

# Using architectural analysis tools for better protection decisions

ICSJWG - October 26, 2011

Dr. Fred Cohen - CEO - Fred Cohen & Associates

- Introduction and Overview
- Security decision making
- Reference architecture and its analytical basis
- Tools to support architectural analysis
- Summary / Conclusions / Discussion



# 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)
  - ISC<sup>2</sup> 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

---

- Protection is a broad, complex, poorly understood issue
  - Perhaps the best exemplar of this is information protection
- 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-prior vs. posteriori)
  - Risk management
    - Two poorly defined terms mashed together reflective of the challenge
- Some decisions can be standardized – others cannot
  - Some of them have a (sometimes sound) basis
  - We have to make choices (because we have limited options)
  - Reference architecture provides a path to better decisions
- Tools can help support improved decision-making

# Outline

- Introduction and Overview
- **Security decision making**
- Reference architecture and its analytical basis
- Tools to support architectural analysis
- Summary / Conclusions / Discussion



**Security is NOT  
One Size Fits All**

**You have to  
Make decisions**





# 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?

# Dimensions of decision-making

- Different sorts of decisions call for different sorts of tools
  - We generally start with a tool to identify the nature of the decisions being made
  - Based on results, we choose tools to help make better decisions.

- 000 – Objective-Subjective: Is the decision process Objective, Subjective, or a combination of both?
- 001 – Quantitative-Qualitative: Is the decision process based on Qualitative or Quantitative data or Both?
- 002 – Nominal-Ordinal-Interval-Ratio: What sort of metrics are available or desired for this decision making process?
- 003 – Hierarchical-Flat: Is the decision space hierarchical or flat?
- 004 – Simple-Complex: Is the decision simple or complex?
- 005 – Explanatory-Predictive: Is the decision process designed to explain what is or predict what will be?
- ✓ 006 – Group-Individual: Is the decision process for individual decision makers or decisions made by groups?
- 007 – Casual-Formal: Is the decision formalized or ad-hoc?
- 008 – Text-Visualization: Is the decision presented and analyzed in a text or visualization format?
- 009 – Strategic-Tactical: Is the decision a local or overarching decision?
- 010 – Optimizing-Satisficing: Is the decision model decision optimizing, satisficing, incremental, cybernetic, or random?
- 011 – Supply-Demand: Is the decision process driven by communications, data, models, knowledge, or users?
- 012 – Evaluation-Criteria: What are the evaluation criteria used?
- 013 – Tempo: What is the interaction rate and tempo of decision-making?
- 014 – Amplitude-Architecture: Are the decisions related to differences in kind or magnitude?
- 015 – Designed: Is the decision process designed and programmed or ad-hoc?
- 016 – Personal: Is the decision personal to the individual or group, or related to work or business?
- 017 – Expertise: What should the expertise level of the decision maker be?
- 018 – Static or Dynamic: Is the decision process static or dynamic?
- 019 – Single or Multiple Intentions: Is the decision in cooperation or competition with other decision makers?

# Protection architecture decisions

- The nature of the protection architecture decision space:
  - Objective and Subjective / Qualitative / Nominal, Ordinal / Flat / Complex (one of many) / Predictive / Group / Casual → Formal / Text (mostly) / Strategic (architecture) / Satisficing / Driven by models and knowledge / Decisions made for periods of 5+ years / Architectural / Ad-hoc → programmed / group, business / professional decision-maker supported by a group / Static for dynamic situations / Multiple intentions in cooperation and competition with other decision makers.
- The nature of the space leads to decisions about the selection of decision-making methodologies and tools e.g.,
  - The mathematical characteristics lead to selections between small numbers of finite alternatives
    - This is amenable to IF-THEN-ELSE conditionals, tables, etc.
  - Satisficing, long time-frame, desire for programmed decisions
    - This is amenable to written decisions with textual basis
  - Etc.



# 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 increasing 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



# Outline

- Introduction and Overview
- Security decision making
- **Reference architecture and its analytical basis**
- Tools to support architectural analysis
- Summary / Conclusions / Discussion

	Low	Med	High	<b>Disaster Recovery Planning</b> 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	<b>Encrypt Data in motion</b> 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	

# Why an architectural framework?

- A house built on an architectural framework





# Why an architectural framework?

- OR- a house built without one



There's a reason we use  
architectural frameworks

# 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

# 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. 

# 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?

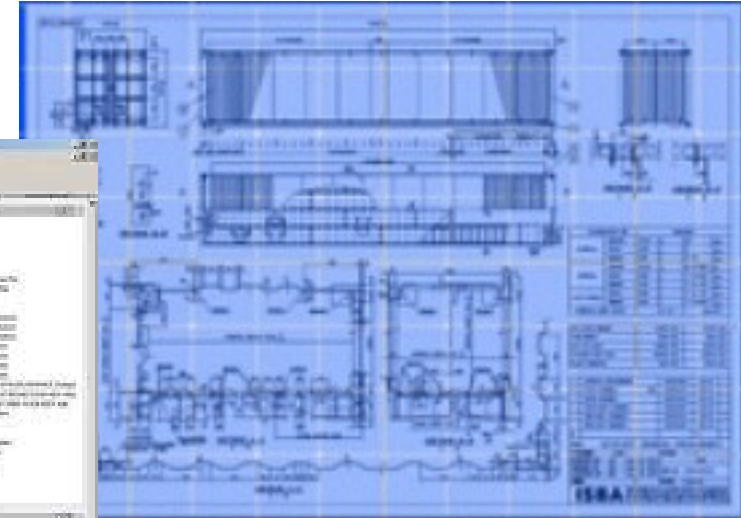
# Reference architecture summary

---

- An approach to better decision-making
- Find commonalities and differences between architectures
- Understand the reasons for different decisions
- Identify the alternatives used and available
- Make rational decisions about which alternative works when
- Codify decisions in a meaningful and justified framework
- Understand and deal with interdependencies

# Outline

- Introduction and Overview
- Security decision making
- Reference architecture and its analytical basis
- **Tools to support architectural analysis**
- Summary / Conclusions / Discussion





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**

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

Medium	<p><b>IF</b> the PLC interaction rate allows for encryption <b>AND</b> encryption does not interfere with an FSM wrapper,</p> <p><b>THEN</b> Use encrypted communications for the PLC.</p> <p><b>IF</b> a restricted network zone for PLC operations is in place in the enterprise,</p> <p><b>THEN</b> Use a restricted access network zone for the PLC.</p>
--------	--

**Decision**

Medium	<p><b>IF</b> the PLC interaction rate allows for encryption <b>AND</b> encryption does not interfere with an FSM wrapper,</p> <p><b>THEN</b> Use encrypted communications for the PLC.</p> <p><b>IF</b> a restricted network zone for PLC operations is in place in the enterprise,</p> <p><b>THEN</b> Use a restricted access network zone for the PLC.</p>
Low	No special protection is used for the PLC.

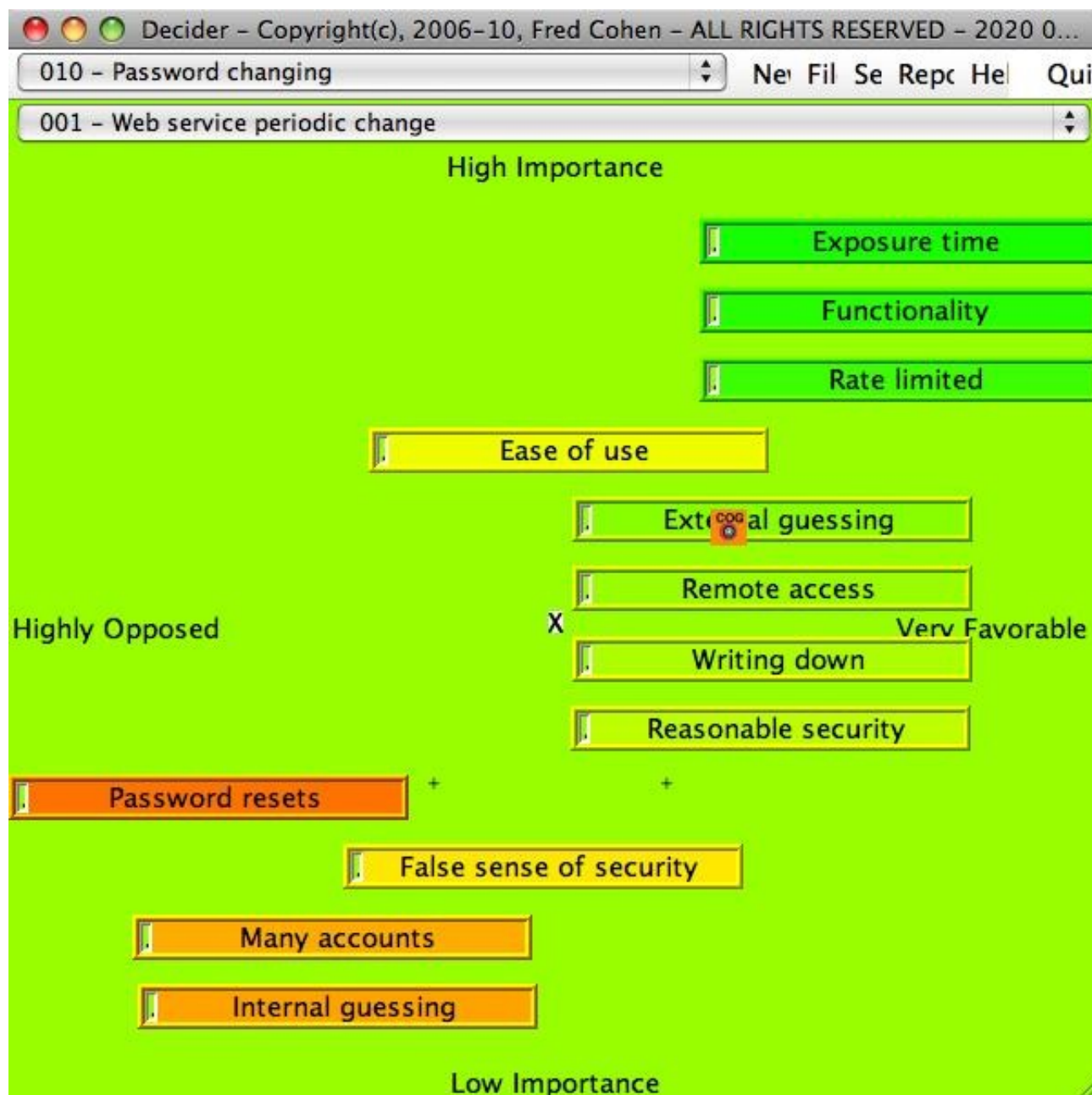
**Basis**

**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.

# Decision-making tool demo





# Metrics tool demo

Metrics - Copyright(c), 2006-11, Fred Cohen - ALL RIGHTS RESERVED Licensed to Fred Cohen & Associates - Fr...

001 - 2011-04-27-ICS-IEC    CheckList    Set   Go   Help   Report   Put   Quit

014 - IEC-4.5-Capability.Silver System capability PAs - Silver Certification level

Select levels for Required, Specified, Managed, Processed, Executed, and add comments as desired.

Req	Pol	Harden the system - Document requirements - RE(1): The Vendor shall document data flows and storage points with identification of sensitive information. NOTE The Principal approves the requirements for sensitive information.	The vendor software does not support ACLs and misoperates when ACLs in our configuration are changed after system startup. This is not documented.
Req	Pol	Harden the system - Document requirements - RE(2): The Vendor shall document the segmentation architecture between the control system domain and other domains e.g., separation between the development domain and the control system domain. NOTE Third party security architecture reviews required by BP.04.03, as supported by BP.22.01, determine the adequacy of separation between domains.	The vendor software does not support ACLs and misoperates when ACLs in our configuration are changed after system startup. This is not documented.
Req	Pol	Harden the system - Document requirements - RE(3): The Vendor shall document the data retention capability provided by the Vendor's system including data pruning functions, retention timeouts, data purging, etc.	The vendor software does not support ACLs and misoperates when ACLs in our configuration are changed after system startup. This is not documented.
Req	Pol	Harden the system - Document requirements - RE(4): The Vendor shall document the formatting of security extensions provided for servers used in the Vendor's system. NOTE The Microsoft Windows® new technology file system (NTFS) with access control lists and files system journaling provides the needed security strength.	The vendor software does not support ACLs and misoperates when ACLs in our configuration are changed after system startup. This is not documented.
Req	Pol	Harden the system - Manage 3rd party software - No added requirements exist at the Silver level.	
Req	Pol	Harden the system - Conduct 3rd party security architecture reviews - RE(1): The Vendor shall document policies and procedures to ensure only those ports and services required for normal and	They used the "Acceptable" method and this is not preferred for our environment. However, it passes the standard per the specifics of the requirement.



- Introduction and Overview
- Security decision making
- Reference architecture and its analytical basis
- Tools to support architectural analysis
- **Summary / Conclusions / Discussion**



# Status

---

- Today, reference architecture exists for:
  - Enterprise information protection
  - ICS protection for select area
  - Physical security for select areas
  - Personnel security for select areas
- Tools are fairly effective for these sorts of decisions
  - Enterprise protection decisions are well codified
  - ICS architectural decisions are increasingly codified
  - But consensus is lacking over ICS reference architecture
- More tools don't mean better tools...
  - Today's architecture frameworks are limited
  - Today's science of security is too rudimentary for better tools
  - ICS has not yet come to maturity in terms of security architecture



# The strategic challenge

---

- The problem today

- 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 we need

- Build structured architectural decisions with defined (sound?) basis

- Create a consistent, acceptable, meaningful decision process
    - Integrate that process across enterprise IT and ICS environments

- The tools are reasonably ready – but the decisions are not

- 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**