ARCHITECT'S GUIDE:
ICS SECURITY USING TNC TECHNOLOGY

October 2013

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Executive Summary and Action Items

Industrial Control Systems (ICSs) are increasingly being connected to networks and exposed to viruses, malware, and attacks that affect other network-connected systems. As a result, many standards organizations including the International Society of Automation (ISA), the International Electrotechnical Commission (IEC), and the Trusted Computing Group (TCG) [as well as the Internet Engineering Task Force (IETF), The Open Group and others] are developing standards-based approaches for increased control system security.

ISA/IEC-62443 defines a zone and conduit strategy to provide ICS security. The zones are layers or subdivisions of the logical or physical assets of a control system, based on their control function. Conduits connect the zones, providing a path for data flow, and must be managed to protect network traffic.

TCG standards developed by the Trusted Network Connect (TNC) workgroup (*see sidebar, page 5*) can be implemented today to provide increased security and protection from unauthorized ICS access. These standards help implement the security defined in ISA/IEC specifications. Specifically, the Interface for a Metadata Access Point (IF-MAP) Metadata for ICS Security specification facilitates the deployment, management, and protection of large-scale industrial control systems by creating virtual overlay networks on top of standard shared Internet Protocol (IP) network infrastructure.

This Architect's Guide shows information technology (IT) and control systems executives and architects how to implement a standards-based, interoperable approach to ICS security as specified in ISA 99 (now IEC 62443) and ISA 100.15.

Critical strategies for architects include:

1. Define the zones to account for all ICS assets
2. Define the attributes of each zone
3. Map all channels or means of data transfer including mobile transfers
4. Define conduits to contain all discovered channels
5. Define controls for the flow of digital information for each zone and conduit in the facility

Introduction

Simple industrial control systems are localized and may be a single work cell in a manufacturing plant. However, data from widely dispersed automation components in geographically distributed physical processes such as oil refineries, oil pipelines, energy transmission, water utilities, manufacturing environments, and others are often communicated to distant control centers over a network infrastructure. From simple to highly complex, traditionally isolated control systems networks are increasingly being interconnected with IP networks.

Supervisory Control and Data Acquisition (SCADA) and ICS systems face a number of unique security challenges that traditional IT assets do not. First, basic authentication and authorization functions for network security are not supported by of the vast majority of ICS, SCADA, and process control devices. Second, since these systems are widely distributed (with the most critical devices scattered over 1000's of miles), remote access is critical. However, traditional **Virtual LAN (VLAN) and Virtual Private Network (VPN)** approaches to secure connectivity have proven to be highly complex, difficult to manage in real time, and not suited for handling the protocols that are found in automation networks.

Finally, the expected life span of ICS products is often 20 to 30 years, meaning that products will remain installed and operational long after the vendor has stopped providing security patches. Even when patches are available, most ICS and SCADA systems operate on 7x24 basis, with shutdowns only yearly (or never). Thus it can be months or years before available security patches can be installed.

There are many compelling reasons to connect industrial/factory control system networks with corporate IT networks, including:

- **Increased visibility** for higher efficiency and cost control
- **Real-time data integration**
- **Agility** to facilitate just-in-time delivery/manufacturing
- **Remote monitoring** of the control systems to resolve problems more quickly and reduce support costs
- **Remote management** to provide coordinated regional production/distribution of products such as electrical power, natural gas, and drinking water

As shown in *Figure 1,* an integrated Secure ICS and IT Intranet is desirable, providing better visibility, control, flexibility, integrity, and reliability.

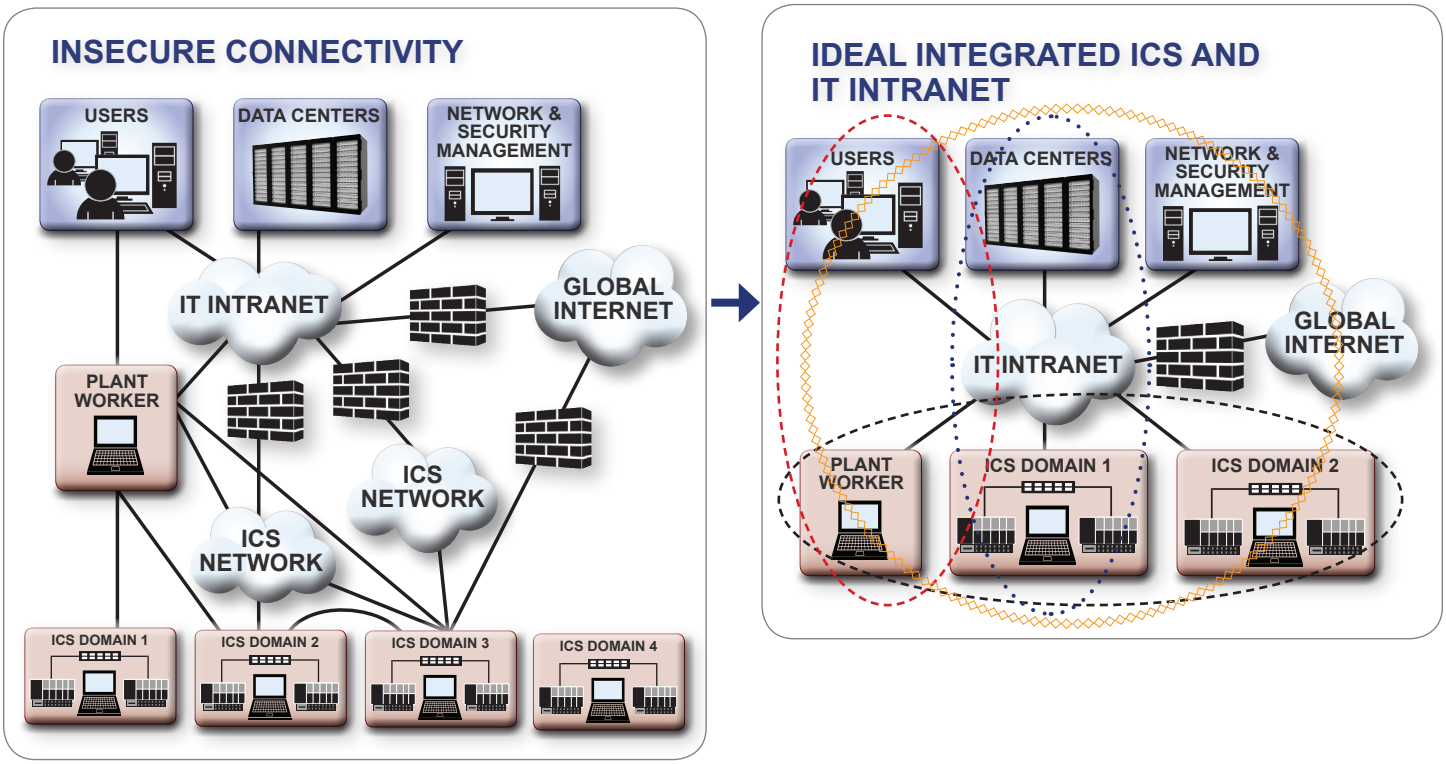

Figure 1: The transition from isolated to integrated networks requires a Secure ICS and IT Intranet.

As Sean McGurk, the Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security, stated in testimony to Congress (May 25, 2011)[1], *In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system, or energy management system separated from the enterprise network. On average, we find eleven direct connections between control system and the enterprise operations in any site we visit."* He added, *"In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.*

However, just as an enterprise network is not adequately secured with merely a firewall, neither is a control system network. Increased risks due to these interconnections include:

- **Exposure of legacy equipment** not inherently secure or able to be secured
- **Substantially increased attacks** from sophisticated groups such as advanced persistent threats (APT)
- **Damage to corporate brand**
- **Downtime for service offerings**
- **Lost production**

All of these threats have a significant cost impact to the enterprise.

Even though each industry and company has different focus and priorities, the increased integration, remote access demands, and monitoring of industrial control sites requires both IT and operations management to determine how they will prevent network attacks against production facilities, distribution systems, and other critical systems..

Solution Requirements

Equipment in factories and remote facilities is extensively monitored for temperature, pressure, flow, vibration and other critical manufacturing and process parameters. Unfortunately, monitoring of critical network parameters is usually minimal to non-existent. In many companies, as long as the ICS network is allowing data to flow, it is working "well enough". Protecting ICS networks requires a thorough, standards-based approach, encompassing:

- **Security solution** for separation / protection through virtual tunnels and access control lists (ACLs)
- **Provisioning of the security solution,** including deployment and certification lifecycle management
- **Monitoring of equipment** in local or remote ICS networks
- **Maintenance of equipment** in local or remote facilities

Solution Overview

An integrated approach to ICS security based on open standards from TCG & ISA is shown in *Figure 2*. Based on zone models and zone management, a virtual private overlay network provides secure communications across an underlay. The overlay networks isolate ICS components into one or more protected virtual enclaves while allowing those components to safely connect over to a shared, untrusted commodity IP infrastructure.

Commodity network substrates in control systems are often called Backhaul Networks. The overlay approach provides automated provisioning of certificates and Backhaul Interfaces (BHIs) — network components that provide connectivity and security to interconnected enclaves — as well as automated application of access control policies from a centralized provisioning system.

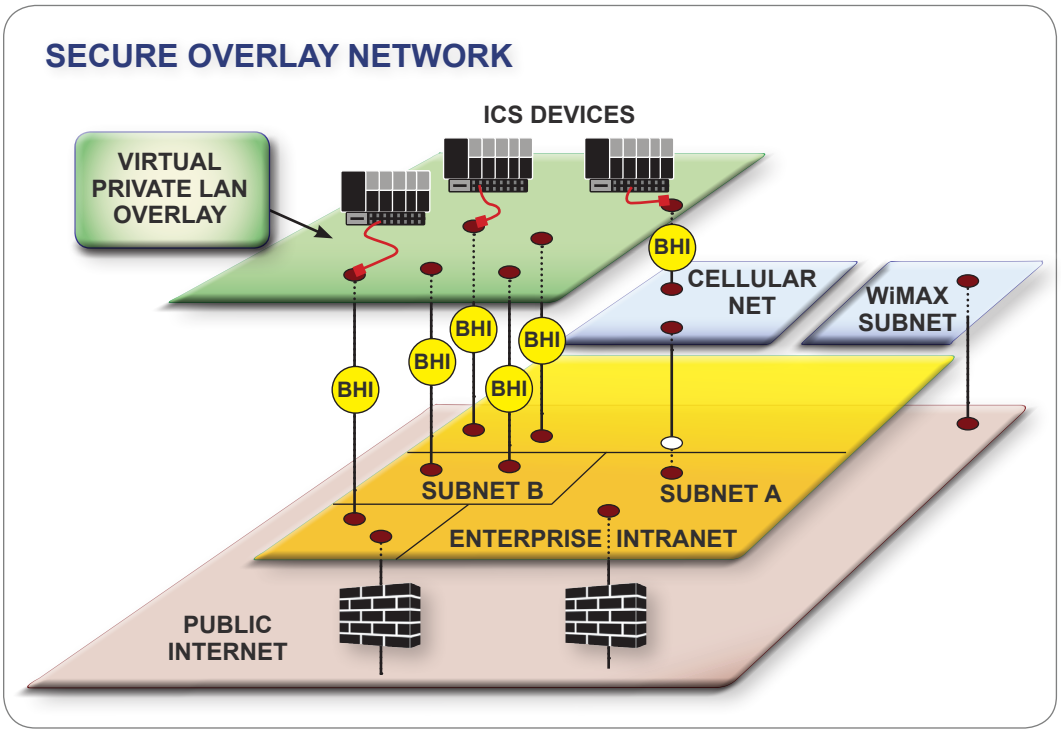

Figure 2: Conceptual diagram of an overlay network for increased network protection.

[1] The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing

Solution Architecture

The “as is” ICS network of a company may exist as a trusted network. With added constructs to perform the protection, SCADA systems can be safely interconnected within a trusted network. However, problems can occur with mobile devices from different paths crossing organization and trust boundaries, or in a dynamic environment where points of connection change, resulting in added complexity to map to physical network ports or requiring mapping in real-time. This easily provides sufficient justification for an alternative methodology.

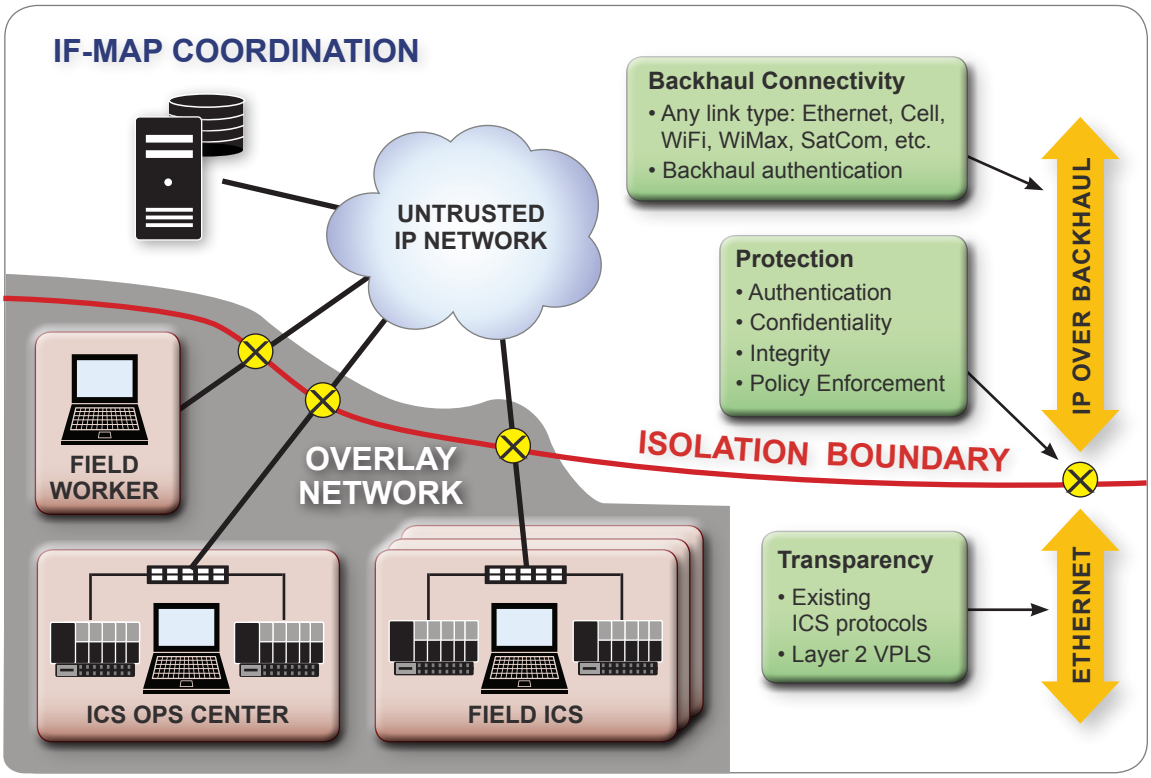

Figure 3: An overlay network architecture that delivers connectivity and protection.

Designed for retrofitting new security functionality into existing industrial control systems as well as incorporating into new ICS products, IF-MAP-based technology creates virtual overlay networks on top of standard shared IP network infrastructure. This approach allows for aggregation and coordinated/controlled response across multiple, frequently remote sites. A specific site can get help from headquarters and from other sites, and headquarters can respond to a common problem at multiple sites. Vendors and contractors can be provided constrained, as-needed access to equipment. There are significant advantages to the overlay approach, particularly when it involves crossing administrative/management boundaries of the networks.

System components include the operator, BHI, overlay network, and ICS devices (such as sensors, actuators, controllers, and supervisory systems such as SCADA systems). Network security policies are orchestrated by IF-MAP using standard metadata. As shown in *Figure 3*, BHIs communicate with each other, and with the environment’s Metadata Access Point (MAP) service, over the backhaul network. Communication between ICS devices occurs through an overlay network that is coordinated and controlled by the BHIs.The encrypted communications include IF-MAP data with the MAP Service over HTTPS/TLS, and virtual private LAN service (VPLS) tunnels from BHI to BHI over host identity protocol (HIP).

IF-MAP provides the capabilities needed for the BHIs to deliver the overlay network functionality, including:

- **Coordination** (including current IP addresses, identity, certificates, etc.) between the BHIs
- **Administrative policy** defining communication between BHIs
- **BHI overlay policies** controlling which ICS devices the BHI allows to communicate across the overlay
- **Administration policies** controlling who is allowed to access and alter the configuration of the overlay network and the BHIs

Case Study

The Boeing Company tackled the complex issue of network visibility and management by control systems and IT experts with TCG's IF-MAP protocol. The implemented solution provides security without the complexity and inflexibility of common VPN solutions.

The assembly of long-range passenger aircraft employs large, highly mobile units called crawlers that have extensive Programmable Logic Controllers (PLC) and Human-Machine Interface (HMI) components. Coordinating the assembly process requires that the PLCs have secure access to each other and to SCADA systems in real time. Additionally, the crawlers need to leverage the corporate wireless infrastructure for their connectivity.

With IF-MAP-based hardware, the IT department can manage non-IT devices on the business network while delegating the control aspects to the ICS team. The ICS devices have network connectivity for control and information-sharing purposes. In contrast to the VPN alternative, the IF-MAP solution results in:

- **Significant cost savings**
- **Significant reliability improvement** by removing the human operator/field worker requirement from the provisioning of the certificates, the enforcement agent, and the actual communications on the network
- **Greater operational simplicity**
- **Improved agility,** since it provides the ability to respond quickly and make required changes
- **Increased flexibility** in the potential decisions
- **Improved delegation of authority,** since the person who is most knowledgeable and responsible for a given set of tools in a factory is able to control those tools

All of this is accomplished without sacrificing security in the control system or the corporate network.

Further details of this solution can be found in the articles "Boeing technology offers secure, efficient way to tie together business, industrial nets"[2] and "*Utilize Open Standards to Protect Control System Networks*"[3].

WHAT IS TRUSTED NETWORK CONNECT?

TCG's Trusted Network Connect (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also enable network-based access control enforcement — granting or blocking access based on authentication, device compliance, and user behavior — and security automation.

TNC provides security automation, Network Access Control (NAC), and interoperability in multi-vendor environments. Products from over two dozen commercial and open source vendors support and help implement TNC standards.

Expanded efforts for enterprise security have resulted in open specifications including the Interface to a Metadata Access Point (IF-MAP). IF-MAP provides a standard way for information security products to rapidly share and respond to information about a variety of security-related topics and events.

Additional TCG resources providing further explanation of IF-MAP include:

Architect's Guide: Security Automation Using TNC & SCAP Technology[4]

TNC IF-MAP[5]

TNC IF-MAP Metadata for Network Security[6]

[2] http://www.networkworld.com/news/2013/042213-boeing-268986.html

[3] http://www.rtcmagazine.com/articles/view/101522

[4] http://www.trustedcomputinggroup.org/resources/tcg_security_automation_architects_guide

[5] http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification

[6] http://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_network_security

Future

IF-MAP-based technology enables implementation of the control system architecture found in the ISA-100 industrial wireless standards, which is aligned with security architectures in ISA/IEC-62443 industrial security standards. With IF-MAP, TCG provides a means to perform that implementation in a standards-based, interoperable manner. ISA is currently exploring the integration of IF-MAP into ISA-100.15 wireless standards and future ISA/IEC-62443 security standards.

Similar to the path of the ISA-99 standards committee's work, ISA-100 will become an IEC specification with global implications. The published ISA-100.15 has been formatted for IEC and is expected to be completed and balloted in 2014.

More broadly, overlay networks apply beyond the ICS arena to environments as diverse as healthcare, financial, automotive, and the Internet of Things. Lessons learned from ICS security advances will be applicable to any ecosystem where protected enclaves are required for security purposes.

Benefits and Value Proposition

With the proper configuration, IF-MAP-based technology allows the IT department to manage access to its services while allowing SCADA and ICS engineers full control over their network systems and devices. This combined capability:

- **Enables secure integration** of ICS and IT networks
- **Reduces cost** of deployment and provisioning of ICS security components
- **Increases agility and flexibility** due to standards-based technology
- **Accommodates legacy infrastructure**
- **Reduces operational cost** of ICS security

Call to Action

- 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, please visit the Trusted Computing Group web site www.trustedcomputinggroup.org.
- Additional information on ICS security will be available over the next several months. Learn about the latest advances by following us on LinkedIn and Twitter.

Contact TCG at admin@trustedcomputinggroup.org with any questions.