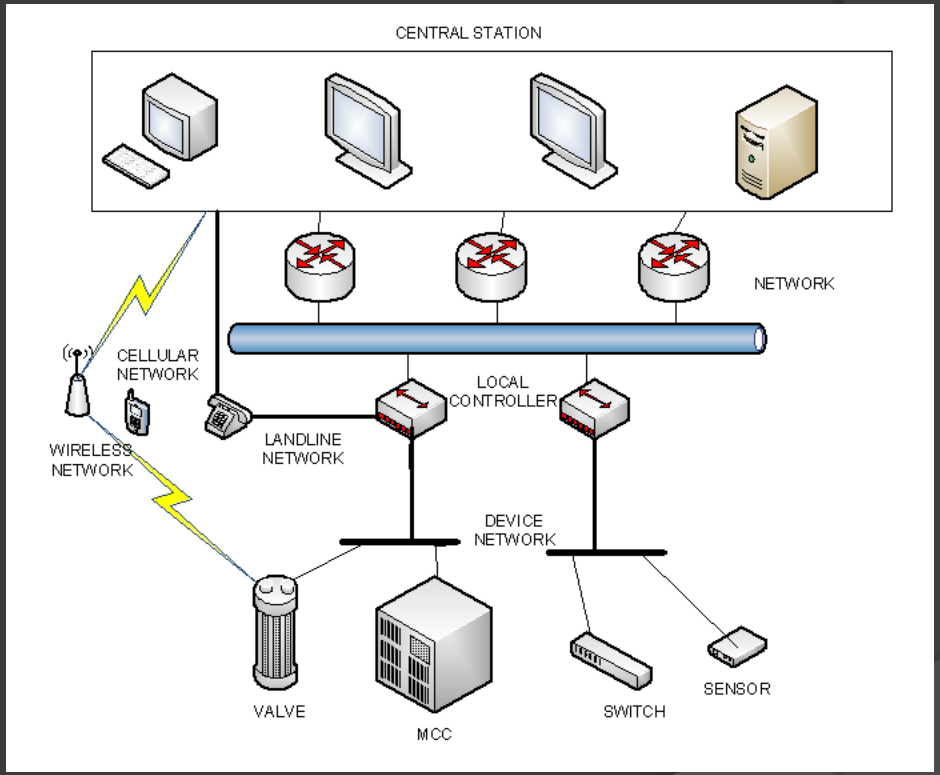
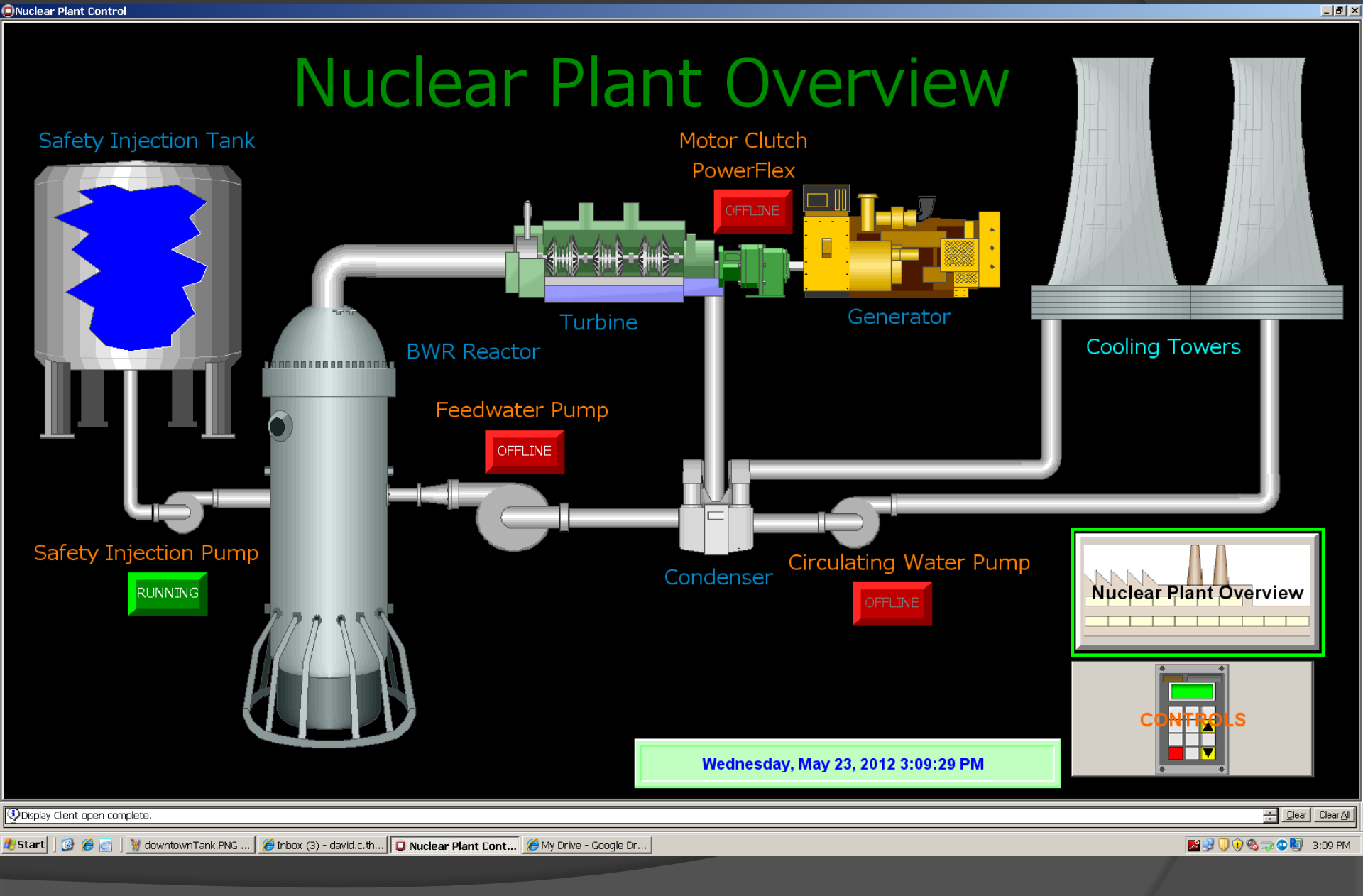
Guillermo Francia, III
David Thornton and Thomas Brookshire
Jacksonville State University

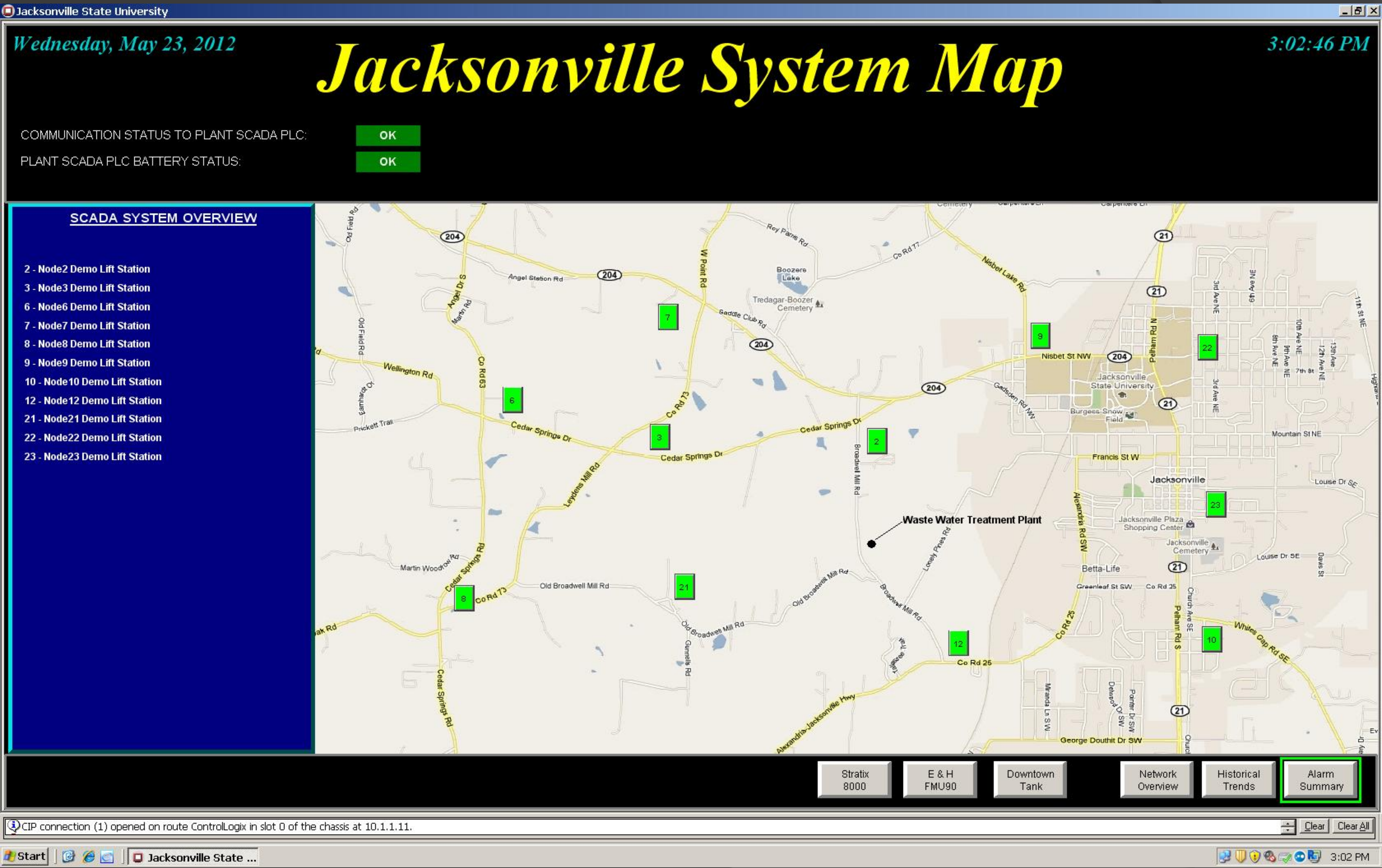
CYBERATTACKS ON SCADA SYSTEMS

Supervisory Control and Data Acquisition (SCADA)

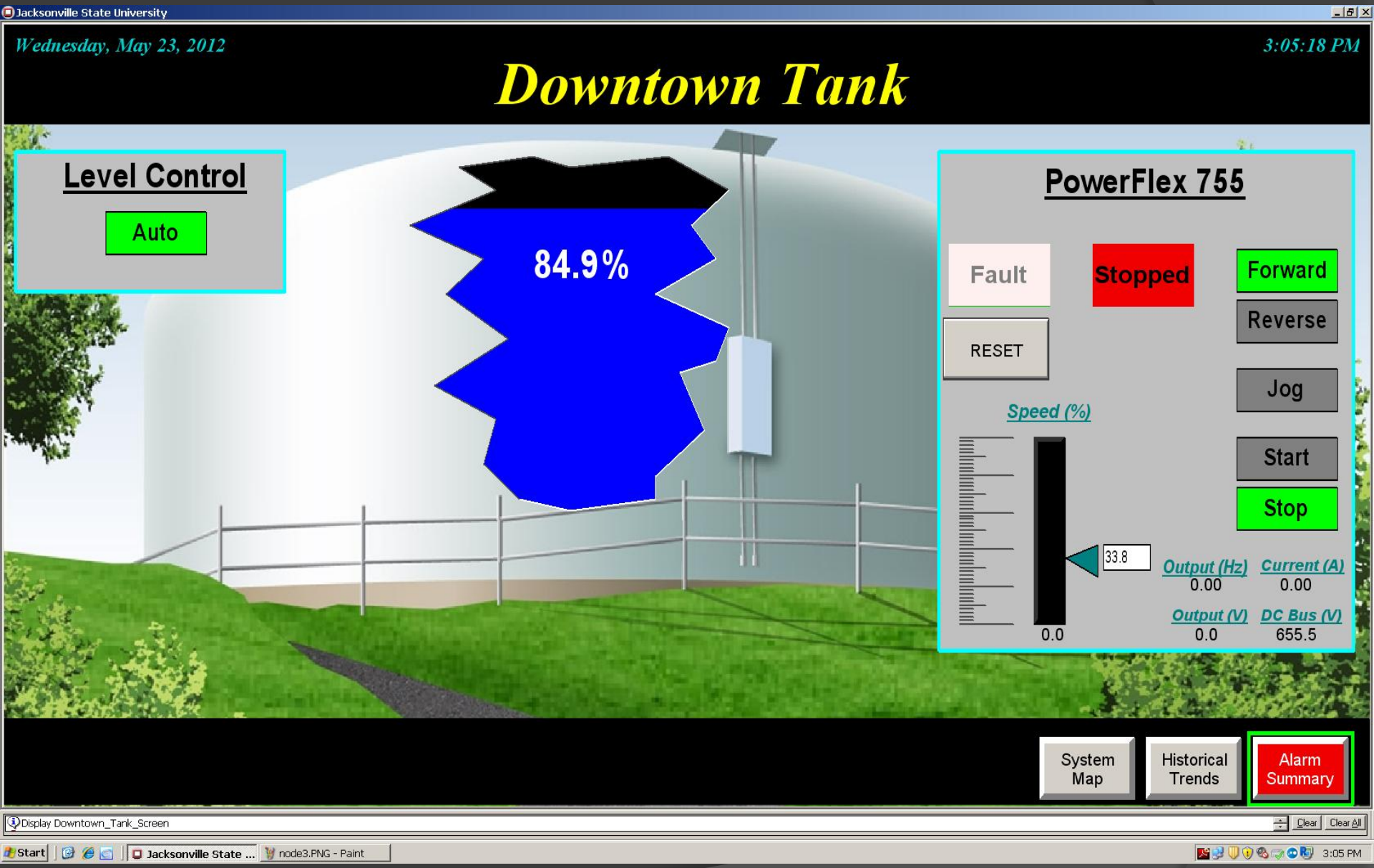
- Critical infrastructure (water, nuclear, gas, electricity, etc.)
- Wireless network expansion
- Connectivity: the tradeoff of vulnerability for convenience




Nuclear Plant Control
Nuclear Plant Overview
Safety Injection Tank
Motor Clutch
PowerFlex
OFFLINE
Turbine
Generator
Cooling Towers
BWR Reactor
Feedwater Pump
OFFLINE
Safety Injection Pump
RUNNING
Condenser
Circulating Water Pump
OFFLINE
Nuclear Plant Overview
CONTROLS
Wednesday, May 23, 2012 3:09:29 PM
Display Client open complete.
Clear
Clear All
Start
downtownTank.PNG ...
Inbox (3) - david.c.th...
Nuclear Plant Cont...
My Drive - Google Dr...
3:09 PM



Jacksonville State University
Wednesday, May 23, 2012
Jacksonville System Map
3:02:46 PM
COMMUNICATION STATUS TO PLANT SCADA PLC:
OK
PLANT SCADA PLC BATTERY STATUS:
OK
SCADA SYSTEM OVERVIEW
2 - Node2 Demo Lift Station
3 - Node3 Demo Lift Station
6 - Node6 Demo Lift Station
7 - Node7 Demo Lift Station
8 - Node8 Demo Lift Station
9 - Node9 Demo Lift Station
10 - Node10 Demo Lift Station
12 - Node12 Demo Lift Station
21 - Node21 Demo Lift Station
22 - Node22 Demo Lift Station
23 - Node23 Demo Lift Station
Waste Water Treatment Plant
Jacksonville
Jacksonville State University
Stratix 8000
E & H FMU90
Downtown Tank
Network Overview
Historical Trends
Alarm Summary
CIP connection (1) opened on route ControlLogix in slot 0 of the chassis at 10.1.1.11.
Clear
Clear All
Start
Jacksonville State ...
3:02 PM


Jacksonville State University
Wednesday, May 23, 2012
3:05:18 PM
Downtown Tank
Level Control
Auto
84.9%
PowerFlex 755
Fault
Stopped
Forward
Reverse
RESET
Jog
Speed (%)
Start
Stop
33.8
0.0
Output (Hz)
0.00
Current (A)
0.00
Output (V)
0.0
DC Bus (V)
655.5
System Map
Historical Trends
Alarm Summary
Display Downtown_Tank_Screen
Clear
Clear All
Start
Jacksonville State ...
node3.PNG - Paint
3:05 PM

General Wireless Threats

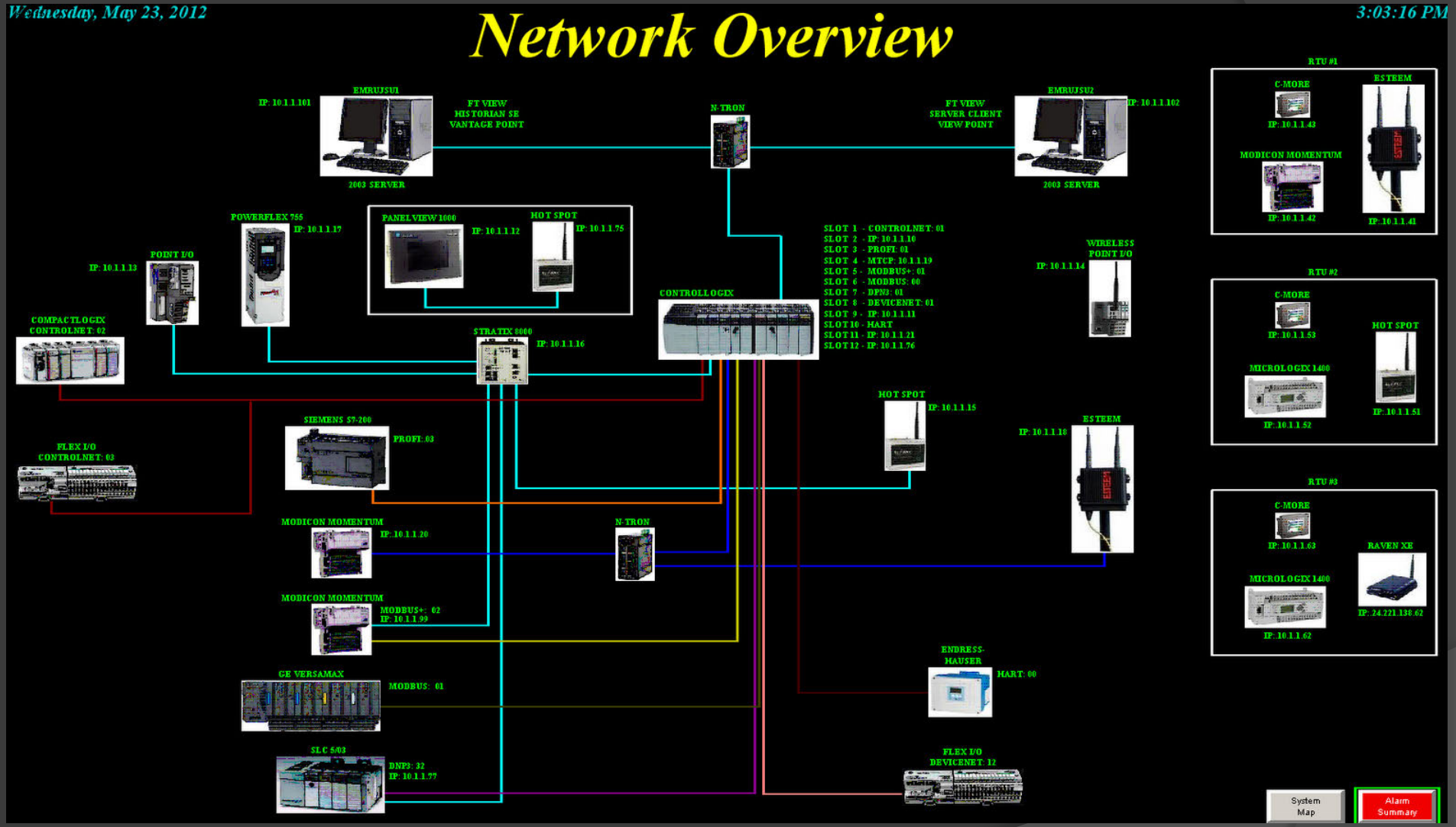
- Shared medium
- WEP / WPA / WPA2 cracking
- Resource-depletion and denial of service
- Rogue access points
- Injection attacks
- Analog wireless eavesdropping

Threats Particular to SCADA

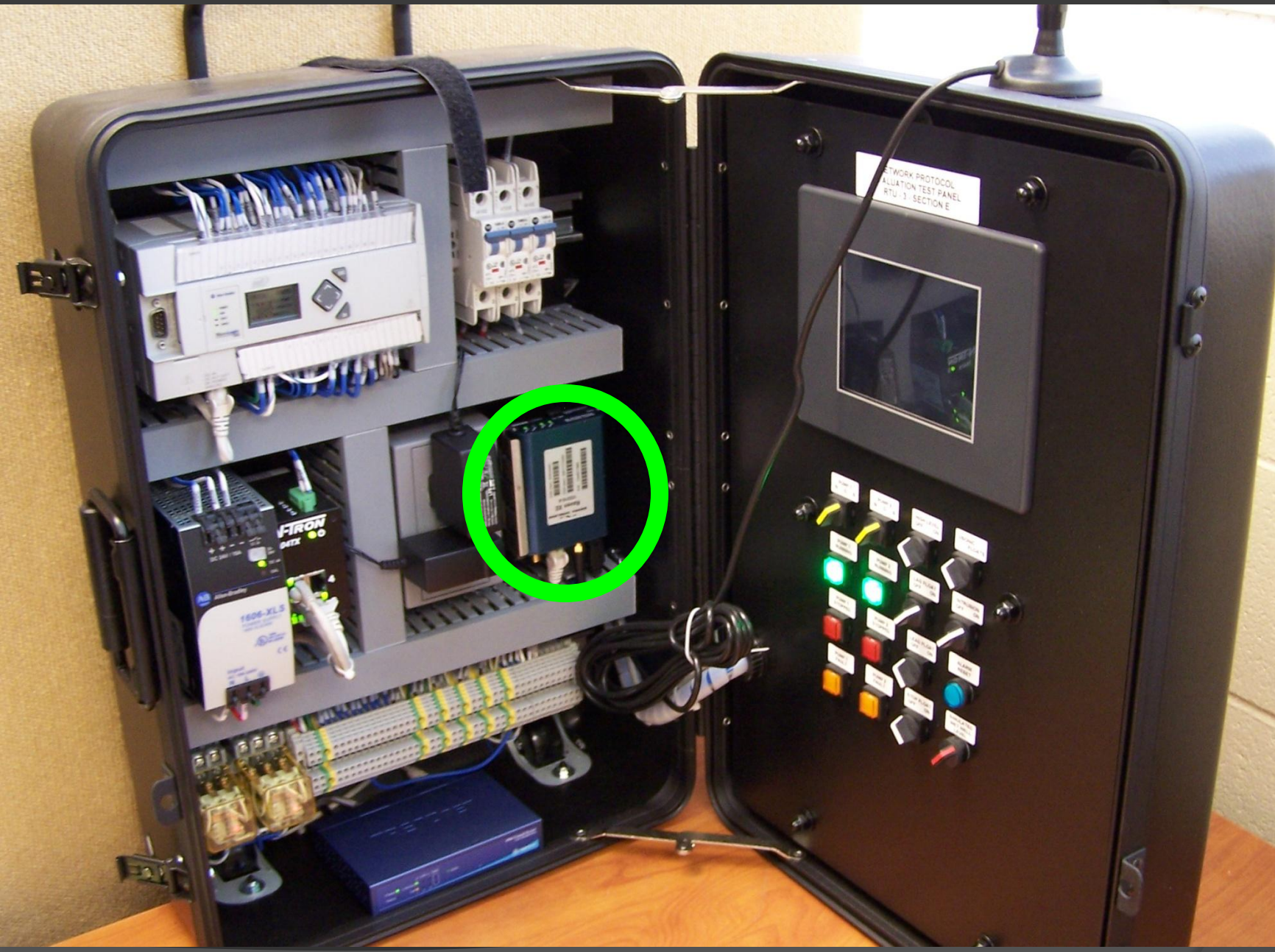
- Standardization
- Shared networking
- Low-speed connections with long polling cycles
- Alternative communications technology
- Radio communication
- Easily programmable RTUs

Laboratory Setup

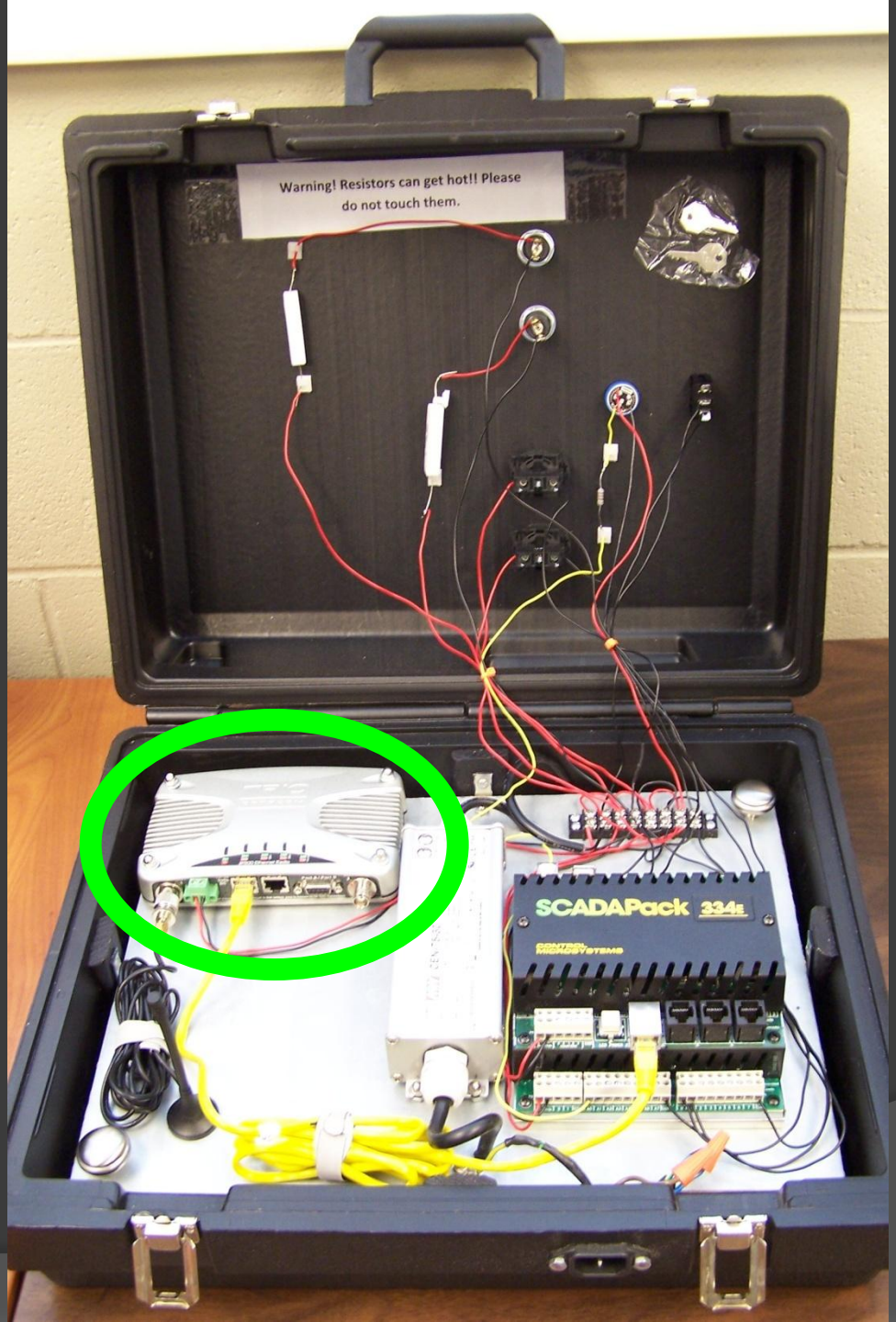
- Central station connects to RTUs via the following technologies:
  - Cellular
  - 900 MHz radio
  - 802.11 wi-fi

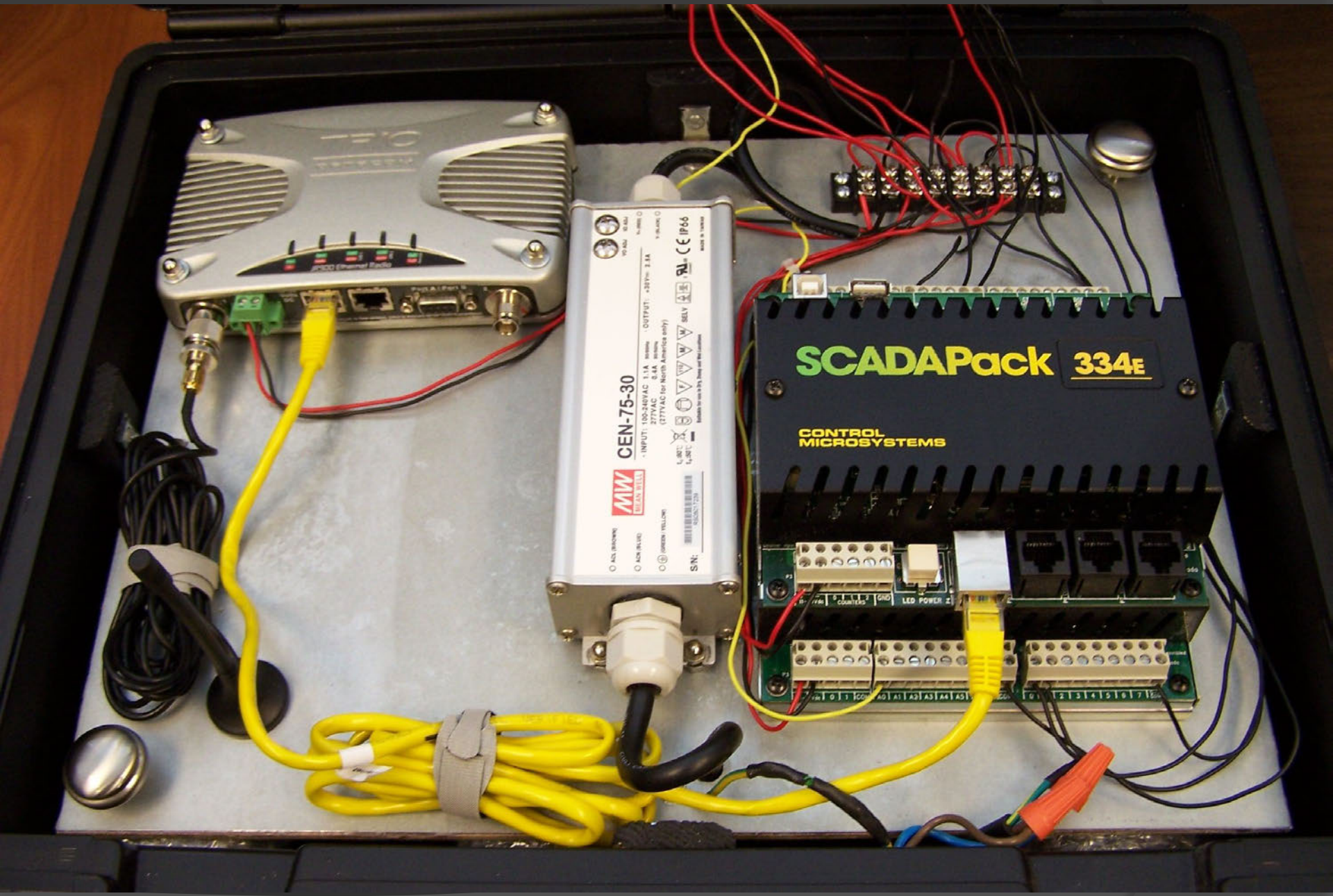

Wednesday, May 23, 2012
3:03:16 PM
Network Overview
EMRUJSU1
IP: 10.1.1.101
FT VIEW
HISTORIAN SE
VANTAGE POINT
2003 SERVER
N-TRON
EMRUJSU2
IP: 10.1.1.102
FT VIEW
SERVER CLIENT
VIEW POINT
2003 SERVER
RTU #1
C-MORE
IP: 10.1.1.43
ESTEEM
MODICON MOMENTUM
IP: 10.1.1.42
IP: 10.1.1.41
RTU #2
C-MORE
IP: 10.1.1.53
HOT SPOT
IP: 10.1.1.51
MICROLOGIX 1400
IP: 10.1.1.52
RTU #3
C-MORE
IP: 10.1.1.63
RAVEN XE
IP: 24.221.138.62
MICROLOGIX 1400
IP: 10.1.1.62
POWERFLEX 755
IP: 10.1.1.17
PANEL VIEW 1000
IP: 10.1.1.12
HOT SPOT
IP: 10.1.1.75
POINT I/O
IP: 10.1.1.13
COMPACTLOGIX
CONTROLNET: 02
STRATIX 8000
IP: 10.1.1.16
CONTROLLOGIX
SLOT 1 - CONTROLNET: 01
SLOT 2 - IP: 10.1.1.10
SLOT 3 - PROFI: 01
SLOT 4 - MTCP: 10.1.1.19
SLOT 5 - MODBUS+: 01
SLOT 6 - MODBUS: 00
SLOT 7 - DPN3: 01
SLOT 8 - DEVICENET: 01
SLOT 9 - IP: 10.1.1.11
SLOT 10 - HART
SLOT 11 - IP: 10.1.1.21
SLOT 12 - IP: 10.1.1.76
WIRELESS
POINT I/O
IP: 10.1.1.14
HOT SPOT
IP: 10.1.1.15
ESTEEM
IP: 10.1.1.18
SIEMENS S7-200
PROFI: 03
FLEX I/O
CONTROLNET: 03
MODICON MOMENTUM
IP: 10.1.1.20
N-TRON
MODICON MOMENTUM
MODBUS+: 02
IP: 10.1.1.99
GE VERSAMAX
MODBUS: 01
ENDRESS-
HAUSER
HART: 00
SLC 5/03
DNP3: 32
IP: 10.1.1.77
FLEX I/O
DEVICENET: 12
System
Map
Alarm
Summary

- Modicon
- Siemens
- VersaMax
- Micrologix
- Allen Bradley



SIERRA WIRELESS
Raven XE
V2221E-S
ESN (hex): 60B3A99C
ESN (dec): 09611774364
S/N: 1044517895


Warning! Resistors can get hot!! Please
do not touch them.
SCADAPack 334E


CEN-75-30
SCADAPack 334E
CONTROL MICROSYSTEMS


NETWORK PROTOCOL
EVALUATION TEST PANEL
RTU - 2 - SECTION D
RADIOLINX
TRITON
1606-XLS


POWER
RF TRANSMIT
RF RECEIVE
SERIAL
ETHERNET
RADIOLINX®
INDUSTRIAL HOTSPOT™
BY PROSOFT TECHNOLOGY®
SIGNAL STRENGTH
RLXIB-IHW
802.11abg

Proof-of-concept Attacks

- Cellular Communications (Modems)
- Industrial Radios (900 MHz)
- Wi-Fi Networks (802.11)

Cellular Communications

- Accessible via IP
- Used Hydra to crack password
- Passwords often left default
- Password maximum length too short

Industrial Radios (900 MHz)

- Trio radios
- Can be located by “war-driving”
- Serial number required, but easily crackable (again, due to short length)

Wi-Fi Networks (802.11)

- Man-in-the-middle attacks
- Passive attack (surveillance)
- Active attack (misinformation)

Conclusions and Future Plans

- SCADA more vulnerable than ever
- Plan to investigate:
  - Advanced protocols (CIP, Modbus TCP, DNP3, etc.)
  - Crafting packets to enable fuzz testing
- Plan to produce:
  - Body of best practices for critical infrastructure security
  - Collection and analysis of digital forensic data

Acknowledgements

- DoD-NSA grant H98230-10-1-0419
- NSF grant OCI-0959687

Contact Information

- Principal Investigator: Guillermo Francia
  gfrancia@jsu.edu