Creating User Manageable Security Zones

The Boeing SCADAnet Technology

Craig Dupler, Boeing

Eric Byres, Byres Security Inc.

TOFINO™

Three Important Things for Security

1. Simplicity
2. Bite-size Pieces
3. Clear Ownership

TOFINO™

Simplicity

"You can't secure what you don't understand.

As systems get more complex, security will get worse. As systems become more interconnected, security will get worse."

Bruce Schneier

TOFINO™

Control Network or Big Sewer?

- *The control network or big sewer?*
- *Too many pieces of equipment connected to the control network without understanding exactly what the impact is.*

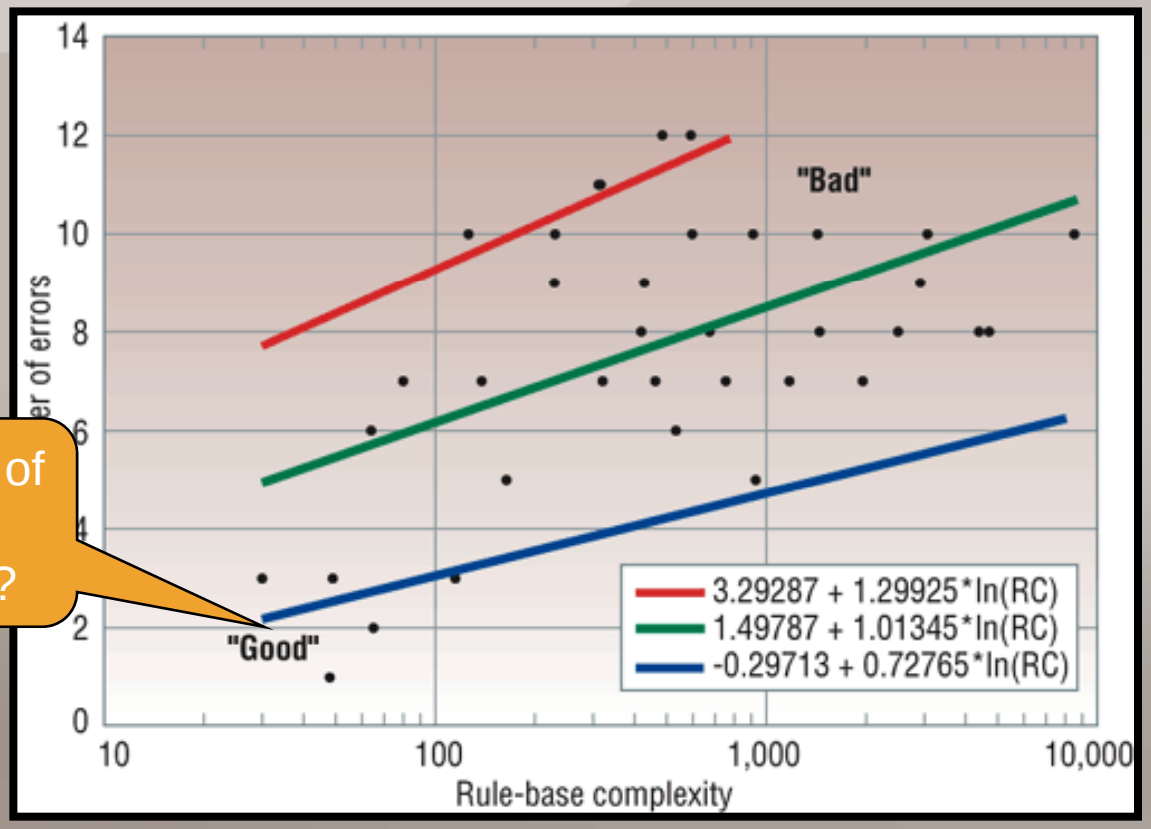
  “it gave us a microscopic view of control traffic that we had never seen before. We discovered misconfigured computers and devices generating traffic that never should have been on our control system, allowing us to clean them up right away.”

  Control Systems Manager

  US Refinery

TOFINO™

A Few Incorrectly Configured Firewalls…



Only 5 out of 37 Good Firewalls?

A quantitative study of firewall configuration errors“
Avishai Wool, " IEEE Computer Magazine, IEEE Computer Society, 2004

TOFINO™

One Big Control Network is too Complex

- Control system need to be broken into manageable pieces.
- ANSI/ISA-99 Zones and Conduits

TOFINO™

Security Zone Definition

- “Security zone: grouping of logical or physical assets that share common security requirements”. [ANSI/ISA–99.00.01–2007- 3.2.116]
  - A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements.

TOFINO™

The Network is a Utility, Not a Product

- Consider electrical power:
  - Power is supplied as a service to “end users”
  - What users do with the power is their responsibility…
  - PROVIDED that this use does not impact the power system
  - There is protection in place to safeguard the system from the users
  - Users are inherently independent from each other
  - Users can get more power, reliability, etc, for additional money
- Communications in a facility need to be considered a service to production

TOFINO™

Example Boeing Wireless Factory Applications

Products with Embedded Wireless Systems

Moving Line Assembly Tooling

SCOTT LEFEBER PHOTO

Roaming Autonomous Guided Vehicles (AGVs)

Parts Measurement and Assembly Alignment

RTLS / NLS Process & Asset Visibility

Factory Tablet PC With On-Line Work Instructions

Monitoring Temperatures of Sealant Freezers

Communications During Large Structure Assembly

Security and Reliability Challenges

Old I.T.

The old approach to ensuring compatible and acceptable client behavior on a network was to impose rigid and heavy handed configuration management.

I.T. downloads what it deems to be necessary, whenever it wants to.

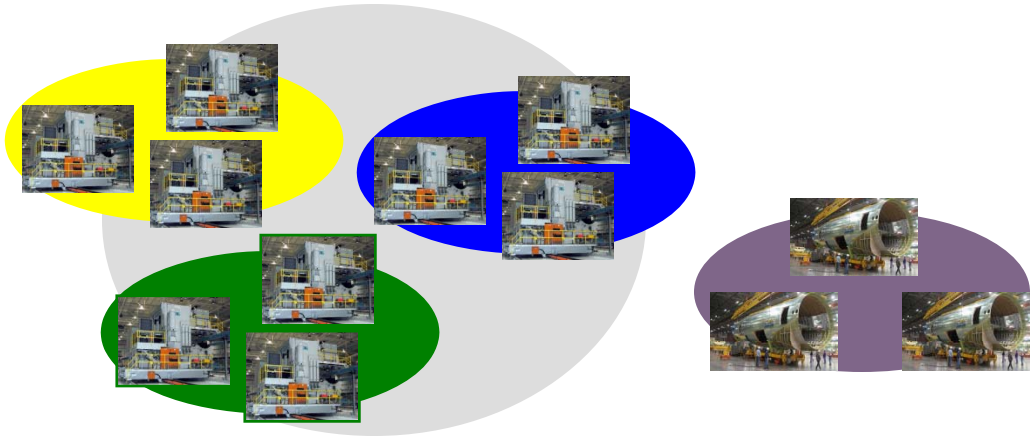
SCADA systems and internal product systems are typically beyond the configuration management reach of I.T. and often intolerant of I.T. configuration standards.

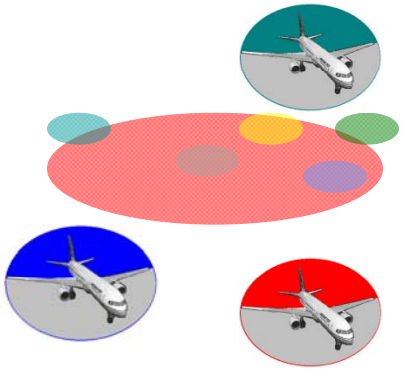
New I.T.

The Security Zone Concept

The security zone concept is valid, except …

- **The zones are logically larger (and smaller) than some thought.**
- **The zones cannot be defined by legacy methods such as VPN, subnet, SSID, etc.**
- **Some data needs to flow between and through zones.**





***n* zones of many sizes and no physical boundaries**

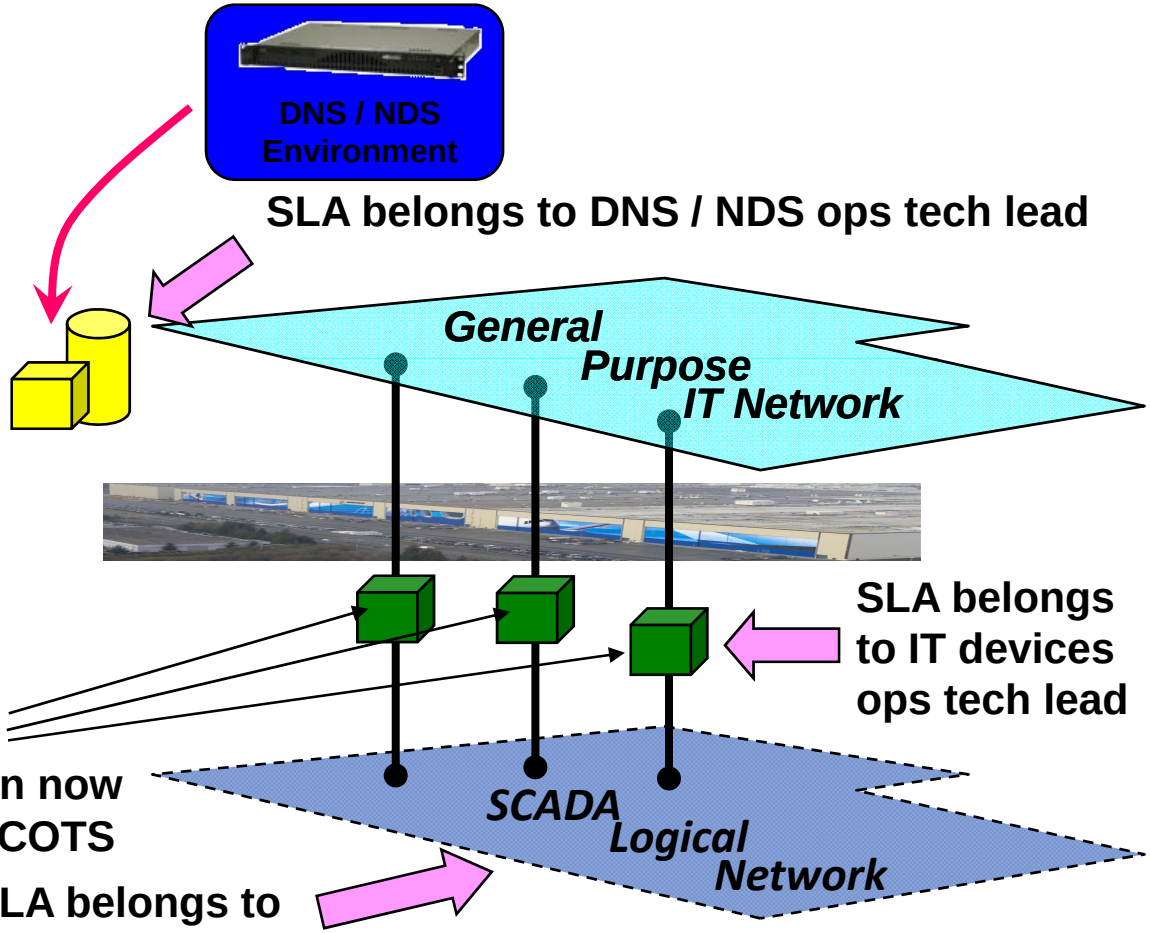
SCADAnet and NLS Lead to the Same Place

HIP Registry and Certificate Service

- New service for now
- Evolved from DNS
- Merges with DNS later

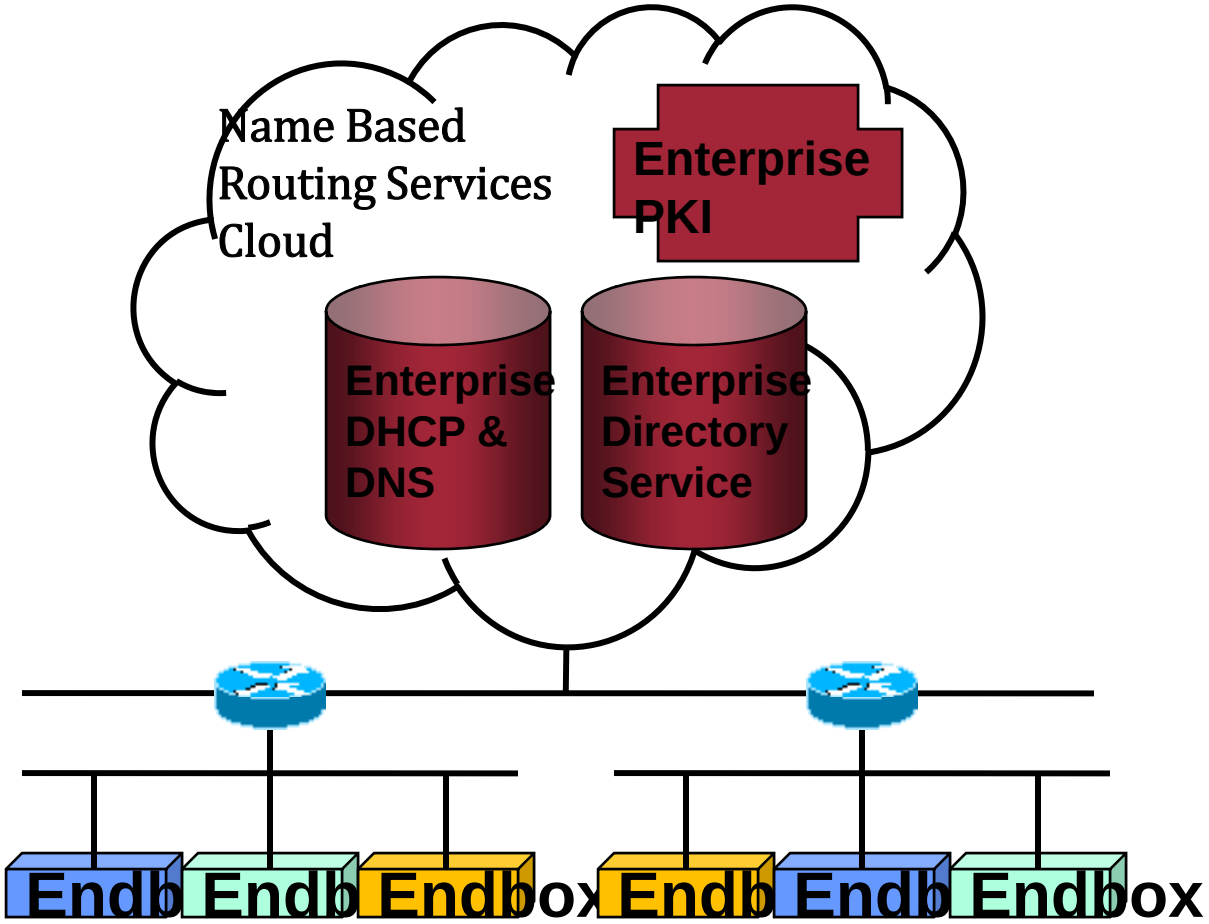
HIP End Boxes

- Boeing developed solution now
- Talking to vendors about COTS



The network enforces HIP groupings in routing and switching.

Endbox ⇔ Infrastructure Requirements



Architecture of Architectures – working draft

Layered Components	**Governance**	**Promotion**
Top Level Integrating Architecture	**The Open Group** • **SMA Architecture Definition** • **Interoperability Testing**	**OG Inter Op Events** **ARC Discrete Manufacturers Group**
PKI Certificate Service • ***Systems Integration Architecture***	**The Open Group + TCG** • **SMA Architecture Definition**	**RSA, OASIS,**
? →	**Trusted Computing Group** • **Security Architecture** • **Security Protocols** • **NDS Standards (IF-MAP?)**	**TCG Inter Op Events**
IF-MAP Registry/Directory (MAP) • ***Publish, Subscribe, Search*** **SCADAnet Registry/Directory** **NLS Lower Layer Data Plane**		
	W3C • self-describing data formats (XML) • related access methods (XPATH, XQUERY) • services frameworks (WSDL).	

EPC Global

ISA - Automation Standards & ISA 100 Wireless Committee

Opportunity!

to page 2

Architecture of Architectures – working draft

Layered Components | **Governance** | **Promotion**

to page 1

EPC Global

ISA - Automation Standards & ISA 100 Wireless Committee

Opportunity!

ISOC and IETF

- DNS, DHCP, and RADIUS **Standards**
- **HIP RFC 4423**
- **HIP Revisions to Account for End and Middle Boxes**
- ***Something new defining DNS-like MAP Directory***
- ***Something new defining NLS Directory Services (***GEOPRIV WG??)

ESDS - Extensible Supply-Chain Discovery Service
EPC Global / IETF (IETF BoF)

Location Record Definition
Active Tag Air Interface
HIP End Box Interface

IEEE

- **802.11 k & v**
- **IEEE 802.11 Active Tag RFID Frame Security**
- **IEEE 802.15.4 (Zigbee)**

WiFi Alliance
Cisco Systems & CCX

TOFINO™

tofinosecurity.com