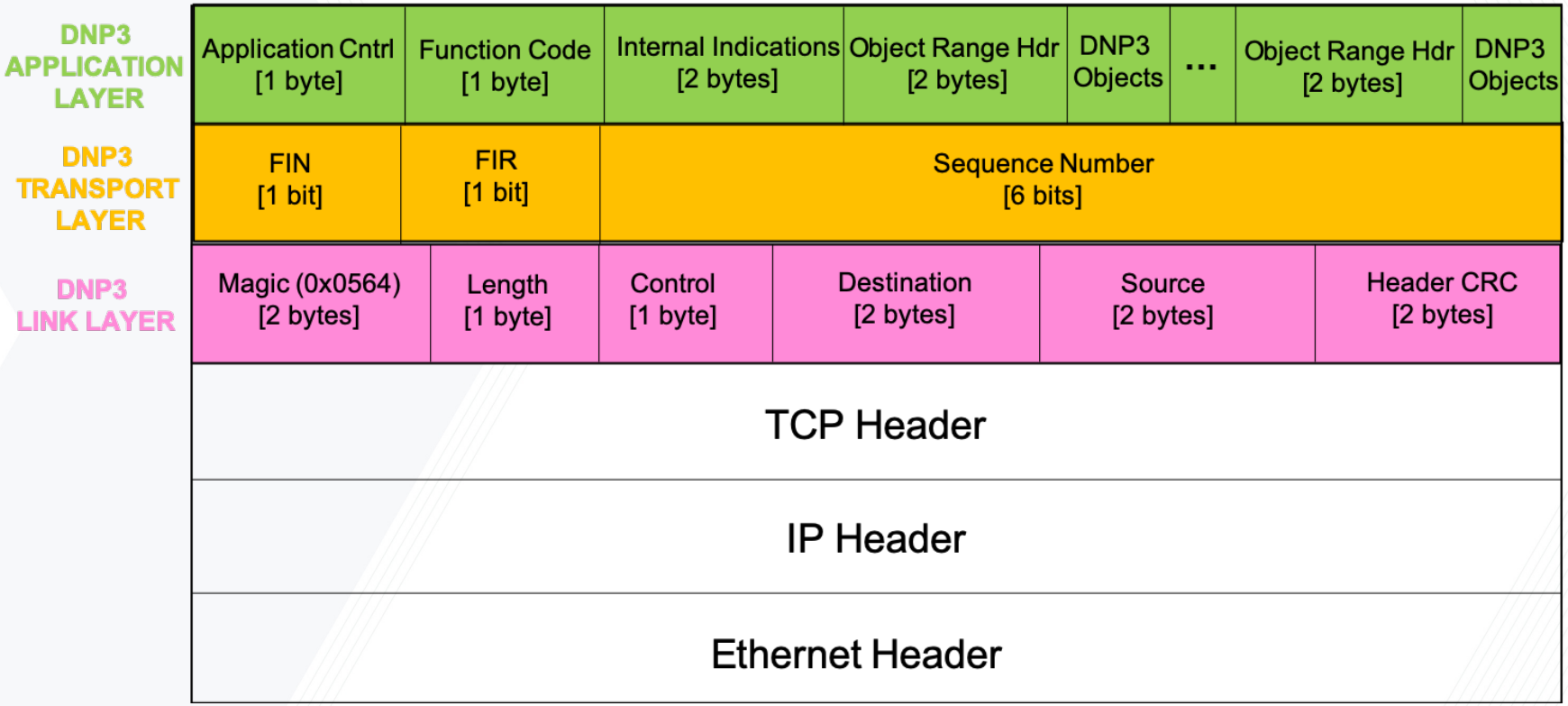

Image credit: Scott Christensen, GrayMatter

Georgia Tech
CREATING THE NEXT

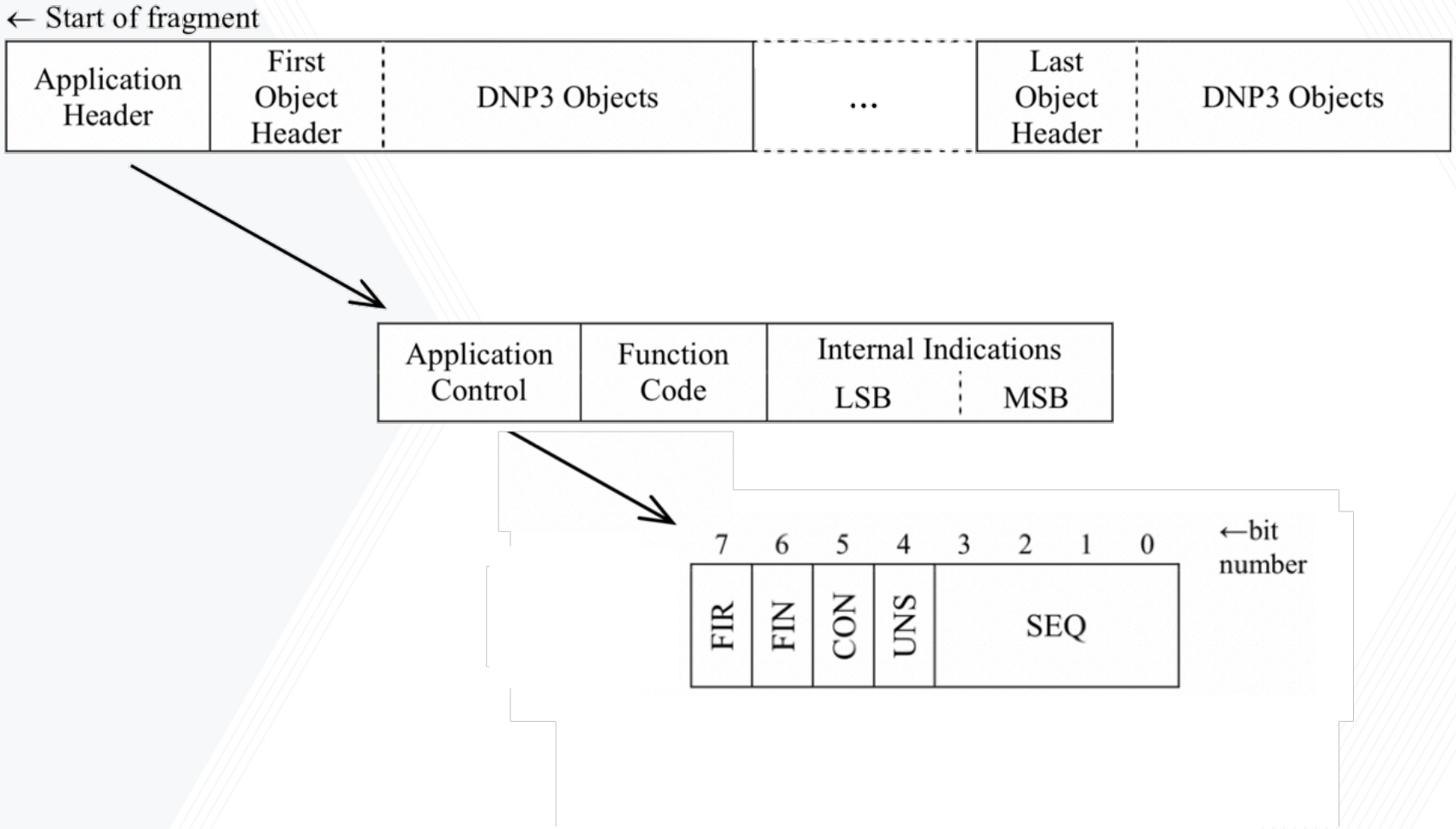
# ICS Communication



# DNP3 Protocol



# DNP3 Application Layer



# Function Codes and IINs

Function Codes

| **Requests** (Hex) | | | |
|---|---|---|---|
| 0 | Confirm | 10 | Initialize application |
| 1 | Read | 11 | Start application |
| 2 | Write | 12 | Stop application |
| 3 | Select | 13 | Save configuration |
| 4 | Operate | 14 | Enable unsolicited |
| 5 | Dir operate | 15 | Disable unsolicited |
| 6 | Dir operate – No resp | 16 | Assign class |
| 7 | Freeze | 17 | Delay measurement |
| 8 | Freeze – No resp | 18 | Record current time |
| 9 | Freeze clear | 19 | Open file |
| A | Freeze clear – No resp | 1A | Close file |
| B | Freeze at time | 1B | Delete file |
| C | Freeze at time – No resp | 1C | Get file information |
| D | Cold restart | 1D | Authenticate file |
| E | Warm restart | 1E | Abort file |
| F | Initialize data | | |
| | | | |
| | | | |
| **Responses** (Hex) | | | |
| 81 | Response | | |
| 82 | Unsolicited response | | |

Internal Indications

| **LSB** | |
|---|---|
| IIN1.0 | All stations |
| IIN1.1 | Class 1 events |
| IIN1.2 | Class 2 events |
| IIN1.3 | Class 3 events |
| IIN1.4 | Need time |
| IIN1.5 | Local control |
| IIN1.6 | Device trouble |
| IIN1.7 | Device restart |
| **MSB** | |
| IIN2.0 | Function code not supported |
| IIN2.1 | Object unknown |
| IIN2.2 | Parameter error |
| IIN2.3 | Event buffer overflow |
| IIN2.4 | Already executing |
| IIN2.5 | Configuration corrupt |
| IIN2.6 | Reserved 1 |
| IIN2.7 | Reserved 2 |

# DNP3 Attacks

**Application Layer most susceptible to attack because it provides the data payload**

Function Code Attacks

Internal Indications Attacks

# Function Code Attacks

| Function Code | |
|---|---|
| **WRITE** | An attacker could use this to overflow or corrupt the outstation's memory |
| **FREEZE/CLR** | Injecting this to an outstation, it could lead to device malfunctions and crashes |
| **COLD/WARM RESTART** | Perpetually sending these messages could DoS the outstation and never let it completely start up |
| **INITIALIZE** | Transmitting with random data objects could cause the outstation to reinitialize itself and lead to system state inconsistencies resulting in device failures |
| **STOP** | Could terminate applications running on the outstation and make it unresponsive to commands from the master |
| **UNSOL RESPONSE** | Assuming unsolicited response mode is enabled, attackers can use this to cause DoS or buffer overflow unsuspecting nodes by repeatedly transmitting data packets |

# Internal Indication Attacks

| Internal Indication Flag | |
|---|---|
| **IIN2.5**<br>**Configuration Corrupt** | Set from the outstation to the master. This triggers the master to send a new configuration file which could then be intercepted by a MITM and swapped with the attacker's desired configuration |
| **IIN2.3**<br>**Event Overflow Buffer** | Will trigger the master to request event data. If an attacker keeps this bit set she can dupe the master into an infinite loop of requesting data, to impede it from performing other tasks |

# The Problem

DNP3, like many ICS protocols, is **insecure**

Data communications in the **wild** may **differ** from protocol operation in **theory**

Little research dedicated to the **characterization** of ICSs or DNP3 with real network traffic

# Contributions

DNP3 Application Layer **traffic analysis** of large-scale power substation dataset

**Attack and mitigation assessment** of previously proposed techniques from real-world dataset perspective

Lightweight application layer defense and **security enhancing recommendations**

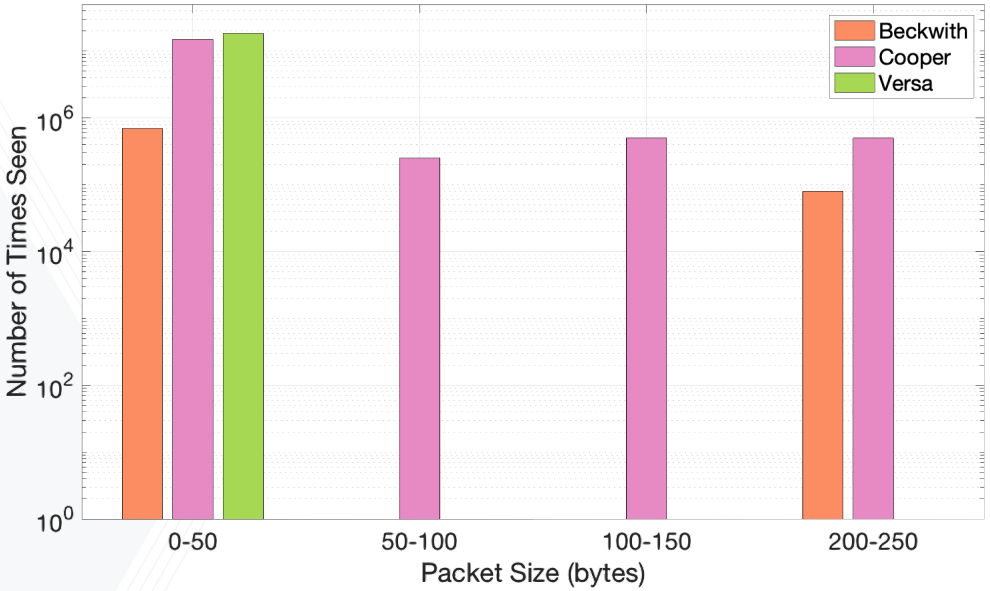
# Power Substation Dataset

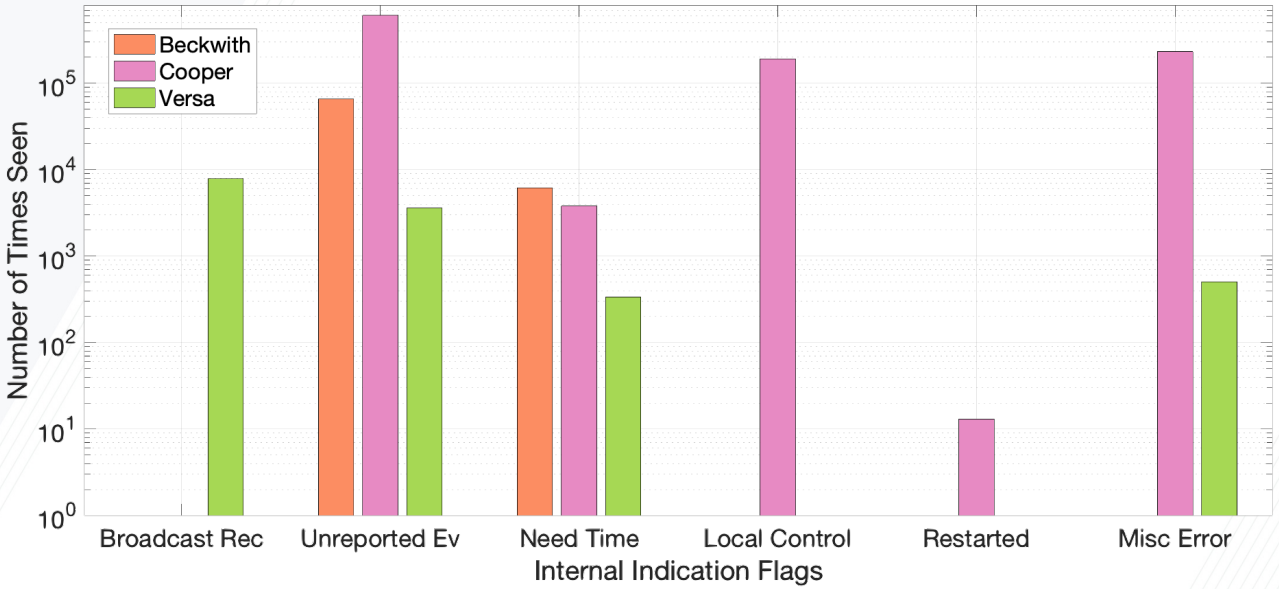
Captured from **Four** Medium-Voltage Distribution Substations

| Dataset | Size (GB) | Nodes | Collection Period |
|---|---|---|---|
| **A1** | 21.7 | 228 | September 2013 - February 2014 |
| **A2** | 146.4 | 300 | January - August of 2015 |
| **A3** | 147 | 300 | August 2015 - April 2016 |
| **B** | 0.34 | 199 | August 10 - August 11, 2015 |
| **C** | 5.7 | 121 | April - May 2016 |
| **D** | 11.7 | 104 | |

Georgia Tech
CREATING THE NEXT

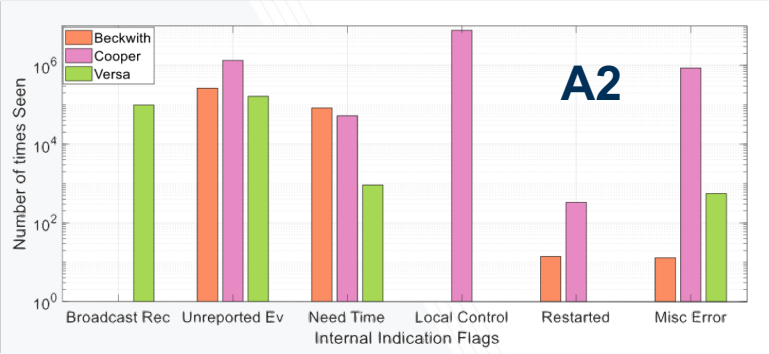
# Traffic Characterization – A1

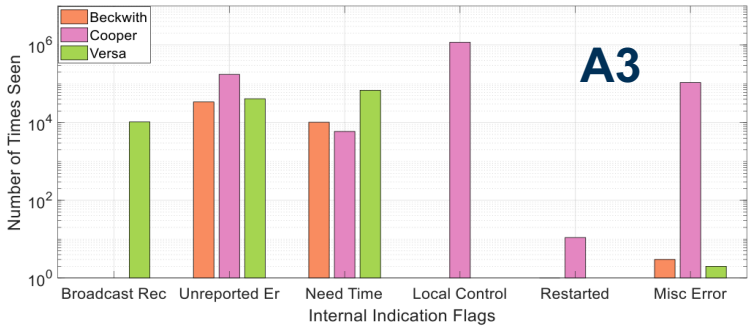


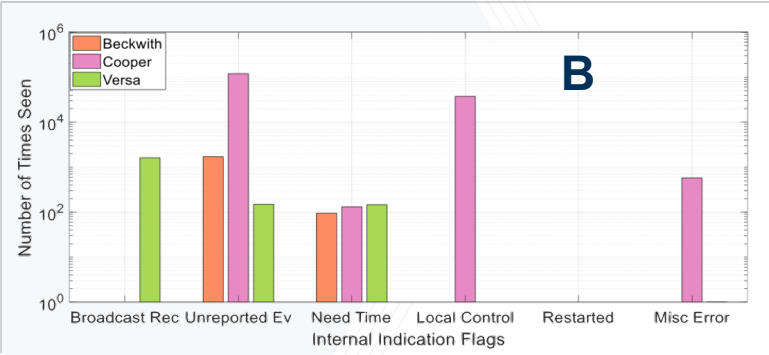



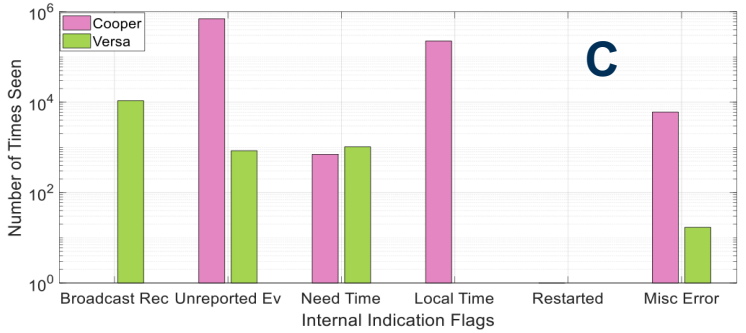

Georgia Tech
CREATING THE NEXT

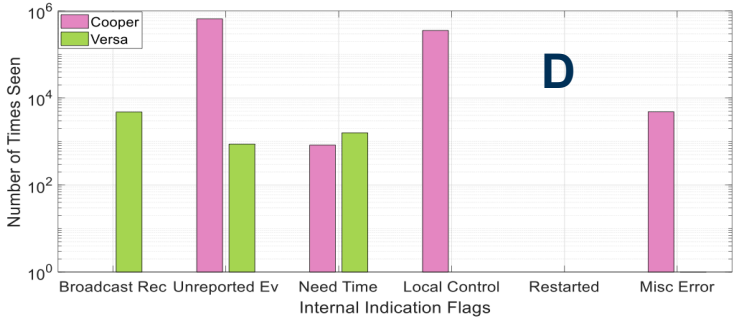
# Datasets A2 - D



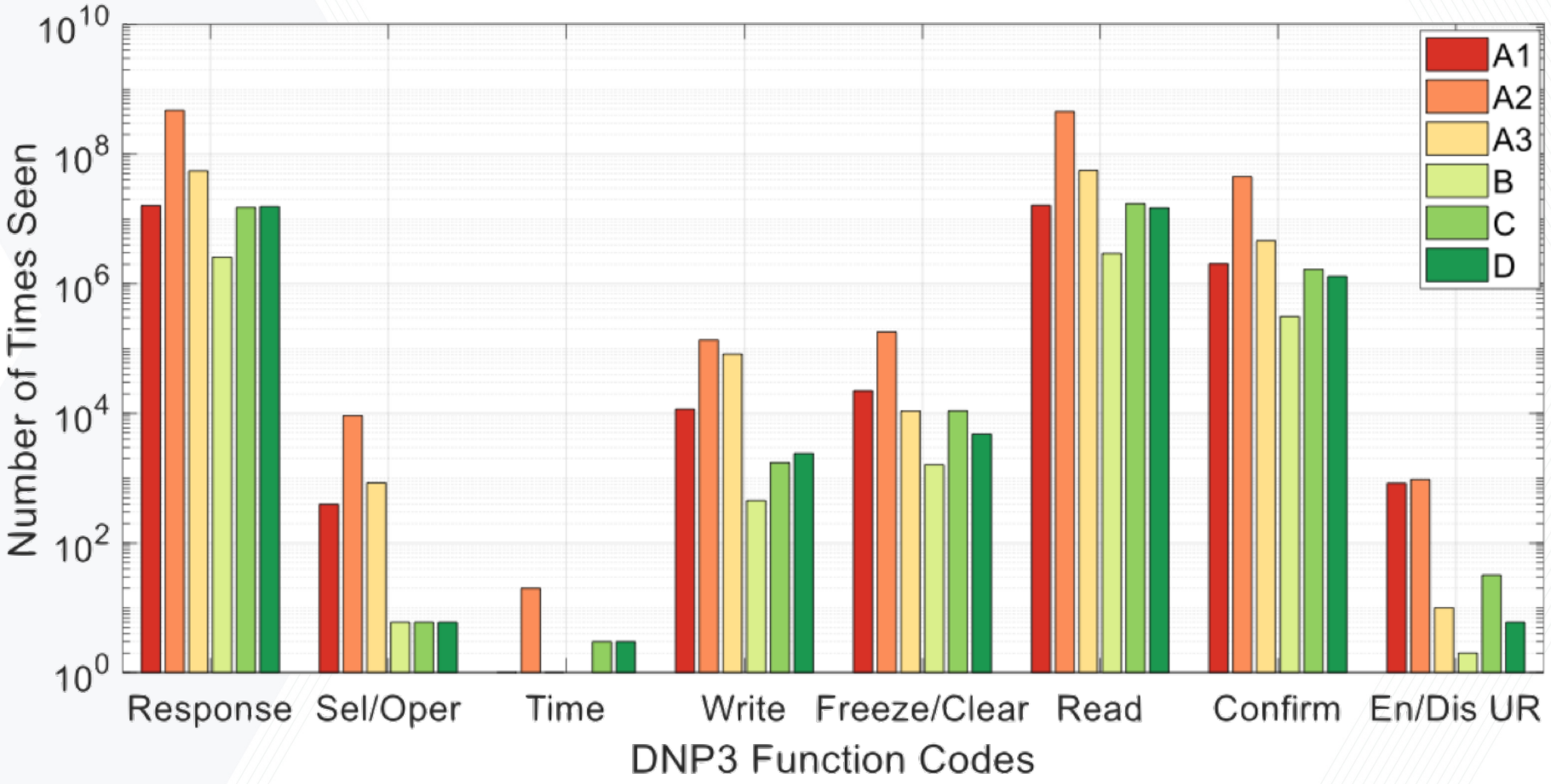




Georgia Tech
CREATING THE NEXT

# Function Code Analysis




Georgia Tech
CREATING THE NEXT

# Key Characterization Takeaways

Real world DNP3 data can **vary** from substation to substation

But data trends **DO EXIST!**

Some of the **worst** attacks from the literature are reasonably detectable

# Assessment of Proposed DNP3 Attacks and Mitigations

**Goal - Better understand the breadth of DNP3 attack landscape**

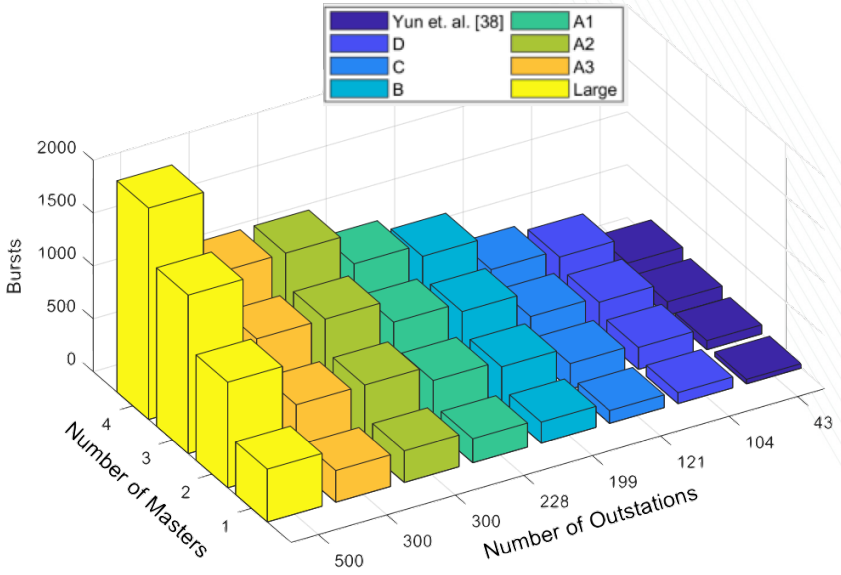
Investigate two DNP3 attacks proposed in the literature

If given, analyze their proposed mitigation techniques

# Attack 1

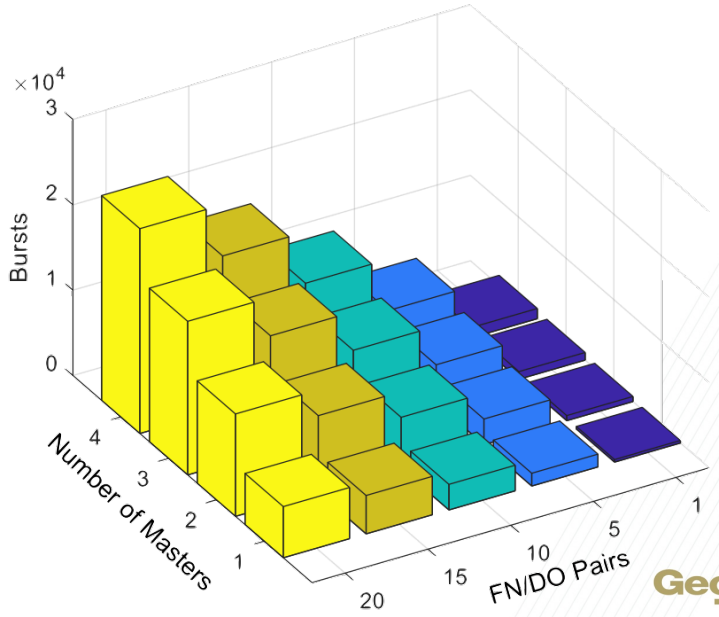
## Proposed Two Scenarios

- Abnormal Control/Data Transfer
- Traffic Flooding




## Countermeasure

- Whitelist-based approach which categorizes all seen network traffic into bursts




## Shortcoming – Expensive

Jeong-Han Yun, Sung-Ho Jeon, Kyoung-Ho Kim, and Woo-Nyon Kim. 2013. Burst- based anomaly detection on the DNP3 protocol. International Journal of Control and Automation 6, 2 (2013), 313–324.

# Attack 2

## Main Goal

- Identify function codes which pose the largest threats to DNP3

## Implementation

- Simulated DNP3 network – 1 MTU and 3 RTUs configured via OpenDNP3

## Shortcoming – Simulated

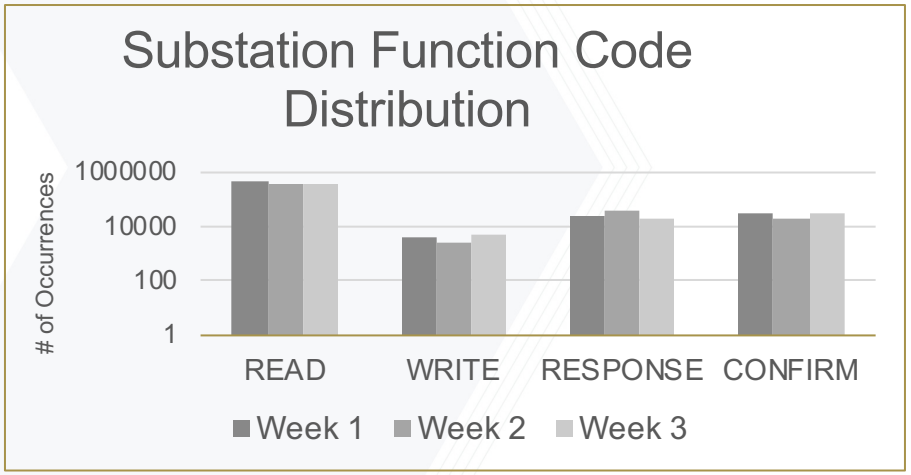
| Function Code | Attack Surface | |
|---|---|---|
| | US | Singh[35] |
| READ | | ✖ |
| WRITE | ✖ | |
| CONFIRM | | |
| SELECT | ✖ | ✖ |
| OPERATE | ✖ | ✖ |
| FREEZE | ✖ | — |
| CLEAR | ✖ | — |
| RESTART | ✖ | — |
| INIT | ✖ | — |
| RESPONSE | | |
| UNSOL RESPONSE | | |
| START | | — |
| STOP | ✖ | |
| EN/DIS UNSOL | ✖ | ✖ |

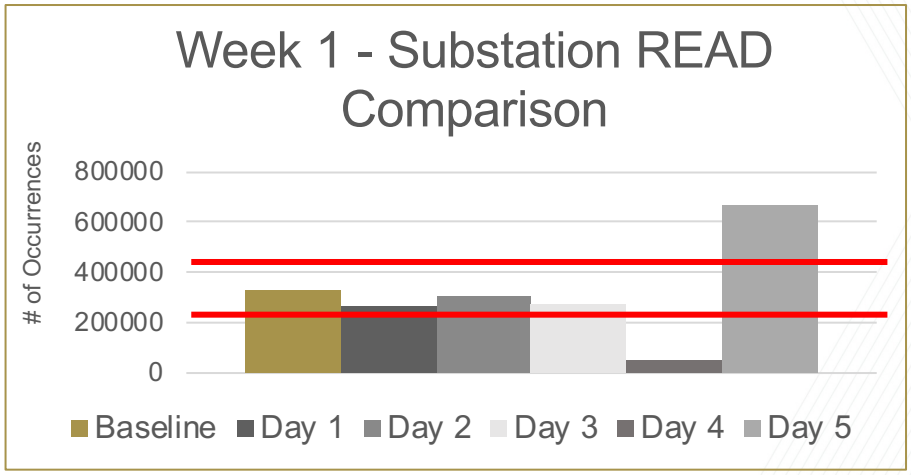
Georgia Tech
CREATING THE NEXT

C. Singh, A. Nivangune, and M. Patwardhan. 2016. Function code based vulnerability analysis of DNP3. In 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). 1–6. https://doi.org/10.1109/ANTS.2016. 7947865

# Baseline Distribution Countermeasure

Use limited set of application layer function codes to generate a baseline of normal network behavior




$$AveragePIT_a = \frac{\sum_{i=1}^{j} t_{i+1} - t_i}{j}$$

Georgia Tech
CREATING THE NEXT

# Defense Recommendations

In addition to the baseline distribution approach for detecting network availability compromises other techniques have been proposed

| Defense | |
|---|---|
| [10] Darwish et al. 2018 | Time based mitigation technique for detecting MITM attacks |
| [23] Lee et al. 2014 | DNP3 Authenticated Encryption method |
| [16] Fovino et al. 2010 | Using IDS rules which describe critical ICS system states |
| [36] Valdes et al. 2009 | Anomaly detection for monitoring host communication patterns and individual network flows |

# Summary and Future Work

Application layer **characterization** of **real** power substation network traffic

Analyzed the efficacy of **previously proposed** DNP3 **attacks** and **defenses**

Proposed a **lightweight application layer defense** and gave security recommendations

**Future Work** - Numerical evaluation on proposed theoretical approaches with real world data

# QUESTIONS?

**Contact:**

**cirvene3@gatech.edu**

**cap.ece.gatech.edu**

Georgia Tech

CREATING THE NEXT