Distributed Network Protocol

TRIANGLE MICROWORKS, INC.

SOLUTIONS FOR COMMUNICATION PROTOCOL DEVELOPMENT

Communication Security Measures for SCADA Systems

Ron Farquharson, MV Consulting, DNP User Group

Jim Coats, Triangle MicroWorks, DNP User Group

Joe Stevens, Triangle MicroWorks

23 September 2014, Raleigh, NC

pacworld
PROTECTION, AUTOMATION & CONTROL WORLD CONFERENCE

Agenda

- Recent events and trends
- Utility situation and objectives
- Vulnerabilities, threats and risks
- Government and industry responses/standards
- NIST Framework and Roadmap
  - Identify, Protect, Detect, Respond, Recover
- DHS ICS-CERT (Alerts, Architecture, Assessments, Recommended Practices, References)
- Other documents and standards
- Practical steps

Cybersecurity Means Many Things!

Source: PWC Presentation, August 2014

Recent Events and Trends

Non-Electricity Sector

- Shamoon (malware) - Saudi Aramco (2012) – 30,000+ PCs wiped clean
- "Dark Seoul" (2013) – 20,000+ PCs

Electricity Sector

- ICS-CERT – 257 cyber incidents in 2013 (56% in energy, 22% in electricity sectors)
- Public Utility Compromised (Q1/14)
- Metcalf Substation (April/14)
- MISO Breach (June/14)


ICS-CERT MONITOR

January - April 2014

NCCIC

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

CONTENTS

INCIDENT RESPONSE ACTIVITY

SITUATIONAL AWARENESS

ICS-CERT NEWS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

INCIDENT RESPONSE ACTIVITY

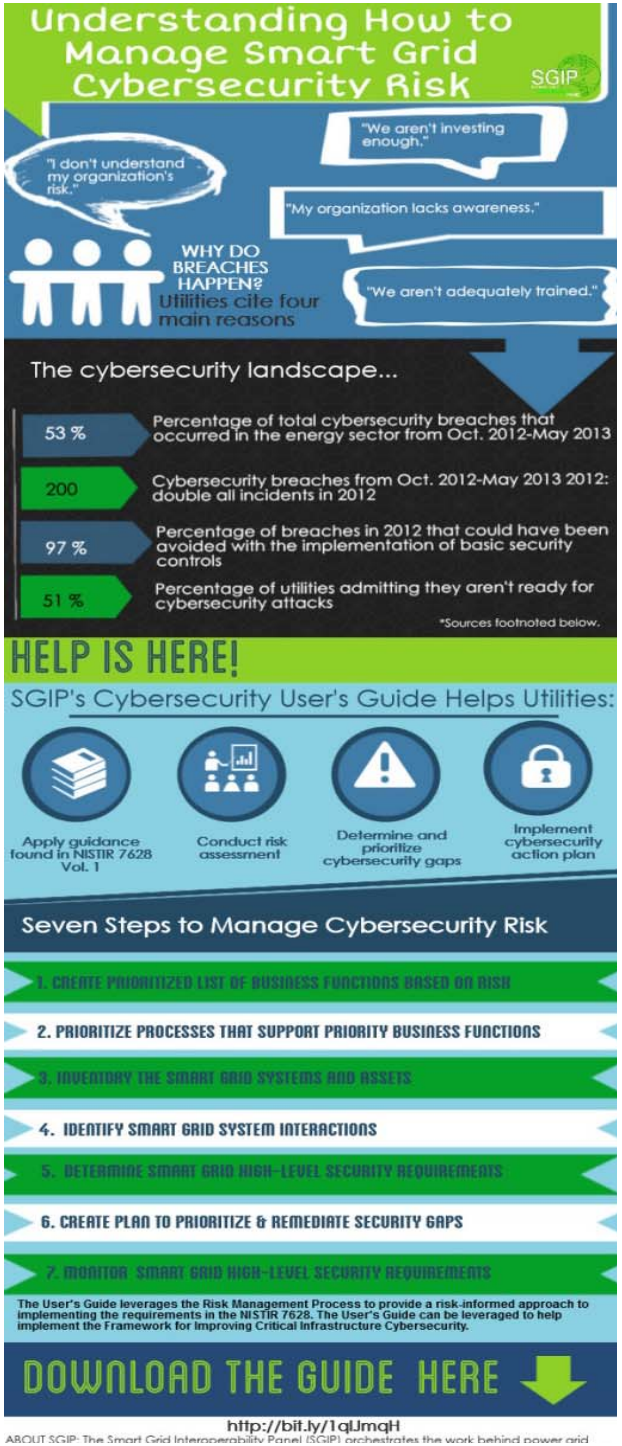
INTERNET ACCESSIBLE CONTROL SYSTEMS AT RISK

pacworld

PROTECTION, AUTOMATION & CONTROL WORLD CONFERENCE

Utility Situation

- SGIP NIST-IR User Guide
- US Congressional report – significant concern regarding electricity sector cyber security
- 44% of energy firms:
  - attack "a certainty" or "highly likely“
  - (attack = APT or targeted malware attack) in next 12 months.



Source: SGIP Smart Grid Cybersecurity Committee (SGCC) NIST-IR 7628 User Guide – Infographic, February 2014

Cybersecurity Objectives

- Protection, deterrence and delay
  - Availability
  - Integrity
  - Confidentiality
  - Non-repudiation

- Detection of attacks
- Logging and assessment of attacks
- Communication and notification
- Response to and recovery from attacks

Vulnerabilities, Threats and Risks

- Threats and Risks:
  - Cyber attacks
  - Physical attacks
  - Deliberate attack (internal/external)
  - Inadvertent error
  - Equipment failure
  - Natural disasters

Vulnerabilities, Threats and Risks

- Vulnerabilities (attack vectors)
  - Web app attacks
  - Email phishing
  - Authentication failures
  - Poorly written driver code (vulnerable to fuzzing)

Vulnerabilities, Threats and Risks

Threat examples:

- Example Threat- Havex Trojan (RAT*) Malware
- Kragany Trojan Malware
- MiniDuke Implant
- Blackshades Malware
- GameOverZeus Botnet

(*) RAT = Remote Access Tool/Trojan. Supports “ICS Sniffing”. Allows attackers to upload and download files, run executable files, collect passwords, take screenshots and catalog documents.

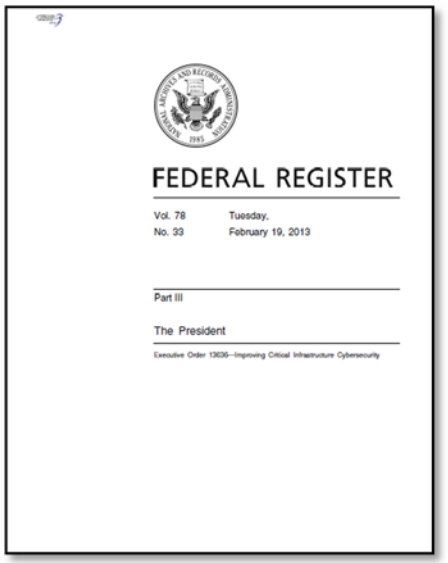
Image Credits: The Quinton Report and The Dragonfly Woman

Vulnerabilities, Threats and Risks

- Threat examples continued:
  - Insiders, organized crime
  - APT – Advanced Persistent Threat
  - "Hacktivists" greatest perceived threat to energy firms
- Threat Groups/Actors examples:
  - Dragonfly (discovered 6/14)
  - Energetic Bear
  - Crouching Yeti
- Campaign: a specific threat by an actor or group

Gov't & Industry Responses/Standards

- Executive Order 13636 - "Improving Critical Infrastructure Cybersecurity"
- Early 2014: President Obama; "cyber-threats pose one of the gravest national-security dangers……"
- FERC Chair quote
- NIST
- DHS ICS-CERT
- NERC, DOE
- SGIP, SGCC
- IEEE, IEC


FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

NIST Framework and Roadmap

- Response to the 2013 Executive Order
- Published in Feb. 2014
- Focus is on business drivers to guide CS activities
- Considers CS risks, part of overall risk management processes
- Three primary components:
  - Profile – Current and Target
  - Implementation Tiers
  - Core (five functions)

NIST Framework and Roadmap

Profile

- Current profile - created by evaluating existing capabilities based on the Core recommended practices:
  - Processes, procedures, technologies, alignment, risk assessment, access control, training, data security, event logging and analysis and incident response.
- Target profile – envisioned future capabilities based on above practices

NIST Framework and Roadmap

Implementation Tiers

Tier	Type	Description
1	Partial	Risk management is informal (ad hoc) with limited awareness of risks, limited sharing of CS information, no coordination with other entities
2	Risk Informed	Risk management processes/programs exist but are not implemented organization-wide; awareness of risks, informal sharing of CS information, limited external coordination
3	Repeatable	Formal risk management processes/programs exist enterprise-wide, with partial external coordination
4	Adaptive	Risk-management processes/programs are based on lessons learned and a part of the culture, proactive external coordination

NIST Framework and Roadmap

Framework Core

NIST Framework and Roadmap

Core – Functions

- Identify
  - Asset Management; Business Environment Governance; Risk Assessment; and Risk Management Strategy.
- Protect
  - Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

NIST Framework and Roadmap

Core – Functions

- Detect
  - Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- Respond
  - Response Planning; Communications; Analysis; Mitigation; and Improvements.
- Recover
  - Recovery Planning; Improvements; and Communications.

NIST Framework and Roadmap

Using the Framework to Create or Improve a CS Program:

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze, and Prioritize Gaps
7. Implement Action Plan
8. “Repeat as necessary”

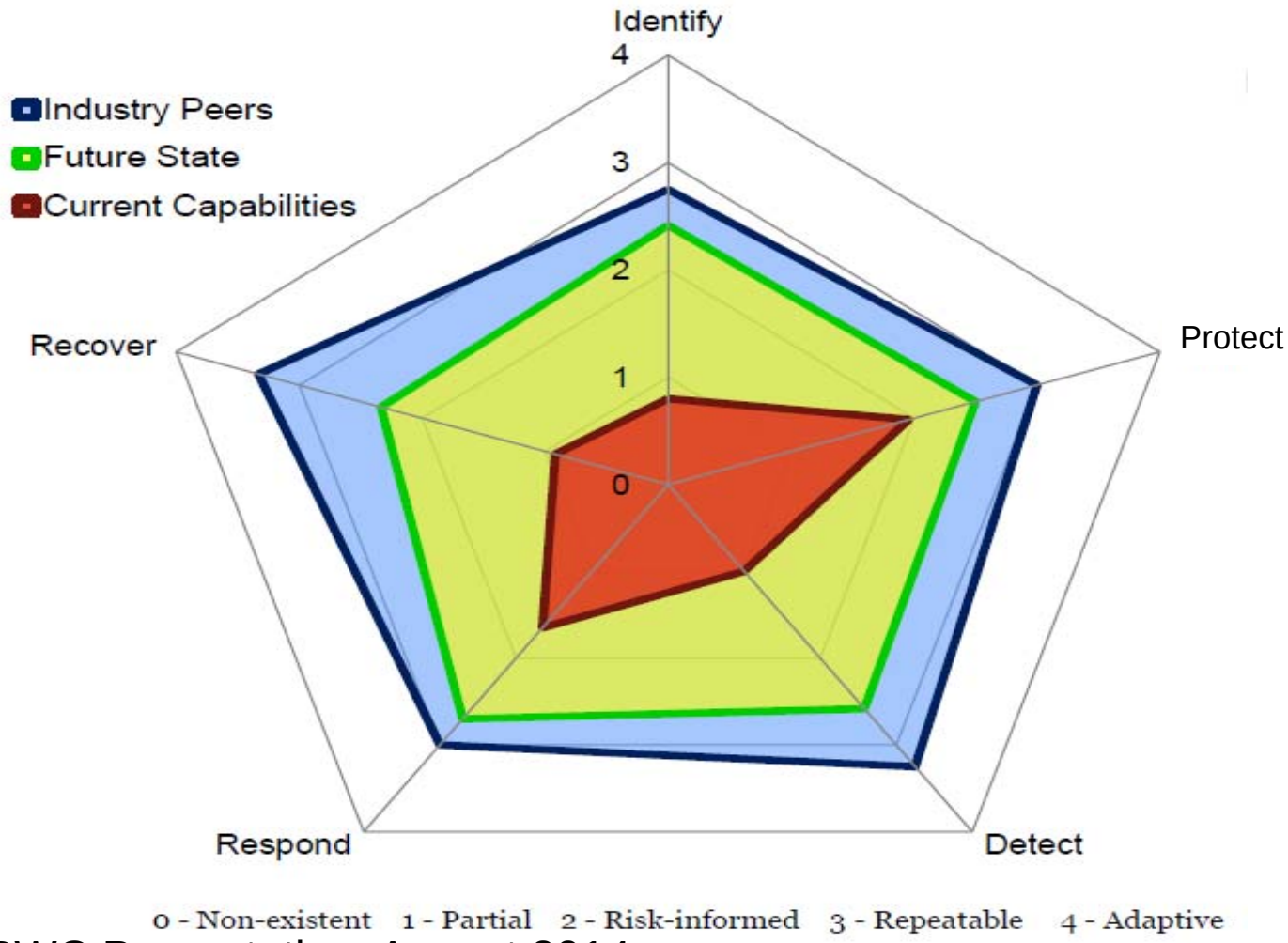
NIST Framework and Roadmap

Also consider.....

- Start with senior support
- Align with business needs/objectives
- The Framework establishes a common nomenclature for sharing CS information
- External collaboration is a essential. Participate in an Information Sharing and Analysis Center (ISAC) or equivalent

NIST Framework and Roadmap

Current, Target, Industry Profiles



Source: PWC Presentation, August 2014

DHS ICS-CERT

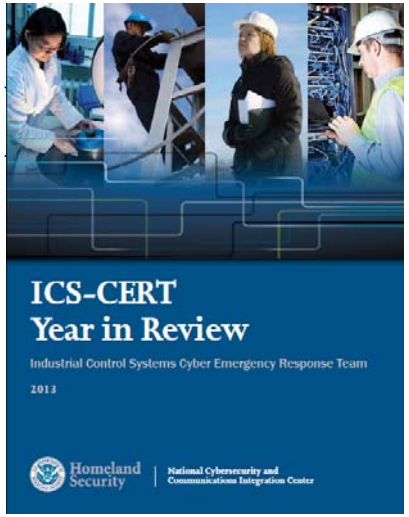
ICS-CERT – four focus areas:

1. Situational awareness for stakeholders
2. Control systems incident response and technical analysis,
3. Control systems vulnerability coordination
4. Strengthening cybersecurity partnerships with government

DHS ICS-CERT

Services provided:

- Incident response
- Alerts, Advisories, Monitor, JSARs
  - JSAR = Joint Security Awareness Reports
- Recommended Practices
  - Threats, vulnerabilities, attack vectors
  - Secure Architecture
- ICSJWG (ICS JointWorkingGroup
- Training
- Assessments (tool)
- Technical references



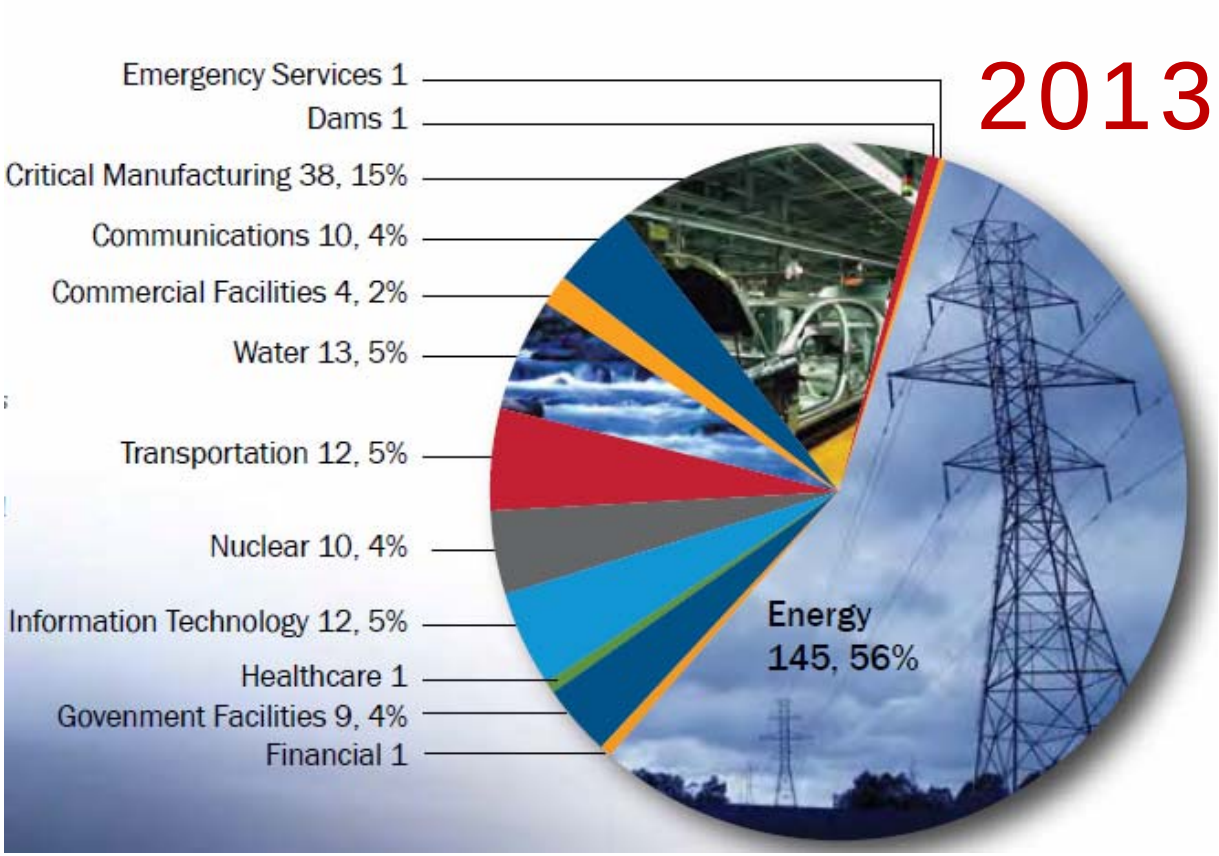
Source: ICS-CERT Year in Review - 2013

DHS ICS-CERT

Total Responses = 257

Energy Sector: = 145 (56%)

Electricity Sector: = 56 (22%)



Incident Response = core service, focus is cyber events that could impact control system operations. ICS-CERT assists with vector ID, extent of compromise, mitigation strategy & recovery. Service may be on-site or remote from Idaho. (DHS External Affairs, Sept. 23, 2014)

Source: ICS-CERT Year in Review - 2013

DHS - National Preparedness

I. Prevention – Engaged Partnership

WHAT: The capabilities necessary to avoid, prevent, or stop a threatened or actual act or terrorism

HOW: Industrial Control Systems Joint Working Group | Outreach

II. Protection – Tiered Protection

WHAT: The capabilities necessary to secure critical infrastructure in the homeland against acts of terrorism and manmade or natural disasters

HOW: Training | Cyber Security Evaluation Tool (CSET®)

III. Mitigation – Scalable, Flexible and Adaptable Capabilities

WHAT: The capabilities necessary to reduce loss of life and property by lessoning the impact of the cyber attack

HOW: Incident Response, Vulnerability Handling | Advanced Analytical Laboratory

IV. Response – Unity of Effort Through Unified Command

WHAT: The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after a cyber incident has occurred

HOW: US Computer Emergency Readiness Team (US-CERT) | Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

HOW: National Coordinating Center for Telecommunications (NCC) | National Cybersecurity and Communications Integration Center (NCCIC) Operations | Industrial Control System Consequence and Effects Analysis (ICS-CEA)

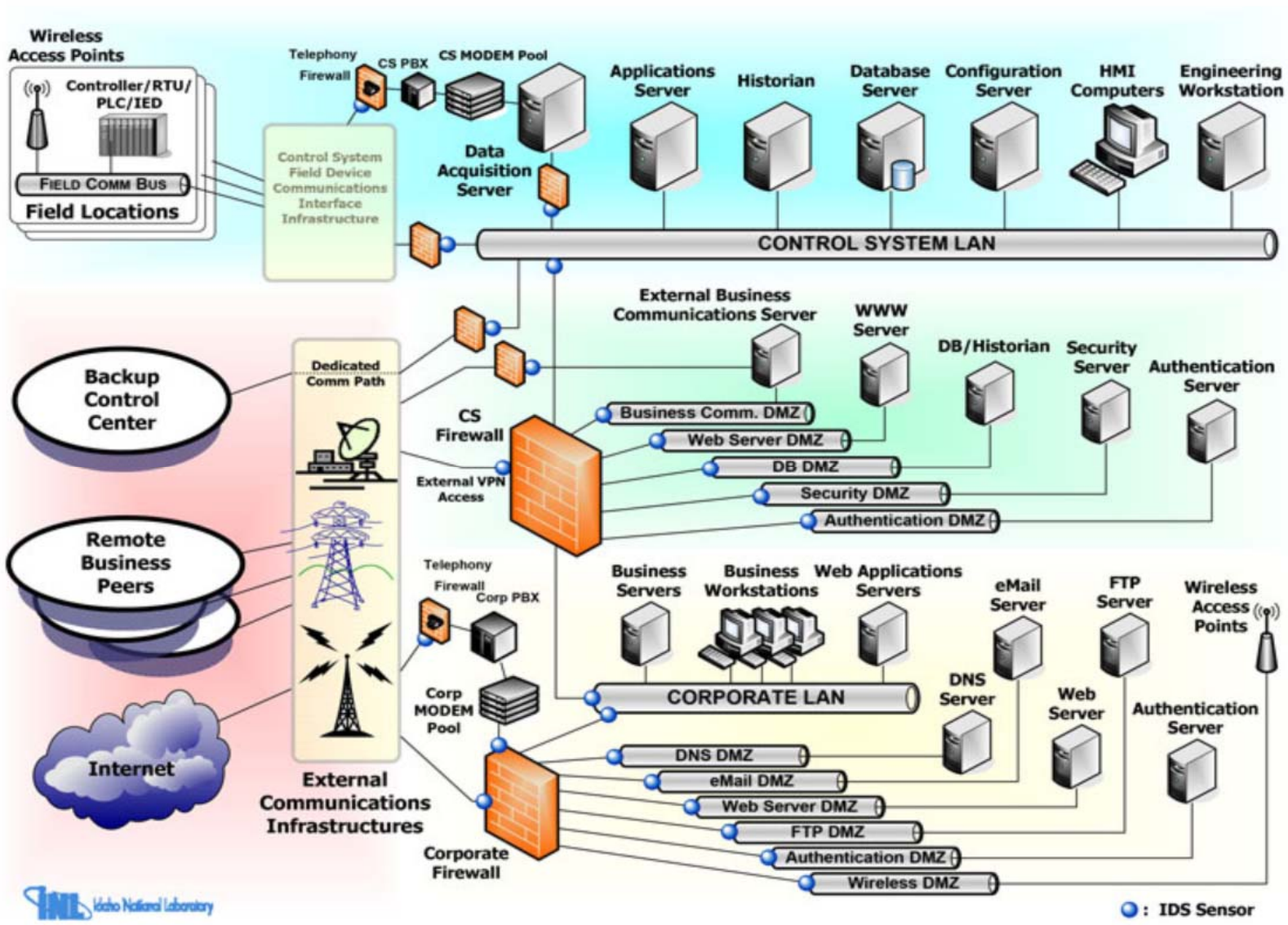
V. Recovery – Applies Advanced Capabilities to Support Recovery

WHAT: The capabilities necessary to assist communities affected by an incident to recovery effectively

HOW: Cybersecurity Assessments | Evaluations and Architecture Reviews

Source: ICS-CERT Year in Review - 2013

ICS-CERT Secure Architecture Design



Source: DHS ICS-CERT: https://ics-cert.us-cert.gov/Secure-Architecture-Design

Other Documents and Standards

Key Cybersecurity Documents:

- NERC CIP documents (compliance standards)
- SGIP NIST-IR User Guide, Framework Mapping to NIST-IR, NIST-IR 7628
- DHS Defense in Depth
- DOE documents (Risk Management, Maturity Model, Procurement Language)

Standards:

- ISO 27001
- IEEE 1815-2012 (DNP3) – Secure Authentication
- IEC 62351
- IEEE 1686, 1711
- NIST SP 800

pacworld
PROTECTION, AUTOMATION & CONTROL WORLD CONFERENCE

IEEE 1815-2012 (DNP3) – Secure Authentication (Version 5)

- Defined in IEEE Std 1815-2012 (DNP3) protocol
- SA authenticates the sender of the message
- Detects whether the message has been modified
- Does NOT encrypt data
- Co-developed with IEC 62351 Part 5
- Minimizes processor, bandwidth impact
- Based on NIST-approved cryptography
  - Although it still permits some deprecated algorithms
- Standardized by UK Water Industry (UK-WITS)
- **EPRI funded demonstration testing underway**

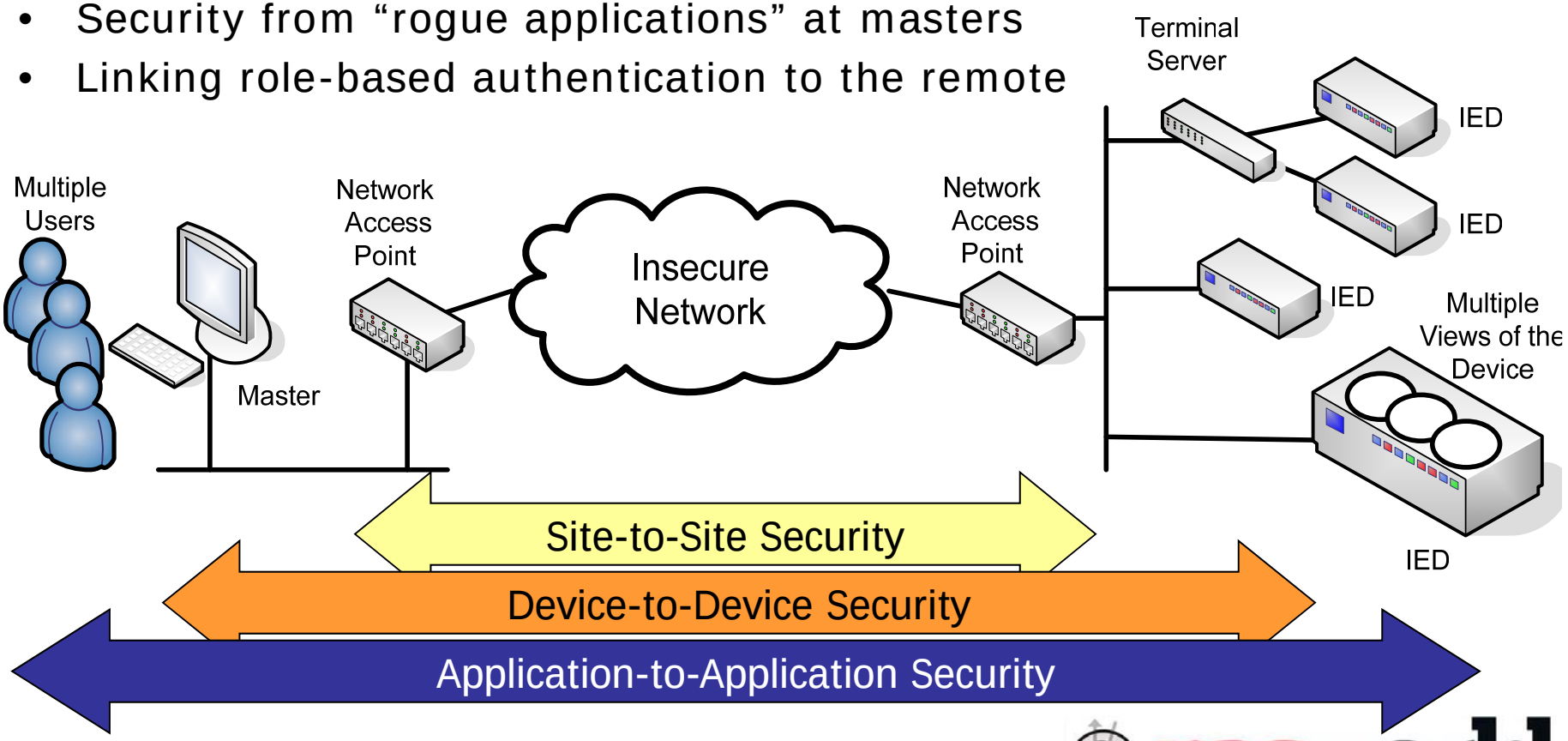
dnp Distributed Network Protocol

pacworld PROTECTION, AUTOMATION & CONTROL WORLD CONFERENCE

Why use IEEE 1815 (DNP3)-SA?

VPN Routers, link encryptors, etc. don't address:

- Security at the local site
- Security of serial DNP over unencrypted radios
- Security of serial DNP over terminal servers
- Security from "rogue applications" at masters
- Linking role-based authentication to the remote



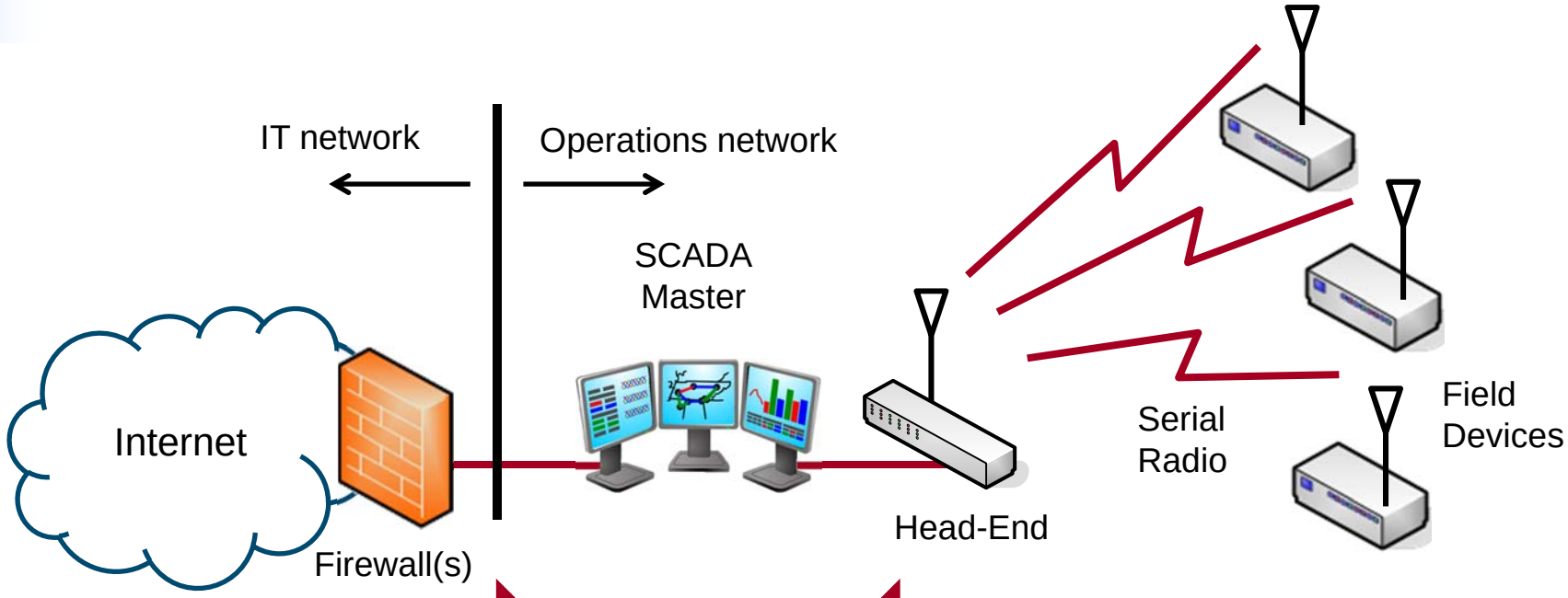
SCADA Security News

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Several ICS-CERT Advisories on Improper Input Validation (http://ics-cert.us-cert.gov/advisories/), e.g.:
  - ICSA-13-276-01
    - Parsing of XML data from one particular vendor
  - ICSA-13-329-01
    - Parsing of Modbus in another vendor
  - ICSA-13-291-01A
    - Parsing of DNP3 (Summarizes issues with 11 products, with about 11 more still to come)

Note: These advisories were issued on the basis of a vulnerability and present a potential or perceived threat. NO actual incidences have been recorded.

DNP3 Software Vulnerabilities Context



A. Commonly expected direction of attack

B. Direction of newly discovered vulnerabilities

C. This direction of attack has always been possible

Note: Input “fuzz” vulnerability is a perceived threat
That could result in a Denial of Service attack.
NO actual incidences have been recorded.

Source: Andrew West, DNP Technical Committee Chair

DNP User Group (Tech Committee) Response

DNP Technical Committee has produced guidelines

- AN2013-004 Validation of Incoming DNP3 Data
  - Provides guidance on secure software development
  - Provides guidelines for testing that can be performed by developers, end users & cyber security researchers
- AN2014-001 Disabling Application Layer Function Codes
- AN2014-002 Secure Management of DNP3 Configuration Parameters
- Ongoing work
  - Guidelines on how to secure field networks

Note: These advisories were issued on the basis of a vulnerability and present a potential or perceived threat. NO actual incidences have been recorded.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Practical steps - 1

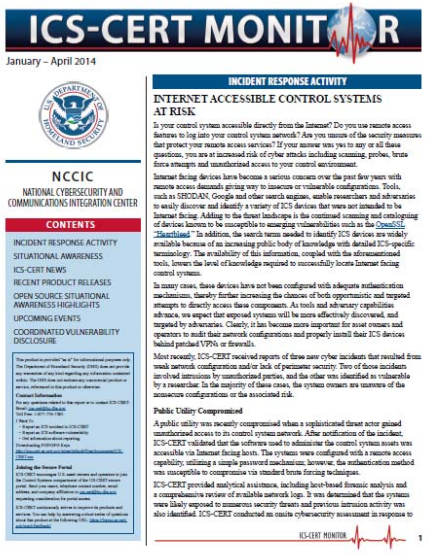
- Employee awareness and training
- Policy development and updating
- Implement the NIST CS Framework
- Establish external collaboration
  - Seek and share information such as IoCs
  - Seek out sources of information such as SCADASec email distribution
  - Access existing information sources such as ICS-CERT Information products (Advisories, Alerts, Monitor etc.)

Practical steps - 2

- Software/firmware patches/device upgrades (firewall priority not IEDs)
- Robust device & master configurations
  - Disable unused serial and network ports
  - Disable protocol functions not used
  - Disable protocols not used
- Robust IP network configurations
- SCADA protocol-aware network tools
- Assessment, penetration and vulnerability testing
- Procurement practices

Practical steps - 3

- Architect a network with standard defenses such as Firewalls, DMZs, and detection/prevention sensors.
- Add a capability to actively hunt for Indicators of Compromise (IoC)
- Adopt formats such as YARA, OpenIoC, TAXII, STIX (eg. ICS-ISAC may host IoCs in STIX format)


ICS-CERT MONITOR

January – April 2014

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

CONTENTS

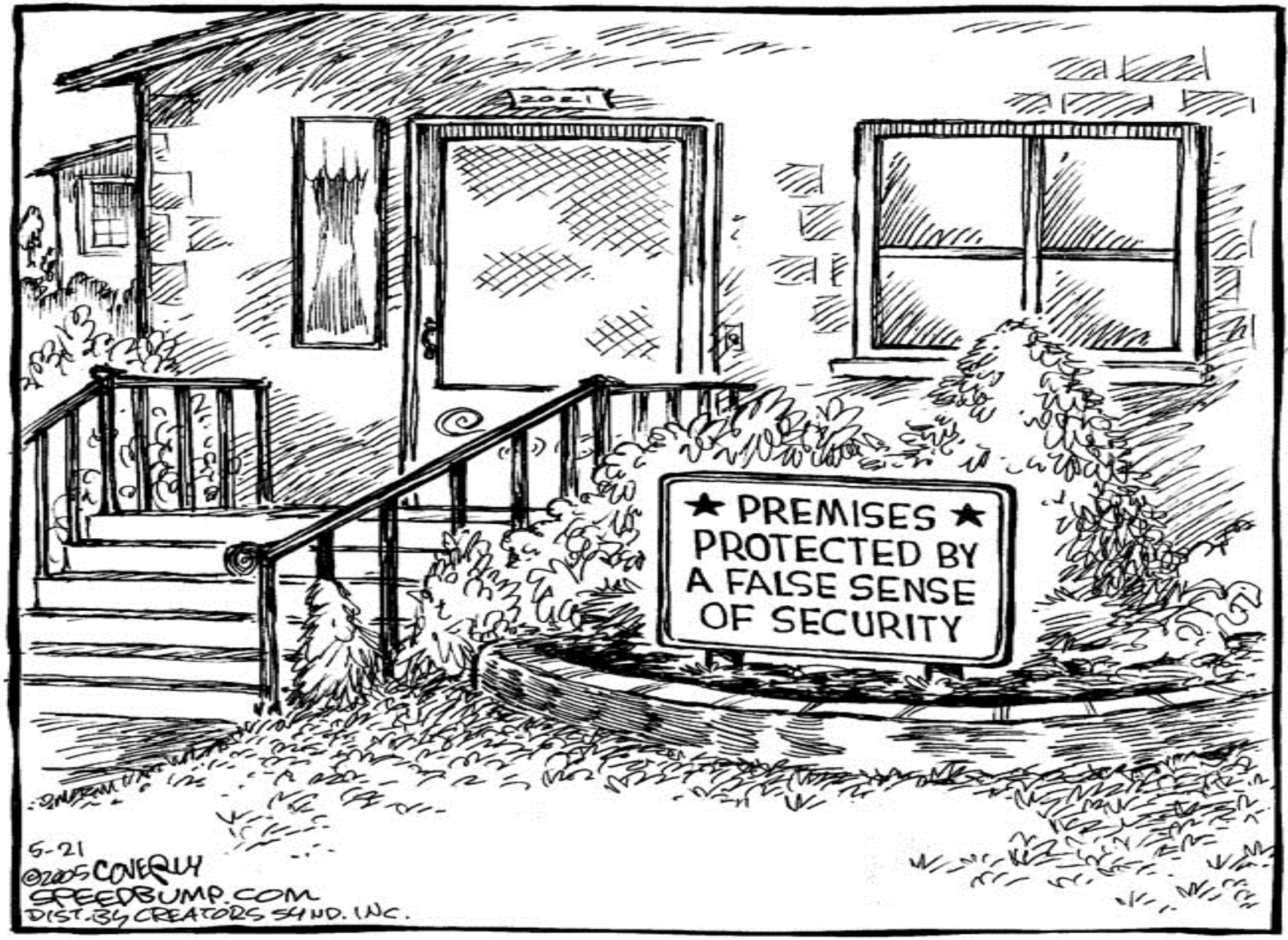
INCIDENT RESPONSE ACTIVITY
SITUATIONAL AWARENESS
ICS-CERT NEWS
RECENT PRODUCT RELEASES
OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS
UPCOMING EVENTS
COORDINATED VULNERABILITY DISCLOSURE

INCIDENT RESPONSE ACTIVITY

INTERNET ACCESSIBLE CONTROL SYSTEMS AT RISK

Public Utility Compromised

Speed Bump



Hack a Tesla Model S and Win $10,000!!

Calling all computer hackers: A Beijing security conference is offering $10,000 to the first person who successfully hacks into a Tesla Model S.

Organizers of the Symposium on Security for Asia Network (SyScan) will set up a Tesla Model S and some computers on July 16 and 17 and are inviting conference participants to crack the code of the high-tech car. The goal of the competition, according to the conference website, is to test the software safety of premium electric vehicle.

http://www.theglobeandmail.com/globe-drive/news/trans-canada-highway/hack-a-tesla-model-s-win-10000/article19578723/

Source: Globe and Mail, July 13, 2014

pacworld
PROTECTION, AUTOMATION & CONTROL WORLD CONFERENCE

Distributed Network Protocol

TRIANGLE MICROWORKS, INC.

SOLUTIONS FOR COMMUNICATION PROTOCOL DEVELOPMENT

Communication Security Measures for SCADA Systems

Ron Farquharson, r.farquharson@ieee.org

Jim Coats, jcoats@trianglemicroworks.com

Joe Stevens, jstevens@trianglemicroworks.com

pacworld PROTECTION, AUTOMATION & CONTROL WORLD CONFERENCE

Back up Material

Situational Awareness – ICS – ISAC - SARA

- Industrial Control Systems, Information Sharing and Analysis Center, Situational Awareness (SA) Reference Architecture
- Components of SA:
  - Identity; Inventory; Activity; Sharing.