SIS TECH

# Cyber Security for SCAI

- Eloise Roche, Senior SCAI Consultant
- Libero Corvaglia, SCAI Advisor

# Eloise Roche
# Senior SCAI Consultant
# SIS-TECH Solutions

- 24 years Chemical Industry background, largely in automation and functional safety management
- Specializes in Safety Controls, Alarms, and Interlocks (SCAI)
- Member of ISA-84 committee and multiple working groups
- Subcommittee Member for revision of “Guidelines for Safe Automation of Chemical Processes”
- Certified Functional Safety Expert

# Cyber Security for SCAI

- Eloise Roche, Senior SCAI Consultant
- Libero Corvaglia, SCAI Advisor

# Copyright and Disclaimer

SIS-TECH SOLUTIONS ASSUMES NO LIABILITY FOR THIS MATERIAL BEYOND THE INTENDED PURPOSE OF INTRODUCING PARTICIPANTS TO CYBER SECURITY FOR SAFETY CONTROLS, ALARMS, AND INTERLOCKS.

Angela Summers, Ph.D., P.E.
President
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120
Houston, TX  77034

281-922-8324 (phone)
281-922-4362 (fax)
asummers@sis-tech.com

# Table of Contents

- Key terms and concepts
- High level introduction to essential standards and technical guidelines for SCAI Cyber Security
- Cyber for IT ≠ Cyber for IACS
- Example IACS Architectures
- Closing Remarks

# Glossary of Acronyms and Abbreviations

COTS : Commercial Off The Shelf

DoS : Denial of Service

DMZ : “Demilitarized Zone” (colloquial term in this context)

**HMI : Human Machine Interface (e.g., operating workstation)**

**IACS : Industrial Automation and Control System**

IEC : International Electrotechnical Commission

ISA : International Society for Automation

**IT : Information Technology**

NIST : National Institute of Standards and Technology

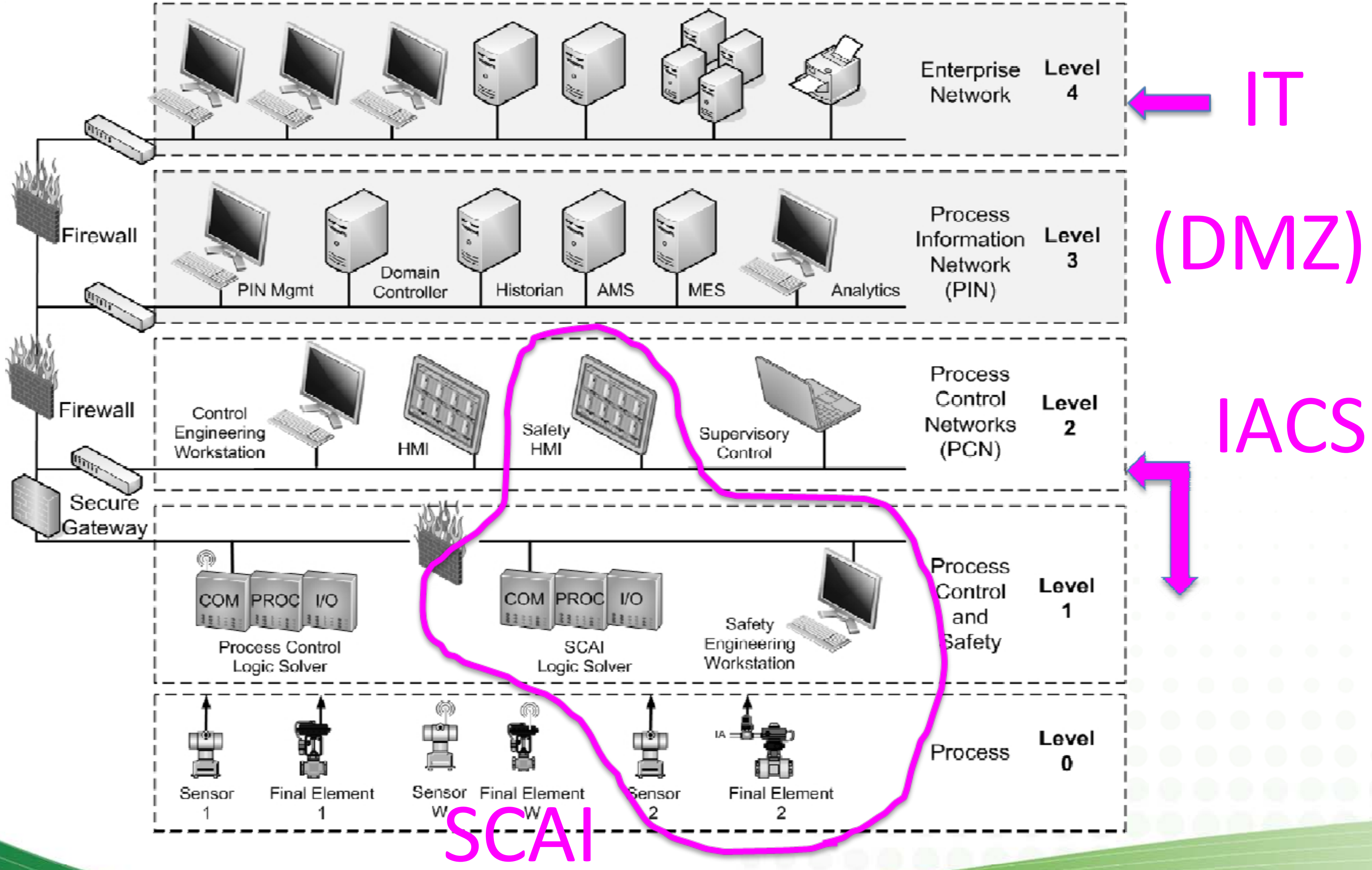
RAGAGEP : Recognized And Generally Accepted Good Engineering Practice

**SCAI : Safety Control, Alarms, and Interlocks**

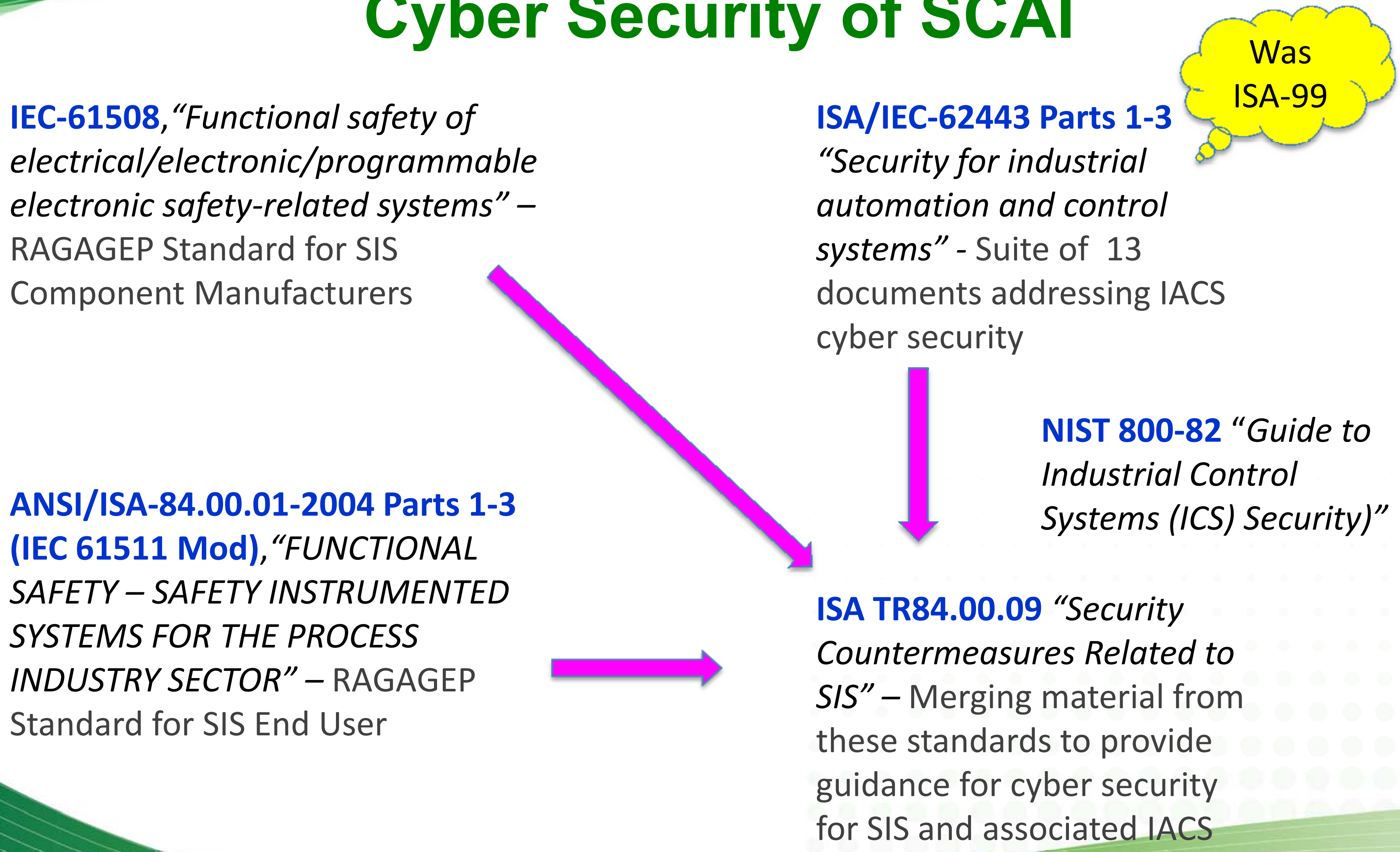
**SIS : Safety Instrumented Systems (subset of SCAI)**

# Overall Automation Network Showing Hierarchical Levels

[Figure 3.8 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]



# Key Standards related to Cyber Security of SCAI



**IEC-61508**,*"Functional safety of electrical/electronic/programmable electronic safety-related systems"* – RAGAGEP Standard for SIS Component Manufacturers

**ISA/IEC-62443 Parts 1-3** *"Security for industrial automation and control systems"* - Suite of 13 documents addressing IACS cyber security

Was ISA-99

**NIST 800-82** *"Guide to Industrial Control Systems (ICS) Security)"*

**ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod)**,*"FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR"* – RAGAGEP Standard for SIS End User

**ISA TR84.00.09** *"Security Countermeasures Related to SIS"* – Merging material from these standards to provide guidance for cyber security for SIS and associated IACS

# Cyber for IT ≠ Cyber for IACS
# Concerns of Defender

| Priority for IT Defense: | Priority for IACS Defense: |
|---|---|
| Accessibility | Data Integrity |
| Data Confidentiality | Accessibility |
| . | . |
| . | . |
| . | . |
| . | . |
| Data Integrity | Data Confidentiality |

# Cyber for IT ≠ Cyber for IACS Likely Objective of Intentional Attacker/Consequences of Attack

Intentional Attack on IT Systems (i.e., Enterprise Network):

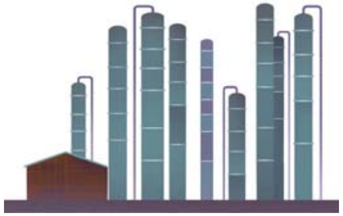
Theft of Confidential or Proprietary Information

Business Disruption (e.g., DoS)

$

Intentional Attack on IACS Systems (i.e., levels 0-2):

Cause of Harm to …



Physical Assets

Personnel

Environment

Reputation/License to Operate

$ $ $

# Cyber for IT ≠ Cyber for IACS Level of Skill Required to Attack an *Unprotected* System

## IT Systems (i.e., Enterprise Network):

Low to no skill needed

Necessary tools and tutorials are publically available

**Past Beliefs:**

Security Through Obscurity

Proprietary controller technologies make it impossible (or prohibitively expensive) to attack IACS

SCAI systems are physically separated  from the process control network

## IACS Systems (i.e., levels 0-2):

It depends…

**Present Realities:**

More IACS components are using COTS hardware and operating system software

Newer commercial SCAI designed to network easily – driven by end user desire to have seamless access to information through mobile technology

Training on common controller systems (and associated malware) readily available to public

Cyberattacks are now BIG BUSINESS

# Cyber for IT ≠ Cyber for IACS Differences in Countermeasures and Recovery From Attack

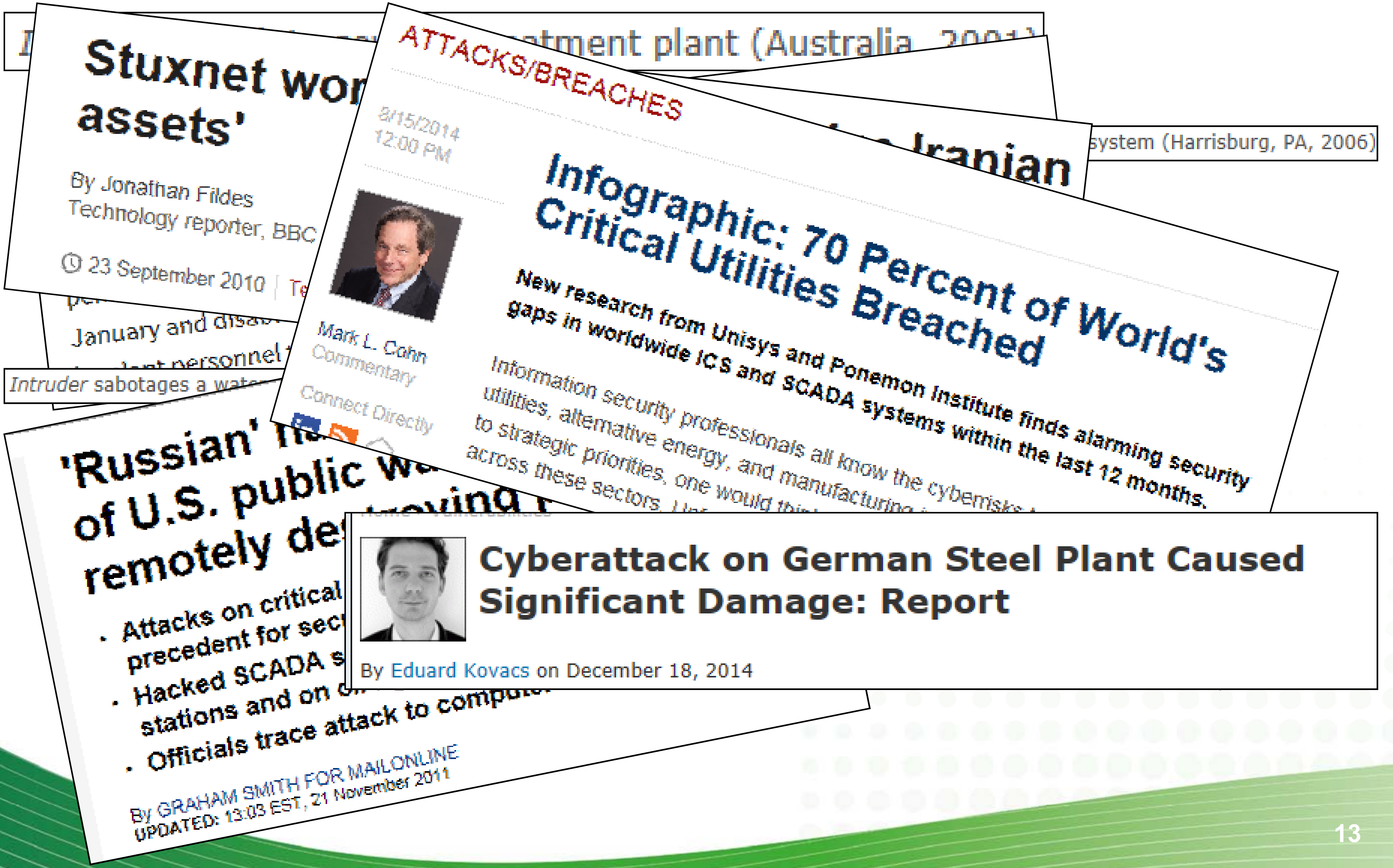
IT Systems (i.e., Enterprise Network):

- Frequent patching (resolve application incompatibility issues later)
- When in doubt…REBOOT
- When rebooting doesn’t work, reload the backup

IACS Systems (i.e., levels 0-2):

- Countermeasures cannot threaten IACS system availability (CONTROL MUST GO ON)
- NO REBOOTING!!! (at least while the process is operating)
- Can’t simply “reload” damaged equipment or injured personnel

# IS THIS REAL???



I... atment plant (Australia, 2001)

Stuxnet wor... assets'

By Jonathan Fildes
Technology reporter, BBC

23 September 2010 | Te

... Iranian

system (Harrisburg, PA, 2006)

pe...
January and disa...
plant personnel ...

Intruder sabotages a wat...

ATTACKS/BREACHES

8/15/2014
12:00 PM

Mark L. Cohn
Commentary

Connect Directly

## Infographic: 70 Percent of World's Critical Utilities Breached

**New research from Unisys and Ponemon Institute finds alarming security gaps in worldwide ICS and SCADA systems within the last 12 months.**

Information security professionals all know the cyberisks ... utilities, alternative energy, and manufacturing ... to strategic priorities, one would thin... across these sectors. Un...

'Russian' ha... of U.S. public wa... remotely des...

- Attacks on critical ... precedent for sec...
- Hacked SCADA s... stations and on o...
- Officials trace attack to comput...

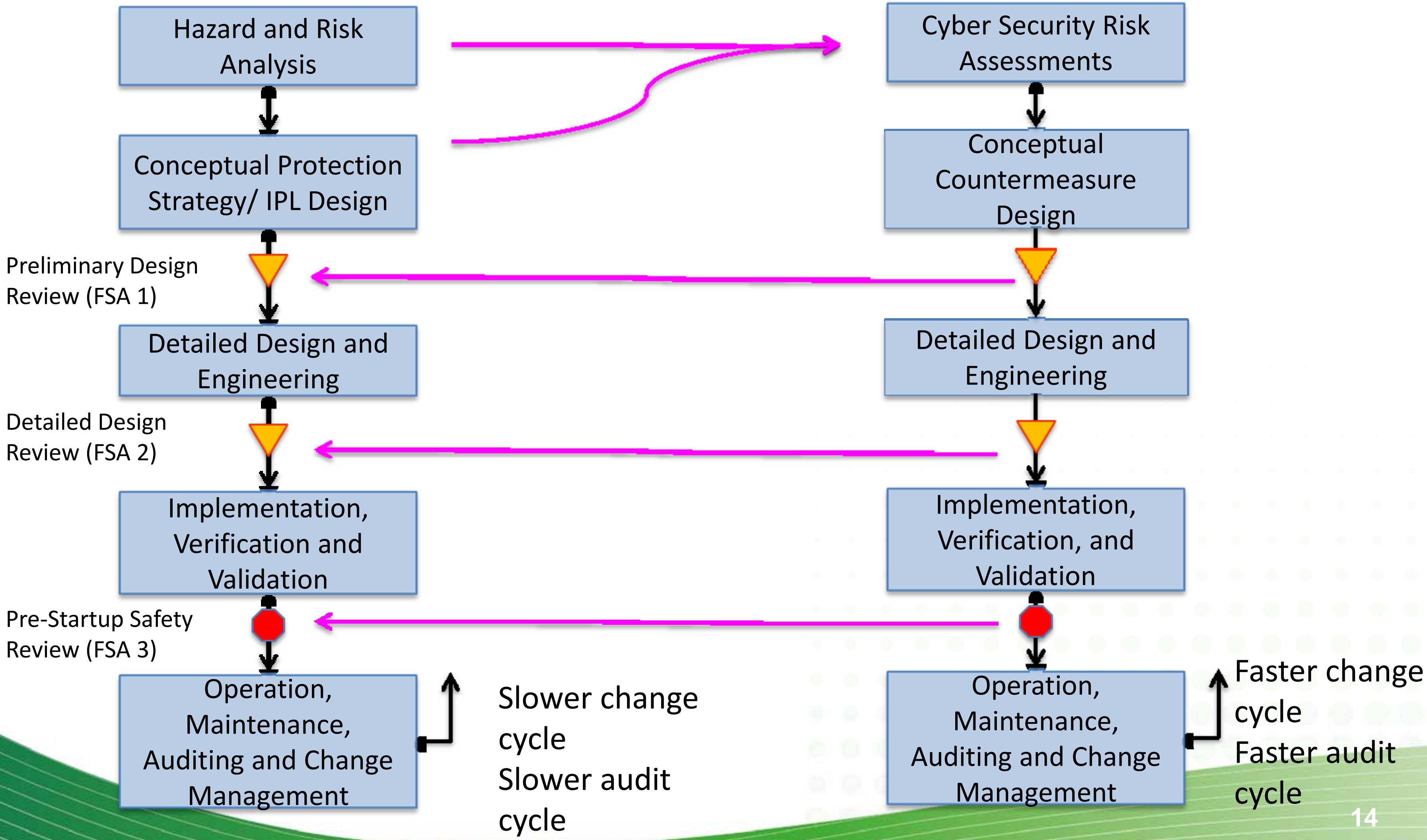
By GRAHAM SMITH FOR MAILONLINE
UPDATED: 13:03 EST, 21 November 2011

## Cyberattack on German Steel Plant Caused Significant Damage: Report

By Eduard Kovacs on December 18, 2014

# Safety Lifecycle (SCAI)

# IACS Cyber Security work process



Hazard and Risk Analysis

Conceptual Protection Strategy/ IPL Design

Preliminary Design Review (FSA 1)

Detailed Design and Engineering

Detailed Design Review (FSA 2)

Implementation, Verification and Validation

Pre-Startup Safety Review (FSA 3)

Operation, Maintenance, Auditing and Change Management

Slower change cycle
Slower audit cycle

Cyber Security Risk Assessments

Conceptual Countermeasure Design

Detailed Design and Engineering

Implementation, Verification, and Validation

Operation, Maintenance, Auditing and Change Management

Faster change cycle
Faster audit cycle

# Cyber Security is a Moving Target

- SCAI functional effectiveness degrades due to entropy and neglect
  - Well known causes and solutions

- SCAI Cyber Countermeasure effectiveness is constantly subject to active erosion
  - "Black hats" actively inventing new attack mechanisms
  - IACS technology changes create new vulnerabilities daily

# Foundational Requirements and Levels of IACS Cyber Security

SEVEN Foundational Requirements:

- Identification and authentication control (IAC)
- Use control (UC )
- System integrity (SI)
- Data confidentiality (DC)
- Restricted data flow (RDF)
- Timely response to events (TRE)
- Resource availability (RA)

Example Cyber Security Target Vector:

SL-T (SCAI zone) = {3 3 2 0 3 1 4}

Security Levels:

0 – no security protection necessary

1 – protection against casual or coincidental violation

2 – protection against intentional violation with simple means, low resources, generic skills, and low motivation

3 – … sophisticated means, moderate resources, IACS specific skills, and moderate motivation

4 – … sophisticated means, extended resources, IACS specific skills, and high motivation

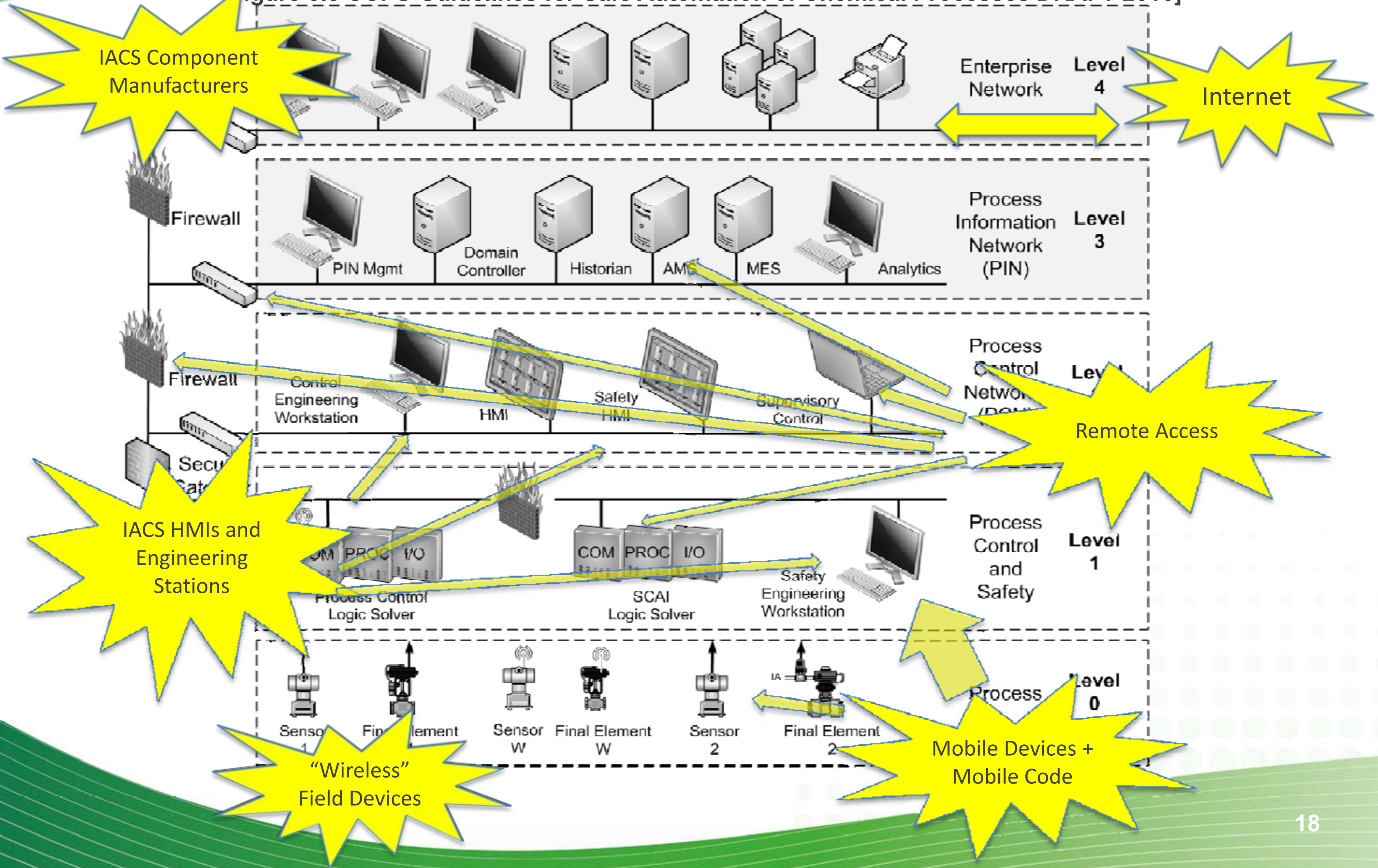
# TR84.09 SCAI Cyber Attack Threat Sources

- Malicious Hacker
- (Authorized) Third Party Contractor (e.g., remote support contracts)
- Well-meaning Insider
- Malicious Insider (i.e., intentional sabotage)

Some attacks can involve a combination of sources (e.g., a well-meaning insider inserting mobile data device infected with mobile data written by malicious hacker)

# TR84.09 SCAI Cyber Attack Vectors

[Figure 3.8 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]



# Cyber Security Countermeasures

Network Firewalls

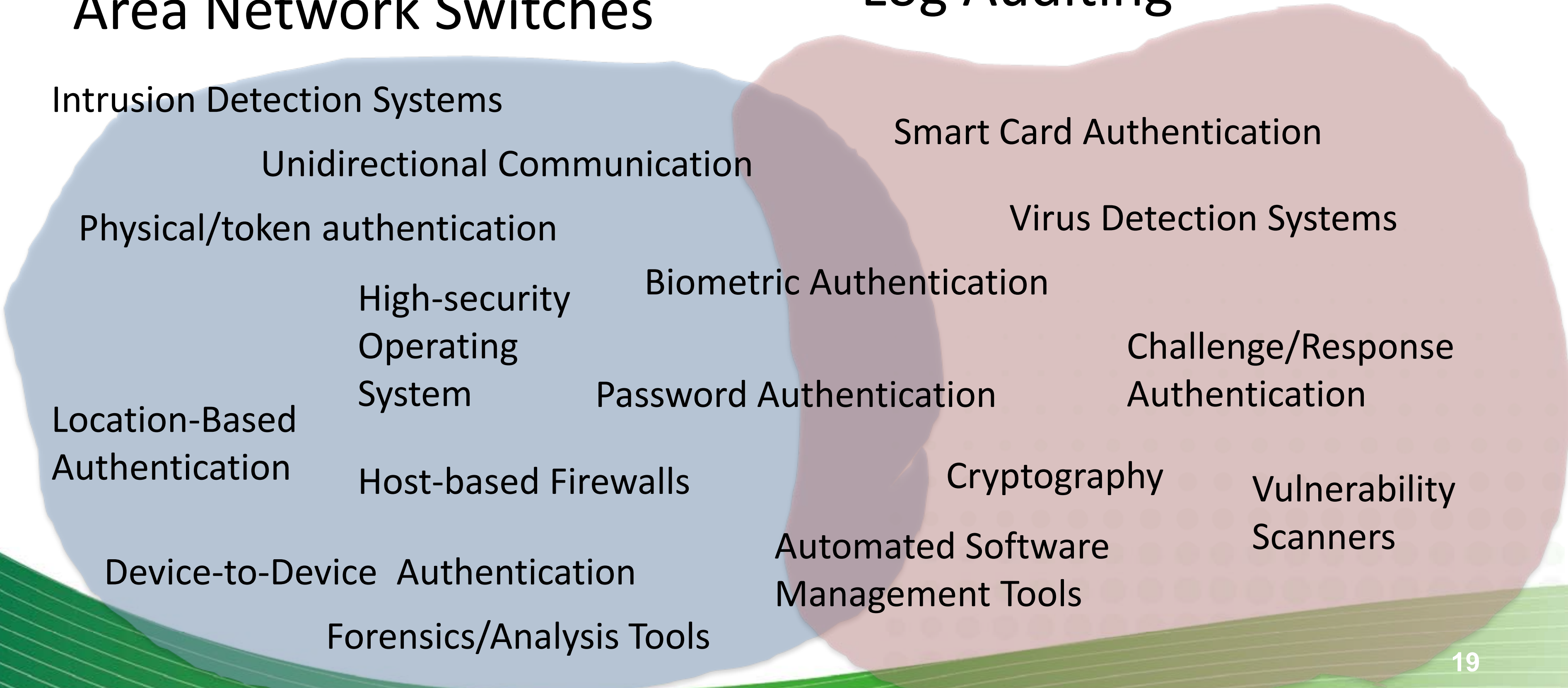
Physical Security Control

Disabling Unused Ports/Apps/Features

Personnel Security Controls

Log Auditing

Area Network Switches



Intrusion Detection Systems

Unidirectional Communication

Physical/token authentication

High-security Operating System

Location-Based Authentication

Host-based Firewalls

Device-to-Device Authentication

Forensics/Analysis Tools

Biometric Authentication

Password Authentication

Smart Card Authentication

Virus Detection Systems

Challenge/Response Authentication

Cryptography

Vulnerability Scanners

Automated Software Management Tools

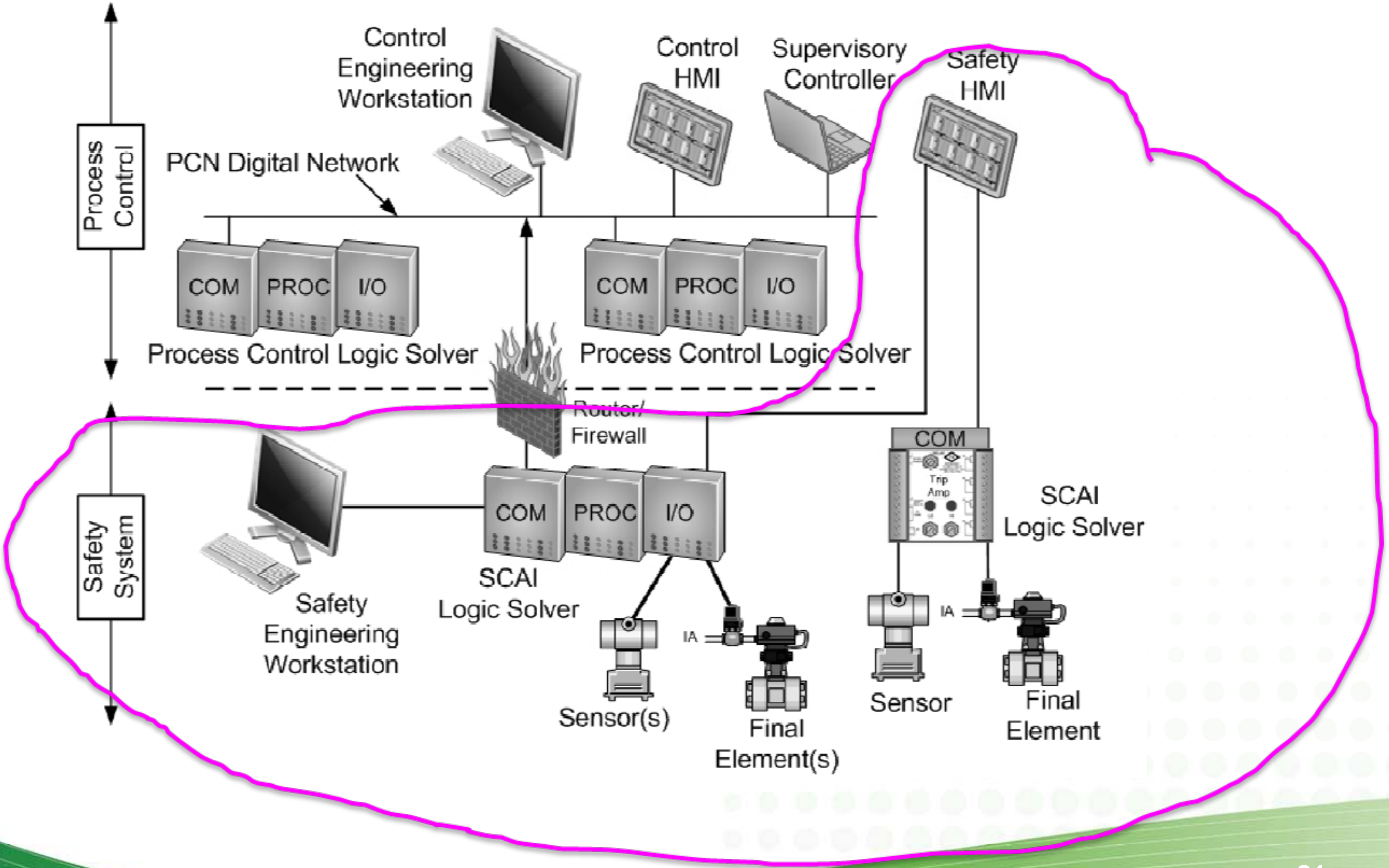
# IACS Network Architecture MATTERS

How the SCAI and the Process Control portions of the IACS are connected to each other will significantly change the countermeasure strategy design for the SCAI system(s).

Examples: ALL of the SCAI functions (safety controls, **safety alarms**, and safety interlocks) are implemented on the controller(s) within the Safety network zone

# Overall Control System includes the Process Control System and Safety System

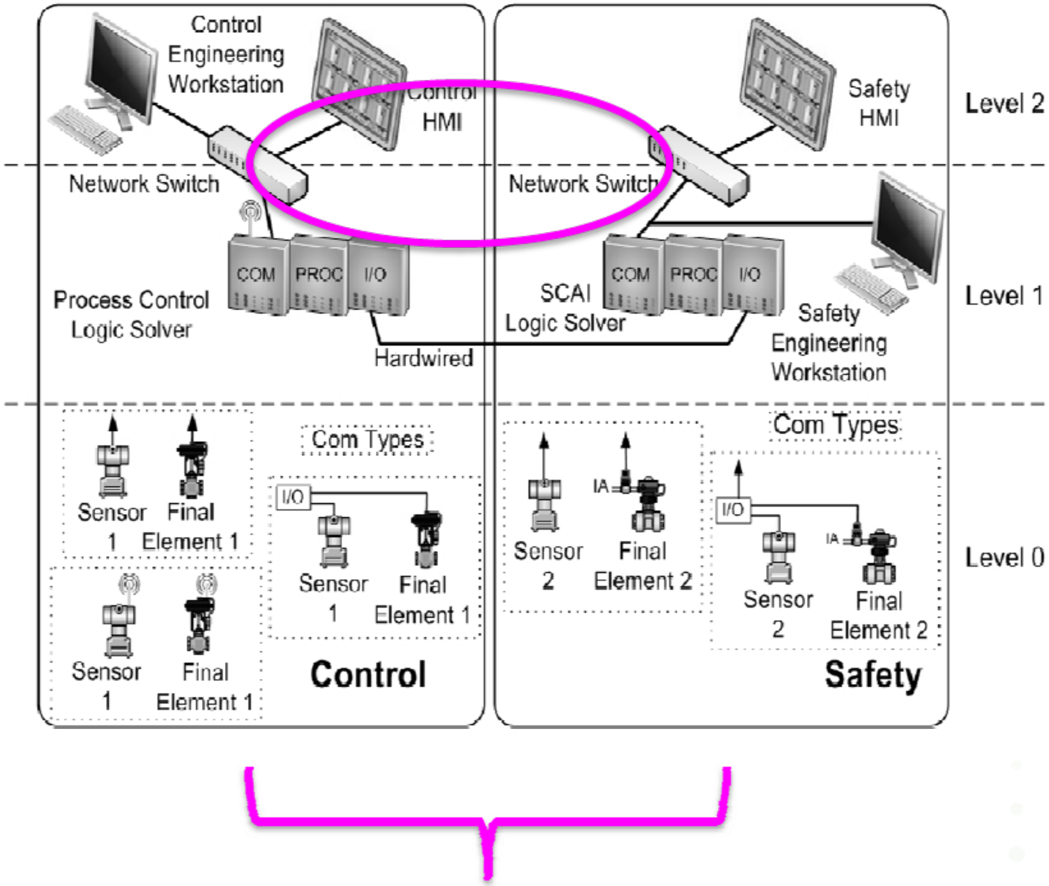
**[Figure 4.1 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]**



Safety Zone

# Pictorial Diagram of Air-Gapped Systems

**[Figure 3.10 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]**



2 security zones

No permanent digital connection between SCAI and rest of IACs network

No remote access capability to SCAI

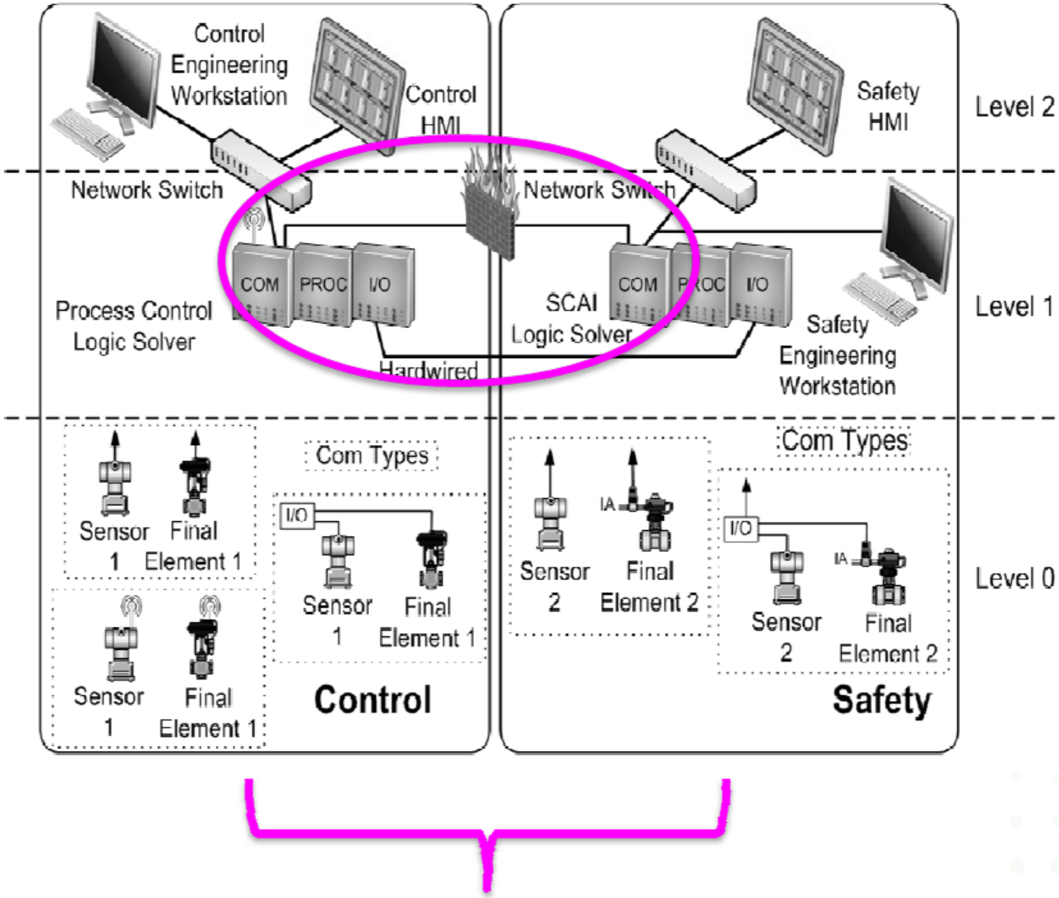
Most inherently secure SCAI zone architecture

Least convenient architecture for data acquisition or upgrade support

Guard against mobile devices/mobile code and access to HMIs/workstations

# Pictorial Diagram of Interfaced Systems

**[Figure 3.12 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]**



2 security zones

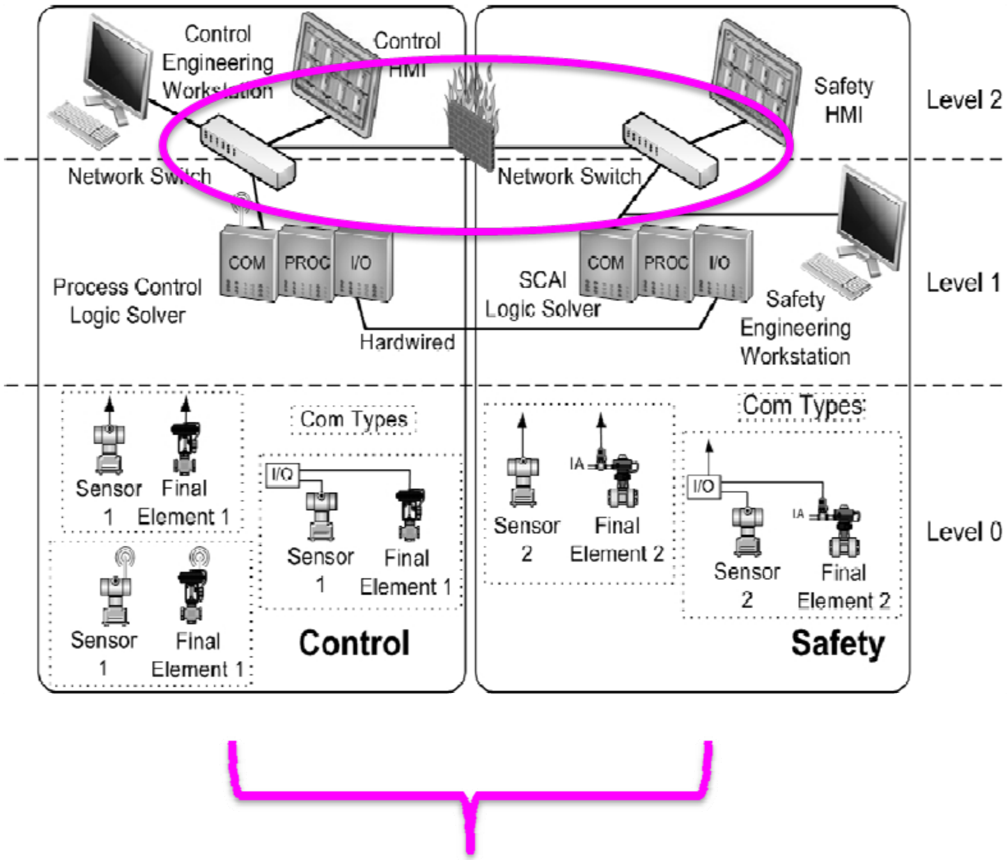
Permanent digital connection between SCAI and Process Controller communication modules(e.g., serial or ethernet)

COM-COM links are usually very constrained in format and not capable of transmitting mobile code or instructions which could result in loss of SCAI controller

Loss of communication should not impact SCAI functionality. Firewall should support point-to-point authentication, use controls, avert overloading the COM module, etc.

# Pictorial Diagram of Integrated with Isolated Networks

**[Figure 3.14 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]**



2 security zones

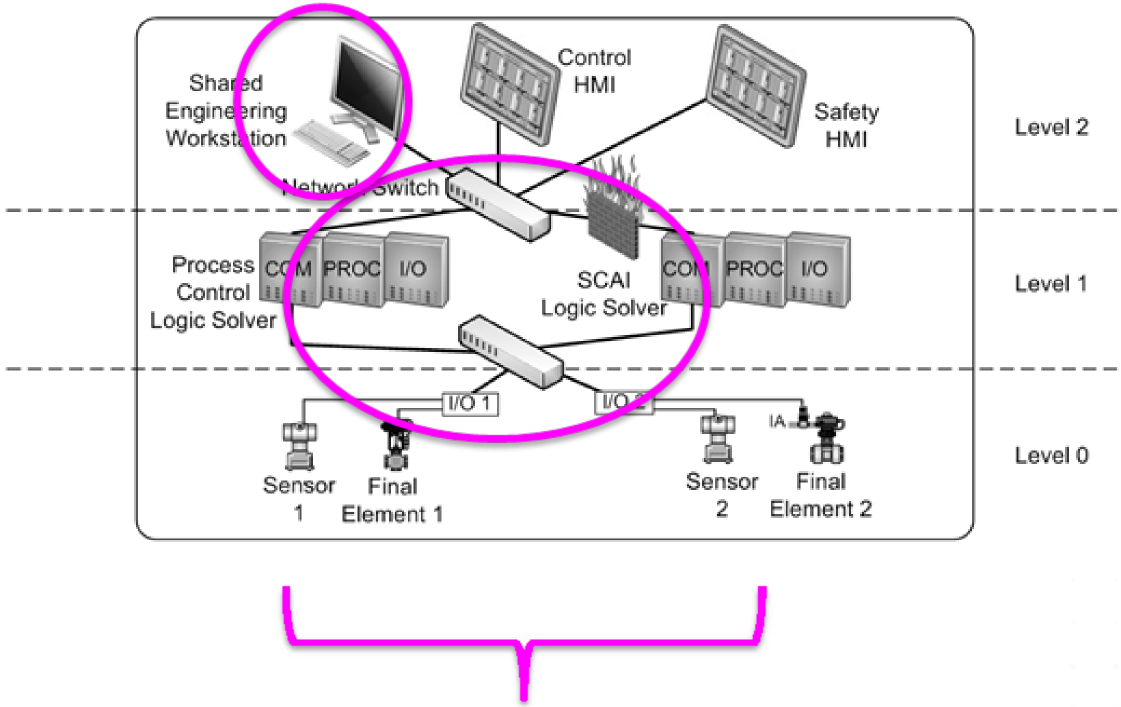
Permanent digital connection between SCAI and Process Controller (COTS) network switches

Vulnerability to the broad range of threats which can be made through network for the safety HMI, engineering workstation, and SCAI controller

Strong controls are needed at switch and firewall to perform the broad range of countermeasures needed to secure SCAI portion of network

# Combined systems with strong dependency – Shared PCN and I/O Bus

**[Figure 3.17 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]**



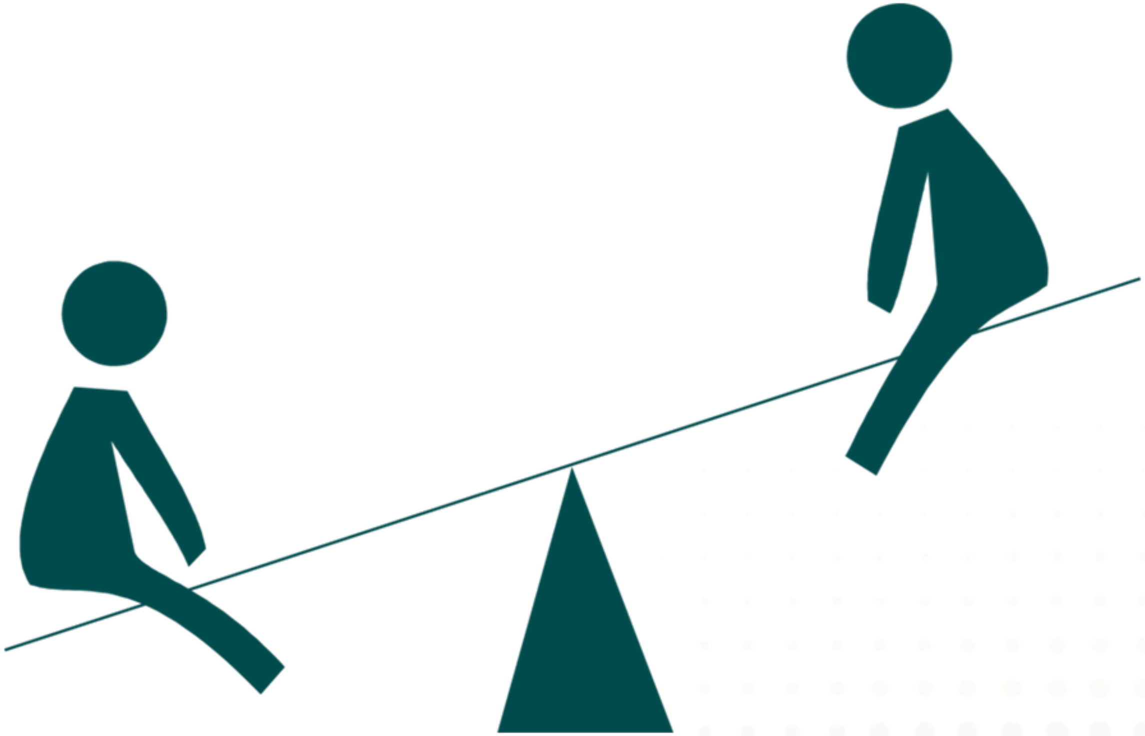
1 security zone

1 zone: Can no longer sever network communications to SCAI controller without losing SCAI functionality (i.e., Safety Alarms), so secure entire zone as SCAI

Often the controllers in this architecture are of identical technology (vulnerable to identical attack) and may share engineering workstation

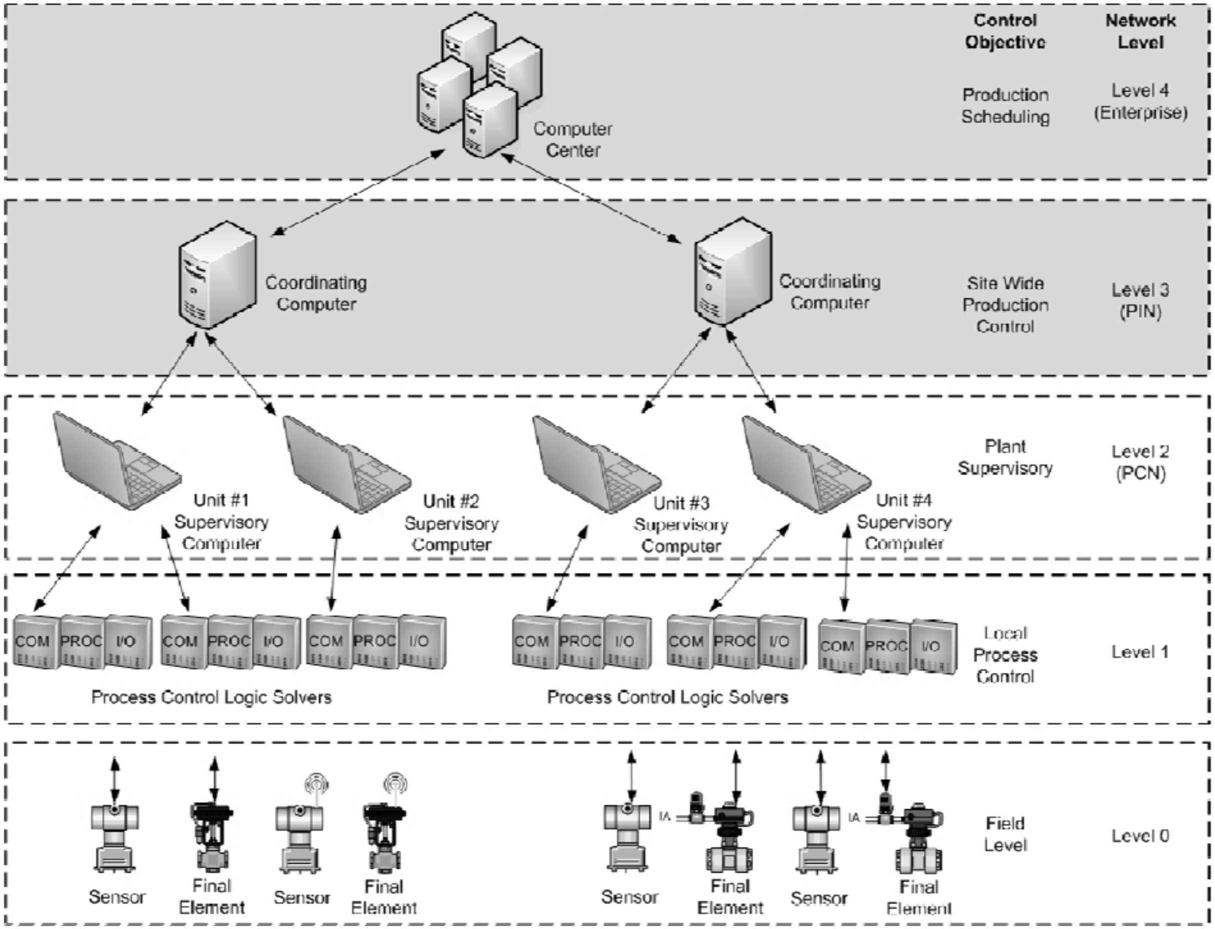
Shared I/O network creates additional vulnerabilities for Safety Controls and Safety Interlocks, as well as Safety Alarms

# Convenient Access ⟷ Ease of Security



# (SCADA) Process Control Architecture

**[Figure 4.9 CCPS Guidelines for Safe Automation of Chemical Processes DRAFT 2016]**



IACS Functionality spreads into IT space

Upper layers often being executed over public networks

Instrumentation more frequently uses “wireless” (broadband, satellite, etc.) technologies

Consider local, hard-wired non-programmable technology for SCAI

Common Uses:
Oil and Gas - Utilities

# ISA TR84.00.09 Current Revision Cycle

- Expanding content to address cyber security impact of IACS associated with Safety Instrumented Systems (e.g., SCAI)
- Adding more detail to the various steps of the cyber security work process for SCAI
- Restructuring existing content to align more transparently with the work process
- Enhanced IACS network example comparison (Annex A).

# SCAI Cyber Security Summary

- Don’t connect what you don’t have to connect
  - Is *convenient* SCAI access worth the risk?
- Actively protect what is connected
  - Threats come from ALL directions: disable unused features and guard all approaches
  - Proactively monitor access through gateways and firewalls, respond promptly, and IMPROVE
- Respect the differences between IT and IACS cyber security– sufficient number of competent resources needed for active management of both
- Train…train…train…DRILL…AUDIT users of the system in their cyber security countermeasure responsibilities and to avoid “social engineering”

# References

- ANSI/ISA. 2004*. Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*, 84.00.01-2004 (IEC 61511-1 Mod) Part 1. Research Triangle Park: ISA.

- ANSI/ISA. 2007-13. *Security for Industrial Automation and Control Systems - Part 1-3*, 62443 (99.01.01, 99.02.01, 99.03.03). Research Triangle Park: ISA.

- CCPS. (DRAFT 2016). *Guidelines for Safe Automation of Chemical Processes 2nd Edition*. New York: AIChE.

- IEC. 2010. *Functional safety of electrical/electronic/programmable electronic safety related systems,- Parts 0-7*, IEC 61508. Geneva: IEC.

- ISA. 2013. *Security Countermeasures Related to Safety Instrumented Systems (SIS)*, TR84.00.09-2013. Research Triangle Park: ISA.

- NIST. 2011. *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MA: NIST.

# Questions?