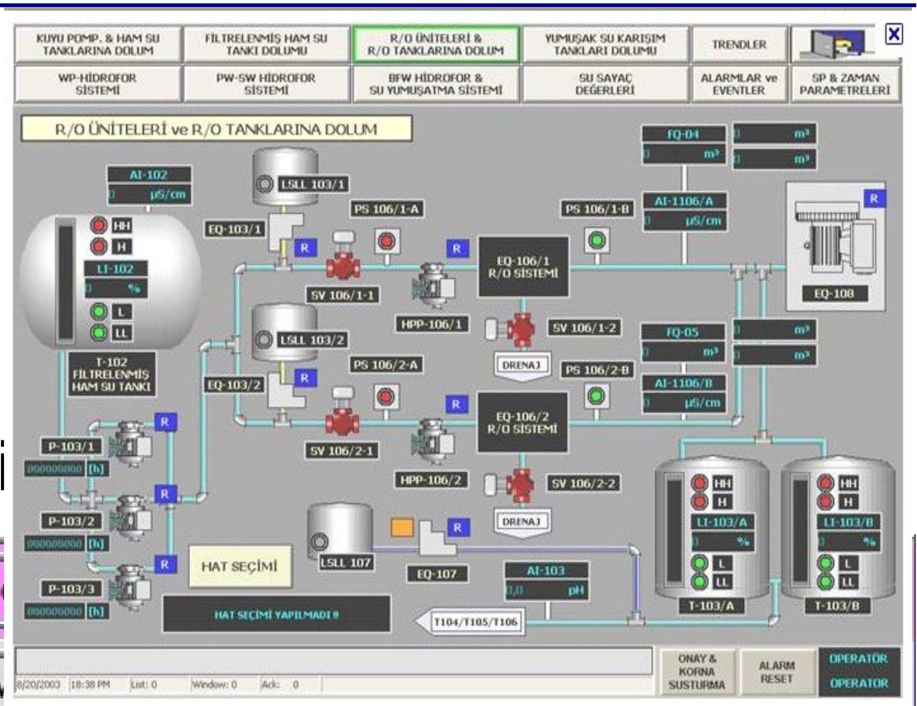
ICS Security Architecture
Where Worlds Collide

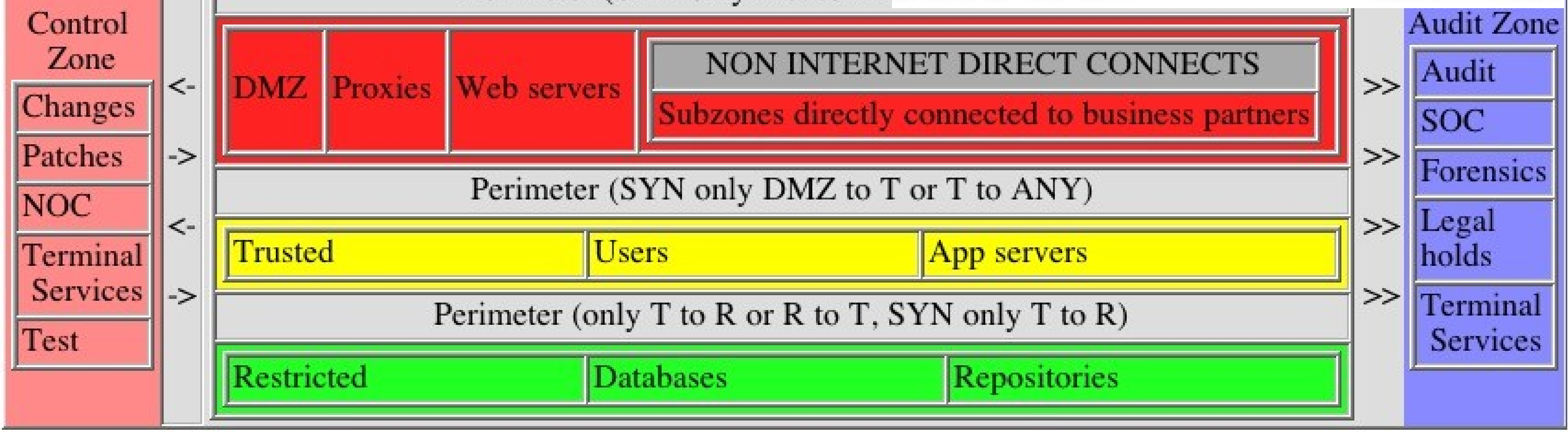
SecureWorld – September 22, 2011

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Outline

- Introduction
- ICS vs. Enterprise technology
- Integration of Enterprise and ICS
- Security Architecture Implications
- Summary / Conclusions / Discussi





Perimeter (SYN only Inet to DM

Control Zone
Changes
Patches
NOC
Terminal Services
Test

<-
->
<-
->

DMZ | Proxies | Web servers
NON INTERNET DIRECT CONNECTS
Subzones directly connected to business partners

Perimeter (SYN only DMZ to T or T to ANY)

Trusted | Users | App servers

Perimeter (only T to R or R to T, SYN only T to R)

Restricted | Databases | Repositories

>>
>>
>>
>>

Audit Zone
Audit
SOC
Forensics
Legal holds
Terminal Services

My Background

- Background in Control Systems and Security
  - First control system designed and implemented in 1975
  - First security system designed and implemented in 1974
  - B.S. E.E. / M.S. Information Science / Ph.D. E.E.
- But a career focus in information protection
  - 1983 Computer Viruses
  - 1992 Critical infrastructure protection (power, water, gas, etc.)
  - 1996 Deception for protection (Deception ToolKit)
  - 1998 Studies for PCCIP (power, water, gas, oil, comms, ...)
  - 1999 Digital forensics tools (ForensiX)
  - 2000 Bootable secure Linux (White Glove)
  - 2002 Security Reference Architecture (Burton Group SRMS)
  - 2006 California Sciences Institute (M.S. and Ph.D. programs)
    - National Security / M.S. Advanced Investigation / Ph.D. Digital Forensics
  - ISC^2 Fellow – Senior Member of the IEEE – Honorary Ph.D. C.S.

Thesis of this talk

- There is a culture clash between
  - Industrial Control Systems and
  - Enterprise Information Technology
- These technologies and systems are being connected
  - Mismatches are occurring
  - They are producing increasing negative consequences
  - Most of the consequences are in the ICS side
- Point solutions will be expensive, slow, and painful

- The solution lies in better strategy and architecture

Outline

- •Introduction
- •ICS vs. Enterprise technology
- •Integration of Enterprise and ICS
- •Security Architecture Implications
- •Summary / Conclusions / Discussion

The culture clash

- Enterprise IT
  - Fundamentally based on sharing with limits
  - High tolerance for failures – they happen every day
  - Little consequence for less than real-time
  - Delays cause increasing loss with time
  - Driven largely by financial and technology leadership
  - Typically highly user-centric, with users demanding services
  - Life cycles 1-5 years

- Industrial Control Systems
  - Fundamentally based on separation
  - Low tolerance for failures – P < 0.00001/y
  - Real-time absolutely critical
  - Delays over threshold cause physical destruction of plant
  - Driven largely by engineering and operations leadership
  - Typically no “users”, only operator oversight
  - Life cycles 5-50 years

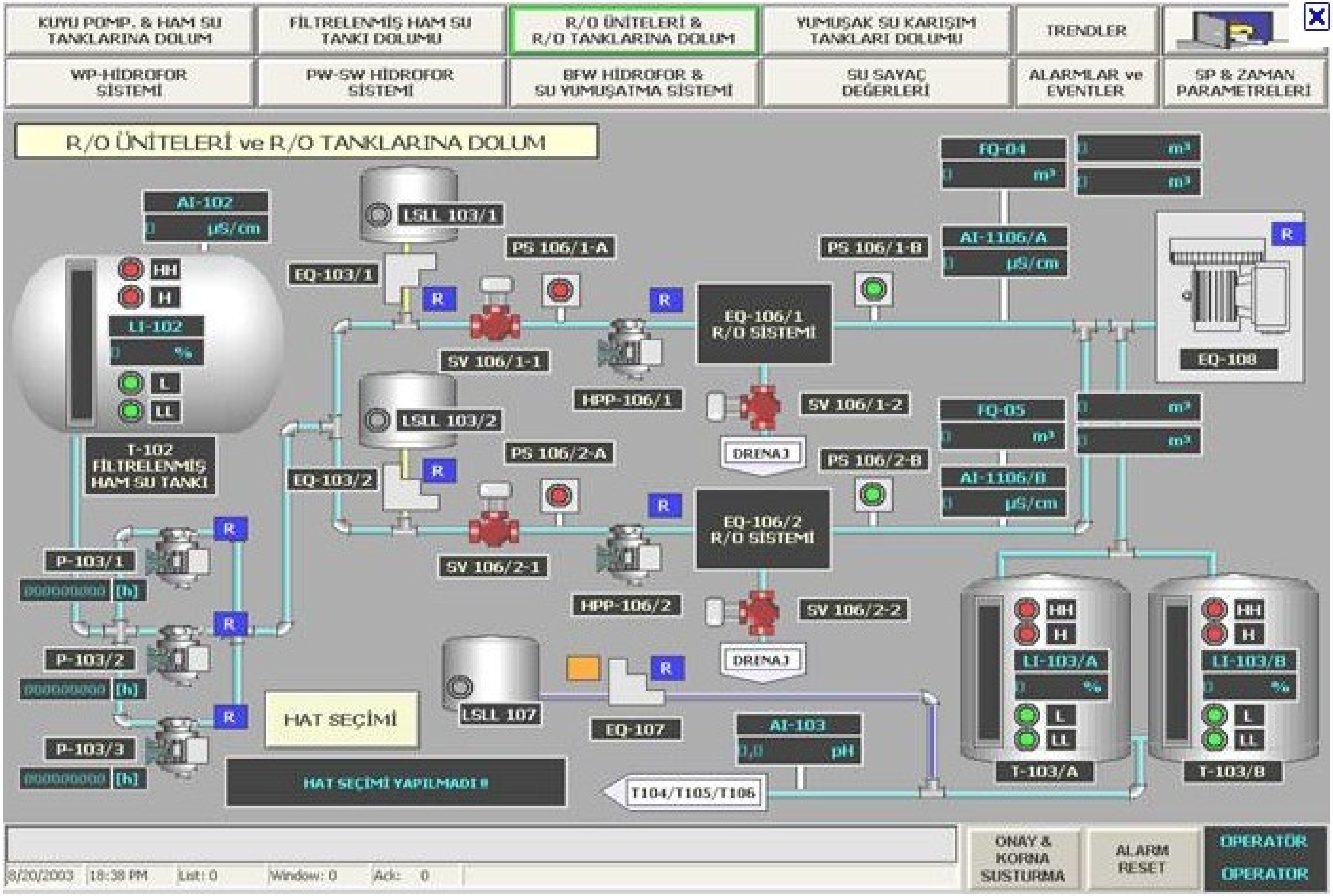
What goes where?

- Enterprise IT
  - User interface devices
    - Desktop, laptop, pad, phone
  - Most databases
  - Most network infrastructure
  - Most user services
    - Mail, Web, Documents, Slides, Spreadsheets, etc.

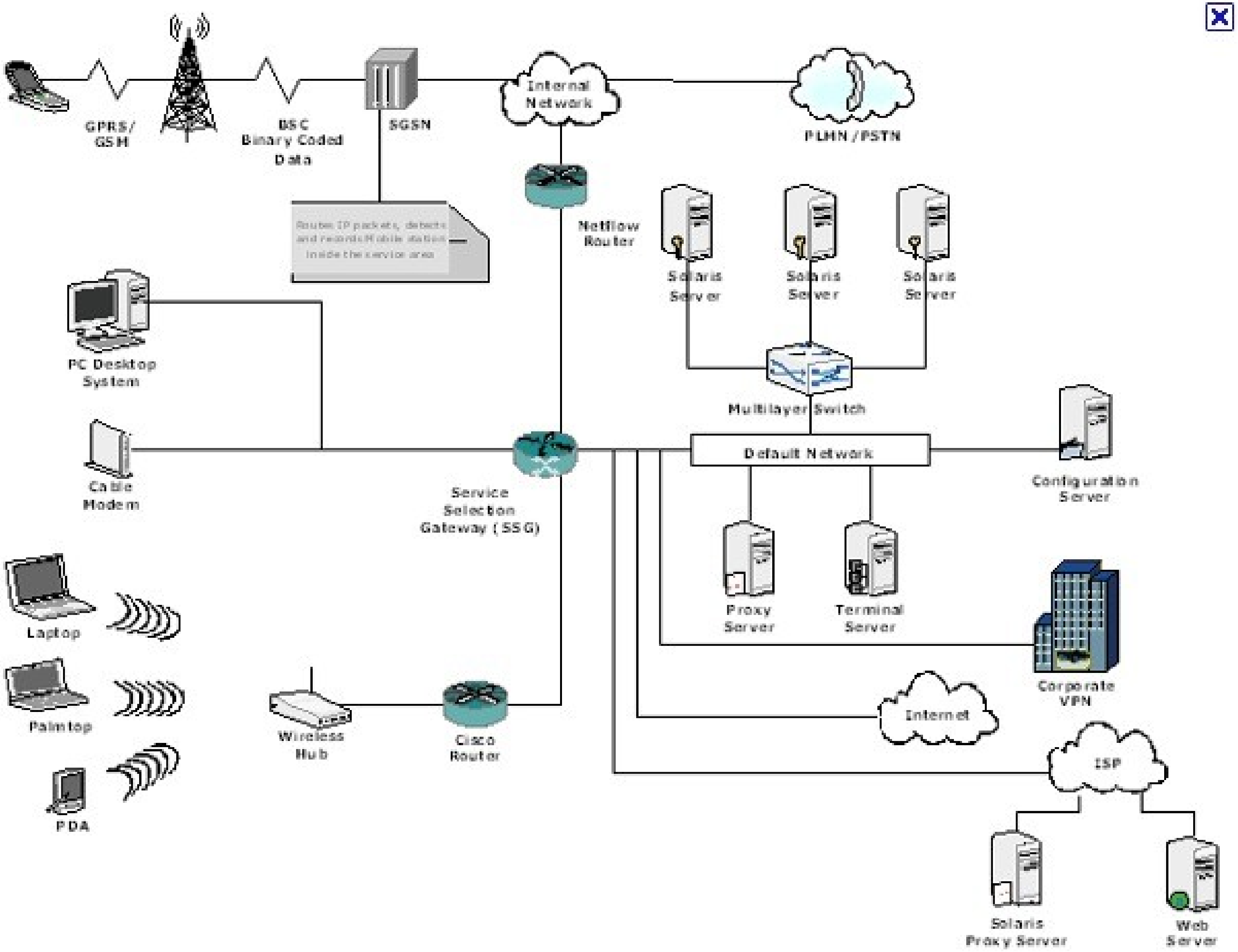
- ICS - control, act, sense
  - Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), and distributed control systems (DCS)
  - Power, water, gas, etc.
  - Manufacturing floor, chemical, pharmaceutical, etc. plants
  - Medical devices, Avionics

- Somewhere in the middle
  - Real-time trading and transaction systems
  - Telecommunications systems
- Many enterprises have substantial mixes

Typical ICS architecture (SCADA) view



Typical IT architecture view

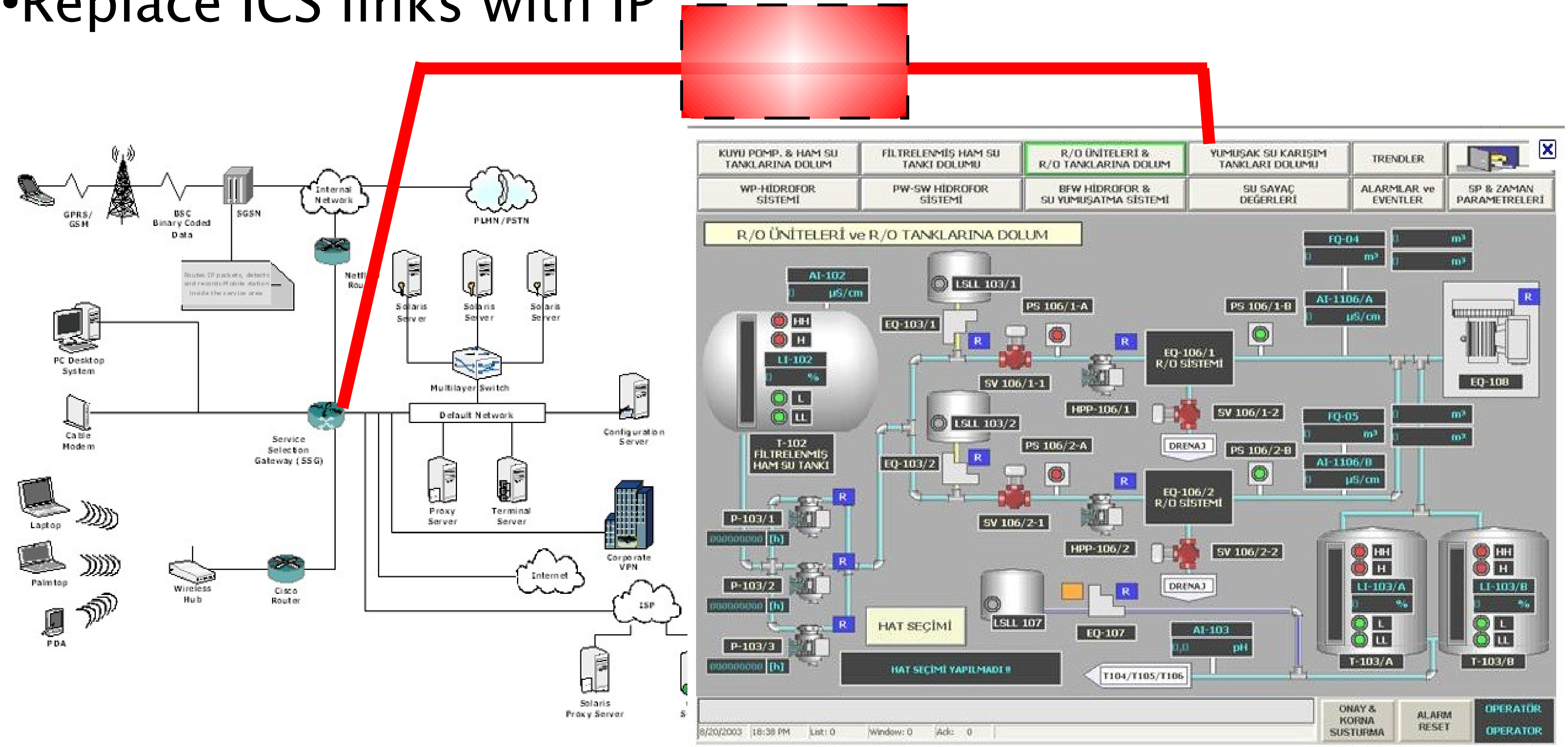


Outline

- Introduction
- ICS vs. Enterprise technology
- Integration of Enterprise and ICS
- Security Architecture Implications
- Summary / Conclusions / Discussion

A typical integration approach

- Connect a router/switch in the enterprise to a router/switch in the ICS environment
- Optionally add firewall(s)
- Replace ICS links with IP



What could possibly go wrong?

- The separation assumption of ICS leads to:
  - Weaknesses never exposed to outsiders in ICS become exposed
  - Interference problems lead to performance deviations
  - Remote control potential leads to unauthorized accesses
  - Authentication requirement changes lead to control loss ...
- Differences in tolerance for failures leads to:
  - IT infrastructure instantly has 6 9's of reliability requirement
  - No change control windows for IT changes w/out ICS approval
  - All IT personnel must meet ICS security clearance requirements
  - Priority controls in networks must be changed for ICS above all ...
- Real-time requirements and consequence curves lead to:
- Leadership differences lead to:
- Differences in support needs leads to:
- Life cycle differences lead to:

What could possibly go wrong?

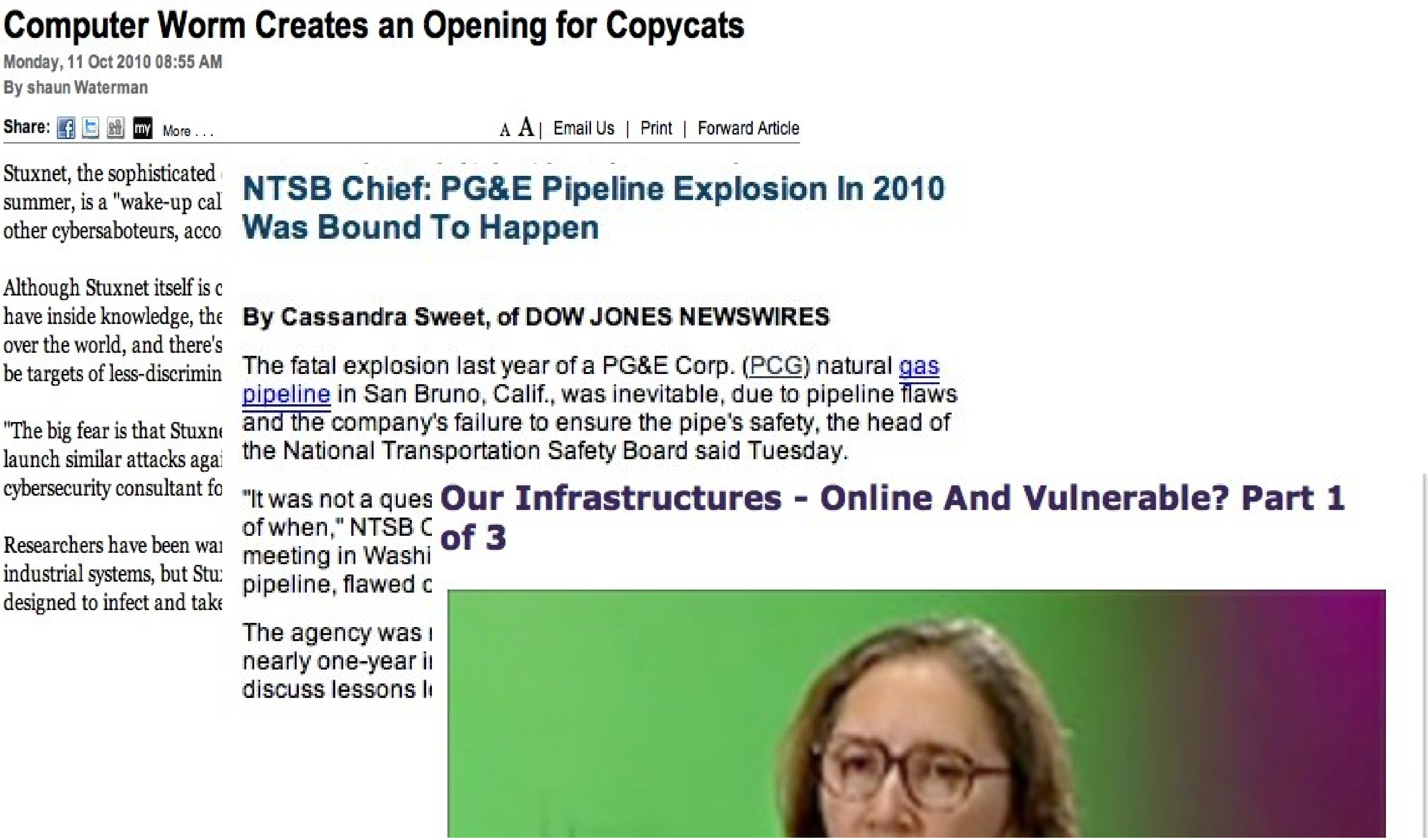
- The separation assumption of ICS leads to:
- Differences in tolerance for failures leads to:
- Real-time requirements and consequence curves lead to:
    - Unanticipated failure modes → production outages or worse
    - Authentication process interdependencies → outages or worse
    - Encryption fails to meet ICS real-time needs → outages or worse
    - “Best effort” delivery of IP fails, must be changed to real-time ...
- Leadership differences lead to:
    - Escalation of issues to CIO/CFO and COO – and it rolls downhill
    - Equities result in food fights / power struggles etc.
    - Whoever “wins”, someone “loses” - hopefully not the enterprise
    - Management structures likely to change to matrixed ...
- Differences in support needs leads to:
- Life cycle differences lead to:

What could possibly go wrong?

- The separation assumption of ICS leads to:
- Differences in tolerance for failures leads to:
- Real-time requirements and consequence curves lead to:
- Leadership differences lead to:
- Differences in support needs leads to:
  - IT change controls fail and must be enhanced for higher surety
  - Changed patching approach required to deal with ICS limitations
  - Work flow systems must be updated and protected for ICS needs
  - IT support has to include legacy for 20+ years ...
- Life cycle differences lead to:
  - IT updates restricted and ICS costs increase to deal with changes
  - Assumptions made in IT must be revisited for ICS environments
  - ICS environments have to go through constant re-certifications
  - Legacy systems and mechanisms must be retained ...

And then...

- Watch the news stories come in...



Computer Worm Creates an Opening for Copycats

Monday, 11 Oct 2010 08:55 AM

By shaun Waterman

Stuxnet, the sophisticated
summer, is a "wake-up cal
other cybersaboteurs, acco

Although Stuxnet itself is c
have inside knowledge, the
over the world, and there's
be targets of less-discrimin

"The big fear is that Stuxne
launch similar attacks agai
cybersecurity consultant fo

Researchers have been wa
industrial systems, but Stu
designed to infect and take

NTSB Chief: PG&E Pipeline Explosion In 2010 Was Bound To Happen

By Cassandra Sweet, of DOW JONES NEWSWIRES

The fatal explosion last year of a PG&E Corp. (PCG) natural gas pipeline in San Bruno, Calif., was inevitable, due to pipeline flaws and the company's failure to ensure the pipe's safety, the head of the National Transportation Safety Board said Tuesday.

"It was not a ques
of when," NTSB C
meeting in Washi
pipeline, flawed c

The agency was
nearly one-year i
discuss lessons l

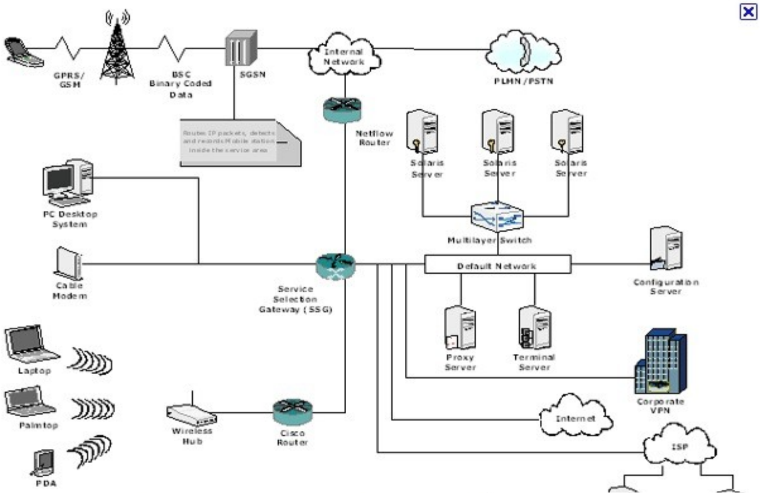
Our Infrastructures - Online And Vulnerable? Part 1 of 3

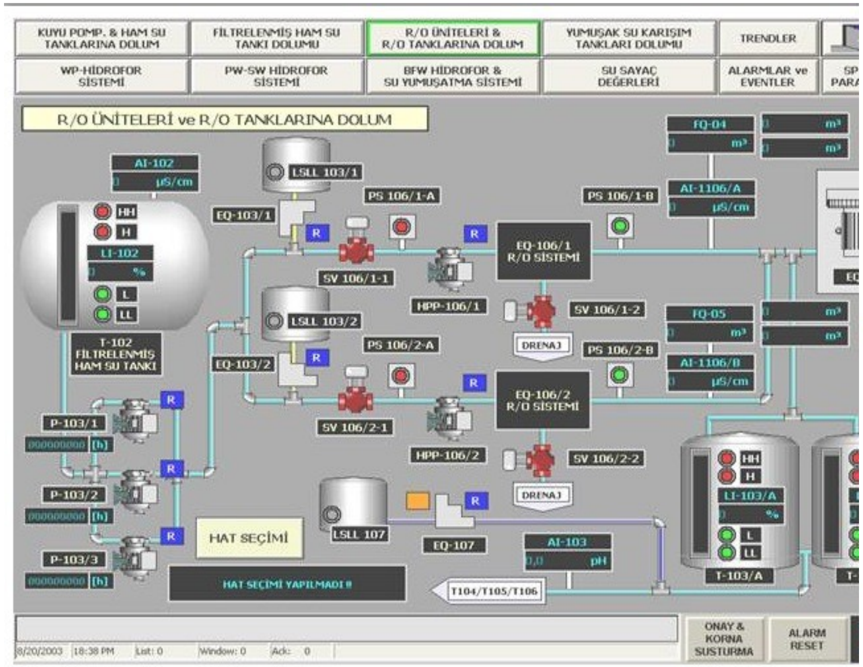
But there are good reasons to integrate

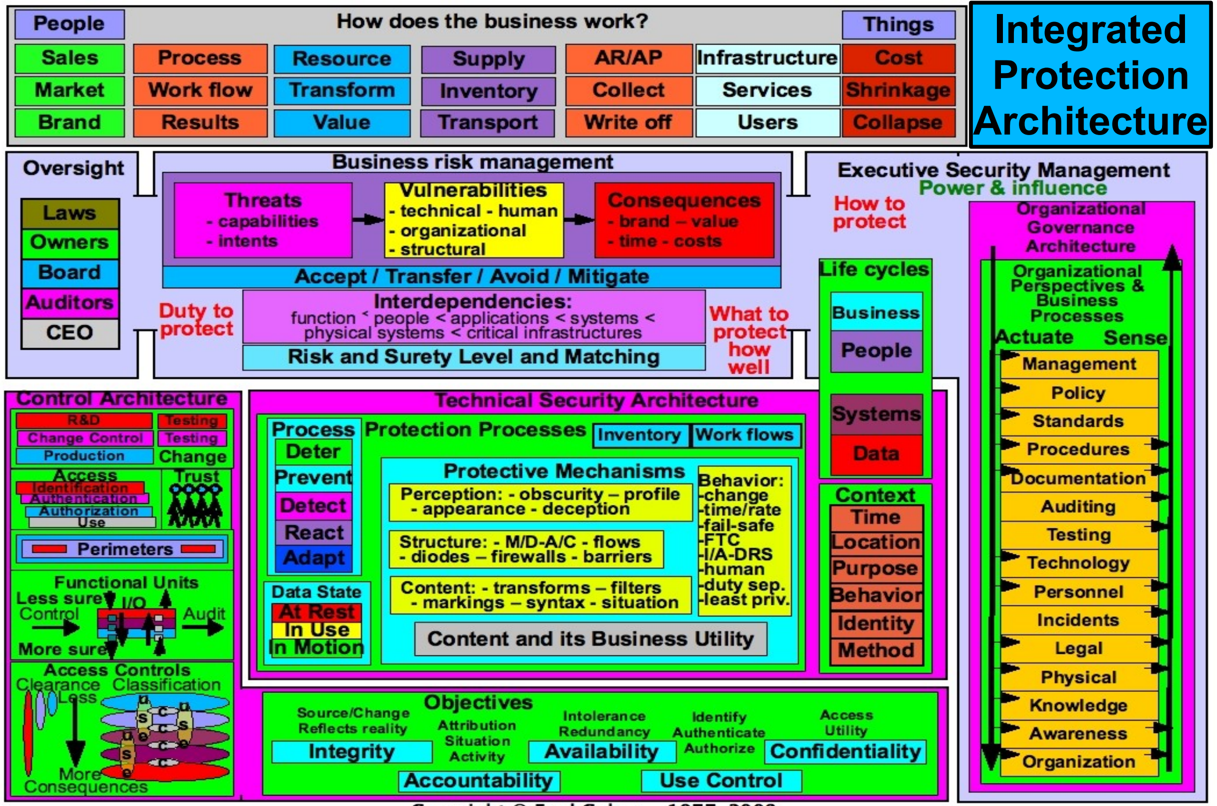
- ICS and IT will integrate
  - –Because there is a good business case to be made
    - Cost savings by shared infrastructure
    - Cost savings by remote administration and management
    - Business efficiency through better status and progress information
    - Just-in-time cost savings / higher customer satisfaction
    - Engineering and research benefit from remote access and information
  - –Because it is mandated by regulatory regimens
    - Power providers must provide real-time information on status
    - The market in (name the commodity) requires situation awareness for all
    - Real-time information on nuclear status delivered to the NRC some day?
  - –Because it is trendy?
    - People follow trends – because that's how people are
    - Don't you want your nuclear facility controlled from the beach?
    - The operators can work from home at night and on weekends!!!

Outline

- Introduction
- ICS vs. Enterprise technology
- Integration of Enterprise and ICS
- Security Architecture Implications
- Summary / Conclusions / Discussion







Integrated Protection Architecture

How does the business work?

People | Things

Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Work flow	Transform	Inventory	Collect	Services	Shrinkage
Brand	Results	Value	Transport	Write off	Users	Collapse

Oversight: Laws, Owners, Board, Auditors, CEO

Business risk management

Threats - capabilities - intents → Vulnerabilities - technical - human - organizational - structural → Consequences - brand – value - time - costs

Accept / Transfer / Avoid / Mitigate

Duty to protect

Interdependencies: function < people < applications < systems < physical systems < critical infrastructures

Risk and Surety Level and Matching

What to protect how well

Executive Security Management

Power & influence

How to protect

Organizational Governance Architecture

Organizational Perspectives & Business Processes

Actuate Sense

Management, Policy, Standards, Procedures, Documentation, Auditing, Testing, Technology, Personnel, Incidents, Legal, Physical, Knowledge, Awareness, Organization

Life cycles: Business, People, Systems, Data

Context: Time, Location, Purpose, Behavior, Identity, Method

Control Architecture

R&D, Testing, Change Control, Testing, Production, Change

Access: Identification, Authentication, Authorization, Use

Trust

Perimeters

Functional Units: Less sure, I/O, Control, Audit, More sure

Access Controls: Clearance, Classification, Less, More, Consequences

Technical Security Architecture

Process: Deter, Prevent, Detect, React, Adapt

Protection Processes: Inventory, Work flows

Protective Mechanisms

Perception: - obscurity – profile - appearance - deception

Structure: - M/D-A/C - flows - diodes – firewalls - barriers

Content: - transforms – filters - markings – syntax - situation

Behavior: -change -time/rate -fail-safe -FTC -I/A-DRS -human -duty sep. -least priv.

Data State: At Rest, In Use, In Motion

Content and its Business Utility

Objectives

Source/Change Reflects reality – Integrity

Attribution Situation Activity – Accountability

Intolerance Redundancy – Availability

Identify Authenticate Authorize – Use Control

Access Utility – Confidentiality

The bigger strategic challenge

- The Problem
  - Security decisions are haphazard, unstructured, and baseless
    - Just like security decisions for enterprises in general
    - No accepted, consistent, and meaningful decision process
    - No sound scientific basis for what we do
    - No serious measurement programs in place
    - Community consensus around well known poor decisions that won't work
- The Solution
  - Build structured architectural decisions with defined (sound?) basis
    - Create a consistent, acceptable, meaningful decision process
    - Integrate that process across enterprise IT and ICS environments
- Part of the solution already exists
  - Security reference architecture has developed over the last 10 years
    - Oriented largely toward enterprise information protection
    - Consolidates variations from across many enterprises into a framework

Reference Architecture Framework

- What the business is about
  - Understanding the reason for everything we do
- Top-level guidance
  - Duties to protect
- Risk management
  - What to protect how well
- Executive security management
  - Controlling activities and people / processes who / that do them
- Control Architecture
- Technical Architecture
- Engineering and implementation
- Operations, maintenance, and disposition

Reference Architecture Framework

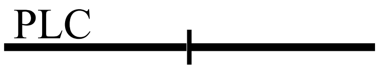
- What the business is about
- Top-level guidance
- Risk management
- Executive security management
- Control Architecture
  - Structural decisions about how things will work
- Technical Architecture
  - Translating how things work into how to do things
- Engineering and implementation
  - Translating how to do it in to mechanisms that do it
- Operations, maintenance, and disposition
  - Doing the things than need to get done
  - End-of-life, recycling, and reuse

Reference architecture

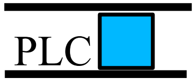
- Not a single architecture – a class of related architectural decisions
  - Not design, implementation, or engineering – structuring
  - Structured decisions of kind – not amount
    - We cannot really tune security like a resistor
    - Architectural solutions need to last unaltered for many years
  - Finite alternatives available – why select each?
- For a set of seemingly pertinent decisions
  - Identify alternatives
  - Determine rational basis for choosing between them
  - Codify decision points in tables / if-then-else / other forms
  - Identify the underlying assumptions / rational
  - Create decisions surrounding those rational as well

Example decision: connect PLCs to networks

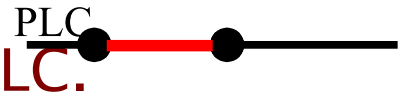
- What are my options?
  - Option A: No special protection is used for the PLC.



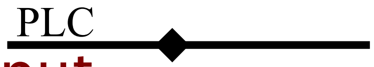
  - Option B: Use a restricted access network zone for the PLC.



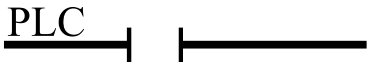
  - Option C: Use encrypted communications for the PLC.



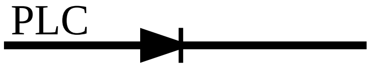
  - Option D: Use a custom FSM wrapper for the PLC input.



  - Option E: Do not connect the PLC to the network.

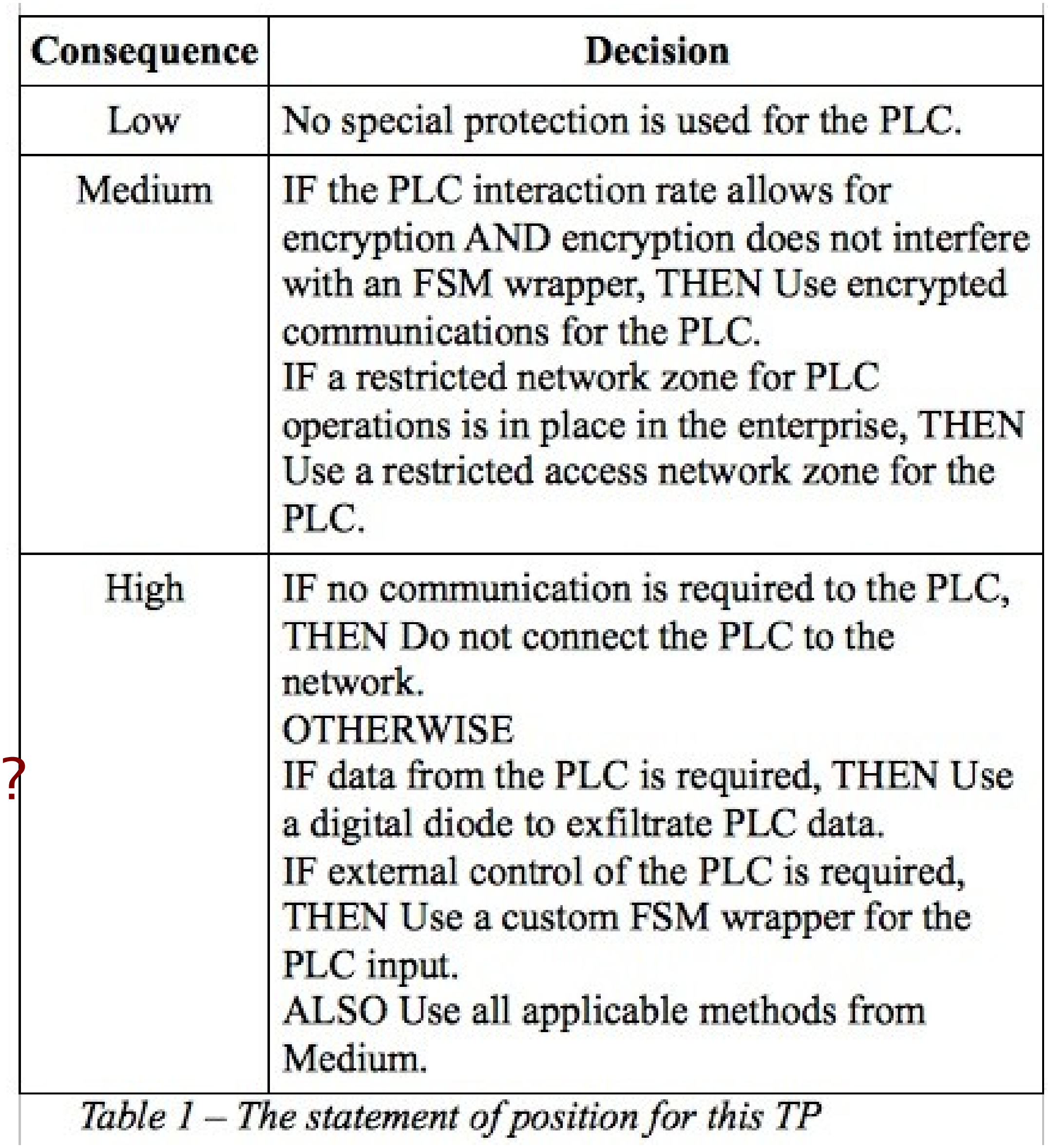


  - Option F: Use a digital diode to exfiltrate PLC data.



How do I decide between the alternatives?

- Decision criteria
  - Consequence of failure
    - Low
    - Medium
    - High
  - Restricted zone available?
    - Yes/No
  - Encryption fast enough?
    - Yes/No
  - Communication requirement?
    - Yes/No
  - FSM interference?
    - Yes/No



Consequence	Decision
Low	No special protection is used for the PLC.
Medium	IF the PLC interaction rate allows for encryption AND encryption does not interfere with an FSM wrapper, THEN Use encrypted communications for the PLC. IF a restricted network zone for PLC operations is in place in the enterprise, THEN Use a restricted access network zone for the PLC.
High	IF no communication is required to the PLC, THEN Do not connect the PLC to the network. OTHERWISE IF data from the PLC is required, THEN Use a digital diode to exfiltrate PLC data. IF external control of the PLC is required, THEN Use a custom FSM wrapper for the PLC input. ALSO Use all applicable methods from Medium.

Table 1 – The statement of position for this TP

The basis for the decisions

- If encryption is too slow to allow for controls to be effective
  - THEN you cannot encrypt and have effective controls
  - THUS don't use encryption in this case
- IF you don't have a Restricted zone (whatever that is)
  - THEN you cannot connect the PLC to a restricted zone
  - THUS don't use a restricted zone in this case
- IF risk is low (defined elsewhere)
  - THEN there is no rational for providing added protection
  - THUS don't waste time and money on it
- Specific bases should be defined for each situation and customized to the specific environment as appropriate.
  - WE don't have a Restricted zone
    - THUS we cannot use a restricted zone

We build from there

- Build up the necessary underlying decisions for these decisions
  - What are the consequence levels and how are they defined?
  - Who make what decisions about them and when?
  - How do we implement zones – or do we?
  - Etc.
- Build out the architecture to meet the range of needs
  - How do we connect a SCADA to the outside / ICS network?
  - How do we determine who can access what?
  - How do we control changes on PLCs, SCADAs, DCSs?
  - How do we connect to remote systems?
  - Etc.
- Cover more situations
  - How are power systems different from manufacturing systems?
  - How are they the same? What can we leverage? How?

Outline

- Introduction
- ICS vs. Enterprise technology
- Integration of Enterprise and ICS
- Security Architecture Implications
- Summary / Conclusions / Discussion

Summing up...

- There is a culture clash between IT and ICS
  - They are being integrated – wisely or otherwise
  - The likely – anticipated – outcomes are not pretty
  - This is unfolding on a variety of planes
    - Management – Technical – Business – Regulatory
- An approach to resolving it is with reference architecture
  - Find commonalities and differences
  - Understand the varying needs and where they can be met
    - Some will be met together and to mutual benefit
    - Others will be met separately and to mutual benefit
  - Codify decisions in a meaningful and justified framework
  - Understand and deal with interdependencies in the framework
- This is not the only approach
  - But has proven cost effective because of an economy of scale.
    - No enterprise can realistically do it on their own

Thank You - Discussion? Questions?

http://calsci.org/ - calsci at calsci.org

http://fredcohen.net/ - fc at fredcohen.net

http://all.net/ - fc at all.net