Transforming the world of energy using open standards

Impact of End-to-End Security on Wide Area Communications for RAS

Ralph Mackiewicz
SISCO, Inc.
6605 19 1/2 Mile Road
Sterling Heights, MI 48314 USA
Tel: +1-586-254-0020 ext. 103
Mob: +1-586-260-2571
E-Mail: ralph@sisconet.com
URL: https://www.sisconet.com

i-PCGRID Workshop 2018
San Francisco, CA USA
28-31 March 2018

Why Implement Security?

"There is a great interest in and capability demonstrated for messing around with the engineering that is the foundation supporting modern economic life, national security and the well being of society."

-- Vytautas Butrimas, NATO Energy Security Center of Excellence

Realistic Threats

- Ongoing evidence of Advanced Persistent Threats (APT) probing and, in some cases, attacking electric infrastructure
  - Capabilities of the attacker can exceed the sophistication of the defender
  - Systems can be infected for a long time without awareness (you don't know what you don't know)
  - PACS are not immune (at least, it is not safe to assume they are immune)
- Can Shodan and Metasploit be integrated?
  - Shodan is an Internet search engine that finds connected control systems by protocol
  - Metasploit is a tool that executes and exploits known vulnerabilities
- Finding vulnerabilities in PACS is not trivial
  - Port and vulnerability scanning can impair the function of PACS
  - Test systems don't behave the same as operational systems
  - There is no magic black box available

Device Protocol Security

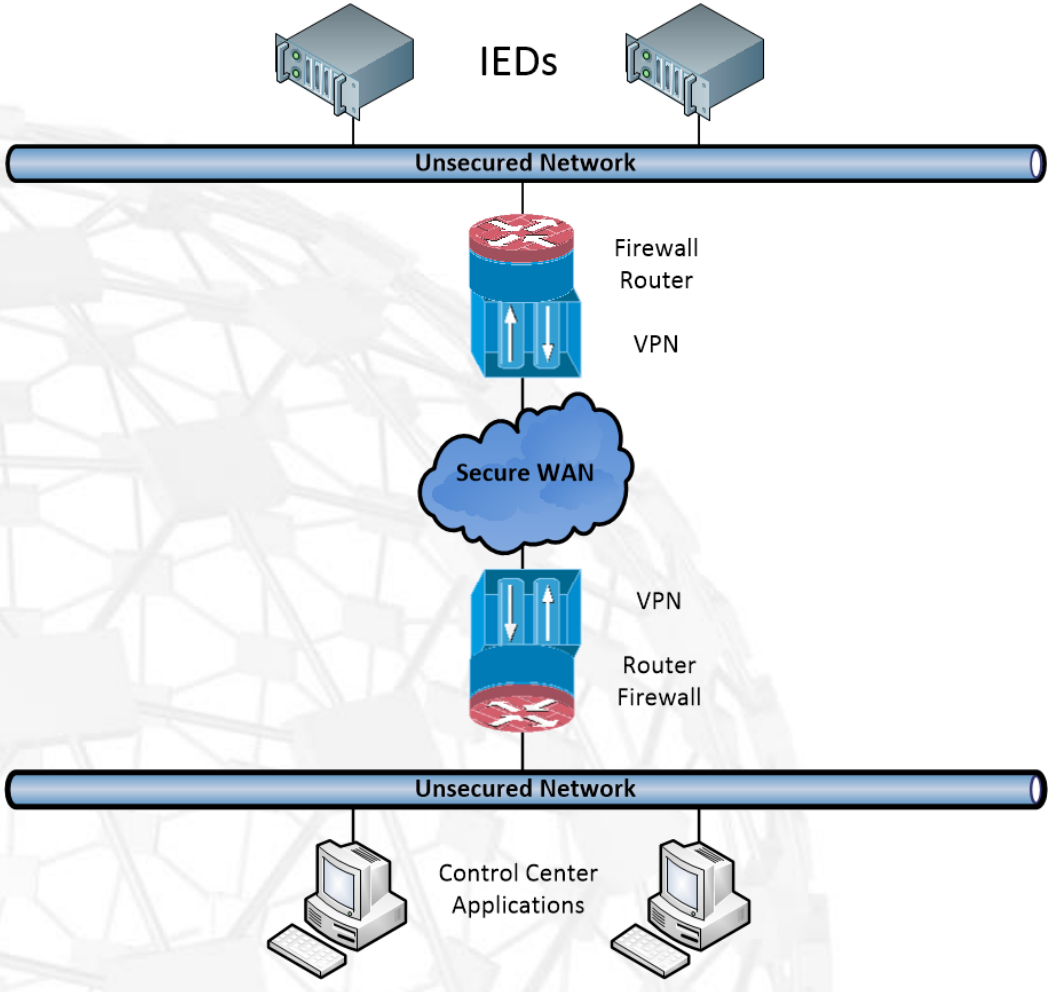
- Protocol security is the point of the spear for securing PACS end points (devices)

- Protocol Security functions provide:
  - Confidentiality – Snooping on the wire does not reveal the data
  - Anti-Spoofing – The identity of communicating entities cannot be faked
  - Anti-Playback – Captured packets cannot be played back into a system
  - Non-repudiation – Proof of the integrity and origin of data

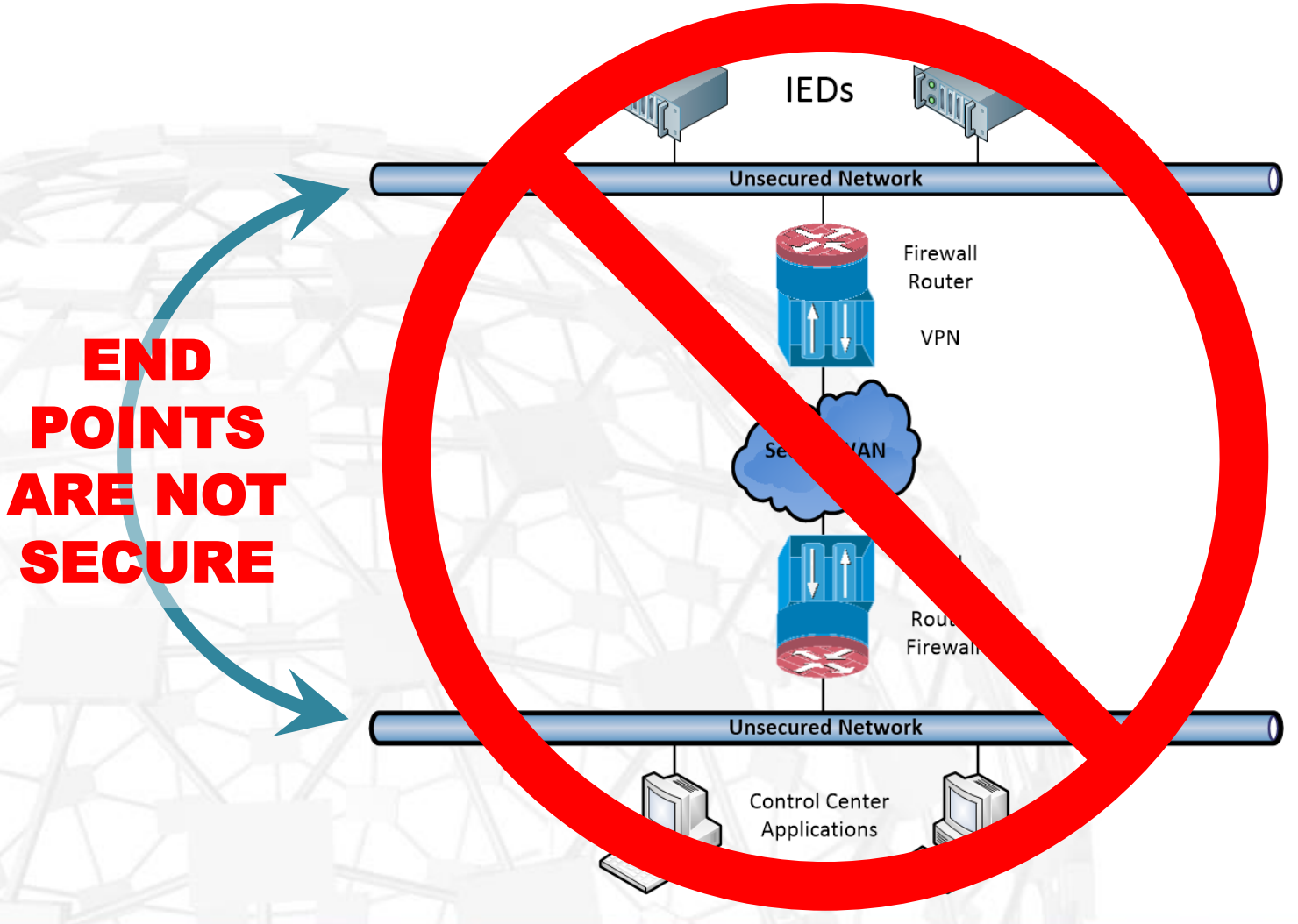
What is End-to-End (E2E) Security?

- Protocol security across ALL networks involved in communications from one application entity to another
- The only access point for data is the device itself
- For instance, to implement secure Role Based Access Control (RBAC) to device functions requires security be integrated into the device that provides such access or control functions

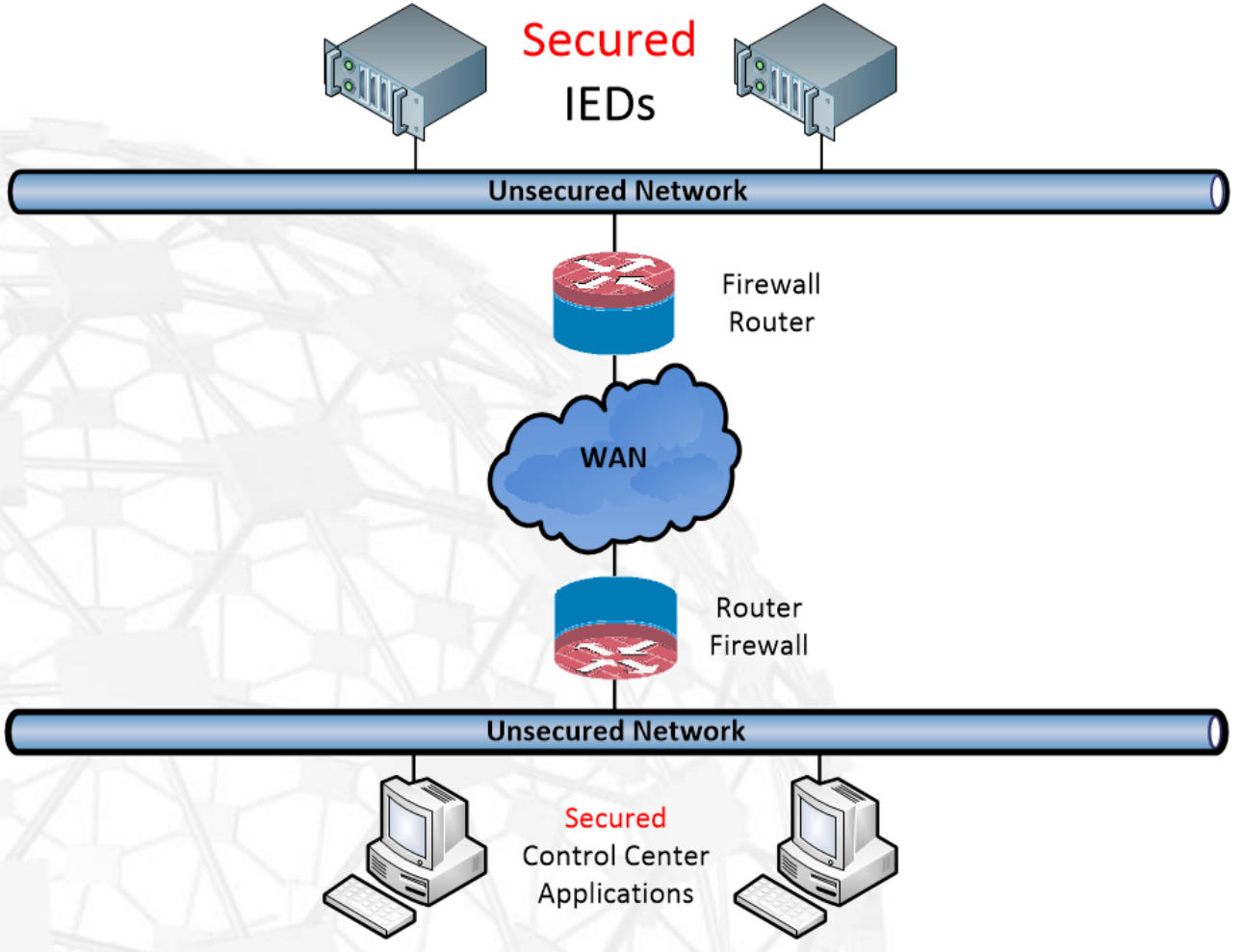
E2E Security Using Traditional Network Architecture?



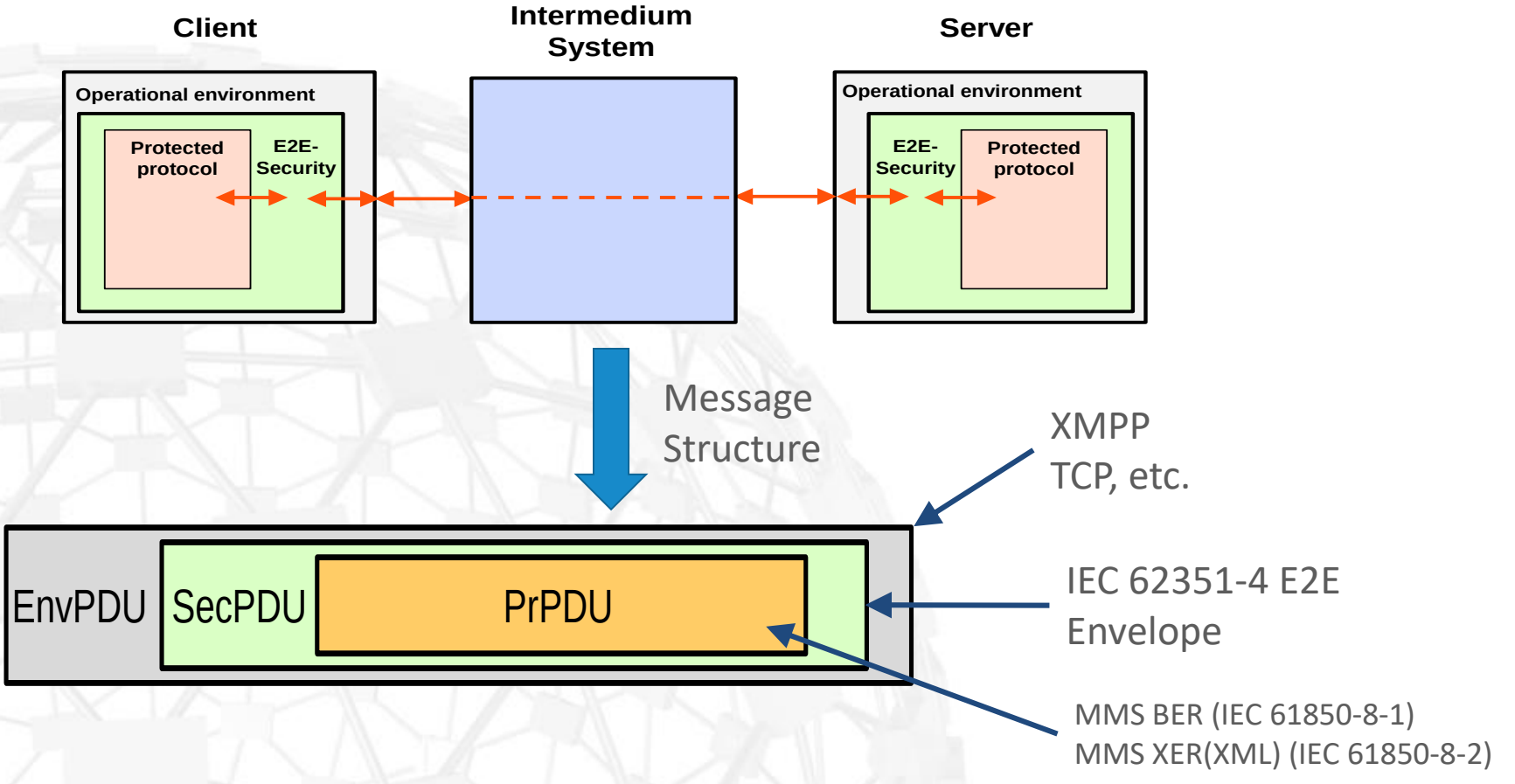
E2E Security Using Traditional Network Architecture?



E2E Security Network Architecture

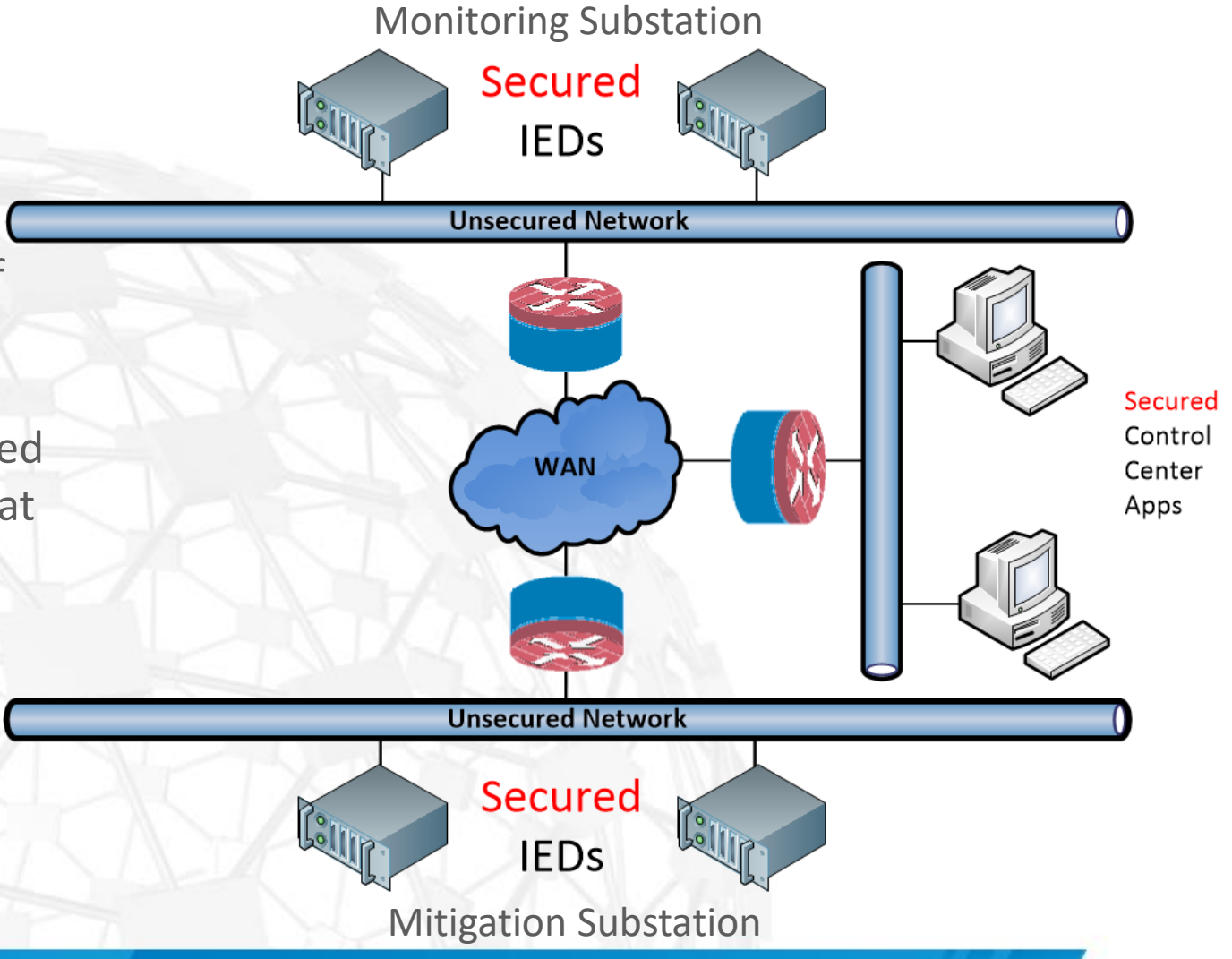


New E2E Security for Devices (IEC 62351-4)



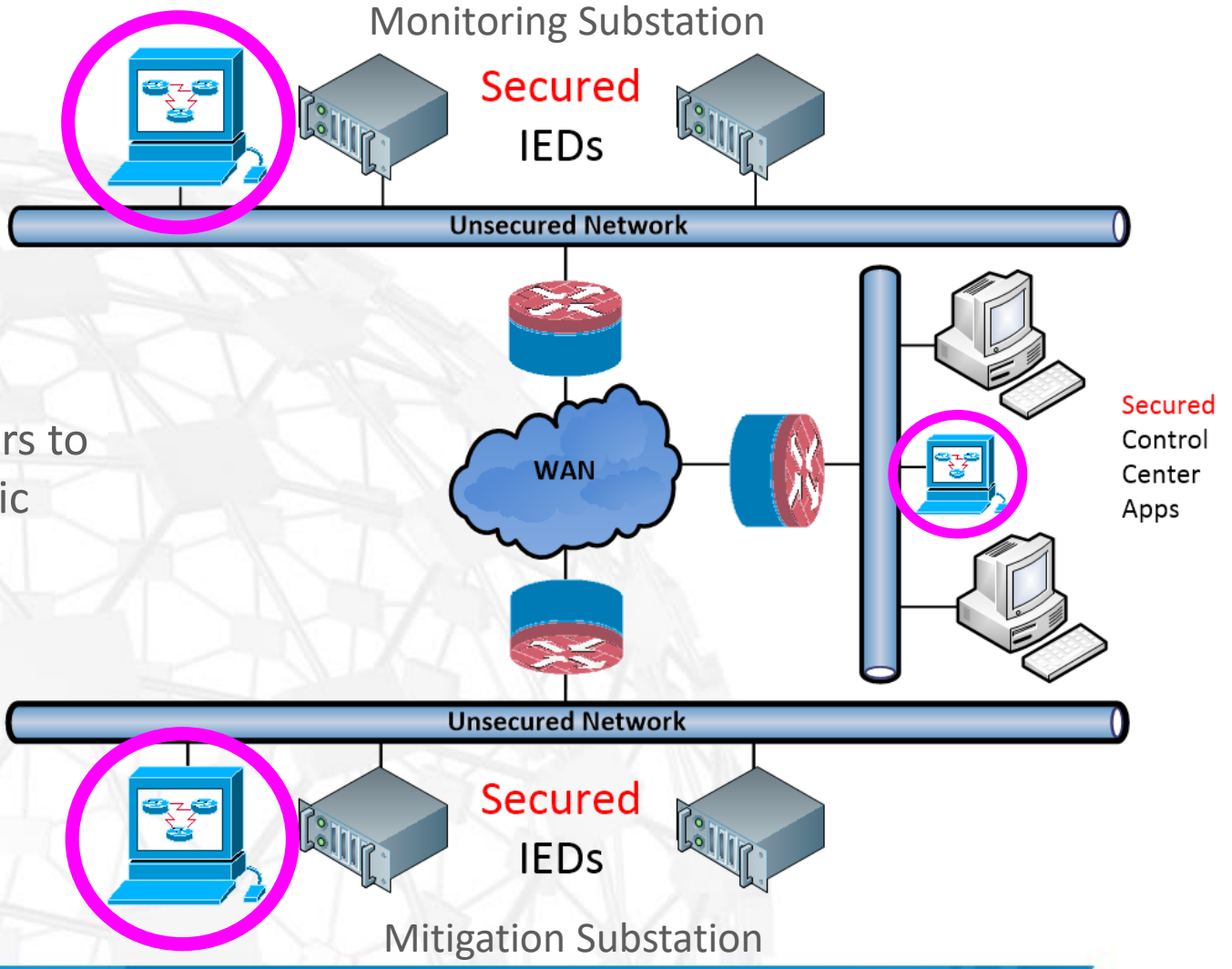
Impact on Wide Area RAS

What do we do if there is a communications issue and you need to determine what the IEDs are receiving and sending?



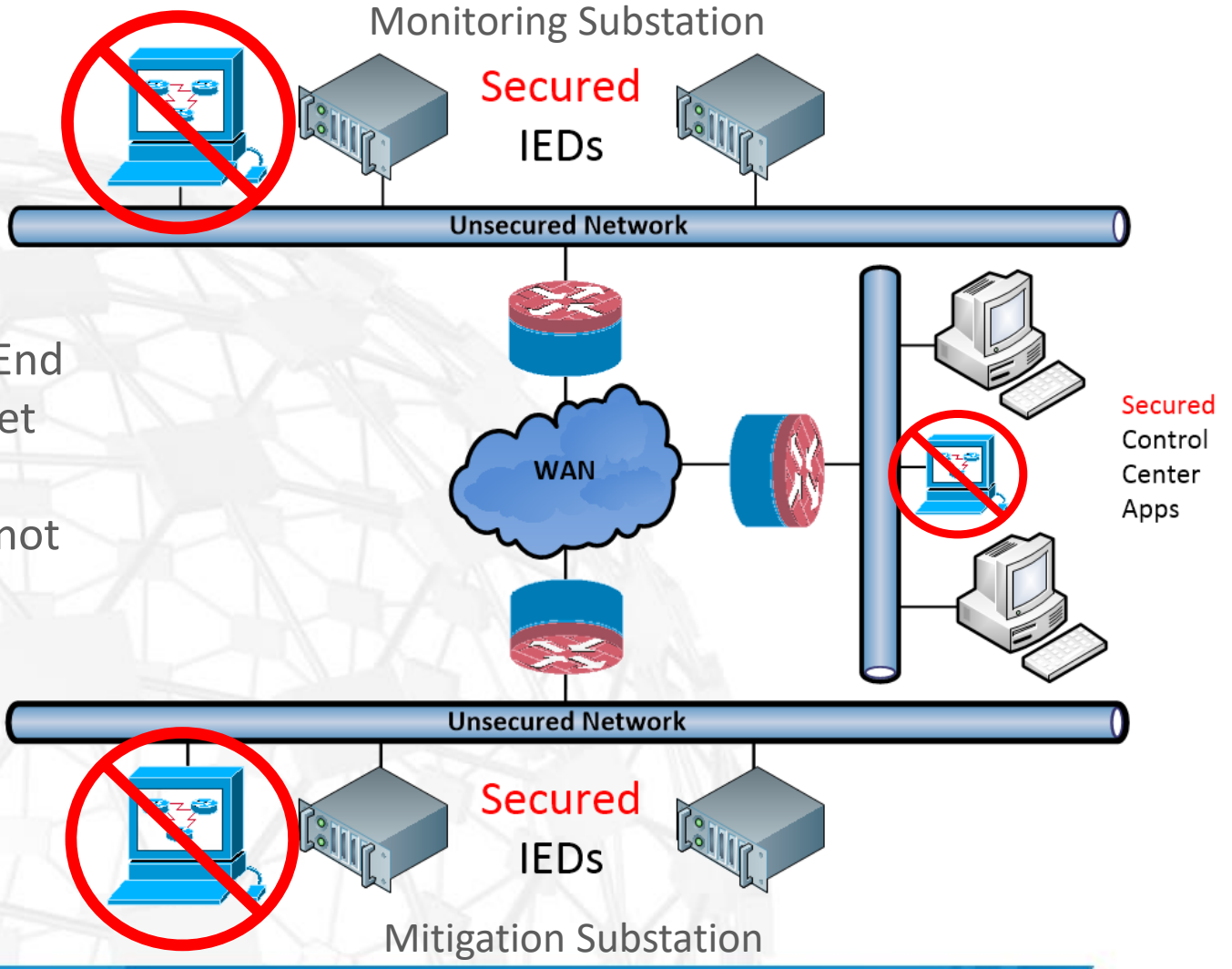
Impact on Wide Area RAS

Add Network Sniffers/Monitors to look at the traffic



Impact on Wide Area RAS

With End-to-End Security packet sniffers and inspection is not functional!



Debugging with E2E Security

- IEC TC 57 WG 15 (IEC 62351 standard committee for communications security) have been developing processes by which private keys needed for decryption could be shared with network equipment for:
  - Monitoring (For debug and testing)
  - Packet Inspection (Firewall processing)
- Initial approach was rejected by the IETF!
- Applications must be enhanced to generate internal logs of data and actions when needed for debug

It is Not Easy Being Secure

- Should security be implemented with the same priority as electrical system protection is implemented?
- If a secured system is harder to maintain than one that is not, should security be implemented?
- Should the failure of a security attribute be treated the same as the failure of comms or a device?

Is E2E Security Needed?

"There is a great interest in and capability demonstrated for messing around with the engineering that is the foundation supporting modern economic life, national security and the well being of society."

-- Vytautas Butrimas, NATO Energy Security Center of Excellence

Authors Note: Consider that the cost to wreak havoc is much lower than the value delivered by an operational system.

Transforming the world of energy using open standards

Thank You

Ralph Mackiewicz
SISCO, Inc.
6605 19 1/2 Mile Road
Sterling Heights, MI 48314 USA
Tel: +1-586-254-0020 ext. 103
Mob: +1-586-260-2571
E-Mail: ralph@sisconet.com
URL: https://www.sisconet.com