Hardened. Resilient. Simple.

Cloak and Secure Your Critical Infrastructure, ICS and SCADA Systems

Building Security into Your Industrial Internet

Phillip Allison
Tempered Networks

TEMPERED NETWORKS™

Secure Connectivity for Critical Infrastructure & Information

Discussion topics

- Threats to network security
- TCP/IP vulnerabilities and the state of ICS/IT networks
- Technologies to address these issues
- Wrap-up

The Escalating Problem

Threat to critical infrastructure is real

- M2M connectivity on the rise
- ICN are no longer isolated
- Every industrial device is a target
- Security is imperative
- Rising complexity
- Constrained IT resources

In 2014, FBI notified 3,000 U.S companies that they had been breached

Project SHINE

Two year study on devices exposed on Internet

Sampled ~2.2 Million devices exposed

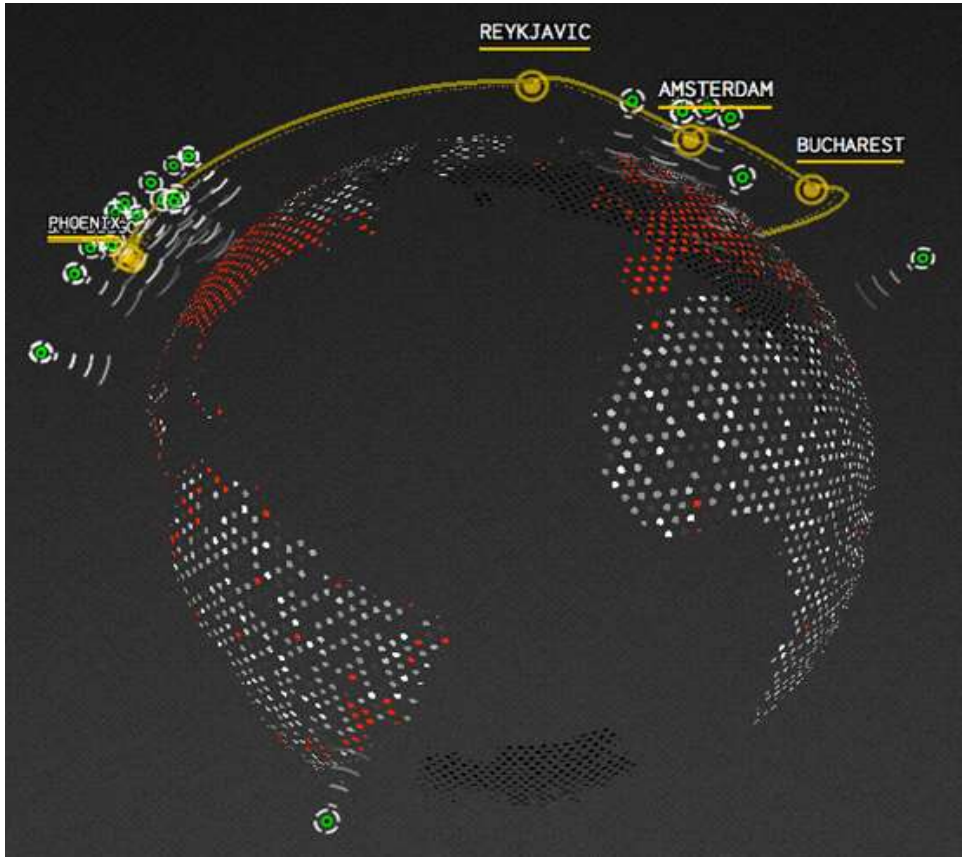
- >25% (587,000) ICS, SCADA systems, HVAC systems

SHODAN reveals a device's:

- IP address, geo coordinates, owner, service port header, firmware details, and more

Source: Infracritical's Project SHINE Findings Report, October 2014

SHODAN Search Engine



● ICS Devices

TEMPERED NETWORKS™

Add to Directory

Results **1** - **10** of about **28** for **wastewater**

Services

Telnet	9
NetBIOS	6
HTTP	5
FTP	4
SMB	2

Top Countries

United States	22
United Kingdom	3
Iran, Islamic Republic of	2
Greece	1

166.159.56.145

Verizon Wireless

Added on 16.04.2015

Details

145.sub-166-159-56.myvzw.com

Unit ID: 0

-- Device Identification: Schneider Electric BMX P34 2020 v2.5

-- CPU module: BMX P34 2020

-- Memory card: BMXRMS008MP

-- Project information: Ashton - V6.0 SCADA-LT \\PW_Server\Telemetry**Wastewater** Liftstations\PLC Programs\

-- Project revision: 0.0.101

-- Project last modified: 2014-10-20 11:51:24

Unit ID: 255

-- Device Identification: Schneider Electric BMX P34 2020 v2.5

Document Moved

204.94.174.187

HTTP/1.1 302 Redirect

TEMPERED NETWORKS™

Home | Search Directory | Data Analytics/ Exports | Developer Center | Labs

+ Add to Directory

Results **1** - **1** of about **3** for **meydenbauer**

Services

HTTP	2
FTP	1

Top Countries

United States	3

67.135.43.183
CenturyLink
Added on 16.03.2015
Seattle
Details

HTTP/1.0 302 Moved Temporarily
Connection: close
Pragma: no-cache
Location: https://**meydenbauer**.mtrxhsia.com/portal/**meydenbauer**?desired_url=http%3A%2F%2F67.135.43.183%2F
Content-Type: text/html; charset=utf-8
X-UA-Compatible: IE=Edge,chrome=1
Cache-Control: no-cache
Set-Cookie:
_rxg_console_session=BAh7CEkiD3Nlc3Npb25faWQGOgZFRkkiJWQ2YzM0NjNkNTQwNjQ3ZjNjZTU3YmU3ZjMwNjIzMjU3BjsAVEkiFmluchV0X2Rld
-9c5baa367b6f51c8a7af37f3f3fe...

Networks and Devices are Exposed and Vulnerable

Project NORSE (map.ipviking.com) - Online Map – Display Cyber Attacks in Real Time

Source: map.ipviking.com

Threat Actors

Nation-states
- Stuxnet, Flame, RSA breach, APT

Criminal Organizations
- Target, City of Detroit

Hacktivist Groups
- Anonymous, Lulzsec

Individuals / Researchers
- Houston water utility

Collateral Damage
- Worms easily infect / disrupt ICS environments

Insiders
- Maroochy Shire, accidents, errors & omissions

ICS Vulnerabilities

ICS products vulnerable by design

- Historical reliance on air gaps
- Functionally driven products skipped threat modelling

ICS disclosed vulnerabilities on the rise

- Researchers focusing on ICS
- ICS vulnerabilities still only ~10% of total IT vulnerabilities

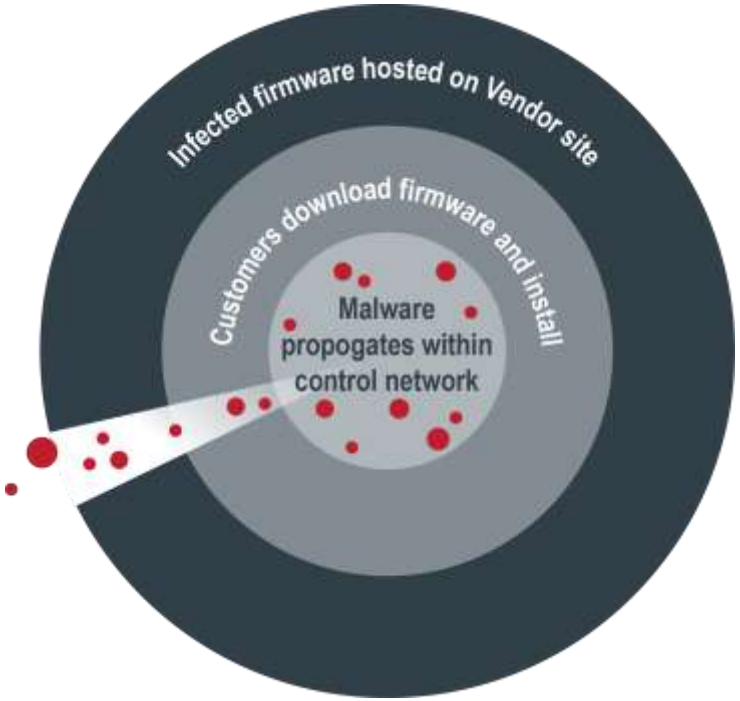
Difficulty patching existing vulnerabilities

- Product lifecycles shorter than operational lifecycles
- Vendor certifications slower than patch cycles
- System complexity makes patches risky

Attacks Focusing on ICS Systems

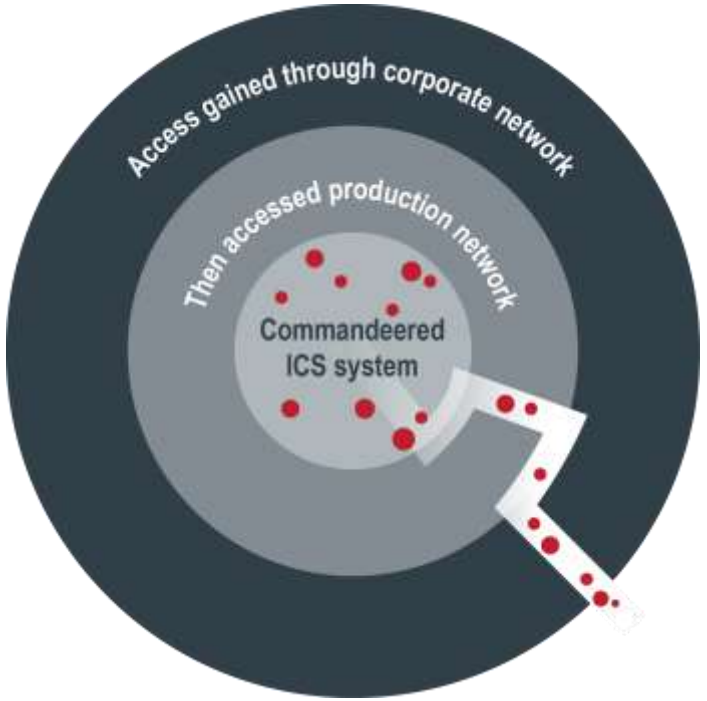
Havex Malware Discovered June 2014

- Targets OPC on Windows
- Vendor download sites compromised



German Steel Mill - 2014

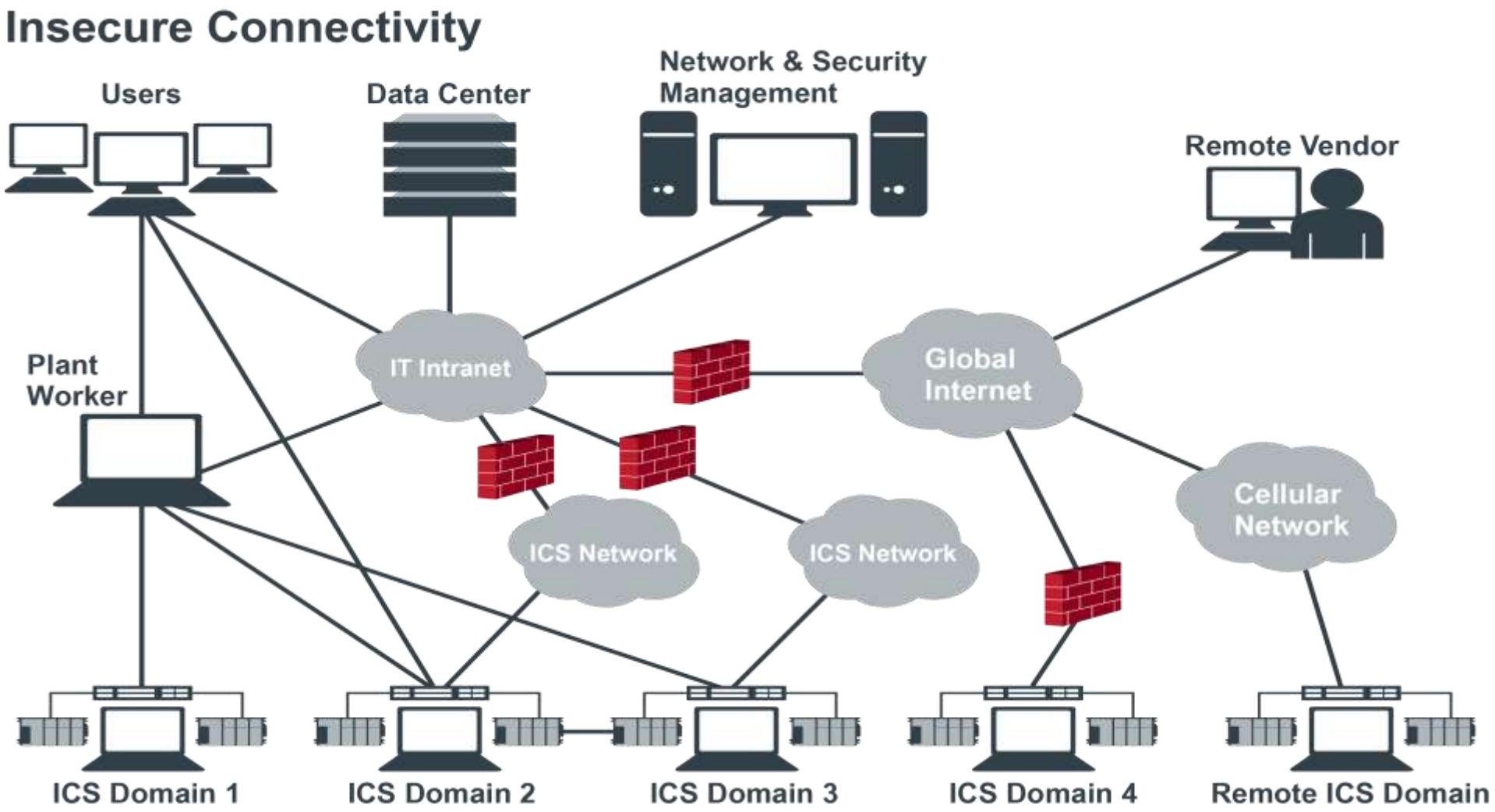
- A cyberattack caused confirmed physical damage



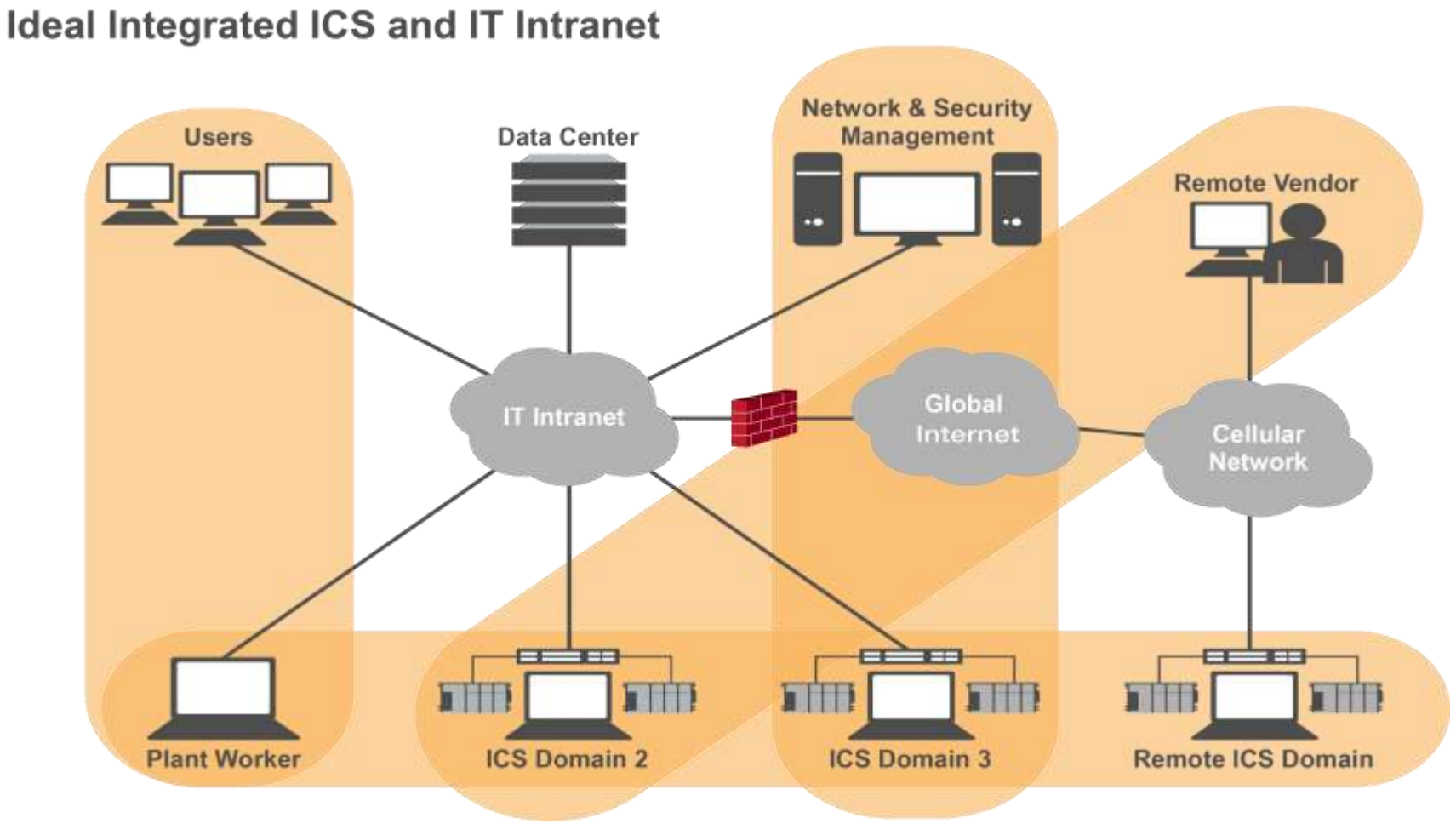
The Achilles Heel of TCP/IP and Network Security

- TCP/IP had its beginnings with ARPAnet in the 1970s
- Designed for resiliency and routing
- No security designed into the protocols at all
- Today these same protocols are part of nearly every transaction and activity on the Internet
- IP address has a dual use, to both identify and locate a host

State of ICS Networks

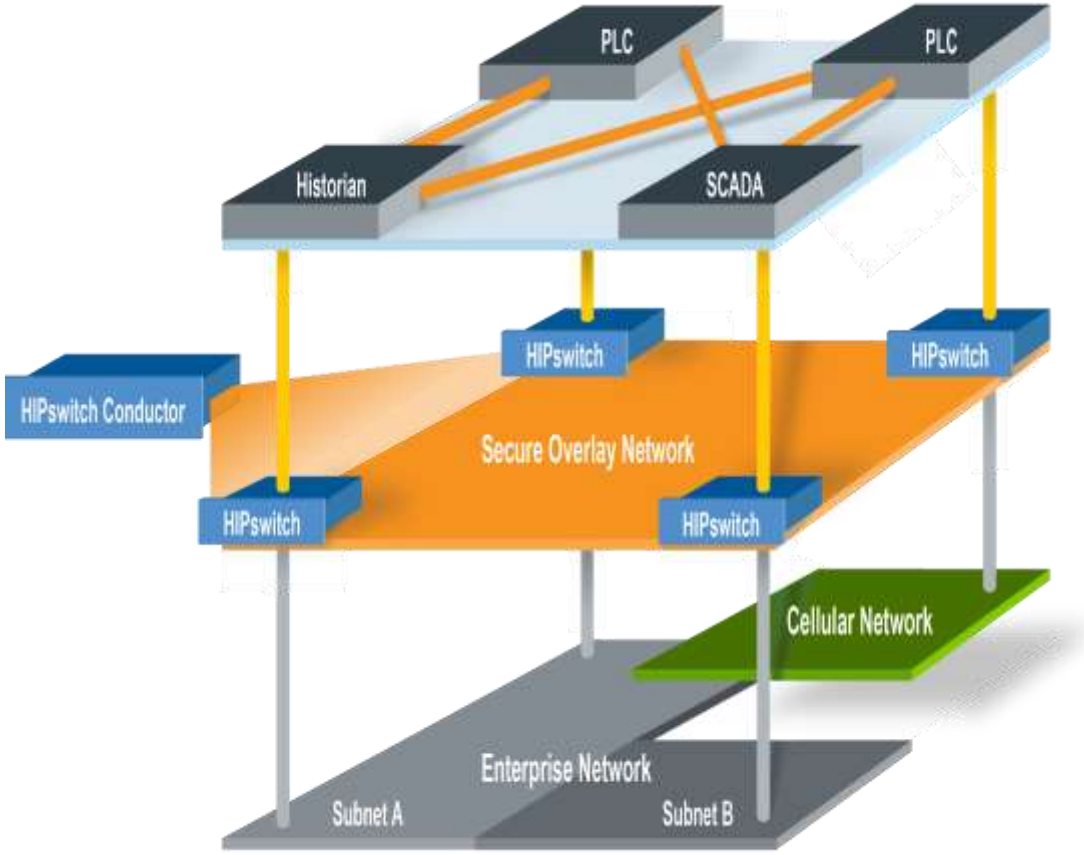


ICS Networks: Ideal



ISA 99 & ISA 100.15.01 Architecture Goals

- Zones and Conduit model and Overlay Networks model
- Leverage shared network infrastructure to minimize costs
- Isolate SCADA and Control networks from shared network
- Dynamic and flexible network segmentation
  - Minimize attack surface - limit connectivity
- Allow automation engineers to manage their own devices
  - Create a clear delineation of roles & responsibilities of engineers and IT

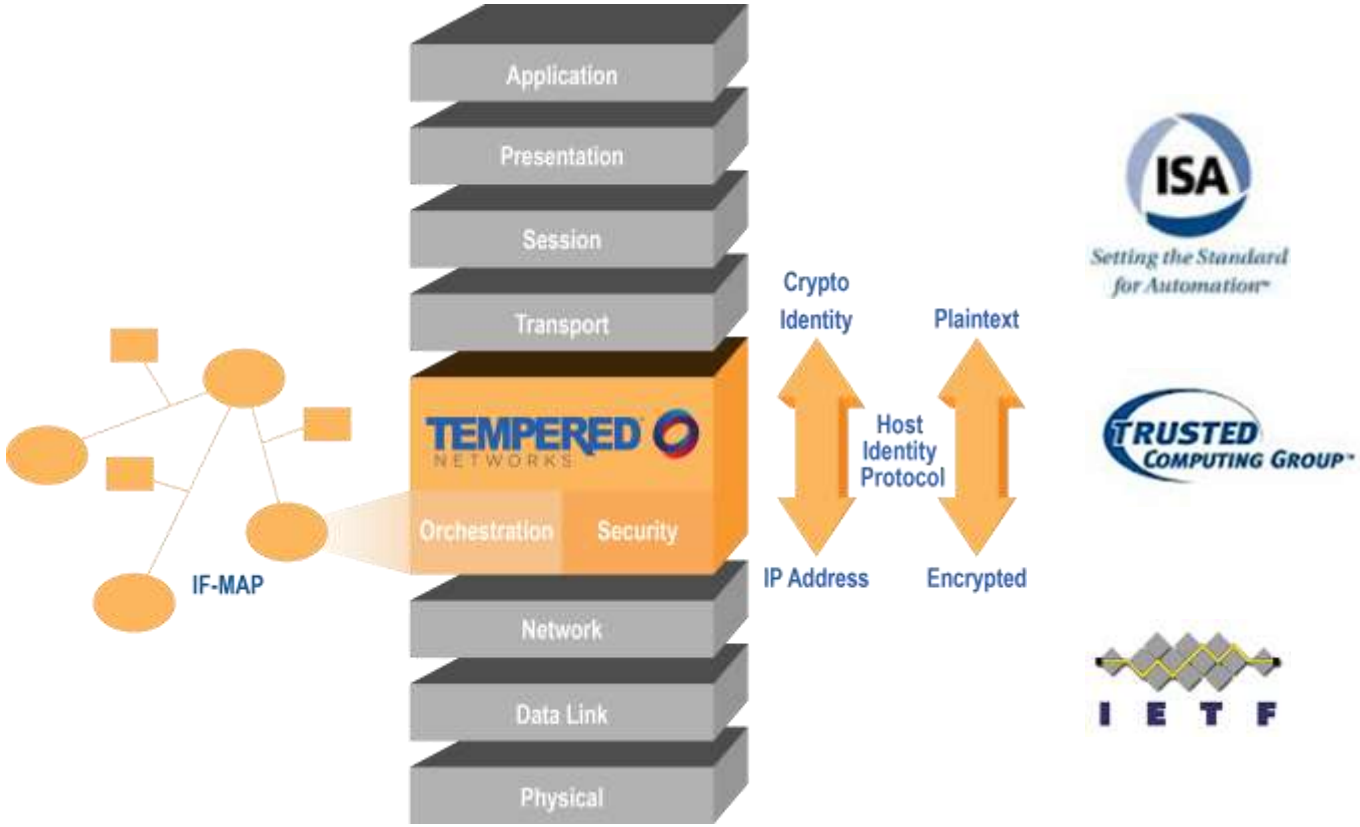


Challenges with Typical Solutions

Firewalls	• Firewalls inspect data - they do not protect data • IP and MAC addresses are spoofable • Management overhead • Prone to misconfiguration – your FW is only as secure as its configuration • Perimeter security is no longer adequate
VPNs	• Can require highly skilled staff to deploy • Management can be time consuming and costly • Do not scale well • Once authenticated, there is broad access to a flat trusted network
VLANs	• High cost per managed port • Change management is time consuming and expensive • Granting & revoking remote access is challenging • Security is embedded in the core of the underlying network

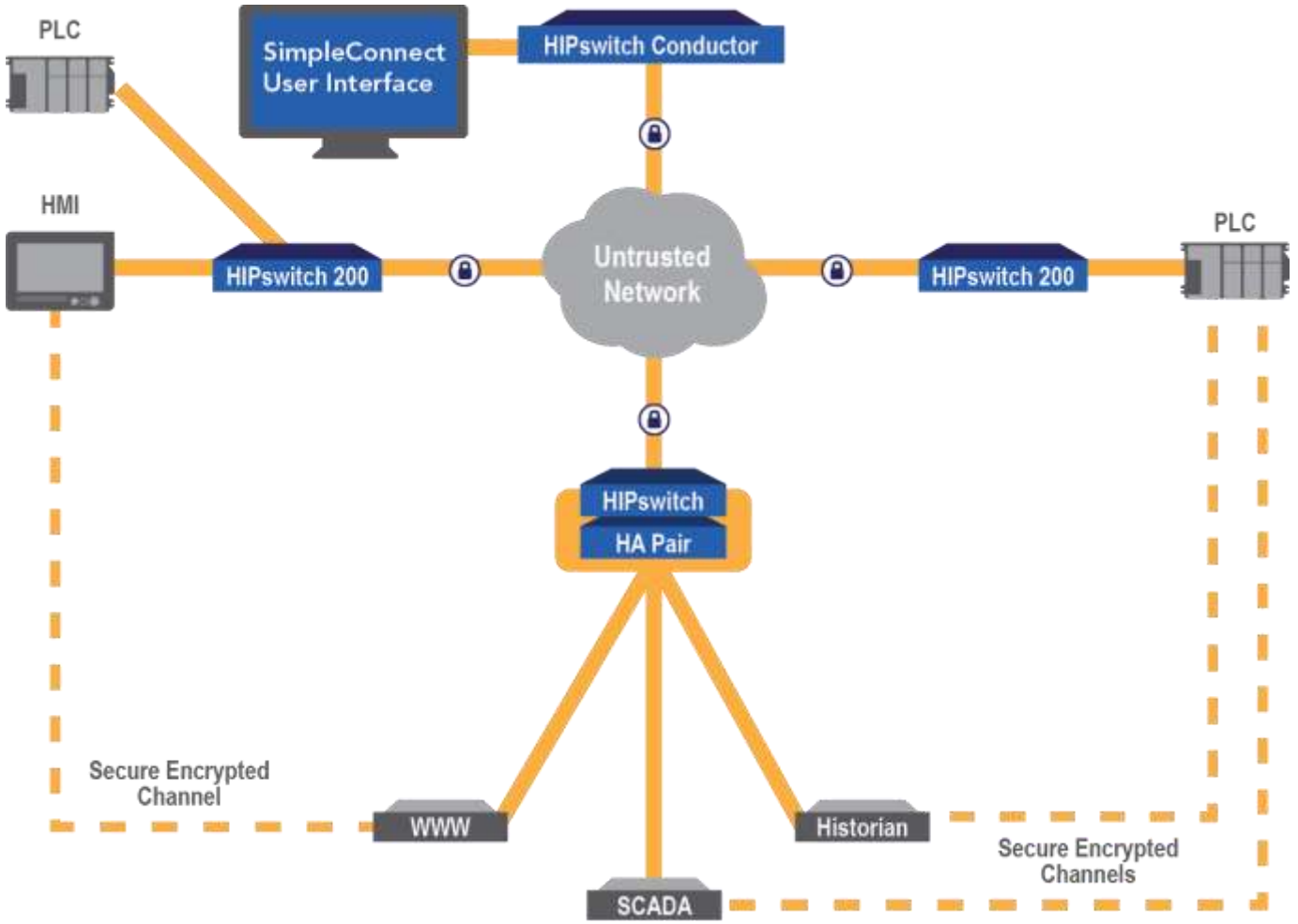
Alternative approach using Host Identities

- Encrypt host identities with industry standard **HIP protocol** and create a secure, peer-to-peer trust mechanism
- Devices are cloaked – no IP
- Industry standard **overlay network** architecture
- Create many encrypted private overlay networks, each with only trusted peers
- Orchestrate and automate, at scale, all overlays, devices and users with industry standard **IF-MAP protocol** for ease of use



*International Society for Automation (ISA), ISA100 TR100.15.01 “Overlay Network Architecture Model”, ISA99, “Zones and Conduits”
**Internet Engineering Task Force (IETF), HIP RFC 5201
***Trusted Computing Group (TCG), IF-MAP Meta Data for ICS Security

SCADA System Overview



New Governance Model

Meeting IT and OT Imperatives

Built for Operations: Retain networking and device configuration control

- Easier to operate/maintain: No configuration changes required
- Modify configuration on your terms
- Centralized life-cycle management of private networks

Vetted by IT: Secure Private Networking as an Internal Service

- Eliminates task of daily change management
- Delegate user admin for self service departmental provisioning
- Enables centralized governance and oversight

Organizational benefits: Protects corporate assets and brand

- Lower TCO than other solutions
- Robust control system networks
- Increased security posture

What a solution should do

Operationally defined connectivity

- Secure by default, simple to deploy and maintain - for any device or scale

Easy to Deploy and Use

- Drop-in hardware and software components leverage existing network infrastructure to efficiently enable secure industrial connectivity

Low TCO (Total Cost of Ownership)

- Leverage existing infrastructure and untrusted networks
- Low operating expense with user friendly management interface

Superior Scalability

- Easily add and isolate devices and create private overlay networks

Unparalleled Security

- Build secure perimeter around industrial devices
- ‘Cloak’ critical infrastructure components

Towards Defense in Depth

Protect

- Raise the bar as high as possible
- Minimize exposure when under attack
- Understand risk exposure

Detect

- Discover attacks quickly
- Feedback with protection
- Use ISACs to stay ahead

Respond

- Isolate incidents quickly
- Remain operational over wide range of events
- Enable disaster recovery, business continuity

Thank you!