



Engineering, Operations & Technology  
Boeing Research & Technology

Research & Technology

# Leveraging Shared IT Networks for Control Systems

Steven C. Venema, PhD  
The Boeing Company  
Steven.C.Venema@Boeing.com

Eric Byres, P.Eng.  
Tofino Security, Inc.  
Eric@ByresSecurity.com

ICSJWG – 07Apr2010

- **A Framework for Describing the Problem**
- **A Proposed Technology Solution**
- **Key Technologies and Standards**
- **Implementation Experience**
- **Discussion and Future Directions**

# Peaceful Coexistence with IT?

A complex mix of  
people, IT, control  
systems & products...



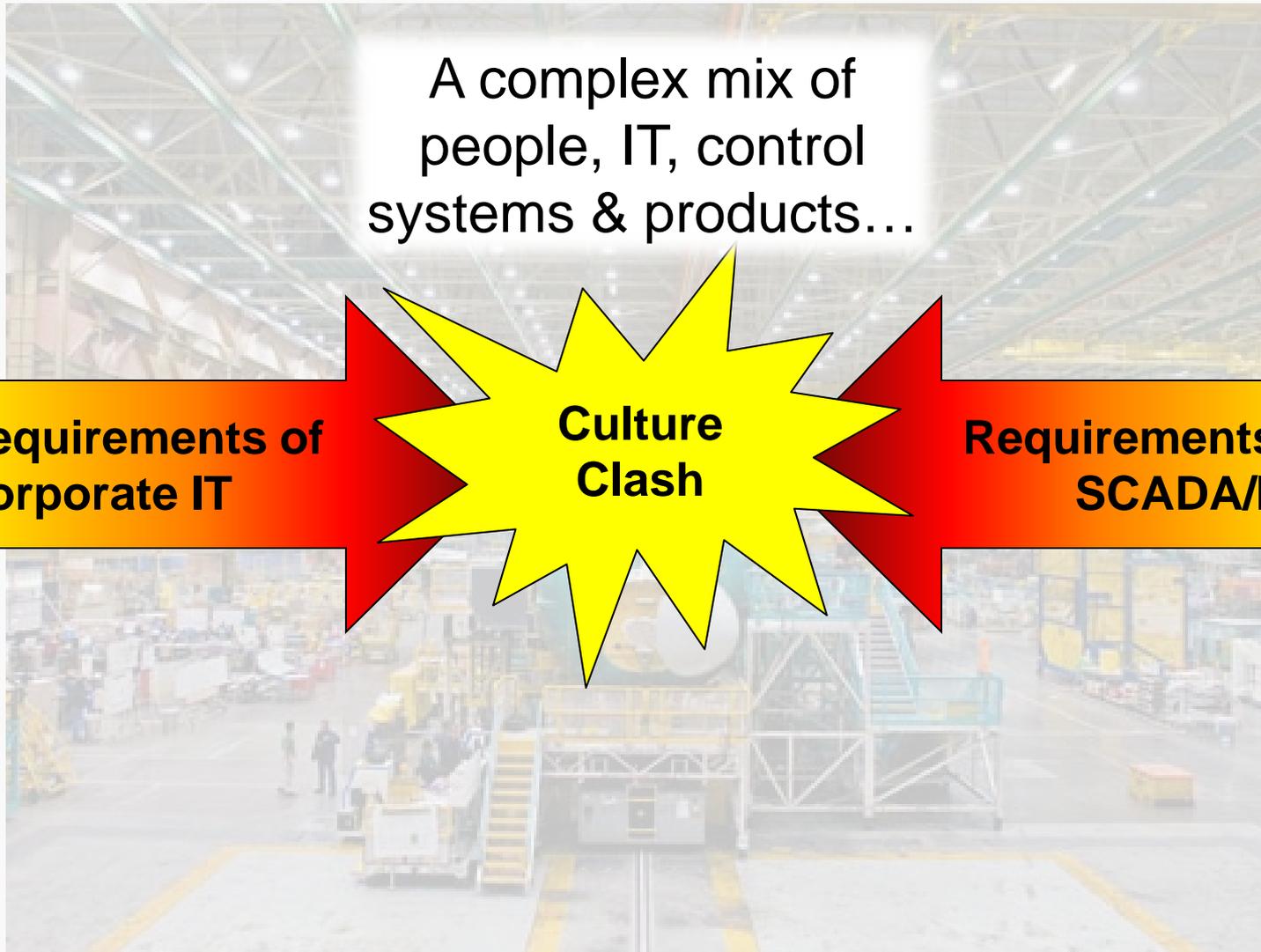
# Peaceful Coexistence with IT?

A complex mix of  
people, IT, control  
systems & products...

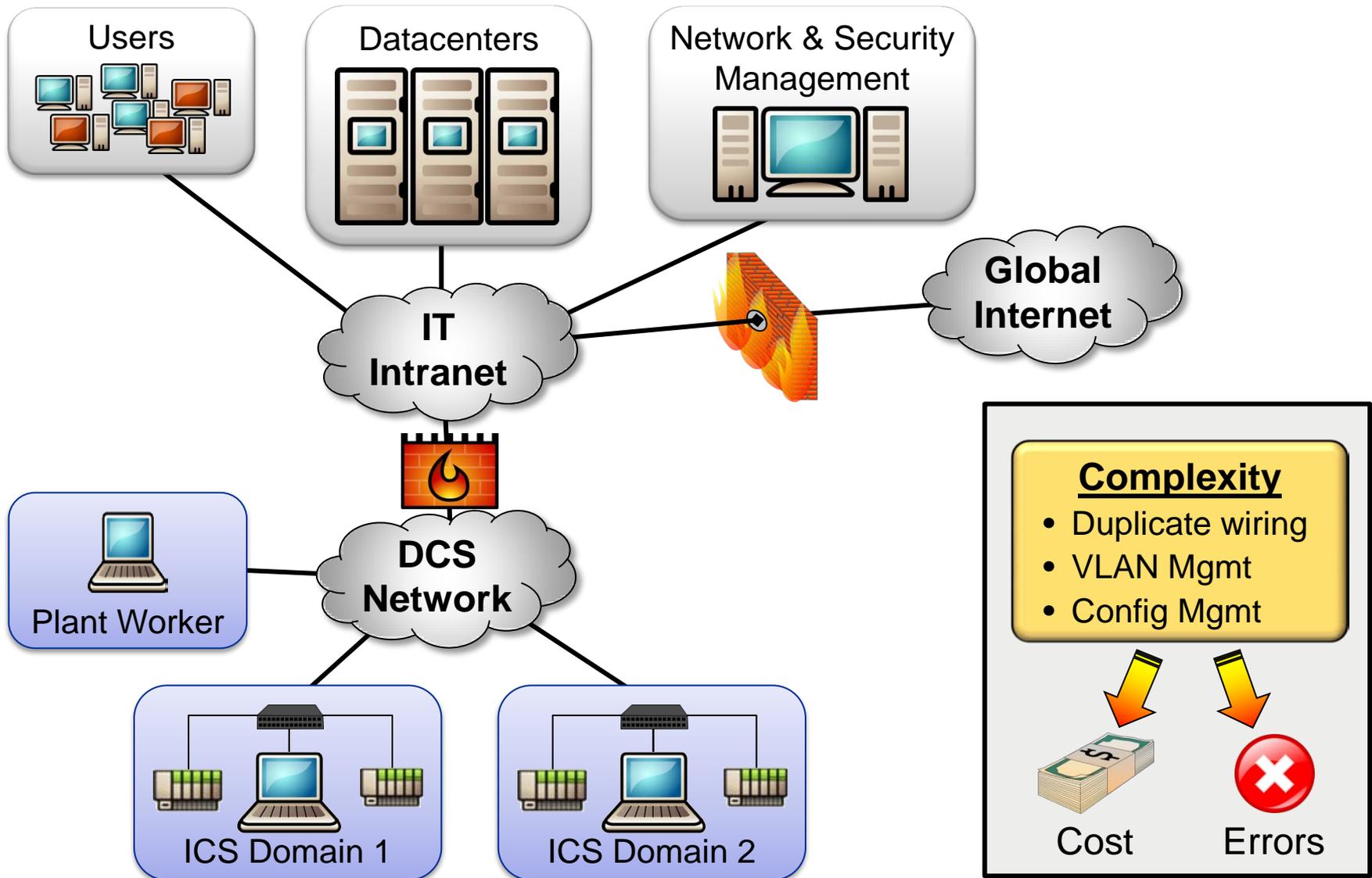
**Requirements of  
Corporate IT**

**Culture  
Clash**

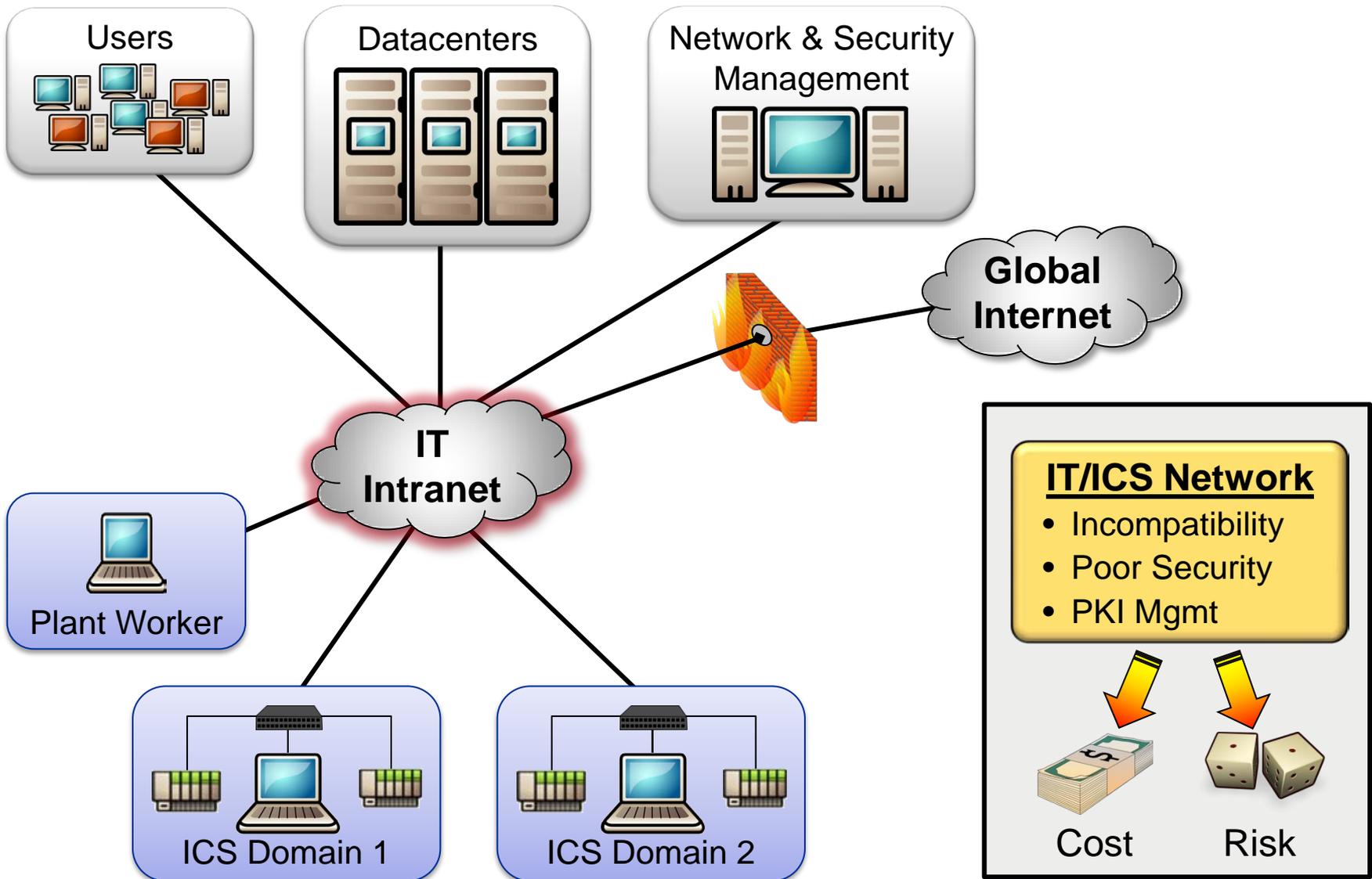
**Requirements of  
SCADA/ICS**



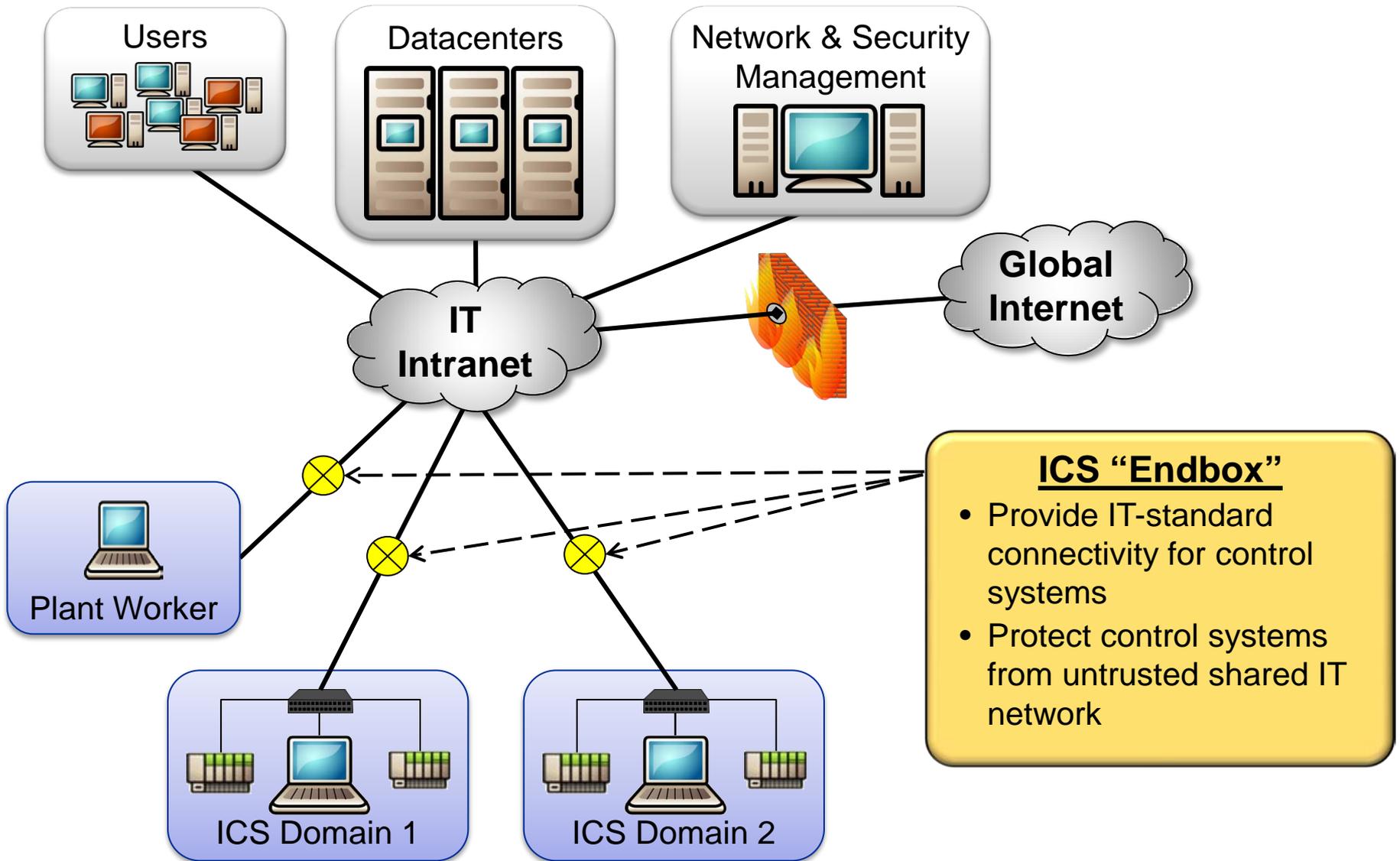
# Typical IT ↔ ICS Isolation Scheme



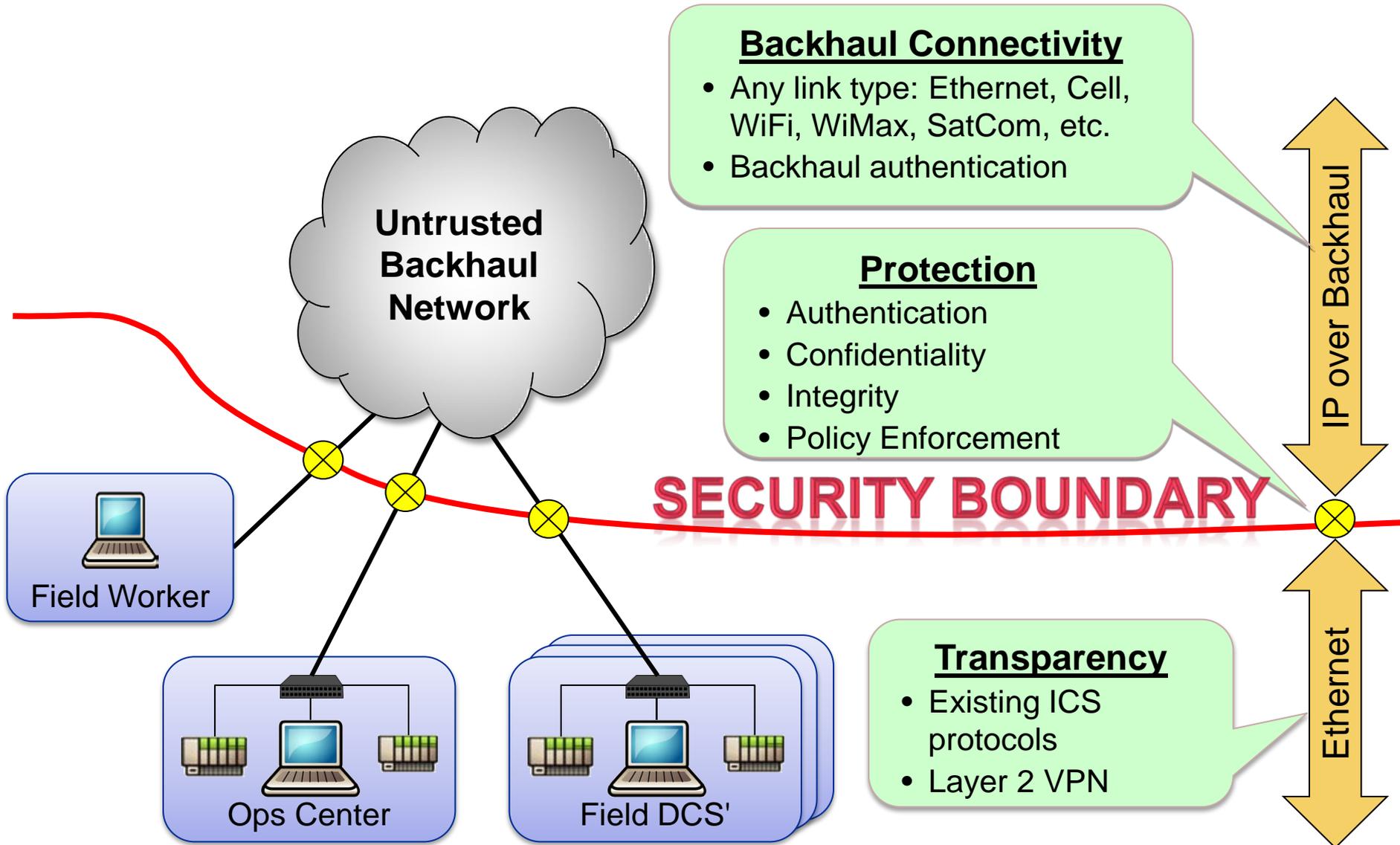
# Ideal ICS ↔ IT Shared Network



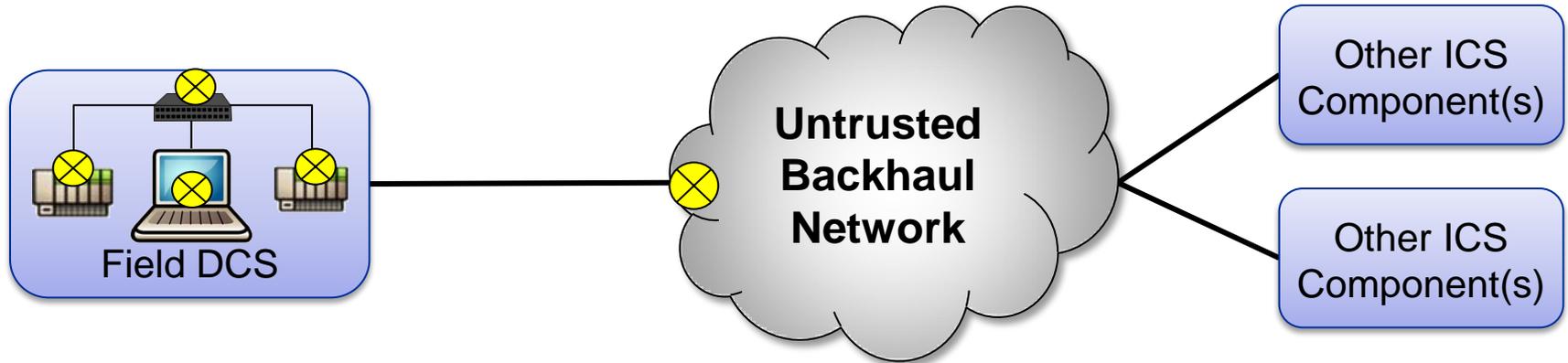
# Protected ICS using Untrusted IT Network



# Generalized Secure Backhaul for ICS



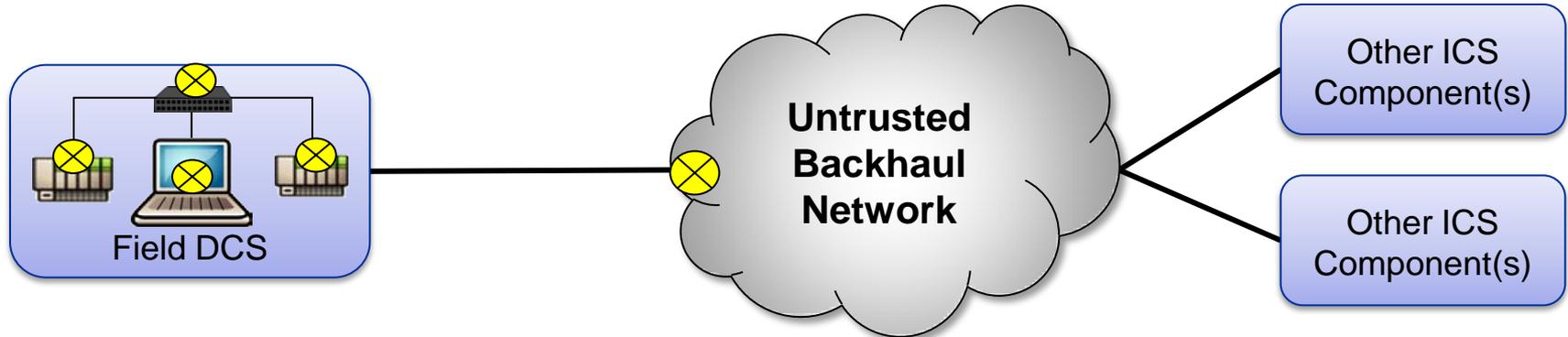
# Where does the Endbox functionality belong?



## **A:** There are multiple implementation approaches:

- 1.** It could be provided by the backhaul “ISP”
- 2.** It could be placed in a separate box in front of a cluster of ICS devices
- 3.** It could be incorporated right into the control system devices
- 4.** It could be any combination of the above

# How do we make this inexpensive to deploy & operate?



## **A:** Automate as much as possible:

- Certificate provisioning and lifecycle management
- Endbox configuration management
- Connectivity policy definition and enforcement
- Monitoring and fault diagnosis

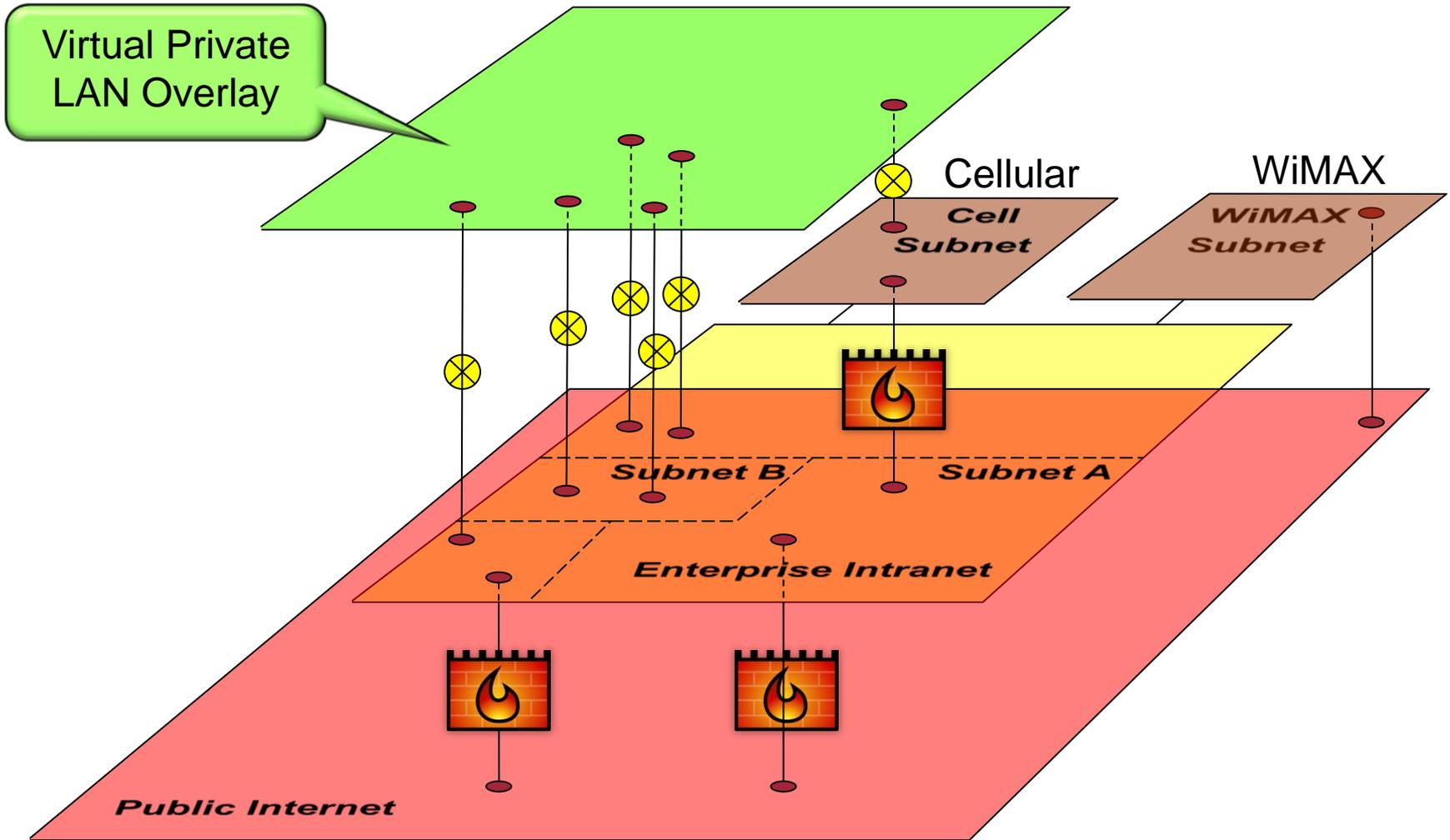
## **A:** Use public standards wherever possible

- IT standard services
- Key protocols and interfaces for interoperability

# High-level Architecture Goals

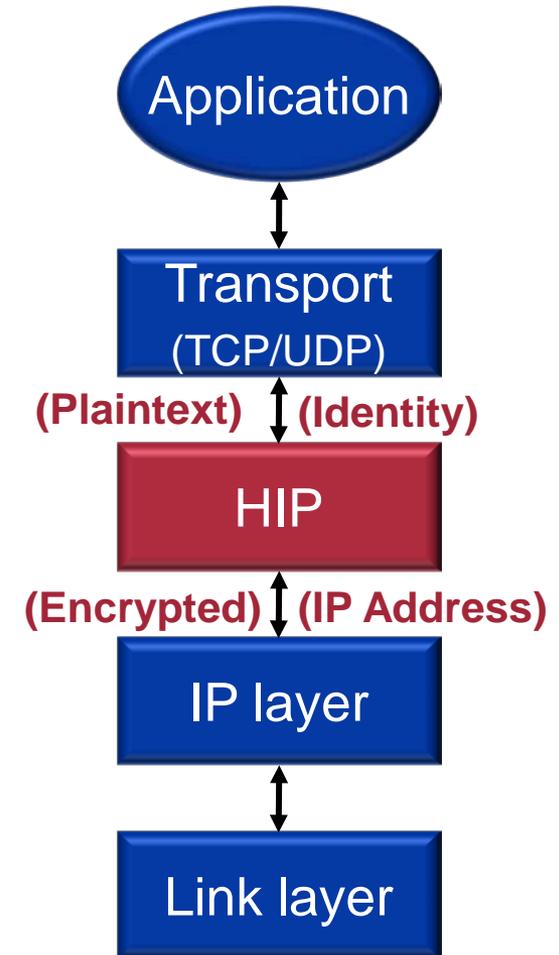
- 1. Allow control systems to utilize a common shared network infrastructure to minimize deployment costs**
  - Both wired and wireless
  - Support hybrid approaches (shared + isolated networking infrastructure) where appropriate
- 2. Isolate control systems from the shared network to protect “primitive” control devices**
  - “Bake in” cryptographic identities and authentication
- 3. Allow controls engineers (not IT) to manage their own devices**
  - Create a clear delineation between the roles and responsibilities of controls engineers and IT services
- 4. Keep CapEx/OpEx costs low and reliability high**

# Virtual Private LAN Service (VPLS)



# Host Identity Protocol (HIP)

- **Devices communicate over end-to-end encrypted HIP tunnels**
- **Basic HIP Features:**
  - Requires no changes to layer 2/3 network infrastructure
  - Like IPsec, but tunnels are bound to cryptographic identities, not IP addresses
  - Creates an arbitrary “overlay networks” without having to mess with VLAN’s
  - Secure over untrusted network infrastructures
- **See IETF RFC’s 5201-5207**

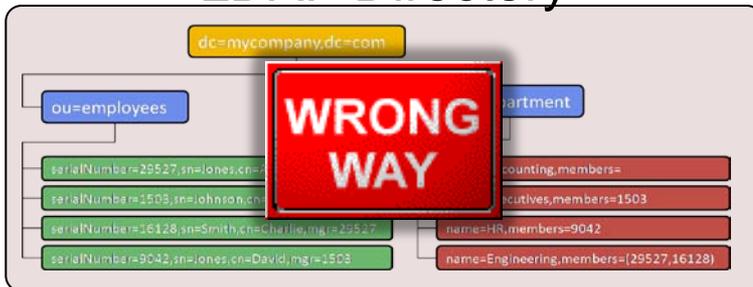


# Interface for Metadata Access Points (IF-MAP)

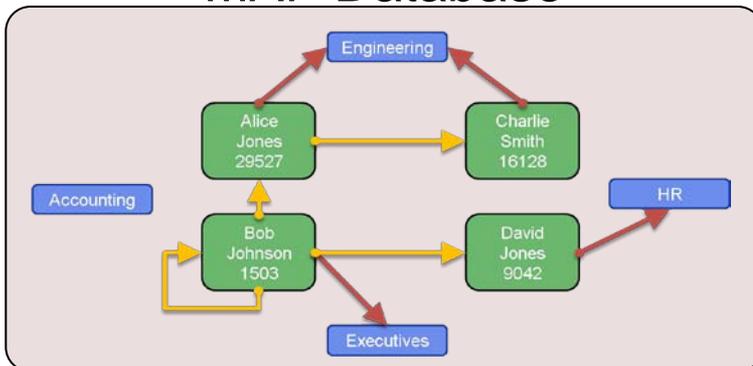
## Relational Database



## LDAP Directory



## MAP Database



## Needed data properties

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

For more information, see the Trusted Computing Group website:

<http://www.trustedcomputinggroup.org>

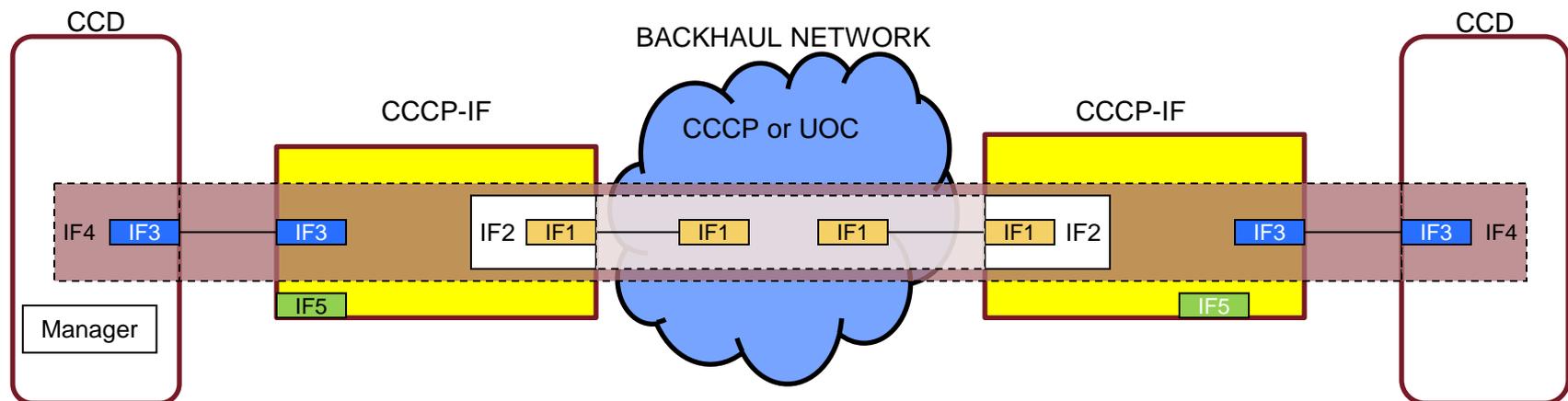
# Public Key Infrastructure (PKI)

- **Full lifecycle management for cryptographic identities must be**
  - Secure
  - Scalable
  - Robust
- **Embedded systems are particularly sensitive to this issue (E.g., certificate expiry or revocation)**
  - **(Re)Bootstrap problem: How do you securely provision & manage a distant embedded system if it doesn't already have a cryptographic credential to identify itself for secure communications?**
- **We are working on automating much of the identity lifecycle management process using coordination through IF-MAP**



# ISA100.15 Working Group

- **Creating a standard for “Secure Backhaul”**
  - Commodity Commercial Communications Provider (CCCP)
  - User Owned Communications (UOC) infrastructure
- **Focus on standardizing functional requirements and interface specifications**
  - Leveraging existing standards wherever possible
  - Interoperability and compatibility are particularly important



# First Implementation at Boeing

- Using 777 F/A as a pilot program
  - 9 “Crawlers”, F/A tug, Integrated Control System (ICS)
  - In production use for more than 2 years
  - Formed baseline for standards & commercialization efforts



**Crawler Data**

Time	Event	Location	Operator
1:07:00	SI Line	SI Line	John Doe
1:07:00	SI Line	SI Line	John Doe
1:07:00	SI Line	SI Line	John Doe

Unit	Comms	Mode	Step	Spine	Loaded	Drive Steer	Lift	Auto Level	Speed	Total Load	Dist. Run
<b>FWD CRAWLER 3</b>	OK	Auto S&I	In SI Line	300 Config	Loaded	Ready	Ready	Off	0.000 fpm	184,420 lbs	180,063 ft
<b>FWD CRAWLER 4</b>	OK	Auto S&I	In SI Line	300 Config	Loaded	Not Ready	Not Ready	Off	0.250 fpm	179,313 lbs	365,823 ft
<b>AFT CRAWLER 1</b>	OK	Auto S&I	In SI Line	300 Config	Loaded	Ready	Ready	Off	0.000 fpm	197,968 lbs	159,817 ft
<b>AFT CRAWLER 2</b>	OK	Auto F&S	In SI Line	300 Config	Loaded	Ready	Ready	Off	0.000 fpm	197,968 lbs	159,817 ft
<b>AFT CRAWLER 3</b>	No Comms										
<b>AFT CRAWLER 4</b>	OK	Auto S&I	In SI Line	300 Config	Loaded	Not Ready	Not Ready	Off	0.000 fpm	211,723 lbs	550,480 ft

7/21/2008 2:19:42 PM

ICS Communication Topology

PLC SW Revision: 20080428  
HMI SW Revision: 20080514

Buttons: 777 Overview, SI Line Overview, Final Assembly Overview, Crawler Data, Alignment Systems Data, Comm Status, Other Programs, Alarms

TUG LINE

FBJ AREA

SI LINE

WBJ AREA

Buttons: 777 Overview, SI Line Overview, Final Assembly Overview, Crawler Data, Alignment Systems Data, Comm Status, Other Programs, Alarms

# Tofino “Endbox” LSM

One Possible Commercial Implementation

Eric Byres, P.Eng  
April 2010



**TOFINO™**

# The Vision

- Standards-based solution for general management of secure control system networks within the constraints of IT infrastructures
- Solution must work with existing legacy devices as well as future standards and products
- Must separate IT and controls group roles and responsibilities

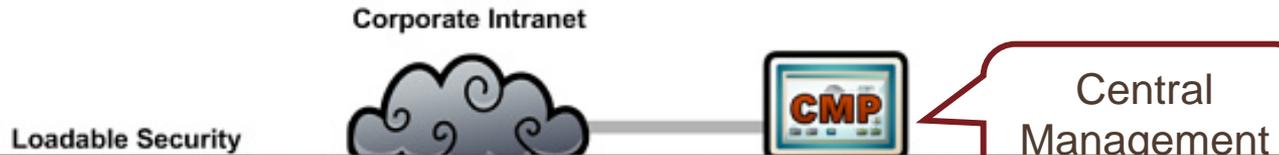
# A Standards Based Solution

- Solution based on open source software and public standards:
  - IPv4/IPV6, TCP/UDP
  - IETF Host Identity Protocol (HIP)
  - TCG Meta-Data Access Protocol (MAP)
- Collaboration between Byres Security and Boeing to incorporate open source software created by Boeing into BSI commercially supported platform

**This is NOT a proprietary solution**

# Incorporation into Tofino™ Architecture

- Created a HIP Loadable Security Module (LSM)



This is an example of an implementation of a non-proprietary solution into one proprietary product.

(Interoperability is one of the goals)



# Endbox Configuration and Provisioning

- Endboxes can connect to standard IT networks
  - Uses internal certificate for network authentication as required
- Certificate and overlay configuration managed through a centralized secured web interface
  - Configuration and provisioning metadata stored in MAP
  - Access control for web interface will depend on each company's policies for IT and Controls teams roles.
- Endbox devices ship with factory certificates and settings that facilitate automated configuration and provisioning bootstrap process.

# Simple Overlay Management for Controls

- Additional existing Tofino capabilities such as firewall and deep packet inspection can be configured through the BSI's CMP tool.

The left screenshot shows the 'Modbus TCP Enforcer' configuration window. The 'Attributes' section is expanded to show 'Global Rules' and 'Talker Rules'. Under 'Talker Rules', there are three entries: 'PLC Programming Station' (CONDITIONAL), 'MODBUS - TCP' (checked, DPI), and 'Supervisor Remote Laptop' (CONDITIONAL, checked, DPI). The 'Firewall' status is 'PREDEPLOYED'. Buttons at the bottom include 'Add Talker', 'Add Protocol', 'Add Special Rule', 'Edit Talker Rule', 'Edit Protocol Rule', 'Delete', and 'Administer Tofino'.

The right screenshot shows a detailed view of the 'Modbus TCP Enforcer' configuration. The 'General / Communications' tab is selected. A table lists the configuration for various talkers and their protocols.

Talker	Function Code Rule	Host Type	Unit ID	Sanity Check
PLC Programming Station	CONDITIONAL	Master		<input checked="" type="checkbox"/> On
40 Program (ConCept)	ALLOW			
42 Concept Symbol Table	ALLOW			
126 Schneider Electric - Program	ALLOW			
Supervisor Remote Laptop	CONDITIONAL	Master		<input checked="" type="checkbox"/> On
1 Read Coils	ALLOW			
Minimum Coil Address	0			
Maximum Coil Address	1024			
2 Read Discrete Inputs	ALLOW			
Minimum Input Address	0			
Maximum Input Address	1024			
3 Read Holding Registers	ALLOW			
Minimum Register Address	0			
Maximum Register Address	2000			

\* Click on a cell to change its value

Buttons at the bottom include 'Administer Tofino', 'OK', 'Apply', and 'Close'.

## Next Steps

- Continued interaction with ISA100 to develop a standardized set of interfaces for this capability
- Continued interaction with the Trusted Computing Group to standardize the ICS use case (provisioning & configuration management)
- Complete productizing and QA testing if sufficient demand is identified in the market space
- Industry awareness

# Future Research

- Short Term
  - Fully automated certificate provisioning
  - Standard MAP authentication system
  - HIP for PCs
- Longer Term
  - Functionality embedded directly into future ICS products
    - No Endbox needed in those cases
  - Completion of ISA100 standardization activities for this functional architecture and implementation interfaces to facilitate interoperability



# Summary

- We've created an architecture that...
  - Is viable, scalable, and addresses the needs of current and future control system deployments
  - Leverages existing and emerging standards as much as possible
  - Is implementable and already has proven operational experience
- Our implementation experience exposed some gaps in existing standards that need work:
  - Certificate provision process for embedded systems
  - Handling of non-IP protocols in routed networks

Questions?