*Pervasive Cybersecurity is our passion …*

# Sifers-Grayson Site Survey & Security Posture Assessment

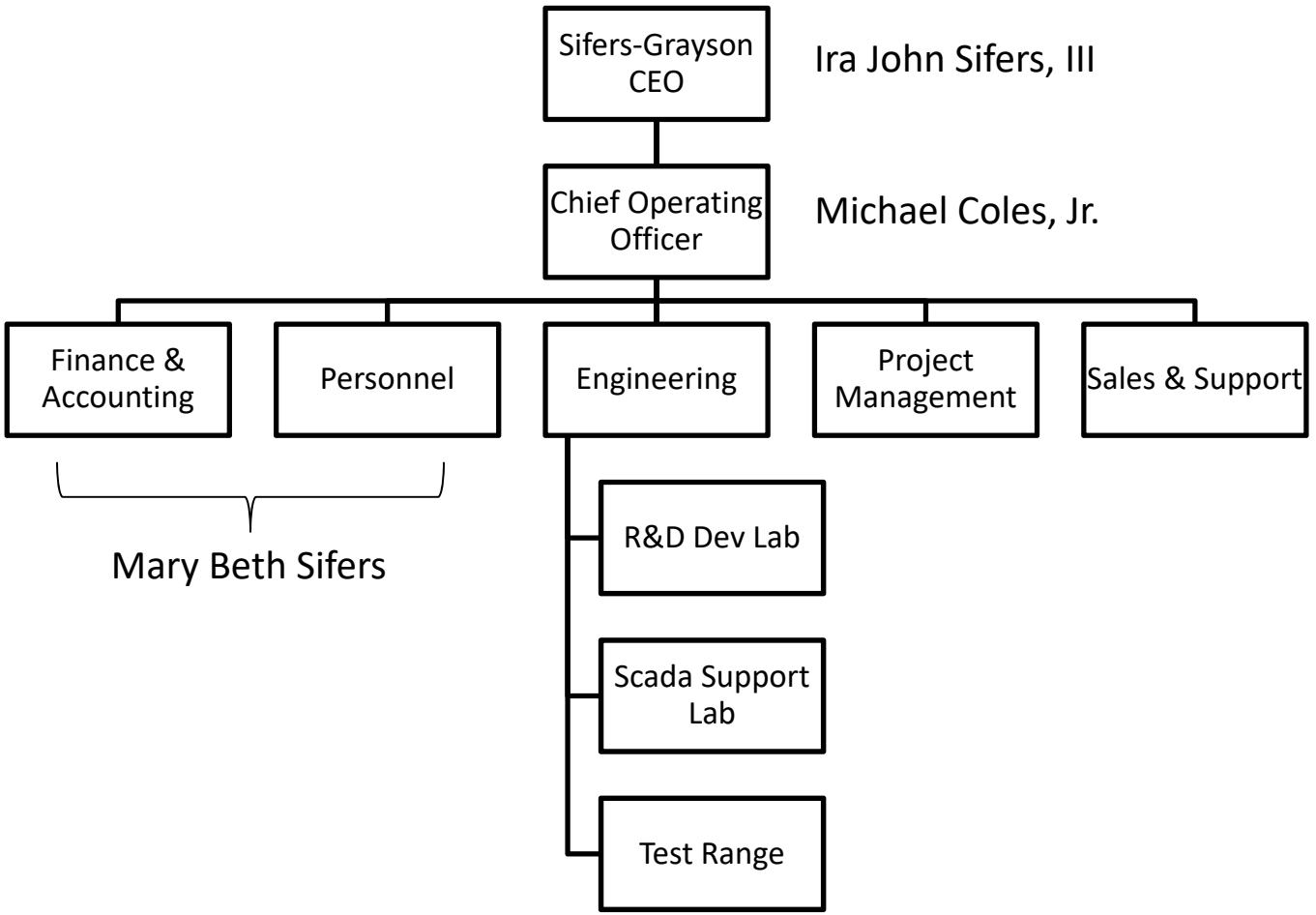
Prepared by: Nofsinger Consulting Services, LLC

PRELIMINARY – NOT FOR DISTRIBUTION

# Company Background

- Founded by Ira John Sifers and John Michael Cole in 1974
- Based in Pine Knob, Grayson County, Kentucky
- Located in the Appalachian Economic Development Region
- Business areas:
  - Industrial Control Systems for Advanced Manufacturing & Utilities
  - R&D for Drones and Robots

# Sifers-Grayson Organization Chart



# Customer Base

- Advanced Manufacturing Firms
- Utility Companies
- U.S. Department of Defense
- U.S. Department of Homeland Security

A Quick Look at the SG Enterprise Architecture

# SITE SURVEY

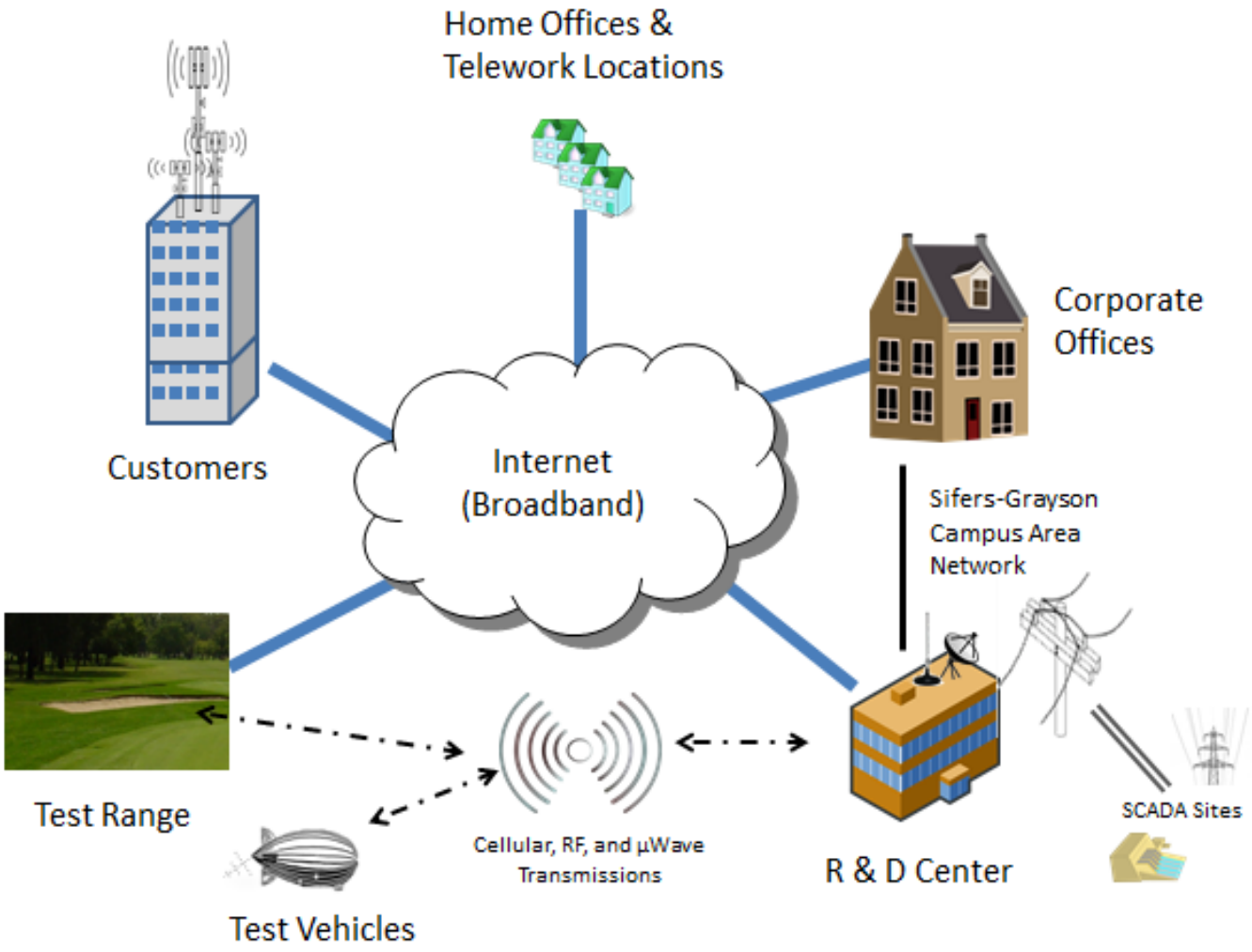



**Figure 1. Overview of Sifers-Grayson Enterprise IT Architecture**

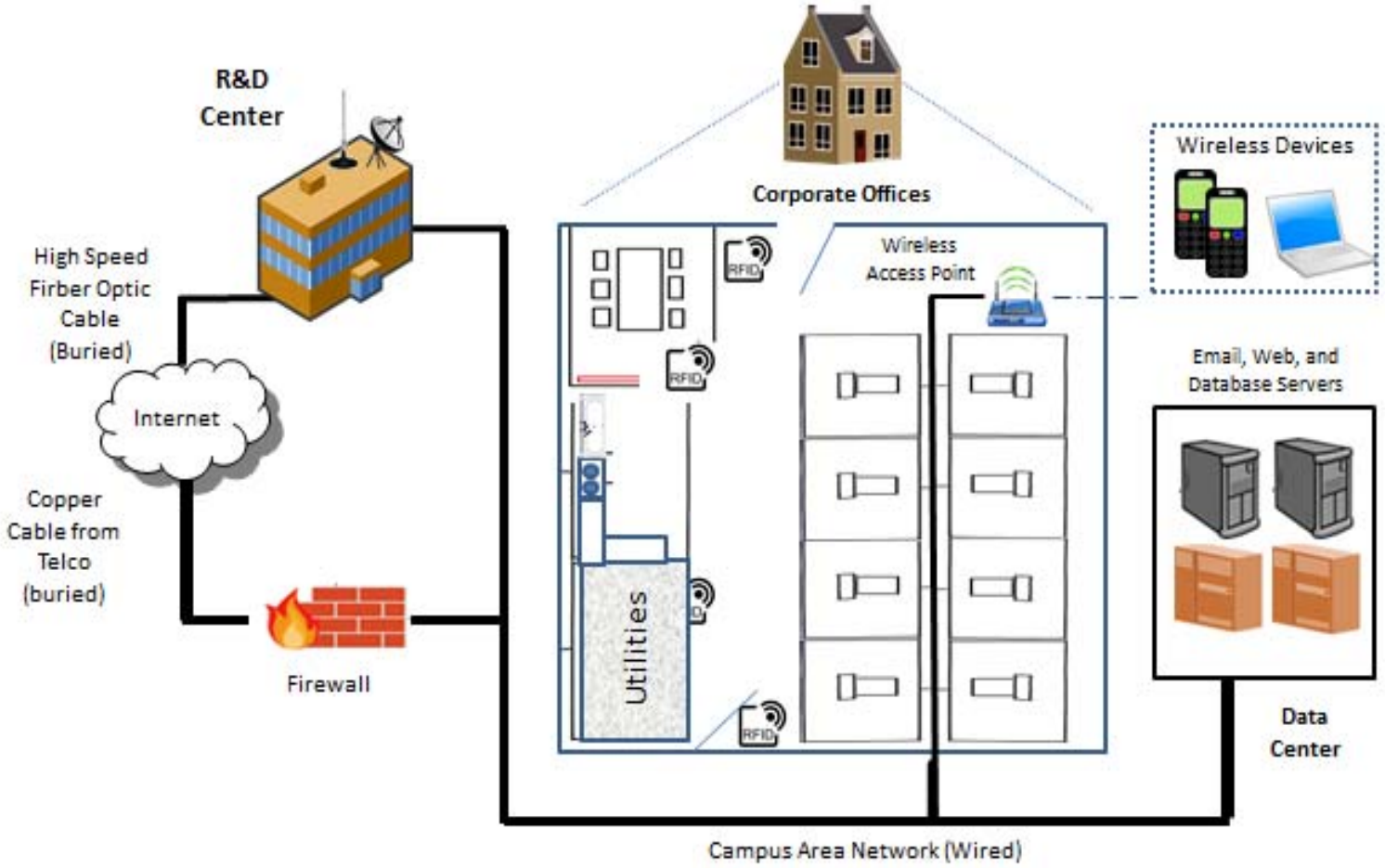



**Figure 2. Combined Networks and Systems Views:**
**Sifers-Grayson Headquarters, R&D Center, and Data Center**

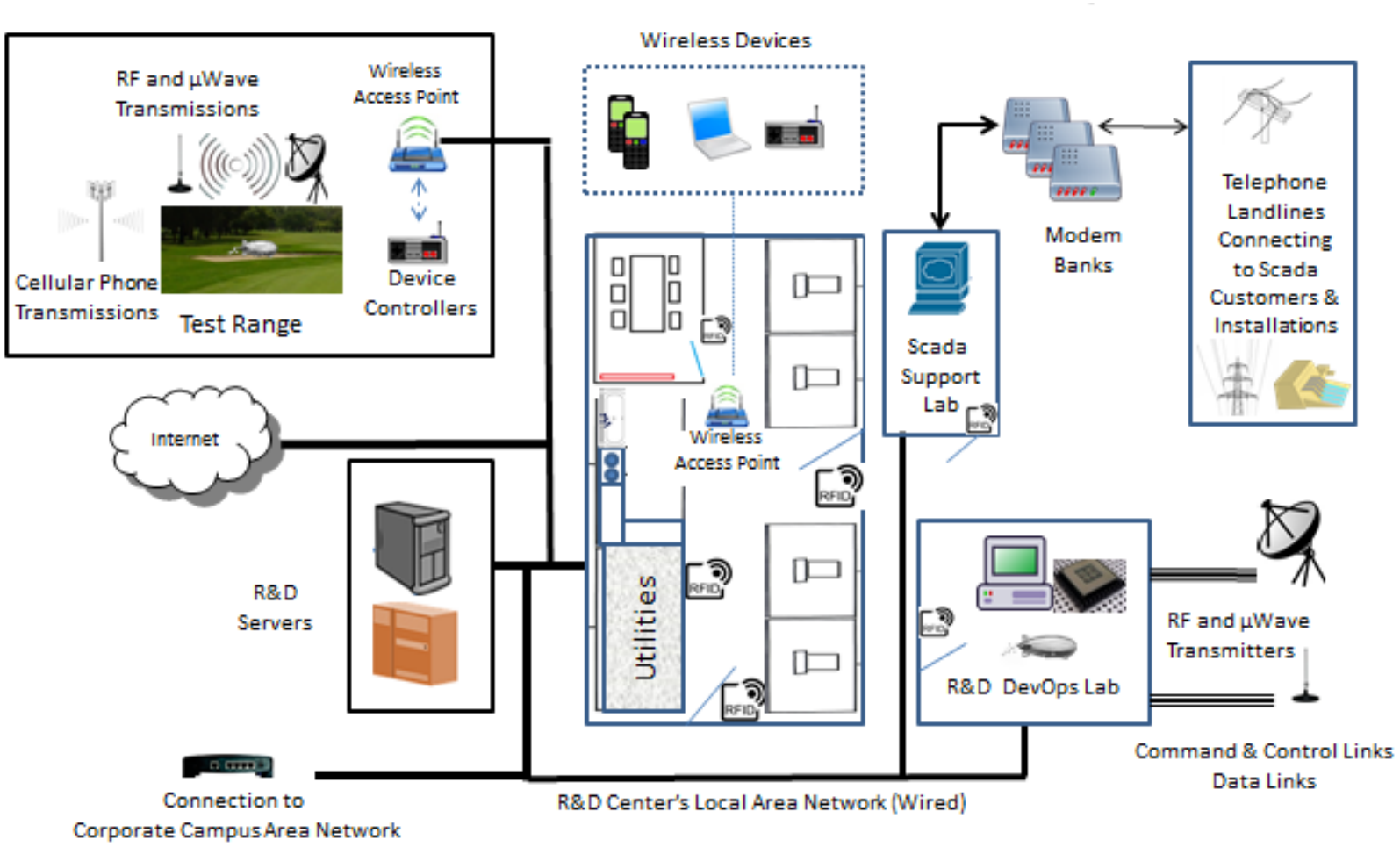



**Figure 3. Combined Networks and Systems Views:**
**Sifers-Grayson Engineering Center**

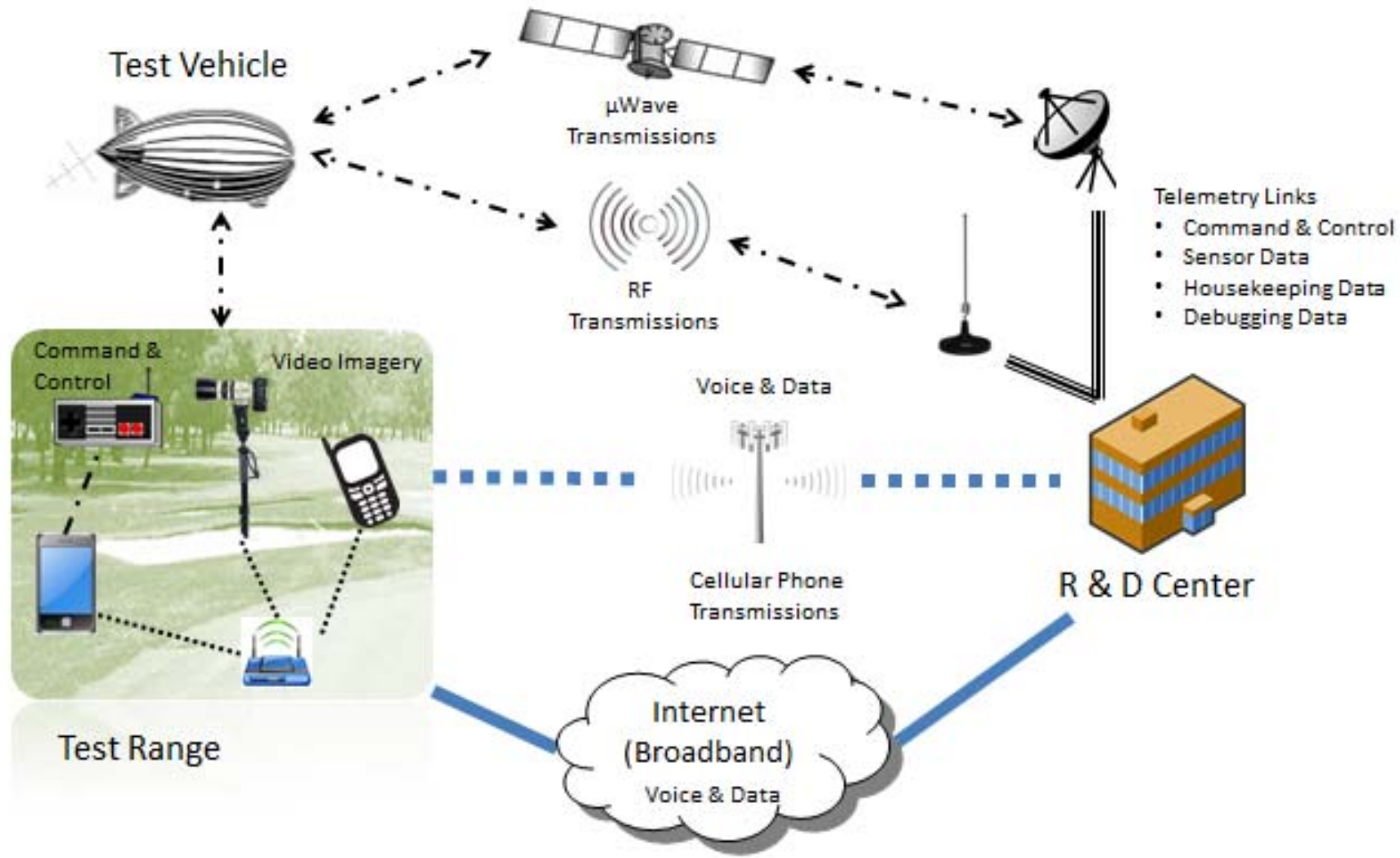



**Figure 4. Combined Communications, Networks and Systems Views: Sifers-Grayson Test Range and R&D Center**

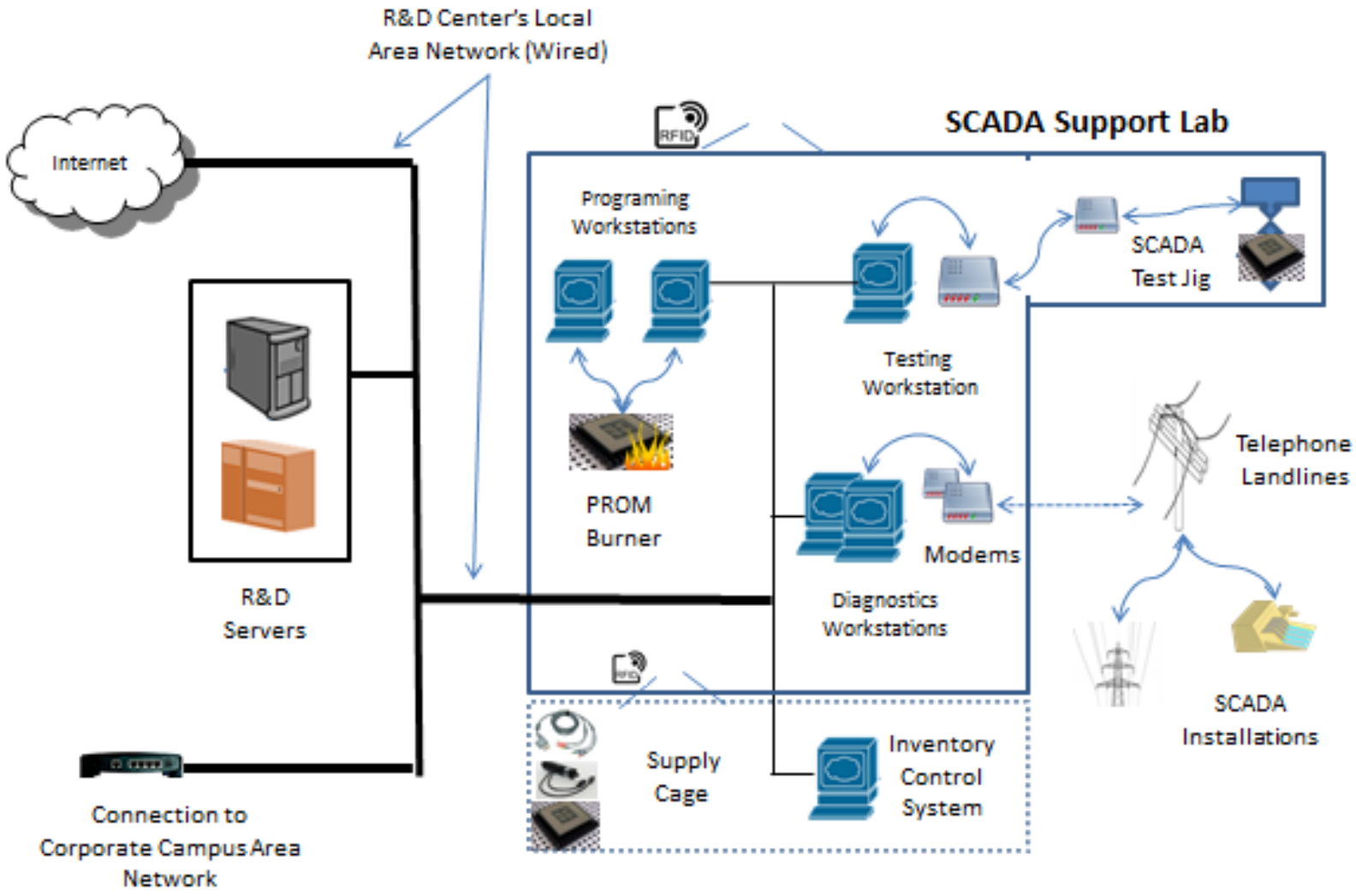



**Figure 5. Combined Networks and Systems Views:**
**Sifers-Grayson SCADA Support Lab**

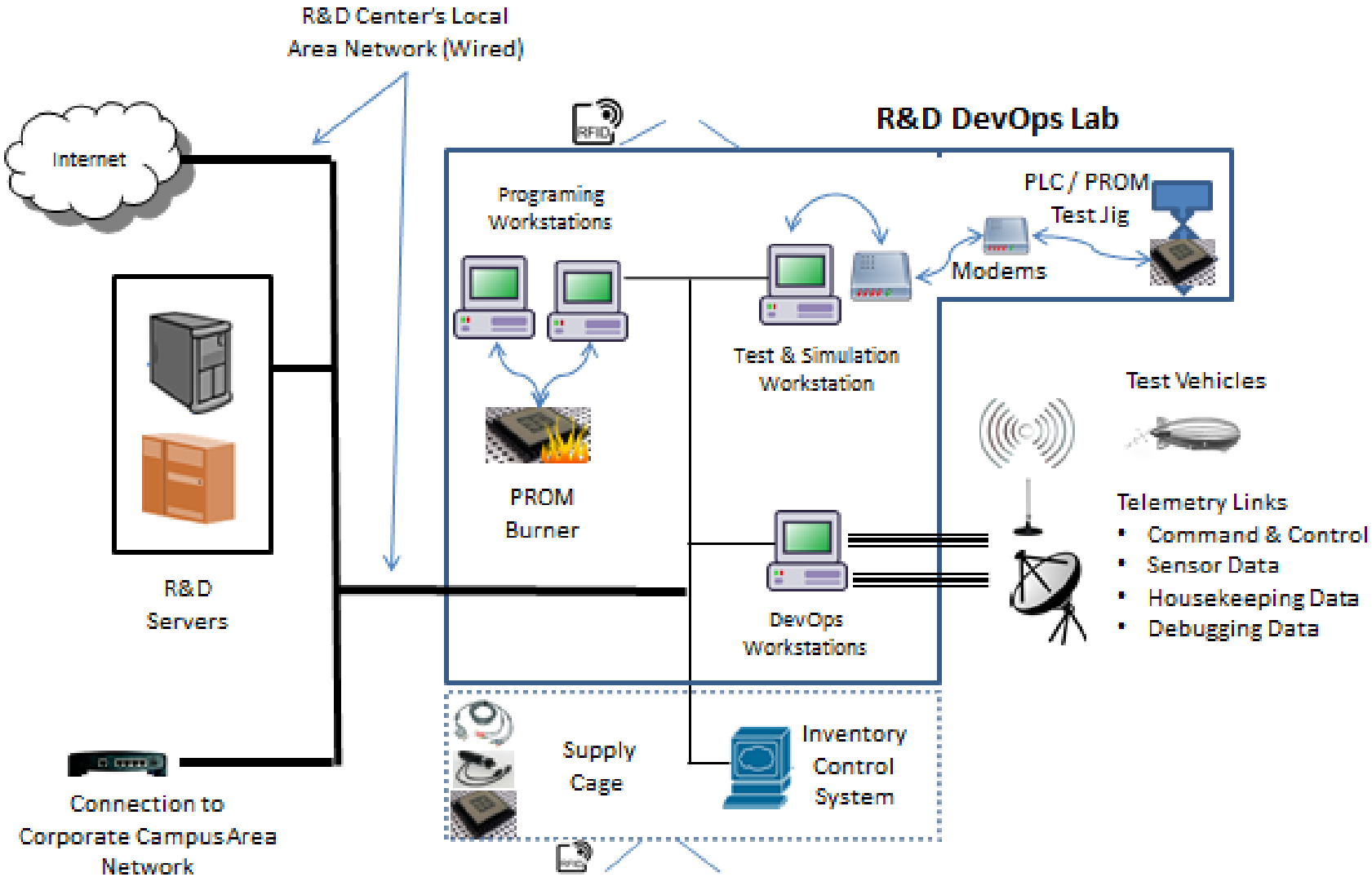


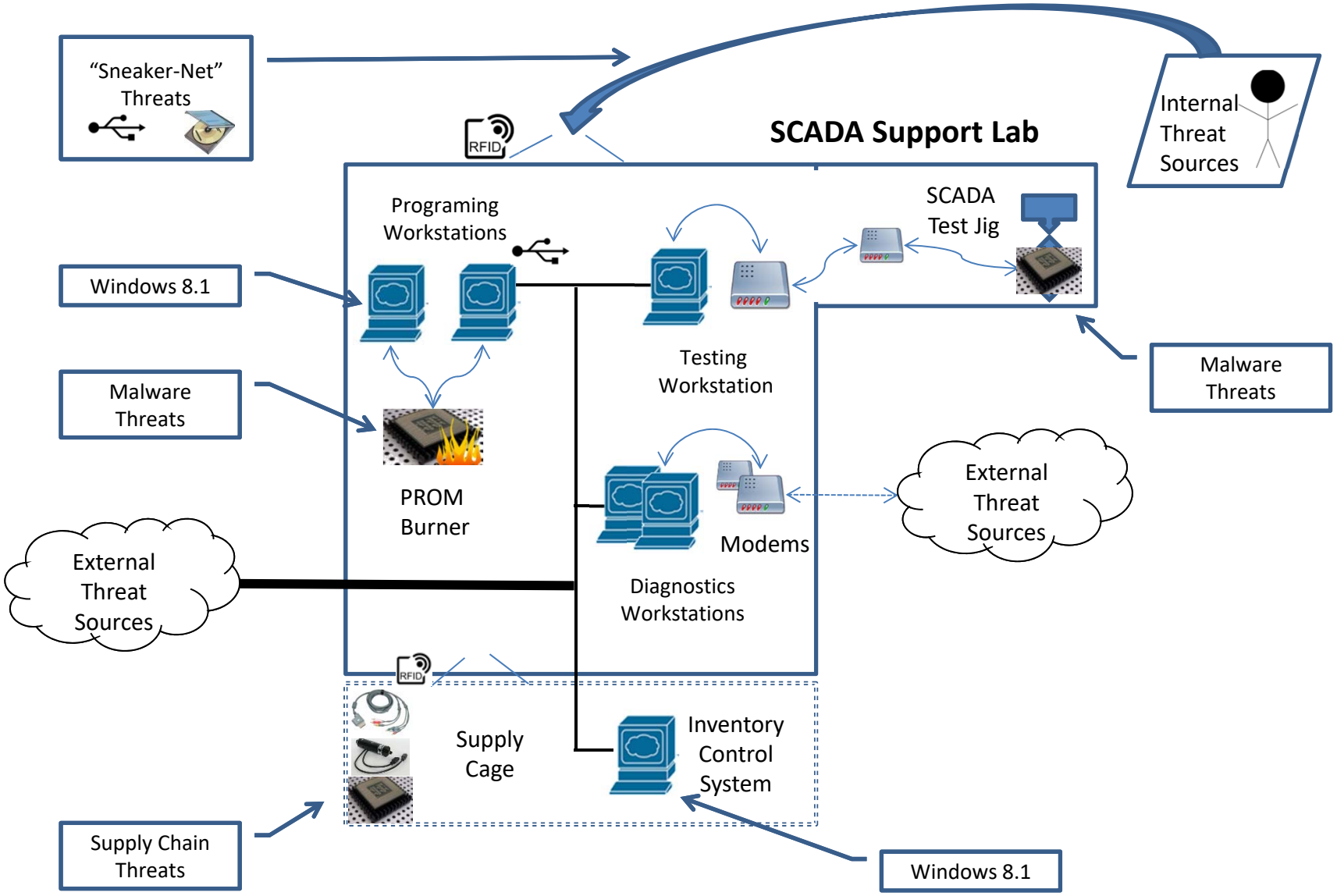

**Figure 6. Combined Networks and Systems View: Sifers-Grayson R&D DevOps Lab**

*Pervasive Cybersecurity is our passion …*

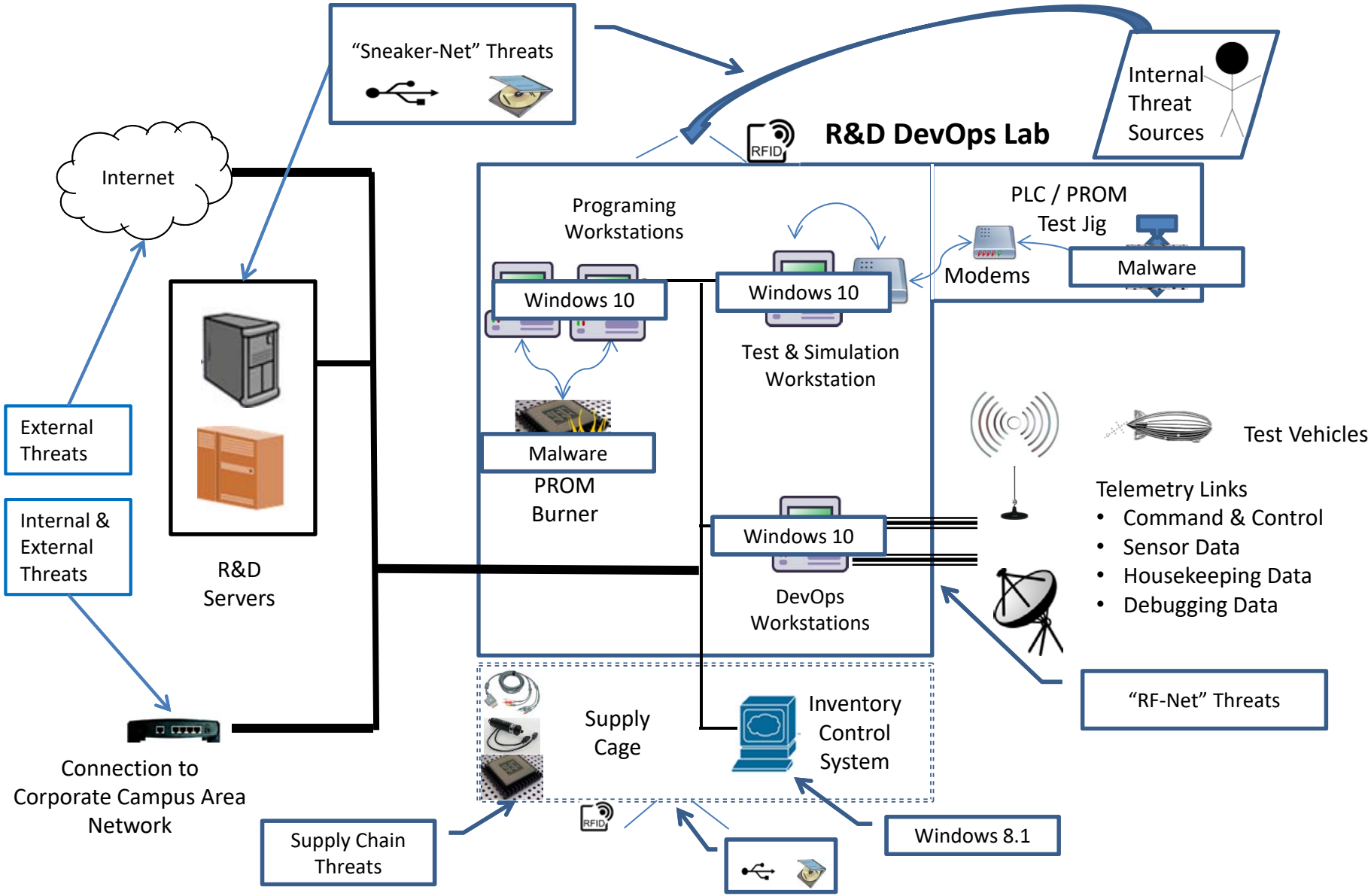
# Threat Landscape

## Sifers-Grayson
## Security Posture Assessment

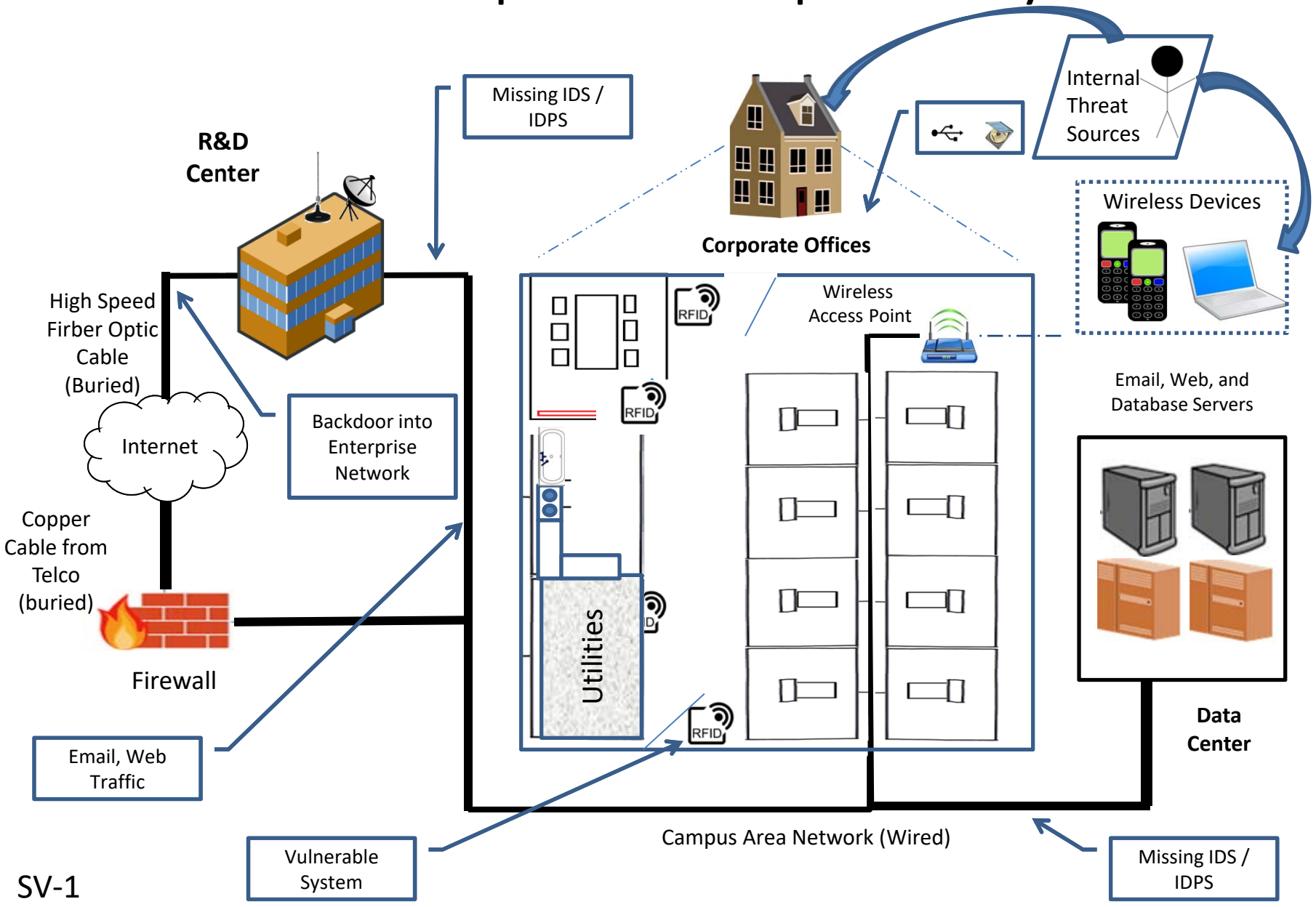
# Threat Landscape for Sifers-Grayson SCADA Lab



# Threat Landscape for Sifers-Grayson R&D DevOps Lab



# Threat Landscape for Enterprise IT Systems




SV-1

*Pervasive Cybersecurity is our passion …*

# "Quick Look" Recommendations & Next Steps

Sifers-Grayson

Security Posture Assessment

PRELIMINARY – NOT FOR DISTRIBUTION

# Issues Summary

1. Newly won government contracts now require compliance with DFARS §252.204-7008, 7009, and 7012
   - http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
   - http://www.acq.osd.mil/se/docs/DFARS-guide.pdf
2. Derivative requirements include:
   - Implementation of and compliance with NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
   - Compliance with DFARS 252.239-7009 *Representation of Use of Cloud Computing* and 7010 *Cloud Computing Services (see http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm)*

# Additional Derivative Requirements

- Use NIST Guidance Documents for
  - Incident Response, e.g. NIST SP-800-61 (*Computer Security Incident Handling Guide*)
  - SCADA Security, e.g. NIST SP 800-82 (*Guide to Industrial Control Systems Security*)
  - Software / Systems Development Lifecycle (SDLC) Security, e.g. NIST SP 800-64 (*Security Considerations in the System Development Life Cycle*)
  - Configuration Management, e.g. NIST sp 800-128 (*Guide for Security-Focused Configuration Management of Information Systems*)

# Recommendations

- Immediate (Phase I)
  - Remove direct network connection between Corporate Campus Area Network (CCAN) and R&D Center's LAN
  - Install a VPN solution to allow R&D Center to access CCAN and internal resources from the Internet
  - Install backup network connections from TELCO to CCAN and TELCO to R&D LAN
- Rationale
  - Segment network to reduce internal & external risks from CCAN to Test Range, SCADA Lab, and R&D DevOps Lab
  - Limit the "reach" of the customer's requirements (per DFARS & NIST guidance) to the smallest allowable footprint
  - Provide backup connectivity to WAN for business continuity

- Recommendations (Phase II)
  - Evaluate & Recommend Acquisitions for Security Solutions to strengthen the company's IT security posture
    1. End Point Protection Platforms
    2. Application Lifecycle Management
    3. Identity Governance & Administration
    4. Security Information & Event Management
  - Develop Incident Response Handbook & Guidance

- Recommendations (Phases III, IV, V, etc.)
  - Build security operations team led by dedicated CISO
  - Identify, evaluate and improve Internal Processes for IT security
  - Implement IT Security Governance & Enterprise Risk Management
  - Establish Security Operations Center
  - Upgrade security appliances to include advanced network monitoring and intrusion detection and prevention systems
  - Join information sharing and analysis center
  - … additional recommendations to be made after further investigation and assessment

*Pervasive Cybersecurity is our passion …*

# "After Action" Review: Sifers-Grayson

## Sifers-Grayson

## Security Posture Assessment

PRELIMINARY – NOT FOR DISTRIBUTION

# The customer's feedback

- Surprised at the extent of the problems
- Dismayed at the potential liabilities and contractual issues
- Concerned about the costs
- Determined not to let technology stand in the way of progress
- Agreed to implement Phase I and II recommendations

# Additional Negotiated Work

- NCS “Red Team” will conduct pentration test within next 60 days
- NCS will establish & train Sifers-Grayson Incident Response Team
- NCS will provide a contract CISO to Sifers-Grayson for 180 days (renewable on a yearly basis thereafter)
- NCS will provide additional staff & services at negotiated rates