Engineering, Operations & Technology
Boeing Research & Technology

# HIP VPLS at Boeing

## IETF 81 HIP RG

David Mattes
david.mattes@boeing.com

# Outline

Engineering, Operations & Technology | Boeing Research & Technology FaST | **Networked Systems Technology**

- **History of HIP at Boeing**
- **Industrial Control System (ICS) Security Challenges**
- **HIP VPLS Architecture**
- **Policy-constrained HIP VPLS**
- **IF-MAP Introduction**
- **IF-MAP graph for VPLS**
- **Status of HIP VPLS Implementation**
- **Standardization and commercialization activities**

# History of HIP Use Case Development at Boeing

- **Boeing project based on OpenGroup "Secure Mobile Architecture" document**
  - **HIP – security and mobility**
  - **PKI – anchoring identity in a trust chain**
  - **IF-MAP – network directory for rendezvous**

- **Use cases**
  - **2004: Location-based endpoint policy enforcement**
  - **2005: Cross interface VOIP mobility handoff**
  - **2006: Security proxy for legacy factory devices (HIP VPLS)**
  - **2007: IPv4 / IPv6 handoff**
  - **2008: Mobile Router for Mobile Network**
  - **2009: IPv4 to IPv6 handoff for Mobile Router**
  - **2010: Policy-constrained HIP VPLS using IF-MAP**

- **Relevant HIP RFCs**
  - **HIP (rfc 5201)**
  - **HIP Mobility and Multihoming (rfc 5206)**
  - **HIP Mobile Router**
  - **HIP NAT Traversal (rfc 5770)**
  - **HIP Certificates (rfc 6253)**
  - **HIP VPLS (draft-henderson-hip-vpls-02)**

# Why HIP for VPLS?

- **VPLS-like use case driven by need to strongly authenticate endpoints of secure tunnels**

- **HIP provides most of the pieces already:**
  - **Lightweight key exchange has sufficient policy granularity**
  - **Can support middlebox identity-based authentication**
  - **Mobility and multihoming support**
  - **Integrates with IF-MAP-based deployments**

# ICS/SCADA Connectivity Challenges (Wired & Wireless)

- **Both legacy and new ICS equipment have connectivity challenges**
  - **Proprietary and insecure protocols**
  - **Parallel wiring plant in manufacturing facilities**
  - **Vendors continue to push custom solutions in 802.11 space**

# ICS: Security Lags Connectivity

## Demand is forcing the evolution of security and connectivity…

***Major Suppliers***

SIEMENS

Rockwell Automation

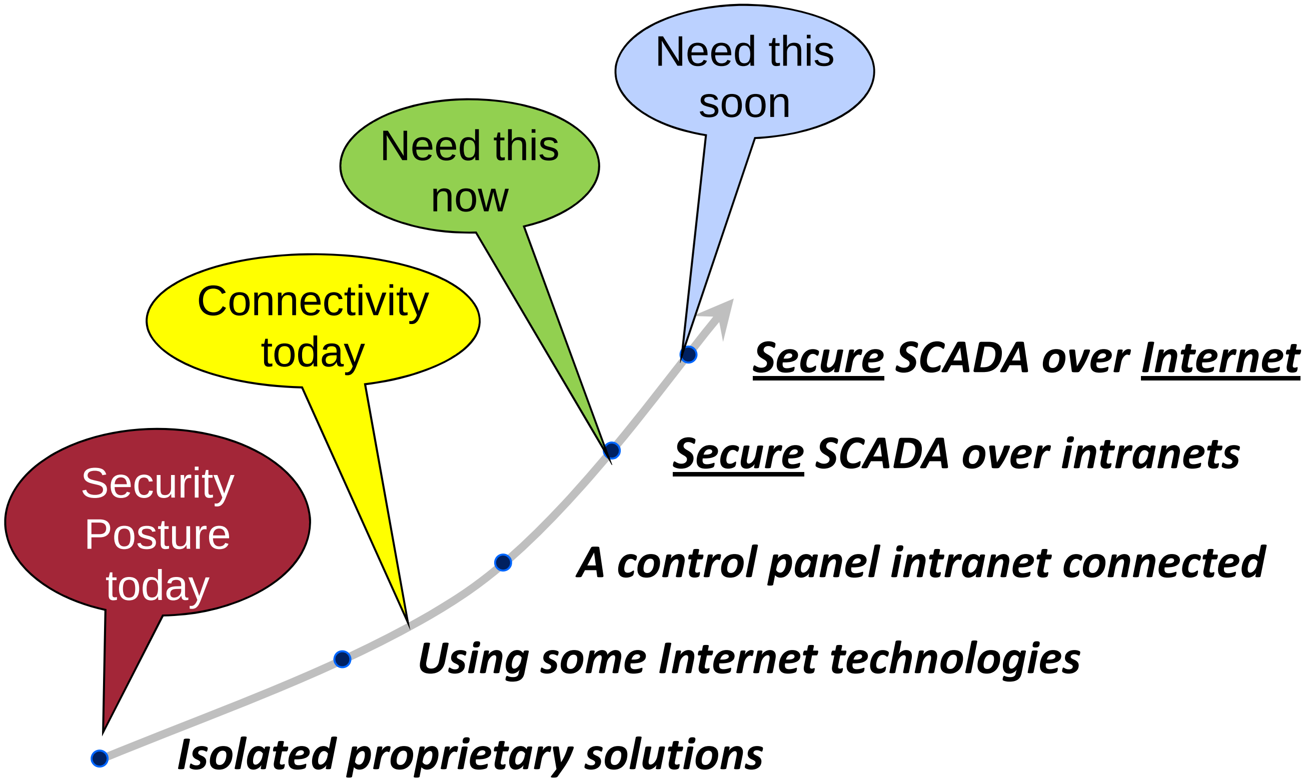
Allen-Bradley

GE FANUC

Honeywell

YOKOGAWA

*and others …*



Need this soon

Need this now

Connectivity today

Security Posture today

***Secure** SCADA over **Internet***

***Secure** SCADA over intranets*

*A control panel intranet connected*

*Using some Internet technologies*

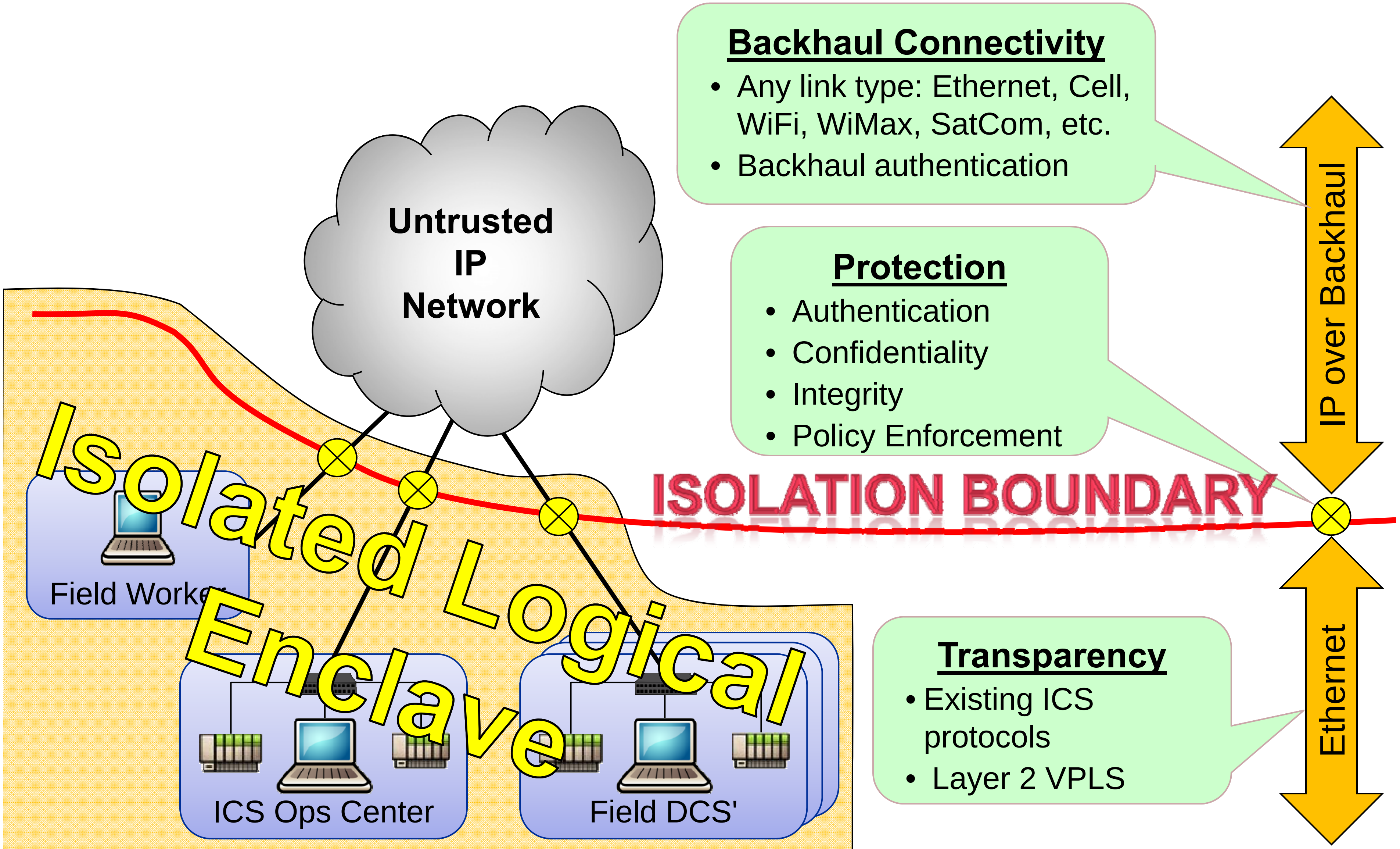
*Isolated proprietary solutions*

# Problem Statement

- **How do we provide the necessary ICS connectivity and security?**
  - ***ICS devices are and will remain highly vulnerable***
  - **Some sort of isolation is needed**

- **How do we isolate ICS systems with…**
  - **Minimized deployment and operational costs?**
  - **Maximized flexibility for manufacturing evolution?**
  - **Maximized interoperability for diverse tooling equipment with a lifecycle measured in decades?**
  - **Avoid cost & complexity of physical network isolation?**

# HIP VPLS Enclave Architecture



**Backhaul Connectivity**

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

**Protection**

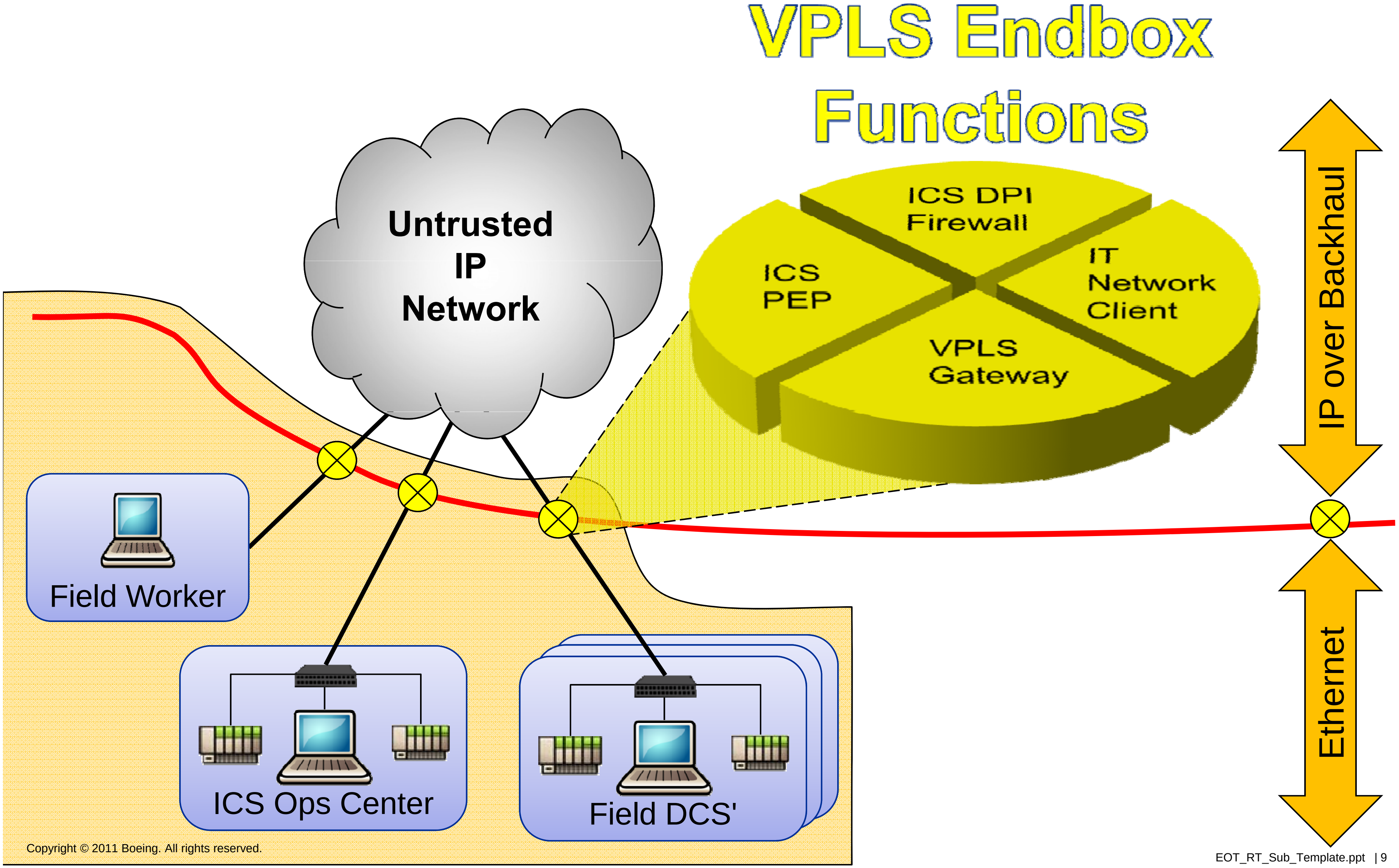
- Authentication
- Confidentiality
- Integrity
- Policy Enforcement

**Transparency**

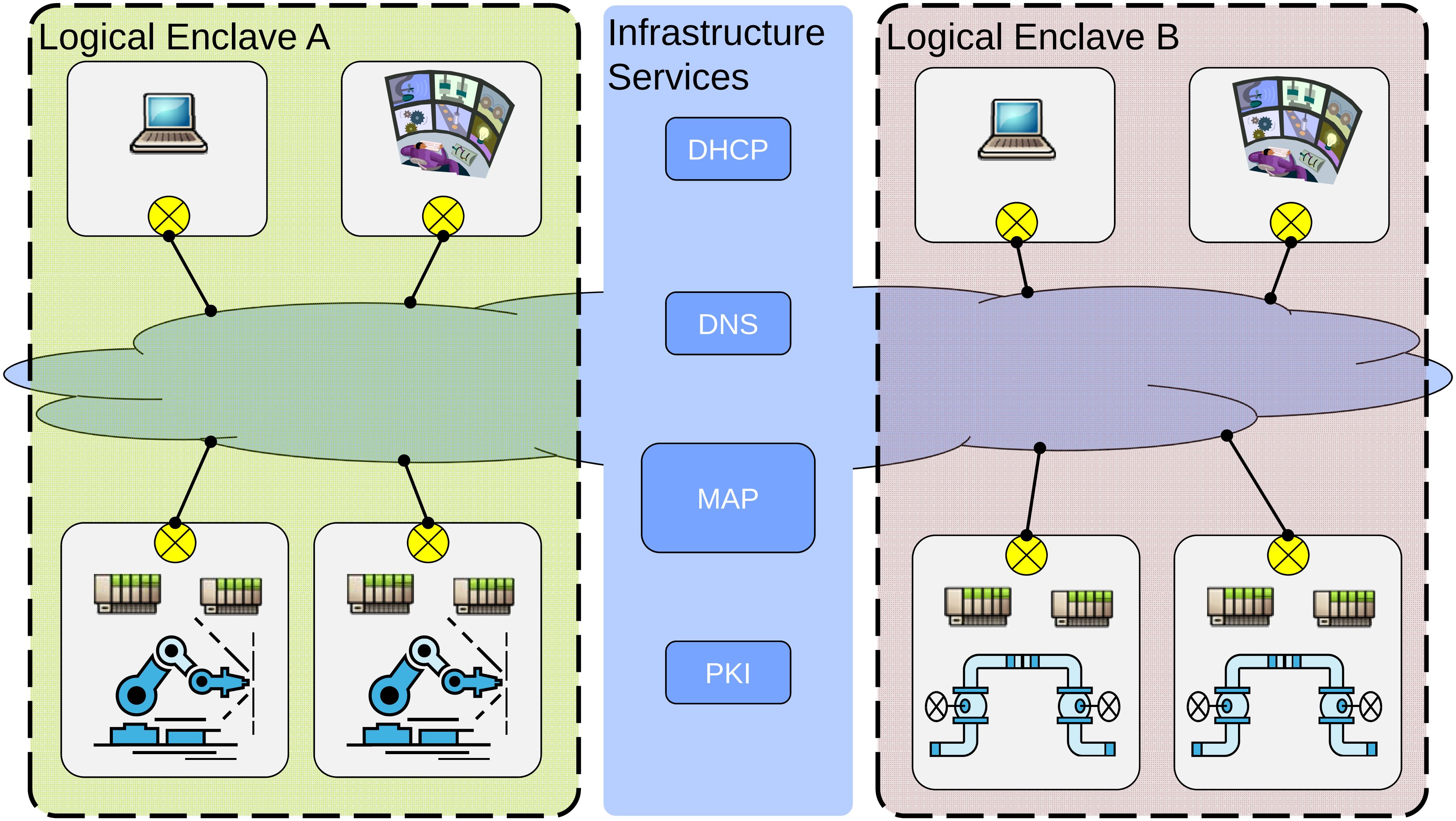
- Existing ICS protocols
- Layer 2 VPLS

# HIP VPLS Endboxes

Engineering, Operations & Technology | Boeing Research & Technology FaST | **Networked Systems Technology**



# Multiple Logical Enclaves Using Common Infrastructure



Logical Enclave A

Infrastructure Services

DHCP

DNS

MAP

PKI

Logical Enclave B

# Policy Constrained HIP VPLS

- **Constrained for efficiency**
  - **Limit number of HIP tunnels**
  - **Limit traffic through tunnels**
- **Constrained for additional security**
  - **Enforce fine-grained isolation for some Legacy devices**
  - **Can react to changing network environment**
- **VPLS policy configuration uses any combination of:**
  - **Static file-based configuration on each VPLS Endbox**
  - **LDAP data services**
  - **IF-MAP coordination service**

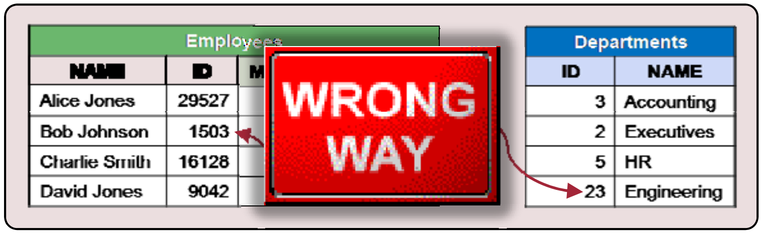
# IF-MAP Introduction

- **IF-MAP ⇔ *Interface for Metadata Access Points***
  - **Real-time metadata coordination service that provides highly scalable publish, search and subscribe capabilities**
  - **Originally developed to serve the needs of TCG's Trusted Network Connect (TNC) workgroup for interoperable NAC**
  - **Allows VPLS Endboxes to have real-time dynamic configuration and security policies**
  - **Enables real-time rendezvous and HIT ↔ Certificate binding**

# Properties of Security Coordination

Engineering, Operations & Technology | Boeing Research & Technology FaST | **Networked Systems Technology**

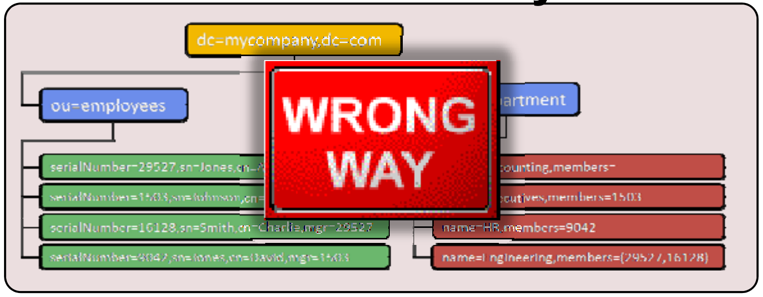
## Relational Database



| Employees | | |
|---|---|---|
| NAME | ID | M |
| Alice Jones | 29527 | |
| Bob Johnson | 1503 | |
| Charlie Smith | 16128 | |
| David Jones | 9042 | |

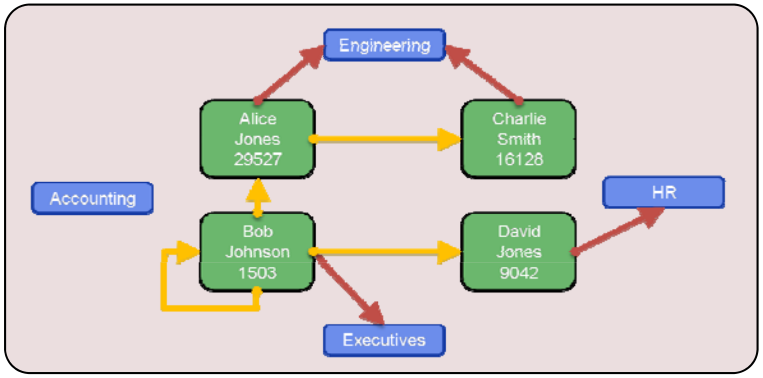
| Departments | |
|---|---|
| ID | NAME |
| 3 | Accounting |
| 2 | Executives |
| 5 | HR |
| 23 | Engineering |

## LDAP Directory



dc=mycompany,dc=com
ou=employees
artment
WRONG WAY
serialNumber=29527,sn=Jones,cn=A
serialNumber=1503,sn=Johnson,cn=
serialNumber=16128,sn=Smith,cn=Charlie,mgr=29527
serialNumber=9042,sn=Jones,cn=David,mgr=1503
counting,members=
cutives,members=1503
name=HR,members=9042
name=Engineering,members=(29527,16128)

## MAP Database

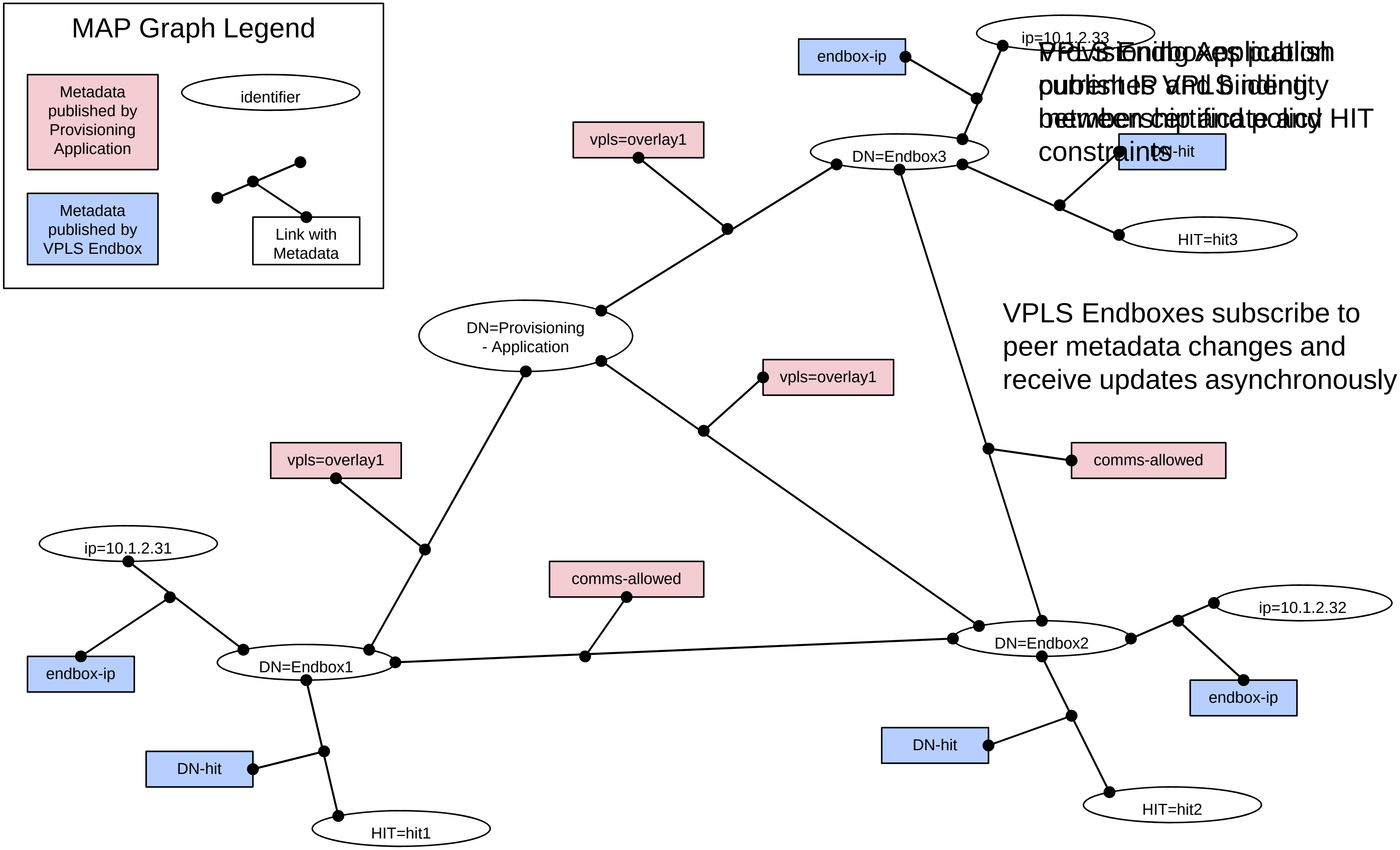


1. **Lots of real-time data writes**
2. **Unstructured relationships**
3. **Diverse interest in changes to the current state as they occur**
4. **Distributed data producers & consumers**

For more information, see IF-MAP info on Trusted Computing Group website

# HIP VPLS IF-MAP Graph

Engineering, Operations & Technology | Boeing Research & Technology FaST | **Networked Systems Technology**



Provisioning Application publishes VPLS identity membership and policy constraints

VPLS Endbox publish outer IP and binding between certificate and HIT

VPLS Endboxes subscribe to peer metadata changes and receive updates asynchronously

# Status of HIP VPLS Implementation

- **HIP VPLS Implementation is part of OpenHIP-0.8**
  - **http://www.openhip.org**
  - **Currently licensed GPLv2**
  - **Planning on relicensing to MIT**
  - **Userspace HIP implementation**
  - **Plugin architecture for the policy configuration**
- **OpenHIP VPLS implementation currently IP-only VPLS**
  - **Support for hub-spoke/full-mesh/arbitrary topologies**
  - **Requires (MAP) configured tunnel-endpoint resolution**
  - **Uses proxy-ARP**
- **Planning to implement layer 2 HIP VPLS this year**
- **Future: VPLS between Intranets**

# Standardization and Commercialization Activities

- **Working in various standards organizations**
  - **ISA, TCG, OpenGroup**
- **OpenHIP is a reference implementation**
  - **Trying to seed a market to drive down TCO**
  - **Collaborating with Byres Security, Inc. to incorporate OpenHIP VPLS capability into their products**
- **Demo at IETF 81 to showcase Byres Tofino with Policy-constrained HIP VPLS with IF-MAP**
  - **Byres planning to release a HIP VPLS product in 2012 as part of its Tofino Security Line**

- **Hope to see other vendors create products**
  - **Standards will provide some hope of interoperability**