Industrial Control System (ICS) Security Using TNC Technology

September 18, 2014, 1:00PM EDT

Webcast Logistics

No Sound?

This is a streaming audio event. Make sure the sound on your PC is turned on.

Questions?

Type your questions using the Ask a Question Text Box

Today's Presenters

David Mattes, Founder and CTO, Asguard Networks

Mattes has developed network security appliances that help companies connect their industrial assets in a way that is highly secure, cost-effective and easy-to-use. He is the founder and lead developer for ompad, an open source IF-MAP server. Prior to Asguard Networks, Mattes was with The Boeing Company where he developed architecture and implementations for managing legacy connectivity for industrial control systems, embedded wireless controllers for hydraulic testing, a secure mobile factory workstation, and other applications.

Steve Venema, PhD, Associate Technical Fellow, Boeing

Venema has worked on large-scale ICS and SCADA networking and security challenges in Boeing's manufacturing facilities over the past 10 years. He is the primary architect of the internally developed solutions which align with the new specifications discussed in this webinar, and which are used across hundreds of manufacturing systems in Boeing today. He is also a co-author for related standards activities including the TCG ("Metadata for ICS Security") and ISA (TR100.15.01 "Backhaul Architecture Model: Secure Connectivity Over Untrusted or Trusted Networks").

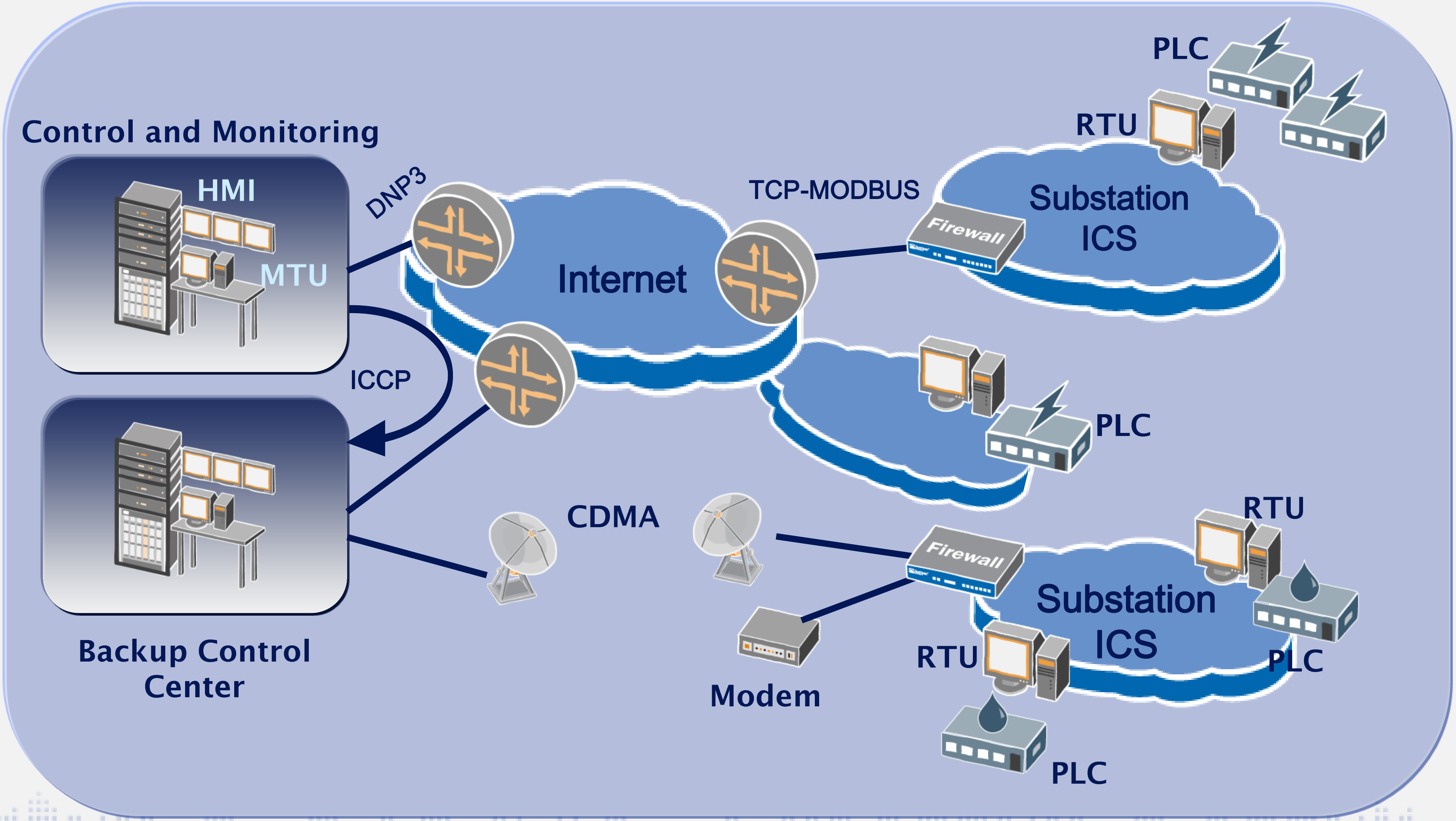
Eric Byres, CTO and Vice President Engineering, Tofino Security

Byres is recognized as one of the world's leading experts in the field of SCADA security, and with a background as a process controls engineer, he has a unique combination of deep technical knowledge plus practical field experience. He has written extensively on Stuxnet, leads various industry standards groups and has consulted with governments and enterprises.

Lisa Lorenzin, Principal Solution Architect, Juniper Networks

Lorenzin specializes in security and mobility solutions and has worked in a variety of Internet-related roles since 1994, with more than a decade of that focused on network and information security. She is currently concentrating on enterprise security - including network segmentation, end-to-end identity-based access control, and integration of mobile security.

Industrial Control Systems Network



Infrastructure Challenges

Designed for safety, not security

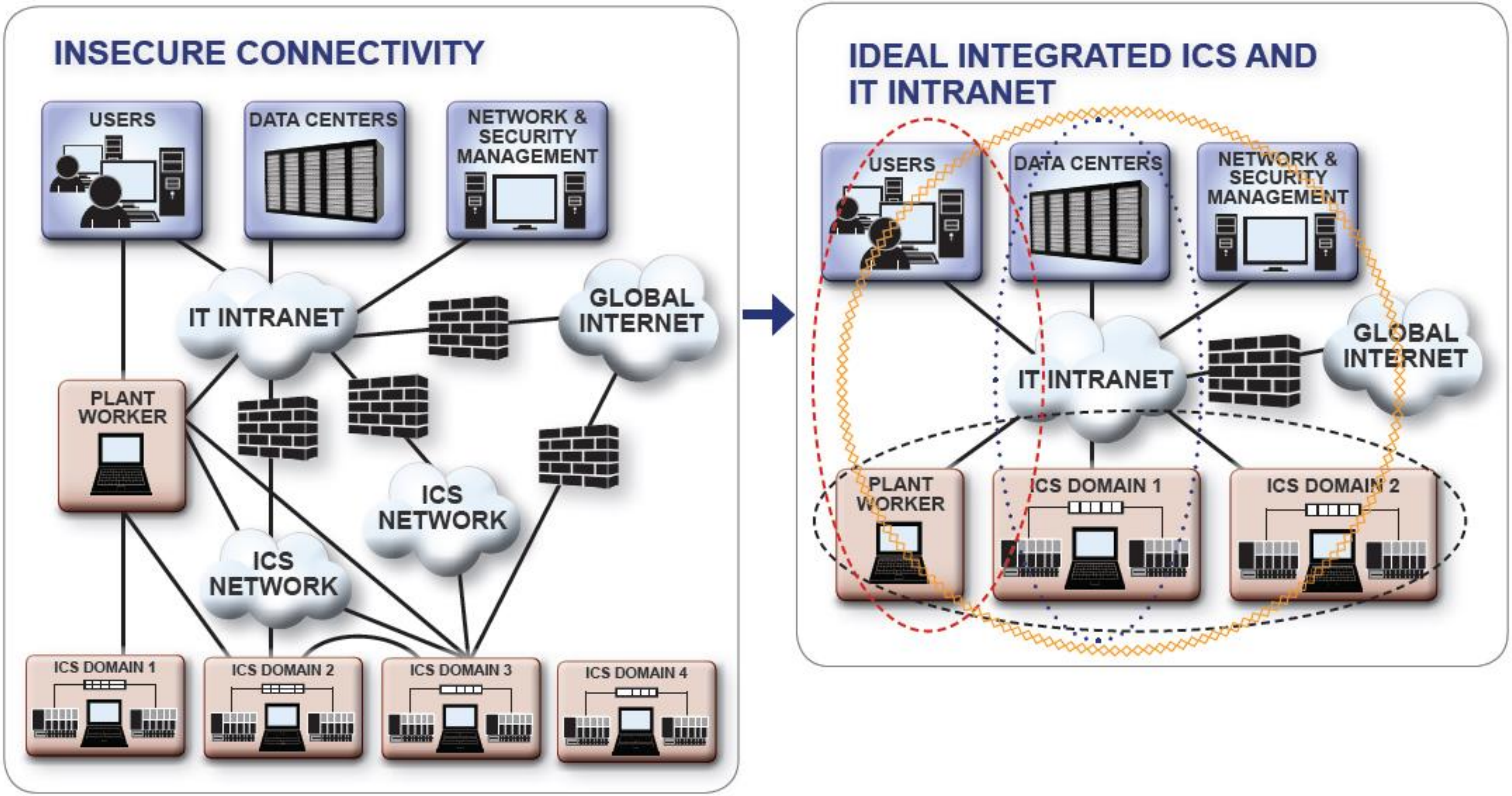
Standard applications, OSes seldom patched

Susceptible to a variety of attacks

Lack forensic capabilities

Logging for operations, not communication

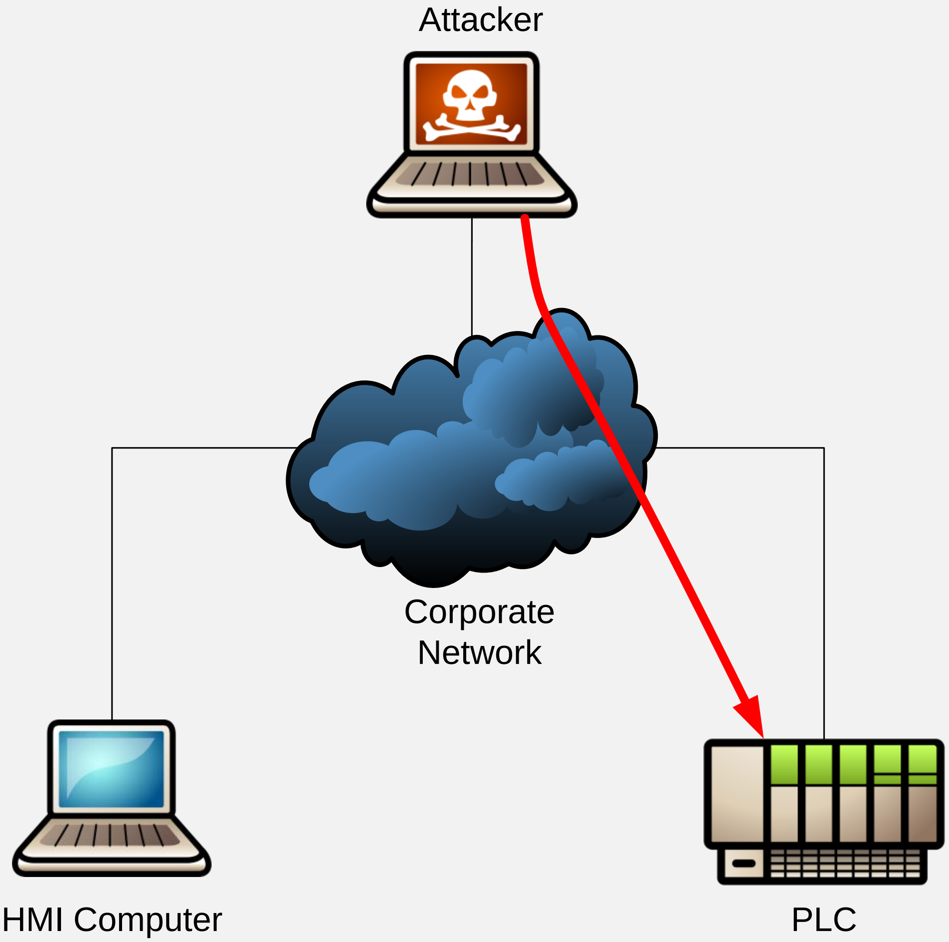
Goal: Integrated ICS & IT Intranet



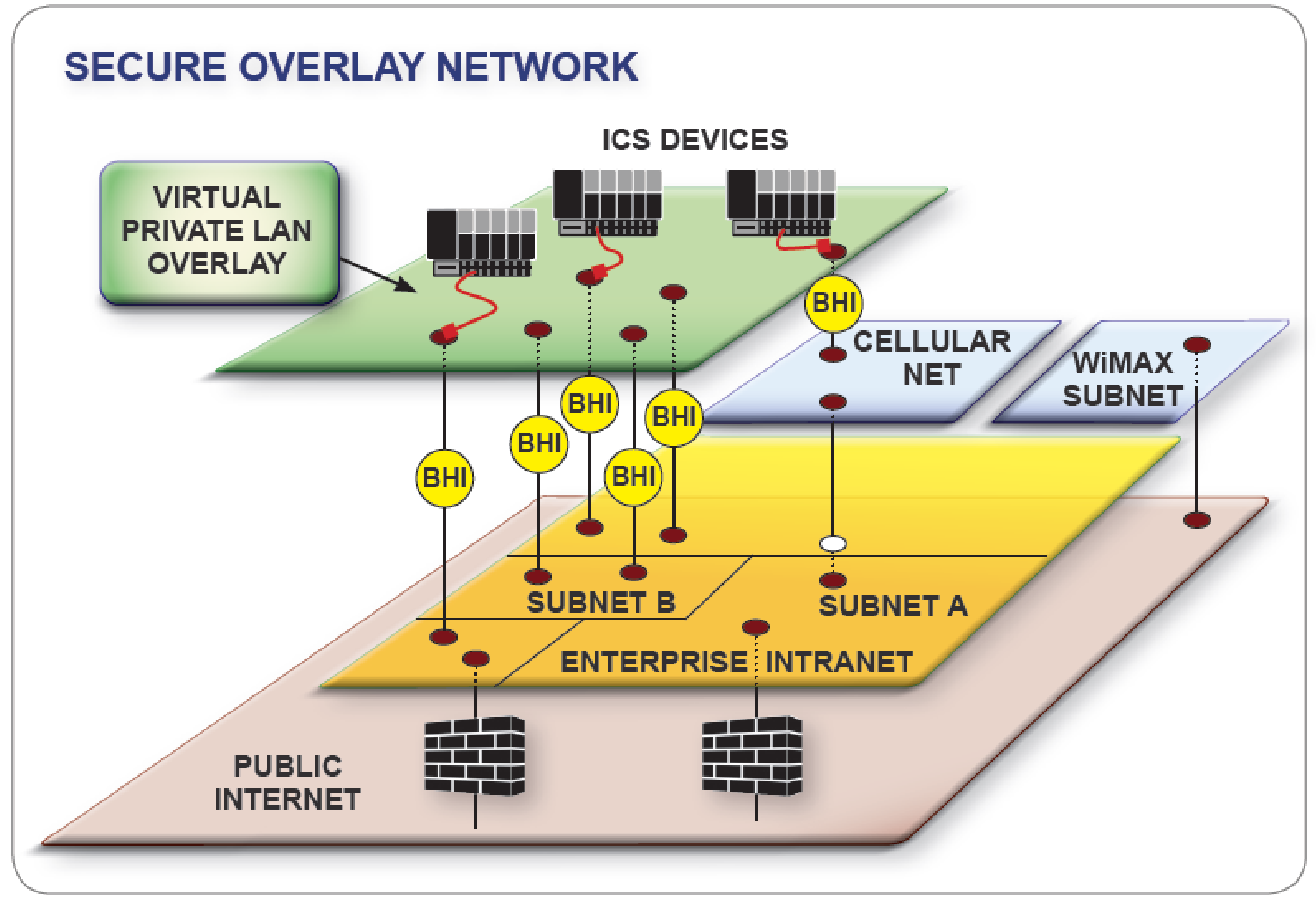
Integration Drivers

- Geographically dispersed systems
- Responsiveness
- Business agility
- Cost savings
- Compliance
- Security
- Safety

Security Challenges



Solution: Secure Overlay Network



Overlay Challenges

Dynamic environment

Visibility

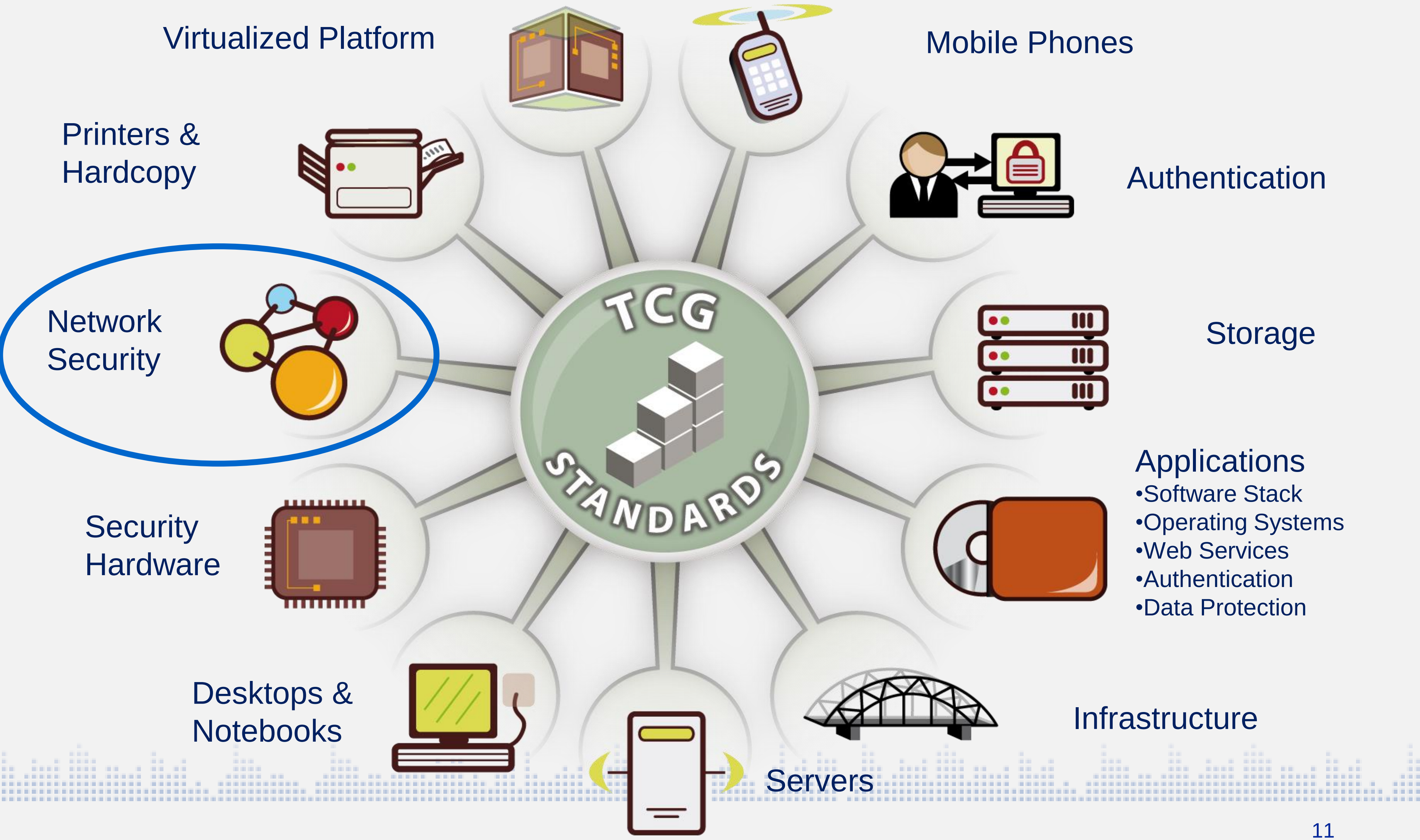
Certificate provisioning

Multiple administrators

Access control policies

For a customer POC, you will receive a license valid for 30 days.
For internal Juniper use, you will receive a license valid for 90 days.

TCG: Standards for Trusted Systems



Virtualized Platform

Mobile Phones

Printers & Hardcopy

Authentication

Network Security

Storage

Applications
- Software Stack
- Operating Systems
- Web Services
- Authentication
- Data Protection

Security Hardware

Desktops & Notebooks

Infrastructure

Servers

Trusted Network Connect

- **Open Architecture for Network Security**
  - Completely vendor-neutral
  - Strong security through trusted computing
  - Original focus on NAC, now expanded to Network Security
- **Open Standards for Network Security**
  - Full set of specifications available to all
  - Products shipping since 2005
- **New Standard for Industrial Control Systems**
  - Aligns with ISA100.15 Backhaul Network Architecture
  - Aligns with IETF standards for PKI and identity-based comms

Problems Solved by TNC

- **Network and Endpoint Visibility**
  - Who and what's on my network?

Compliance Service

- **Endpoint Compliance**
  - Are devices on my network secure?
  - Is user/device behavior appropriate?

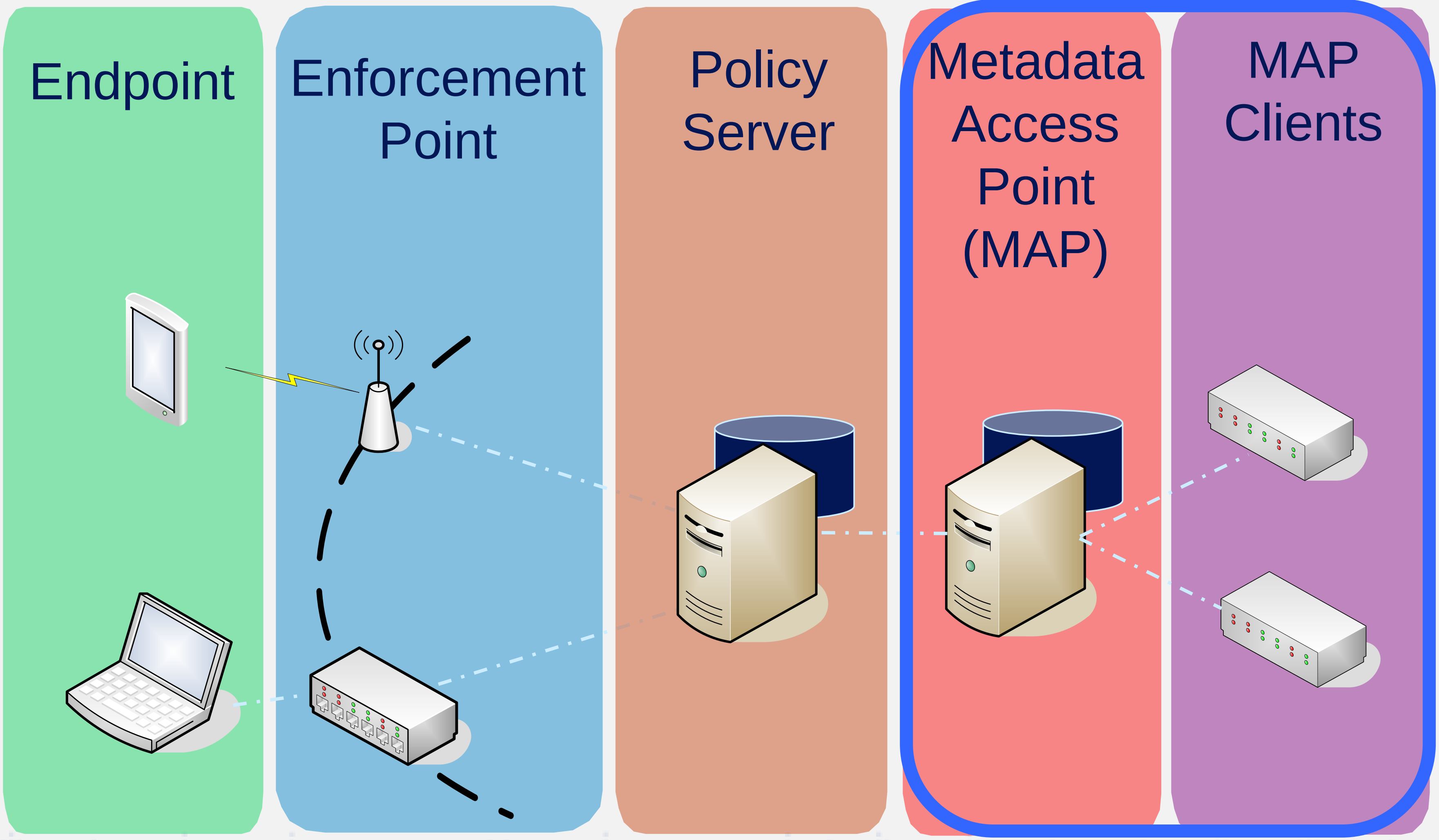
Access Control Service

- **Network Enforcement**
  - Block unauthorized users, devices, or behavior
  - Grant appropriate levels of access to authorized users/devices

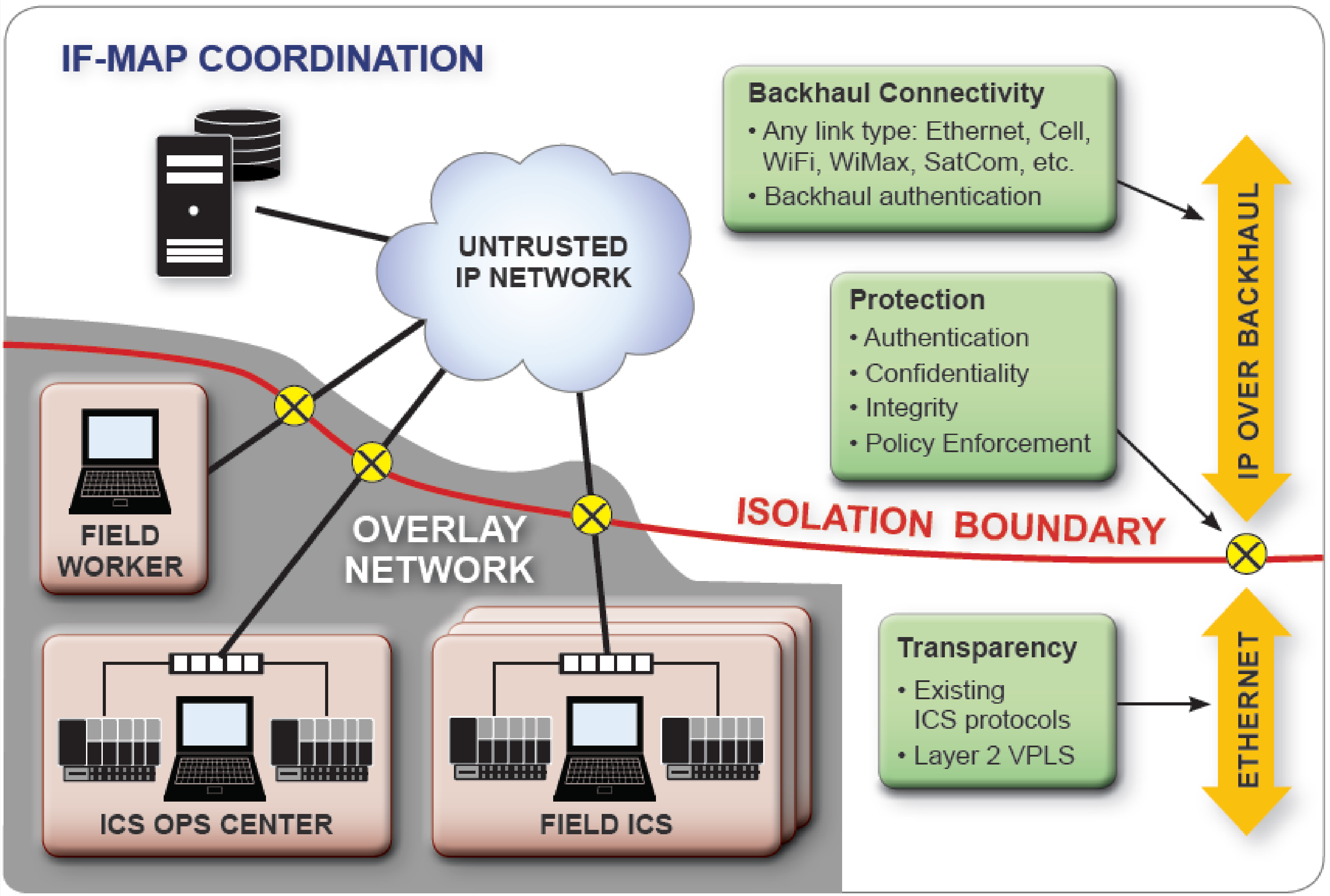
- **Security System Integration**
  - Share real-time information about users, devices, threats, etc.

Orchestration Service

TNC Architecture



Dynamic Connectivity and Trust Management



IF-MAP COORDINATION

UNTRUSTED IP NETWORK

FIELD WORKER

OVERLAY NETWORK

ICS OPS CENTER

FIELD ICS

ISOLATION BOUNDARY

Backhaul Connectivity

- Any link type: Ethernet, Cell, WiFi, WiMax, SatCom, etc.
- Backhaul authentication

Protection

- Authentication
- Confidentiality
- Integrity
- Policy Enforcement

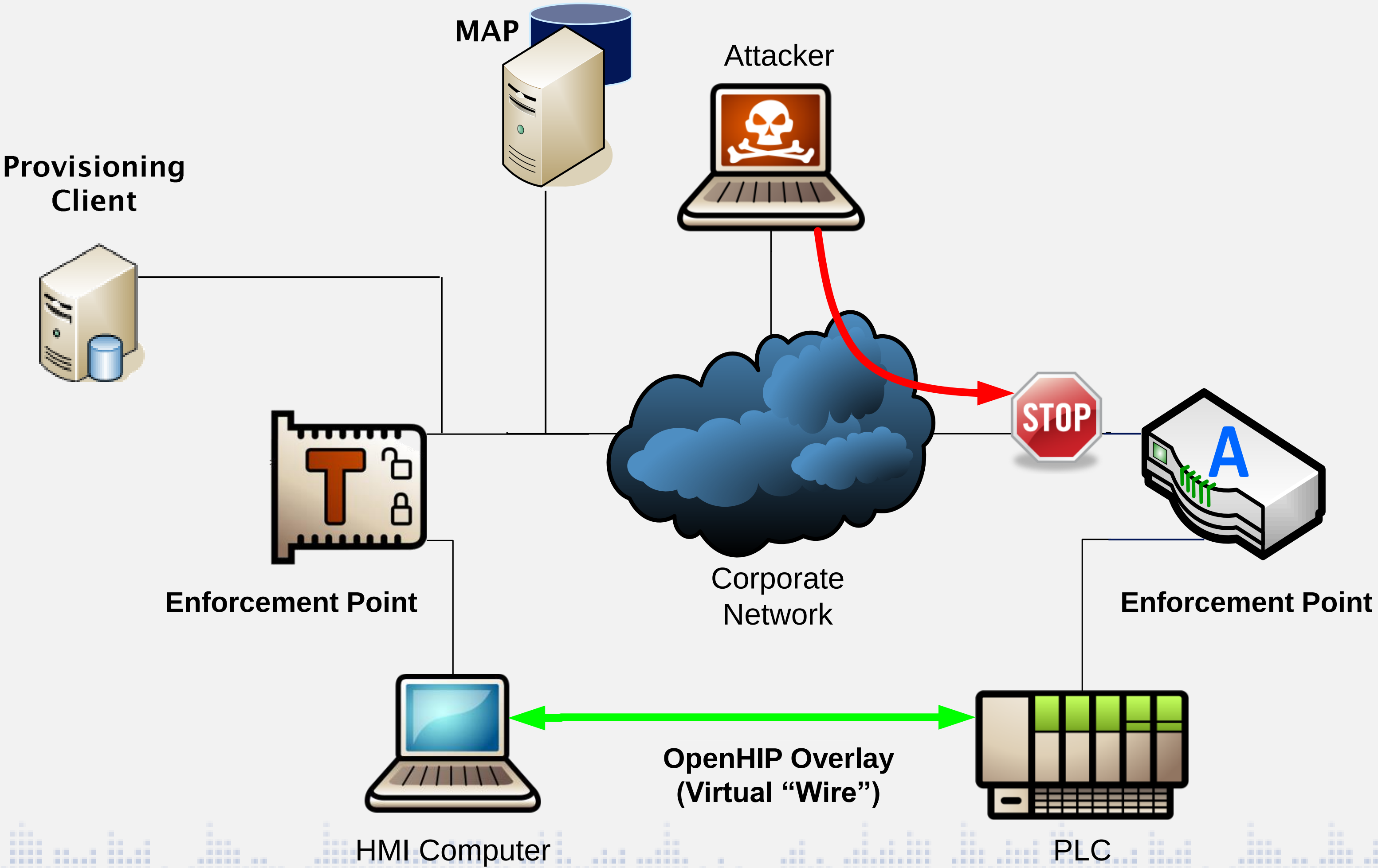
Transparency

- Existing ICS protocols
- Layer 2 VPLS

IP OVER BACKHAUL

ETHERNET

Solution – Intelligent Isolation



Next Steps and Call to Action

- Read the ICS Security Using TNC Technology Architects Guide: http://bit.ly/HQsqaT
- Design ICS security solutions customized for your unique environments.
- Contact vendors and insist on acquiring TCG-certified ICS security solutions based on the TNC and ISA standards.
- Deploy solutions in pilot first, observe and correct issues, then deploy into production.
- For more information on TCG technologies and architects guides, visit www.trustedcomputinggroup.org

Questions?

Post your question now.

David Mattes
Asguard Networks

Steve Venema
Boeing

Eric Byres
Tofino Security

Additional Resources

Specifications:

- TNC IF-MAP Metadata for ICS Security, Version 1.0: http://www.trustedcomputinggroup.org/files/static_page_files/8073E5D9-1A4B-B294-D0CD4D06B6C53D1D/IFMAP_Metadata_For_ICS_Security_v1_0r45.pdf
- TNC IF-MAP Binding for SOAP, Version 2.2

  http://www.trustedcomputinggroup.org/files/static_page_files/FF3CB868-1A4B-B294-D093D8383D733B8A/TNC_IFMAP_v2_2r9.pdf

Architect's Guide:

- ICS Security Using TNC Technology:

  http://www.trustedcomputinggroup.org/files/resource_files/2F5D1C84-1A4B-B294-D025ED10D0826F2F/ICS%20Security%20Using%20TNC%20Technology%20Architects%20Guide.pdf

Resource Documents:

- TNC IF-MAP Metadata for ICS Security Frequently Asked Questions:

  http://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_ics_security_10_faqs
- TCG Specifications for Network Segmentation:

  http://www.trustedcomputinggroup.org/community/2014/09/fending_off_attacks_on_the_robots_tcg_specification_for_network_segmentation