



EnergySec

National Electric Sector
Cybersecurity Organization

&

Fred Cohen & Associates

Presents

**Security Reference Architecture
Frameworks**

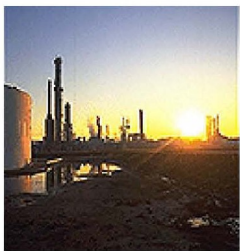
An Approach for the Energy Sector

Presented by - Dr. Fred Cohen - CEO - Fred Cohen & Associates

NESCO Webinar – September 29, 2011

- **Introduction**
- The many facets of energy security
- Security decision making
- Energy Sector Security Reference Architecture
- Summary / Conclusions / Discussion

Energy Security



My Background

- Education: B.S. E.E. / M.S. Information Science / Ph.D. E.E.
 - Government security work starting in 1970s
 - 1974: Secure video, voice, and data in DoD networks
 - 1977: Signals security and countermeasures for RF systems
 - 1984: Computer viruses in trusted systems (lots of follow-ons)
 - 1988: Security for government systems (many specific systems)
 - 1992: Critical infrastructure protection (power, water, gas, etc.)
 - 1996: Cognitive error mechanisms and deception operations*
 - 1998: Studies for PCCIP (power, water, gas, oil, etc.)*
 - 2000: Digital forensics and information assurance systems*
 - 2004: Information Security Reference Architecture+
 - 2006: Co-founded CalSci (M.S. and Ph.D. in National Security)
 - ISC² Fellow – Senior Member of the IEEE – Honorary Ph.D. C.S.
- *Sandia National Laboratories – Principal Member of Technical Staff
- +Burton Group – Principal Analyst – Security and Risk Management Strategies

Overview

- Security is a broad, complex, poorly understood issue
 - Perhaps the archetypical exemplar of this is information security
- But we still have to make decisions
 - Sound decisions would be better than unsound ones
 - What makes a sound decision anyway?
 - The choices are limited
 - We don't know what will happen in advance (a-priori vs. posteriori)
 - Risk management
 - Two poorly defined terms mashed together reflective of the challenge
- Some decisions can be standardized
 - They have a (sometimes sound) basis
 - We have to choose between them (limited options)
- Reference architecture provides a path to better decisions
 - The energy sector can benefit from a reference architecture

- Introduction
- **The many facets of energy security**
- Security decision making
- Energy Sector Security Reference Architecture
- Summary / Conclusions / Discussion



Energy Security

- **Lots of different energy supplies / deliveries / demands**
 - **Power (electrical systems)**
 - Supply: Nuclear / Coal / Oil / Water / Gas / Wind / Solar / Bio / Tidal ...
 - Deliver: Transmission / Distribution / Wires / Switches / Transformers / ...
 - Demand: Industrial / Business / Military / Public Services / Home / ...
 - **Fuel (self-contained generation)**
 - Supply: Gasoline / Propane / Natural Gas / Oil / Wood / ...
 - Delivery: Pipelines / Ships / Trains / Trucks / Cars
 - Demand: Industrial / Military / Ships / Trains / Planes / Trucks / Cars / ...
 - **Food and water (human energy)**
 - Supply: Sun / Rain / Seed / Soil / Other food / Artificial versions
 - Delivery: Trucks / Trains / Nature
 - Demand: Human consumption / Animal and plant consumption
- Lots of different security facets
- Most issues are complex and they interact
- ICS and IT information security as a microcosm

Energy Security

- Lots of different energy supplies and demands
- **Lots of different security facets**
 - Continuity of governments around the World
 - Physical security of source, deliver, consumption
 - Personnel security of those involved in the industry
 - Information security of the control and financial systems
 - Research and development of supply / delivery / consumption
 - Carrying capacity and balancing load with supply
 - Industrial capacity to support energy systems
 - Knowledge capacity to support the sector
 - Financial security of the system that allows commerce
- Most issues are complex and they interact
- ICS and IT information security as a microcosm

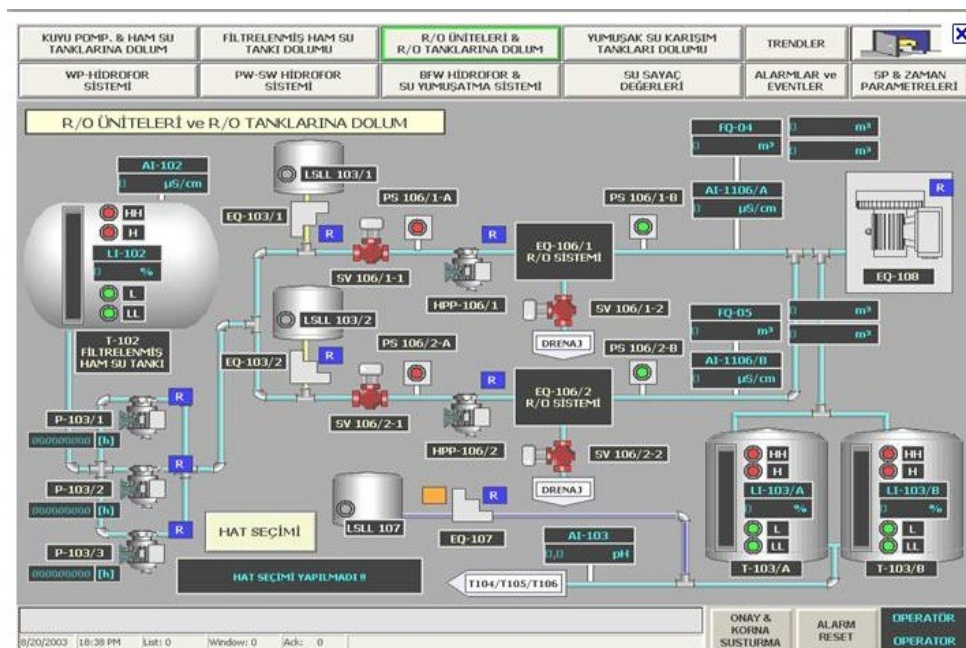
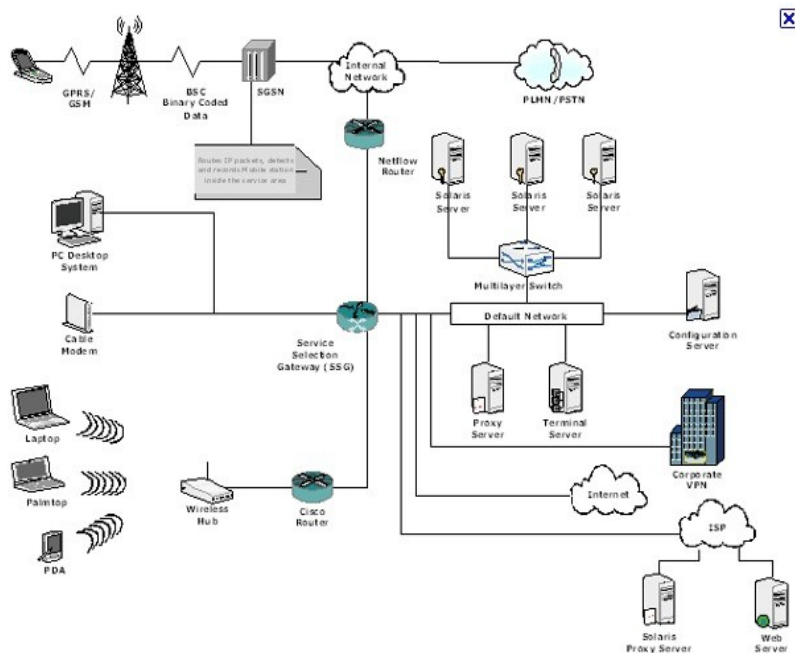
Energy Security

- Lots of different energy supplies and demands
- Lots of different security facets
- **Most issues are complex and they interact**
 - As governments encounter budget cuts
 - Support for R&D, education, physical security, etc. fail
 - Leading to strategic reduction in resources and infrastructure weakness
 - Leading to inadequate supply and reliability for industry / business
 - Leading to less revenue for government ...
 - If power fails, finance fails, leading to inability to pay for fuel, leading to transportation failures, leading to no fuel available to workers, leading to no transport to plants, leading to more power failures, etc.
 - There are many such issues with complex interactions
 - Decisions about any of them may affect all of them
- ICS and IT information security as a microcosm

Energy Security

- Lots of different energy supplies and demands
- Lots of different security facets
- Most issues are complex and they interact
- **ICS and IT information security as a microcosm**

–As an example, let's look at the information security interaction between enterprise information technology (IT) and industrial control systems (ICS)



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

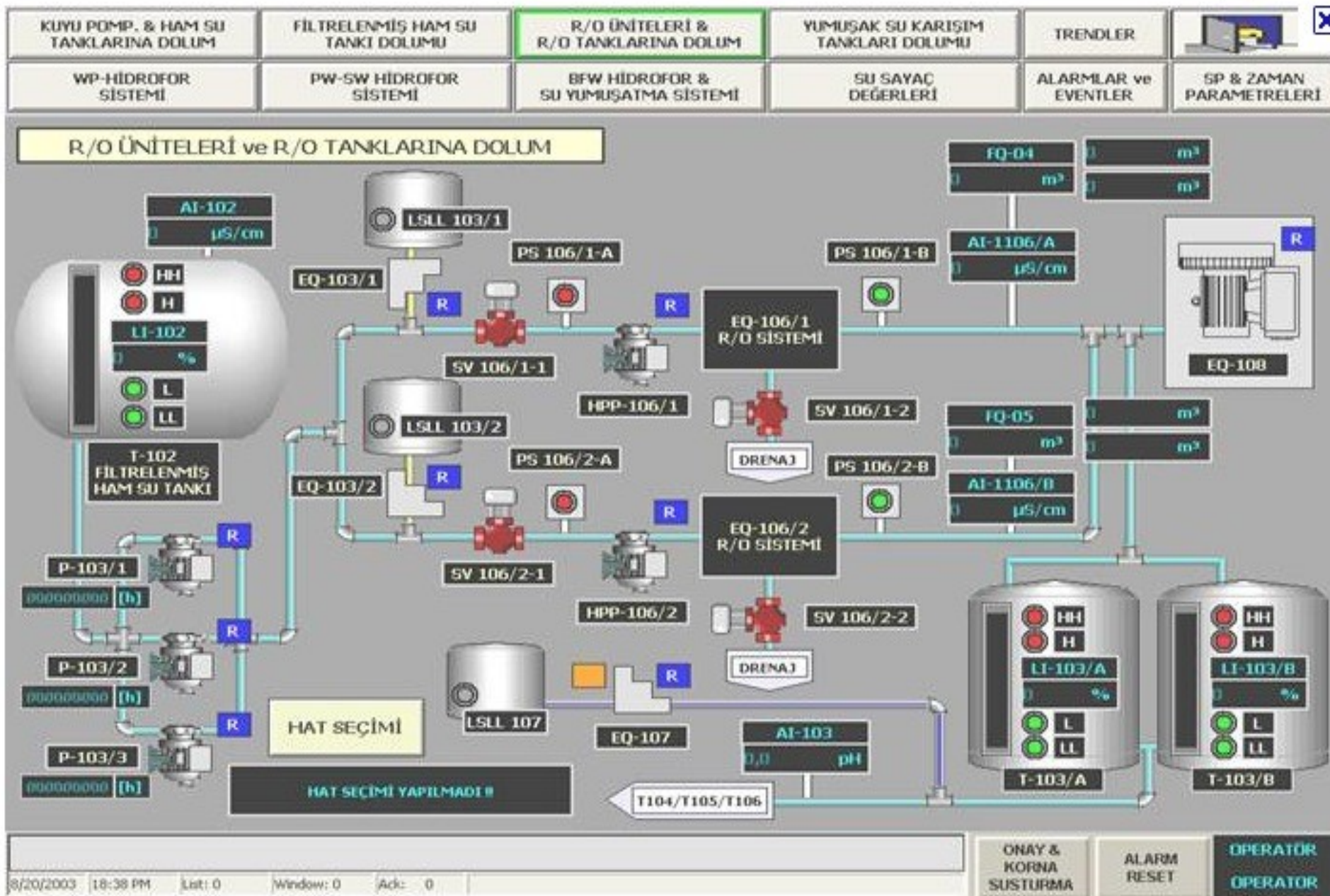
- Somewhere in the middle

- Real-time trading and transaction systems

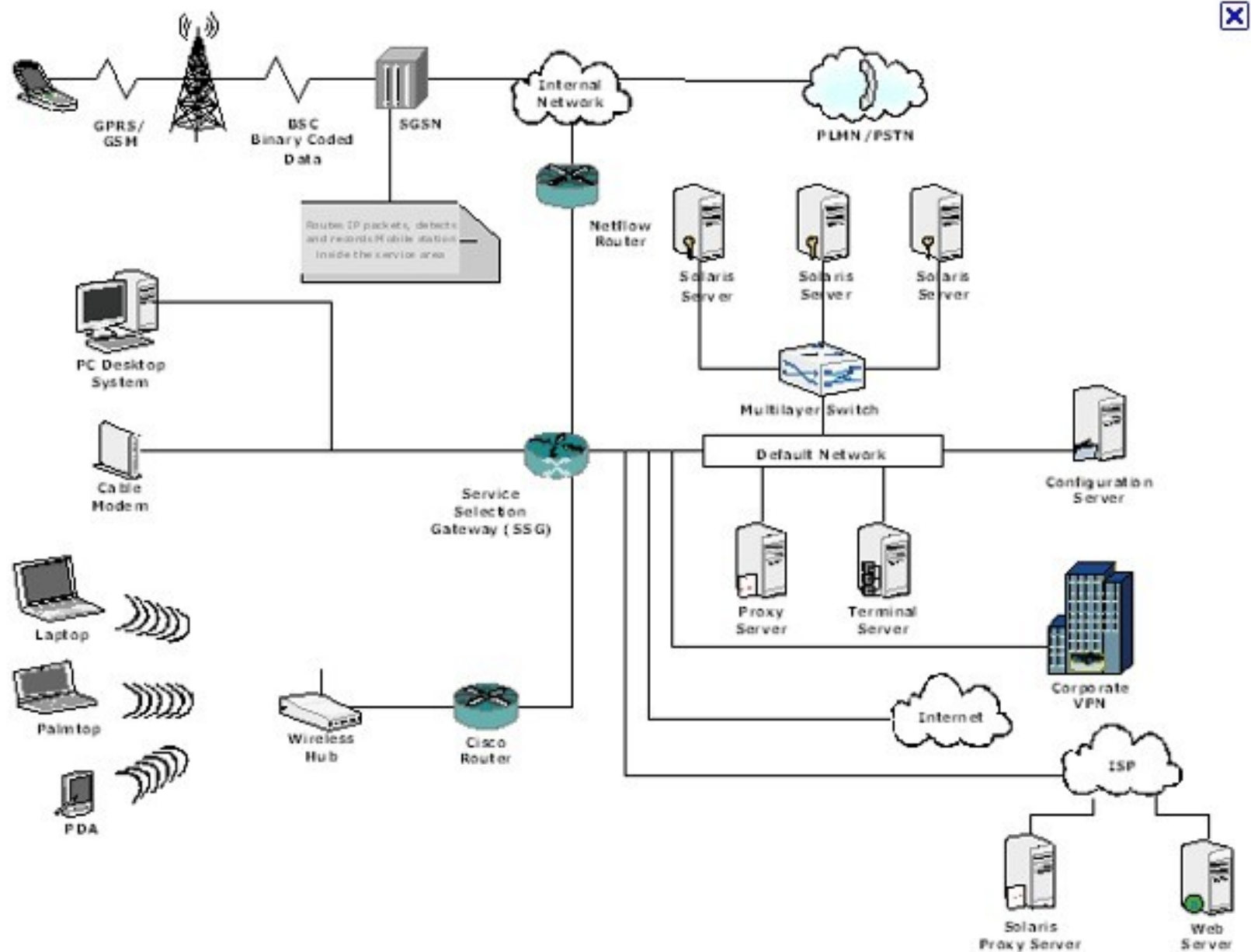
- Telecommunications systems

- Many enterprises have substantial mixes

Typical ICS (SCADA) view

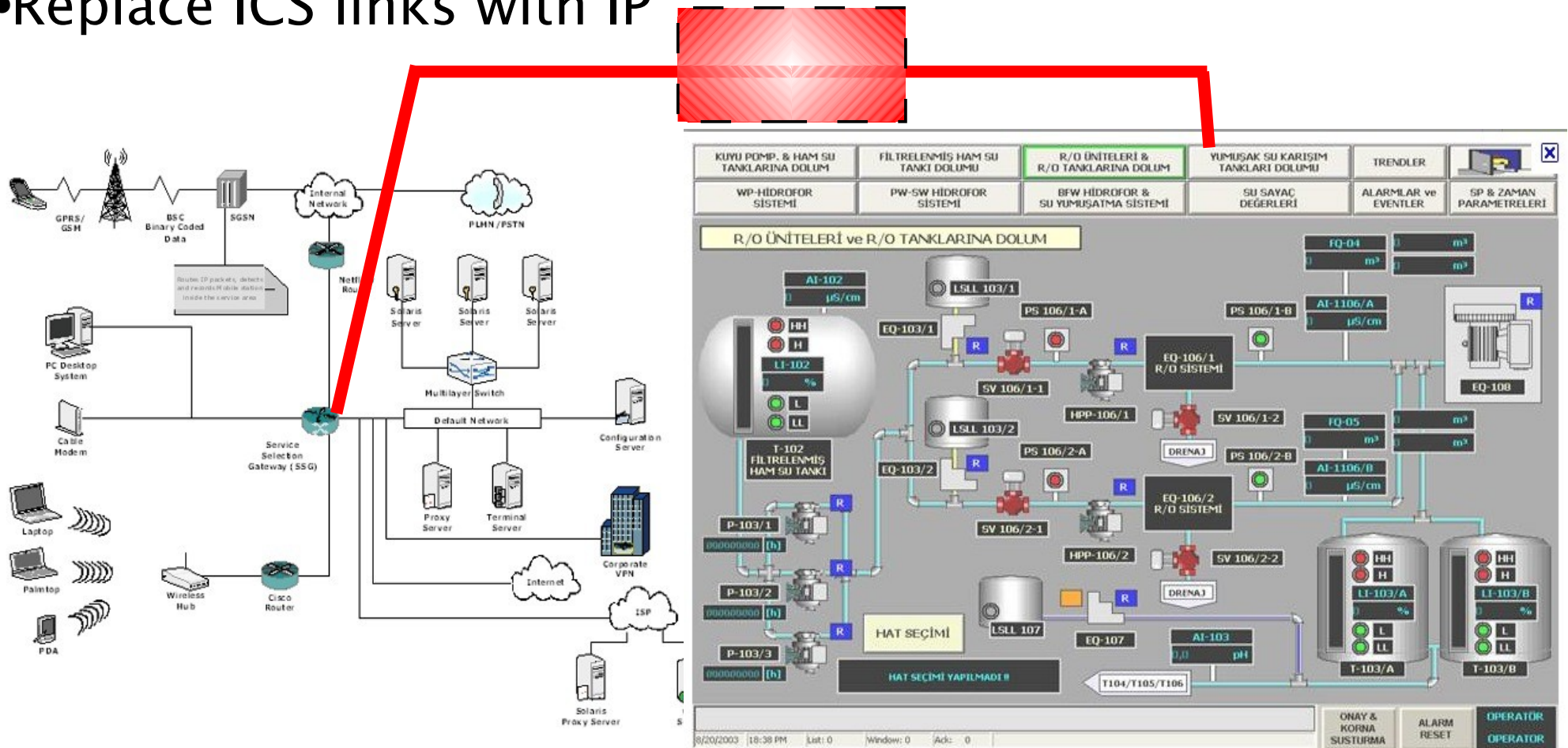


Typical IT architecture view



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 ...

• Watch the news stories come in...

Computer Worm Creates an Opening for Copycats

Monday, 11 Oct 2010 08:55 AM

By shaun Waterman

Share:     More ...

 | [Email Us](#) | [Print](#) | [Forward Article](#)

Stuxnet, the sophisticated summer, is a "wake-up call" for other cybersaboteurs, according to a cybersecurity consultant for

Although Stuxnet itself is considered to have inside knowledge, the worm has spread over the world, and there's no doubt it will be targets of less-discriminating

"The big fear is that Stuxnet will be used to launch similar attacks against other industrial systems, but Stuxnet was designed to infect and take

Researchers have been warning about the vulnerabilities of industrial systems, but Stuxnet was designed to infect and take

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

By Cassandra Sweet, of DOW JONES NEWSWIRE

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 question of when," NTSB Chief of Transportation Safety Board said Tuesday at a meeting in Washington. The pipeline, flawed since it was built, was

The agency was set to release a report on the nearly one-year investigation on Tuesday. It will discuss lessons learned

Our Infrastructures - Online And Vulnerable? Part 1 of 3



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!!!

- Introduction
- The many facets of energy security
- **Security decision making**
- Energy Sector Security Reference Architecture
- Summary / Conclusions / Discussion

	Low	Med	High	Disaster Recovery Planning 1 no disaster plan should be in place, 2 backup copies of critical data in a media safe 3 off-site copies of backups & tested recovery process 4 pre-arranged systems available a short time frame 5 multiple sites with redundant operational capabilities
s-h	123	34	5	
d-w	123	23	34	
w-m	12	23	3	

Time x Consequence

nature	location	Low	Med	High	Encrypt Data in motion never: don't encrypt it require: only if externally required convenient: if easy and inexpensive always: always encrypt
all	inside	never	required	required	
all	outside	required	required	required	
sensitive	inside	convenient	always	always	
sensitive	outside	required	always	always	

Decision-making frameworks

- A statement of belief (with some scientific support):
 - Decision-makers trying to make good decisions toward defined objectives tend to make better decisions (that is, decisions that more often move toward or attain their defined objectives) when they have a greater proportion of better information (that is, information that is more accurate and with defined and explained precision) than when they have a lesser proportion of better information.
- Luck favors the better informed
 - Better informed decision-makers tend to make better decisions
- How do we better inform decision-makers?
 - That depends on the nature of the decisions they have to make
 - Different sorts of decisions call for different sorts of information
- What are the properties of most security decisions?

What decision-makers see/need

- Security “requirements” are the most visible thing
- Standards are a good example
 - Risk management must be applied in making security decisions
 - COSO is the standard approved framework
 - Consider all levels of the organization
 - Get input across a variety of different aspects
 - Consider them in light of your tolerance for risk
 - Document a calculation method for your decisions (PRA)
 - Document the decision
 - Carry it out
- How exactly do I do that? No guidance is provided!
- In simple terms:
 - What are my alternatives?
 - Under what conditions should I choose which alternative?
 - How do I measure which condition I am in?

The keys to good decisions

- What are my alternatives?

- Security tends not to be “tunable”

- You can't increase protection by 2.31% based on a 0.0231 higher Fred*

- Most security decisions come down to deciding which of a small finite number of things will be done

- What maturity level will my security program have?

- None / initial / repeatable / defined / managed / optimizing

- Will I use a single perimeter, a layered defense, or no perimeter?

- Within those decisions, there are more decisions – of similar sort

- Decisions interact – so choosing some may rule out others

- If my maturity is initial, I cannot expect to have repeatable processes, which means I cannot support advanced technologies for detection and response, because they will break down

- Under what conditions should I choose which alternative?

- How do I measure which condition I am in?

* a Fred is an arbitrary unit of risk as defined by Fred

The keys to good decisions

- What are my alternatives?
- Under what conditions should I choose which alternative?
 - Some are fairly simple:
 - If maturity < defined THEN [various things I cannot do – they won't work]
 - Others are more complex:
 - They may be represented by other forms of decision support
 - Matrices of various sorts, Diagrams, Complex conditionals, etc.
 - There is no mapping for all security decisions and interactions
 - Enterprise information protection has been reasonably well covered
 - ICS information protection is being mapped in
 - Physical security is largely mapped in but not integrated
 - Other security fields have partial mappings but are not integrated
 - The basis for the various decisions are currently tenuous
 - There is no real science of security – and there is little support for it
- How do I measure which condition I am in?

The keys to good decisions

- What are my alternatives?
- Under what conditions should I choose which alternative?
- **How do I measure which condition I am in?**
 - Given specific conditions, specific metrics can be devised
 - What is my maturity level?
 - The CMM for security has detailed instruments that can be evaluated
 - But it's easy to approximate it with a few questions – for example:
 - Do you have detailed descriptions of processes?
 - Do you keep track of every step in each process?
 - Do you document each step in each process?
 - What do you do with the documented results?
 - Given the answers to these questions, the current level is pretty easy to get
 - **How do we know these measurements are good enough?**
 - They only have to be good enough to differentiate between the alternatives
 - If there are only 6 maturity levels, we might be able to determine which level by asking only 3 Yes/No questions

Decisions end up codified

JDM - Copyright(c), 2006-11, Fred Cohen - ALL RIGHTS RESERVED Licensed to Fred Cohen & Associates - Fred Cohen Until 2012 01 01

ICSSec AsIs Last Next Edit Mode Go 0:5-0 SABGFT Show Not New Set Quit

067 - PLCs: Network Connection: What protection mechanisms should be used between a PLC and a network??

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.

As-Is

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.
--------	---

Decision

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.
Low	No special protection is used for the PLC.

Basis

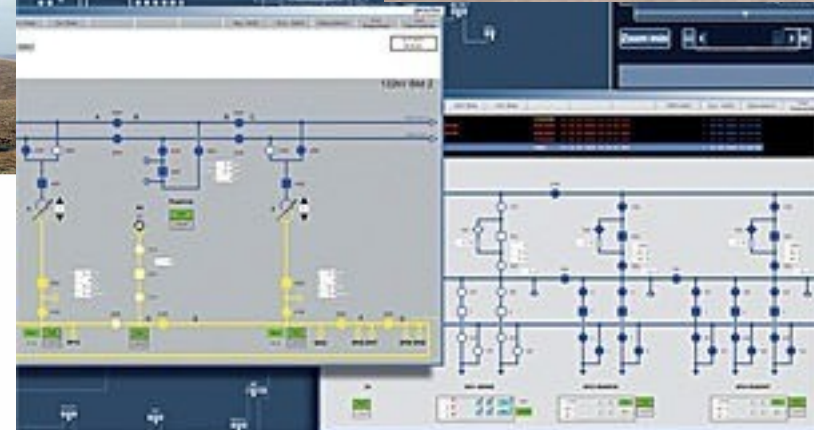
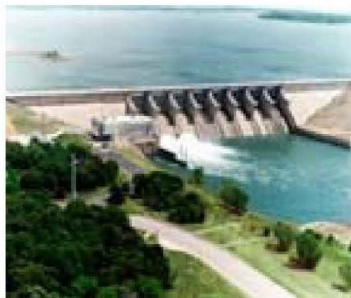
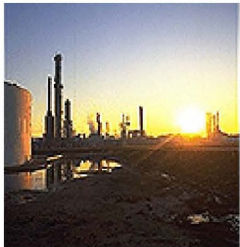
Restricted access network zone: Such a zone reduces the sources that can be used to directly influence and observe PLC inputs and outputs. When such a zone is available, it should be used unless there is a reason not to use it.

Use a custom FSM wrapper for the PLC input: A custom FSM for the input of a PLC provides a means by which all inputs can be checked for validity in the context of the expected machine state. This provides a high degree of certainty that unauthoriaed and unanticipated input sequences cannot appear at the PLC input.

Use a digital diode to exfiltrate PLC data: A digital diode can be used to prevent output channels from being used for input to a high degree of certainty.

Outline

- Introduction
- The many facets of energy security
- Security decision making
- **Energy Sector Security Reference Architecture**
- Summary / Conclusions / Discussion



- 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 into mechanisms that do it
- Operations, maintenance, and disposition
 - Doing the things that 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 / rationale
 - Create decisions surrounding those rational as well

Decision: connect PLCs to networks

•What are my options?

- Option A: No special protection is used for the PLC. A horizontal line representing a network with a vertical tick mark on the left labeled "PLC".
- Option B: Use a restricted access network zone for the PLC. A horizontal line representing a network with a vertical tick mark on the left labeled "PLC". A blue square is positioned to the right of the tick mark, and the entire area between the tick mark and the right edge is enclosed in a double-line border.
- Option C: Use encrypted communications for the PLC. A horizontal line representing a network with two black dots on it. A red line segment connects the two dots. The left dot is labeled "PLC".
- Option D: Use a custom FSM wrapper for the PLC input. A horizontal line representing a network with a vertical tick mark on the left labeled "PLC". A diamond shape is positioned to the right of the tick mark.
- Option E: Do not connect the PLC to the network. A horizontal line representing a network with a vertical tick mark on the left labeled "PLC". There is a gap between the tick mark and the rest of the line.
- Option F: Use a digital diode to exfiltrate PLC data. A horizontal line representing a network with a vertical tick mark on the left labeled "PLC". A triangle pointing to the right is positioned to the right of the tick mark.

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 rationale 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 makes 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?

- Today, reference architecture exists for:
 - Enterprise information protection
 - ICS protection for select areas
 - Physical security for select areas
 - Personnel security for select areas
- But trying to boil the ocean will not work today
 - Other areas largely uncovered
 - Trying to be all things for all people takes a lot of time, effort, expertise, money, commitment, etc.
- Alternative: build it for some portions of some sectors
 - Energy is a prime candidate – but not being widely supported yet
 - Finite problem space with a limited set of industries and situations
 - High importance and value for national and global security
 - Organizations dedicated to the space (e.g., EnergySec, DoE)

Outline

- Introduction
- The many facets of energy security
- Security decision making
- Energy Sector Security Reference Architecture
- **Summary / Conclusions / Discussion**

nature	location	Low	Med	High
all	inside	never	required	required
all	outside	required	required	required
sensitive	inside	convenient	always	always
sensitive	outside	required	always	always

Encrypt Data in motion
never: don't encrypt it
require: only if externally required
convenient: if easy and inexpensive
always: always encrypt



The strategic challenge

•The Problem

- Security decisions are haphazard, unstructured, often 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 frameworks

- An approach to better decision-making
 - 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?



info@fredcohen.net