The 2012 OWASP AppSec DC

Cyber Threats to Civil Infrastructure:

...Are we meeting the challenge?

BAYSHORE NETWORKS

Presented by:

Francis Cianfrocca
CEO, Bayshore Networks LLC

5 April 2012

“Who is this guy?”

“Who is this guy?”

I’m Francis Cianfrocca, pleased to meet you.

I’m the CEO of

BAYSHORE NETWORKS

Information Assurance for YOUR Mission

“What does Bayshore Networks do?”

"What does Bayshore Networks do?"

...We make next-generation firewalls for enterprises

...We make SCADA firewalls for industry and infrastructure

...Founded in 2002, we're based in New York City

...And we're proud to sponsor OWASP!

BAYSHORE NETWORKS

www.bayshorenetworks.com

“Who are YOU?”

What we’re talking about today:

The Cyberthreat to Industry and Infrastructure

BAYSHORE NETWORKS

The Cyberthreat to Industry and Infrastructure

Understanding the Problem

The Cyberthreat to Industry and Infrastructure

Understanding the Problem

Understanding Current Practice

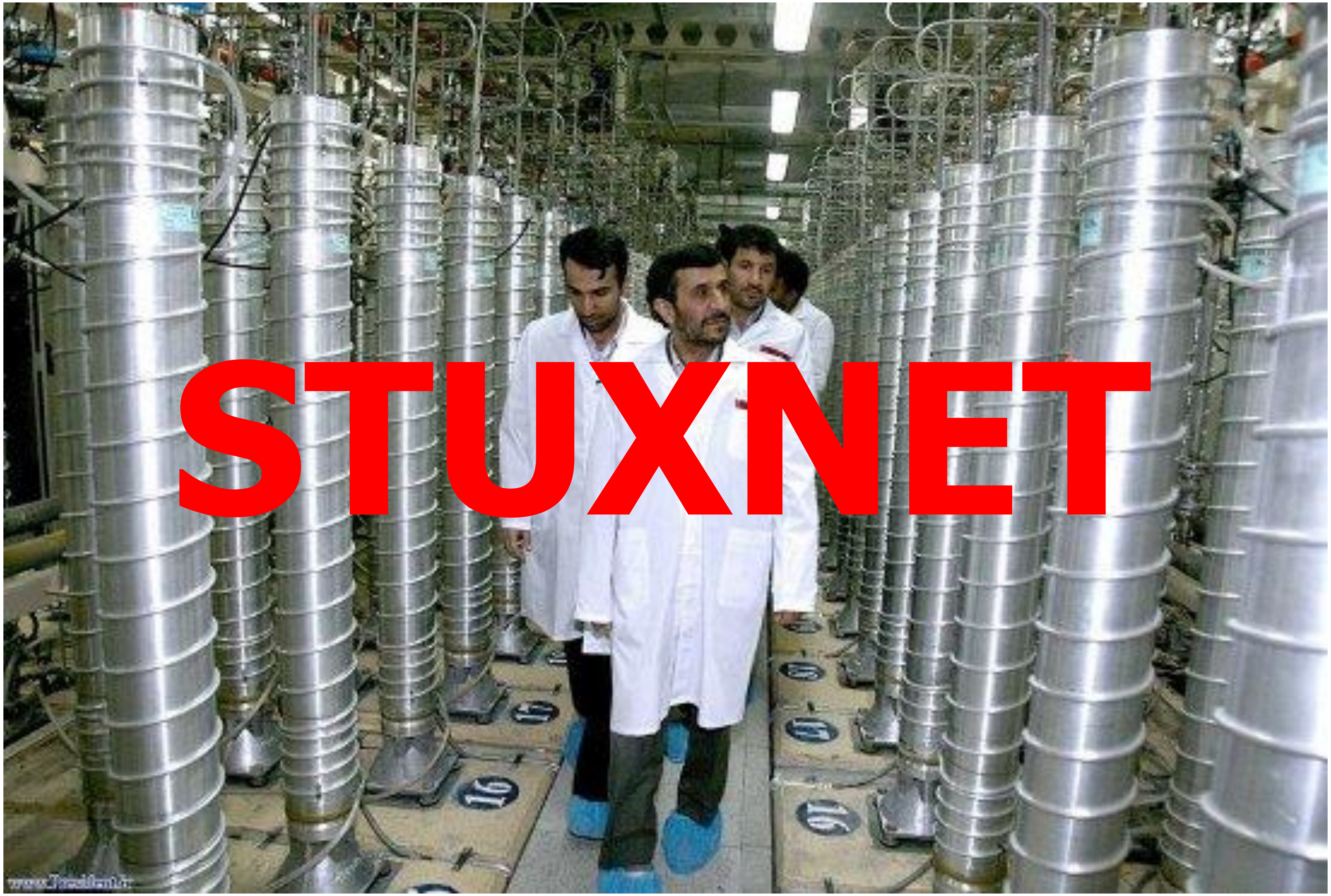
Where are the gaps between need and action?

How can we improve on current practice?

How **will** we improve on current practice?

Caption Contest!

STUXNET



"Hey, What Could Go Wrong?"

Could we have an “oh shoot” moment?

...Well, what’s vulnerable?

...Well, what's vulnerable?

The electric-industry was early to recognize the risks.

Still, security efforts are compliance-driven and reliability-constrained.

BAYSHORE NETWORKS

www.bayshorenetworks.com

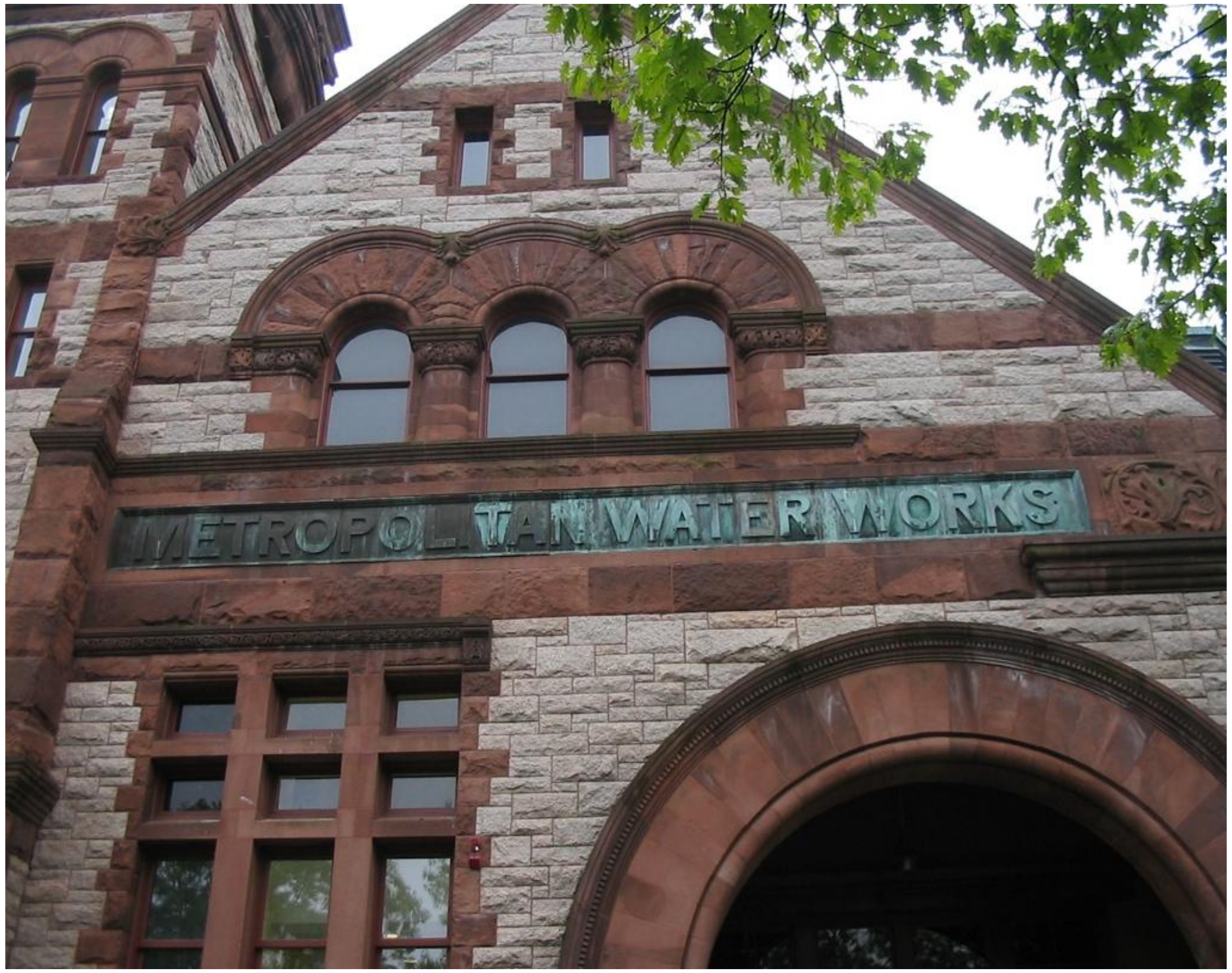
...What's vulnerable?

In oil and gas, there are meaningful business drivers for better cybersecurity.

BAYSHORE NETWORKS

www.bayshorenetworks.com

...What's vulnerable?



...What’s vulnerable?

BAYSHORE NETWORKS

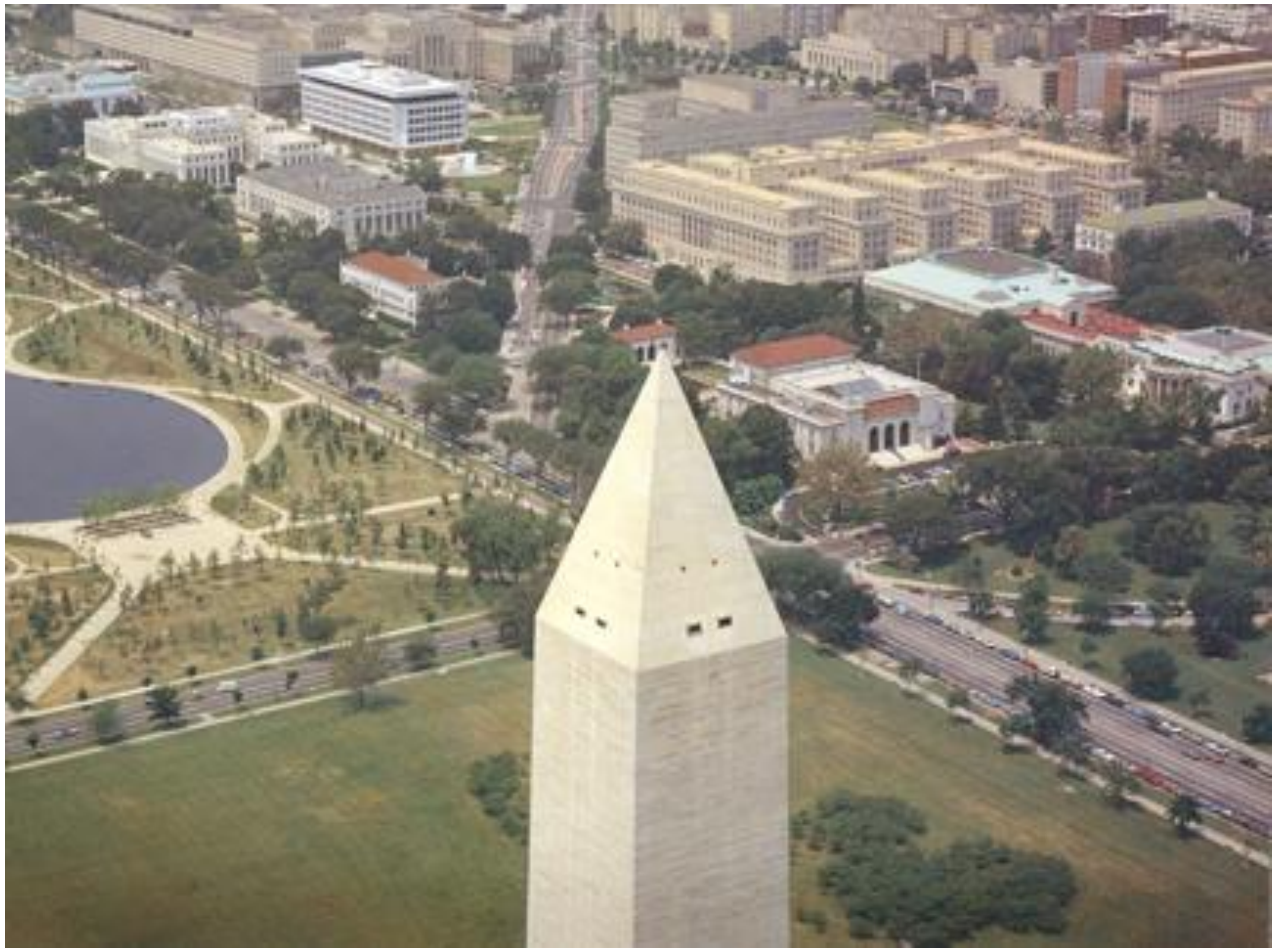
www.bayshorenetworks.com

...What's vulnerable?

Copyright © 2012 by Bayshore Networks LLC. All Rights Reserved

...What's vulnerable?

...What's vulnerable?



But is the threat overhyped... or realistic?

...Let’s take a closer look.

What is SCADA anyway?

What is SCADA anyway?

Supervisory **C**ontrol **a**nd **D**ata **A**cquisition

SCADA is a systems-management architecture

“What does it manage?”

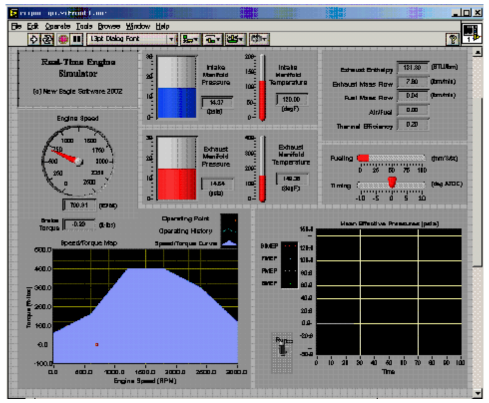
Industrial Processes

Infrastructure

Facilities Management

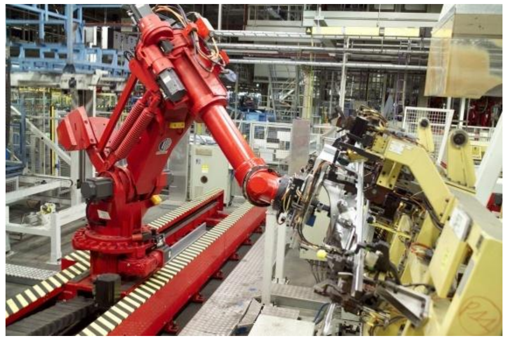
Government/Military

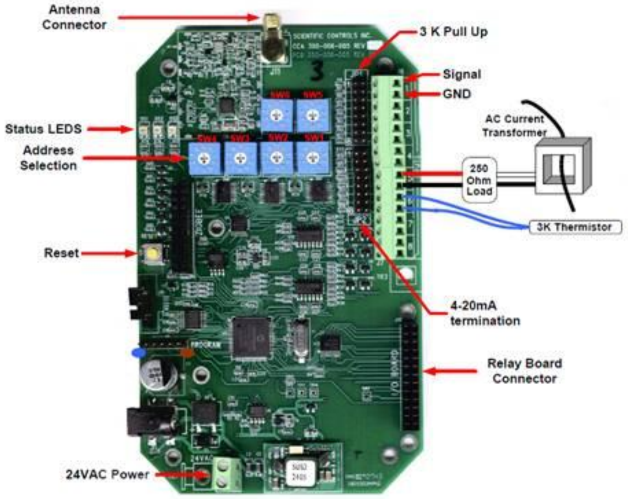
“What are the key SCADA components?”



Engine Speed 700.91 (RPM)
Brake Torque -0.23 (ft-lbs)
Intake Manifold Pressure 14.37 (psia)
Intake Manifold Temperature 120.00 (degF)
Exhaust Manifold Pressure 14.64 (psia)
Exhaust Manifold Temperature 149.36 (degF)
Exhaust Enthalpy 131.30 (BTU/lbm)
Exhaust Mass Flow 7.80 (lbm/min)
Fuel Mass Flow 0.04 (lbm/min)
Air/Fuel 0.00
Thermal Efficiency 0.20
Fueling (mm^3/str)
Timing (deg ATDC)

Human-machine interfaces





Remote terminal units

Programmable logic controllers

And all the stuff we're trying to manage...

Copyright © 2012 by Bayshore Networks LLC. All Rights Reserved

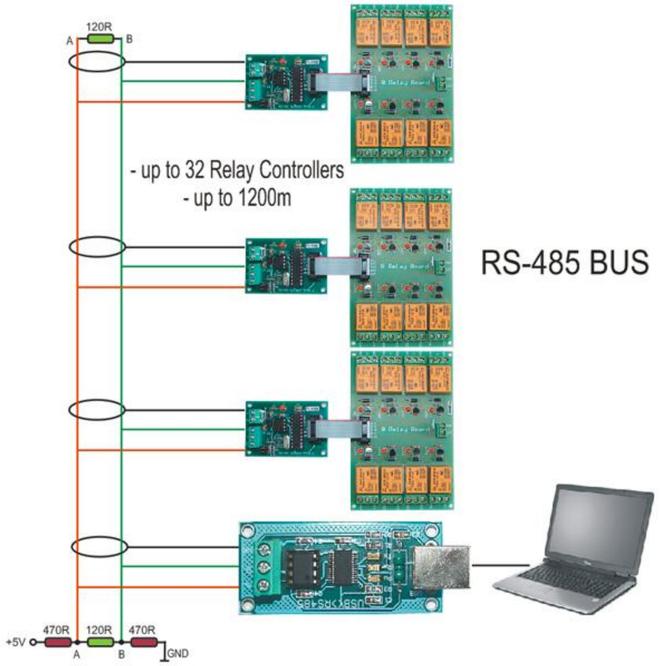
www.bayshorenetworks.com

“What about Communications?”

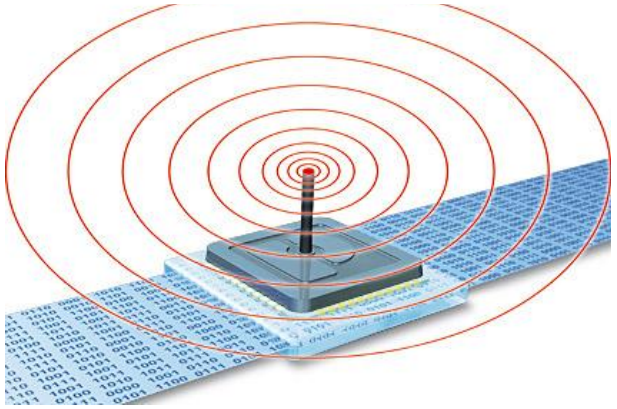
“What about Communications?”

Radio/Satellite

Serial RS-422/485



Wireless



Proprietary Electrics

Ethernet

“What about Protocols?”

“What about Protocols?”

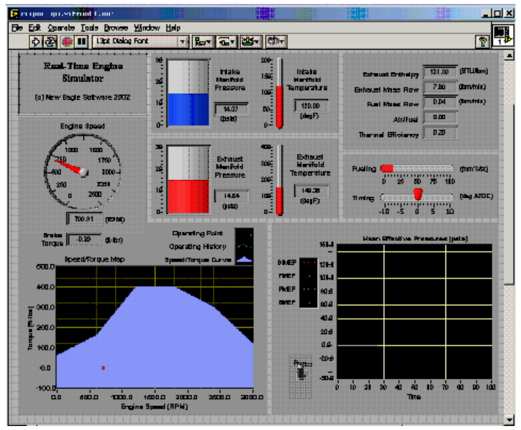
Modbus (TCP)
DNP3
IEC 61850
ANSI C12.19/C12.22

BacNet
Profibus
Proprietaries

Many, many others

And SCADA has been around for decades...

...which leads to **major** security problems.



Intake Manifold Pressure 14.37 (psia)

Intake Manifold Temperature 120.00 (degF)

Exhaust Manifold Pressure 14.64 (psia)

Exhaust Manifold Temperature 149.36 (degF)

Exhaust Enthalpy 131.30 (BTU/lbm)

Exhaust Mass Flow 7.80 (lbm/min)

Fuel Mass Flow 0.04 (lbm/min)

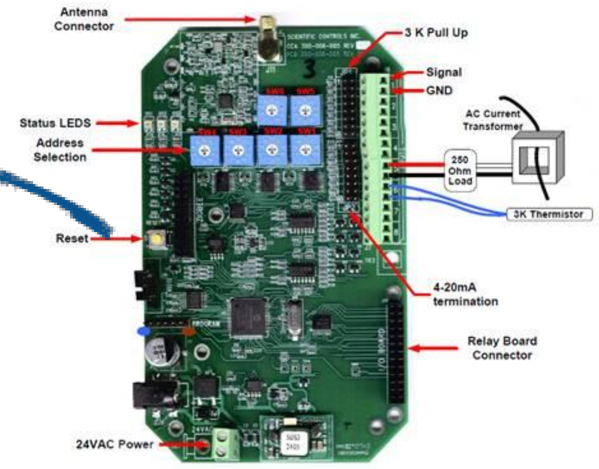
Air/Fuel 0.00

Thermal Efficiency 0.20

700.91 (RPM)

Brake Torque -0.29 (ft-lbs)

Increase motor speed to 8500 RPM!



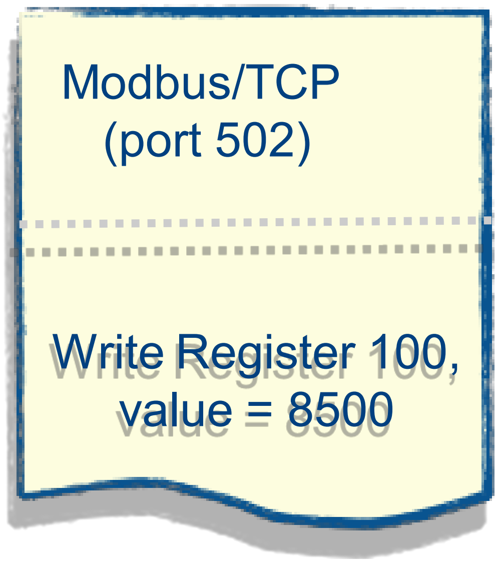
Copyright © 2012 by Bayshore Networks LLC. All Rights Reserved

www.bayshorenetworks.com

Increase motor speed to 8500 RPM!

Modbus/TCP (port 502)

Write Register 100, value = 8500



Modbus/TCP
(port 502)

Write Register 100,
value = 8500

Not just motor speeds...

Pressure-vessel settings

Boiler temperatures

Solenoids and actuators

...simply *anything*

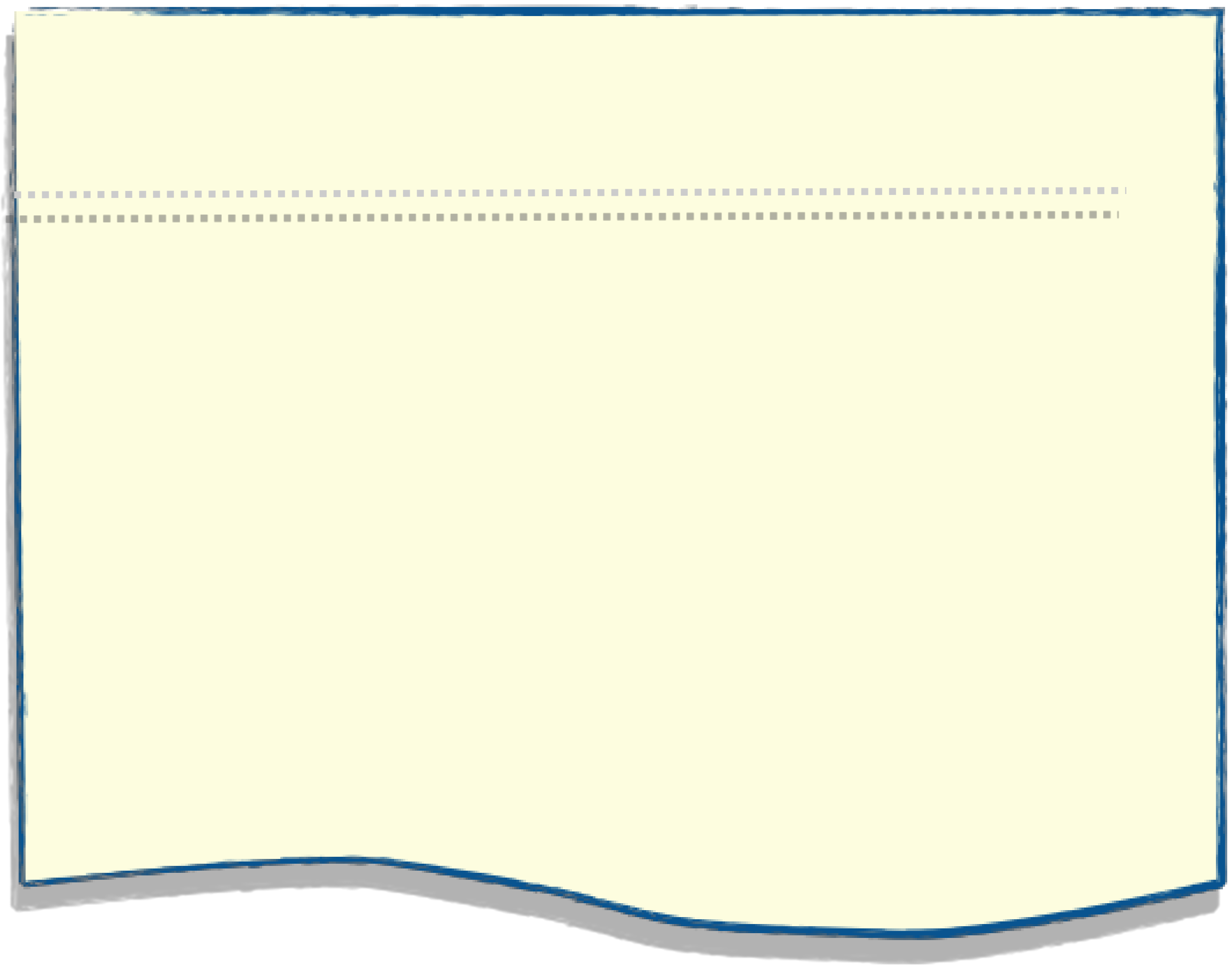
Modbus/TCP (port 502)

Read Registers 1-100

Execute functions 17, 43

Read coil values

You can read data as well.



And there are all the other protocols too.

Evil!

What does it take to do real damage?

...or, just how threatening is all this?

Evil!

What does it take to do real damage?

...or, just how threatening is all this?

The bad guys need to know the protocols

They need to know your gear

They need privileged access

That's a determined, knowledgeable, we
resourced bad guy.

Evil!

What does it take to do real damage?

...or, just how threatening is all this?

The casual-hacking threat is not as high as it is with enterprise applications

And SCADA has been around for decades...

...which leads to **major** security problems.

And SCADA has been around for decades...

...which leads to **major** security problems.

Why?

Security by obscurity

Security by obscurity

Operators often assume physical and network isolation

...And they assume ignorance of protocols and operations

...And they're focused on compliance and risk-management anyway

What's missing?

BAYSHORE NETWORKS

What’s missing?

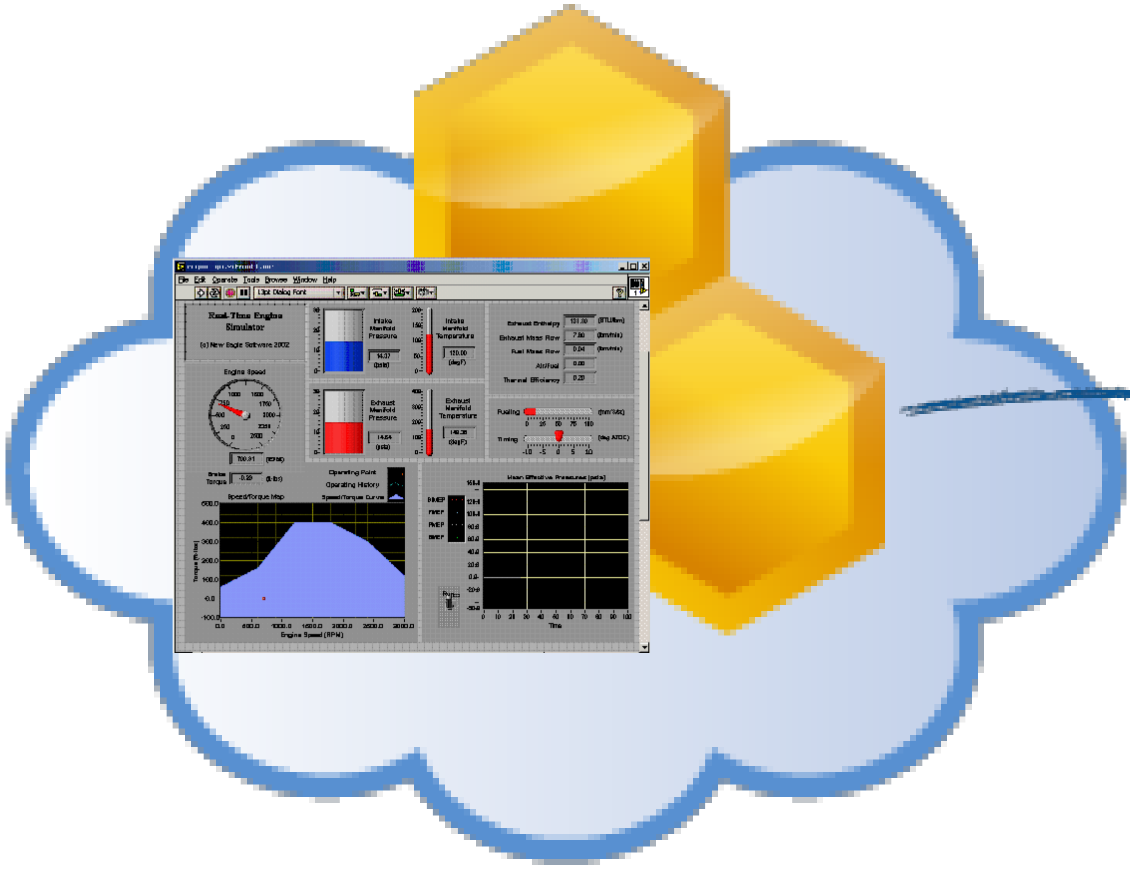
Oh, right, the enterprise network.

“But control data shouldn’t be on the internet”

News flash: **It already is.**

How did it get there?

How did it get there?


File Edit Operate Tools Browse Window Help
13pt Dialog Font
Real-Time Engine Simulator
(c) New Eagle Software 2002
Engine Speed
Intake Manifold Pressure
Intake Manifold Temperature
Exhaust Manifold Pressure
Exhaust Manifold Temperature
Speed/Torque Map
Torque (ft-lbs)
Engine Speed (RPM)
Operating Point
Operating History
Speed/Torque Curve
Mean Effective Pressures (psia)
BMEP
FMEP
PMEP
IMEP
Time

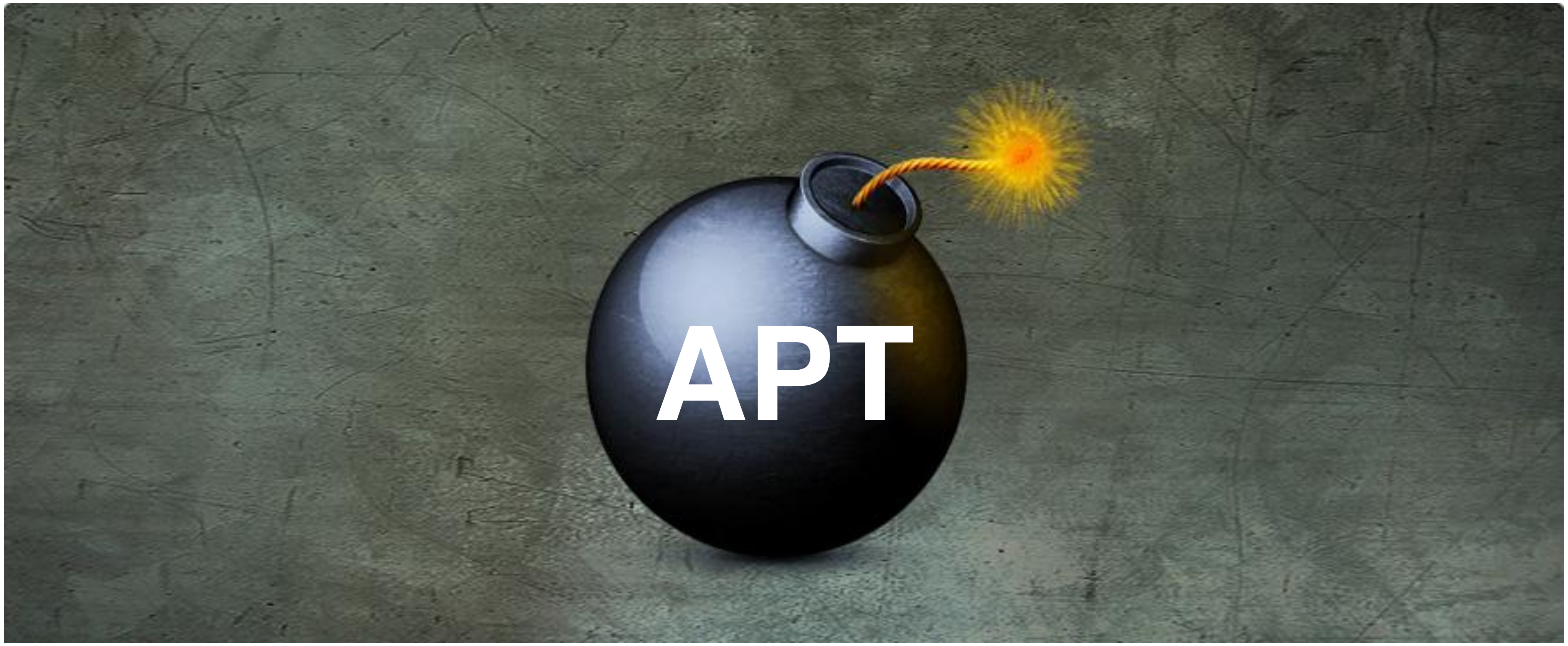
Exhaust Enthalpy 131.30 (BTU/lbm)
Exhaust Mass Flow 7.80 (lbm/min)
Fuel Mass Flow 0.04 (lbm/min)
Air/Fuel 0.00
Thermal Efficiency 0.20
Fueling (mm^3/st)
Timing (deg ATDC)
700.31 (RPM)
Brake Torque -0.29 (ft-lbs)
14.37 (psia)
120.00 (degF)
14.64 (psia)
149.38 (degF)

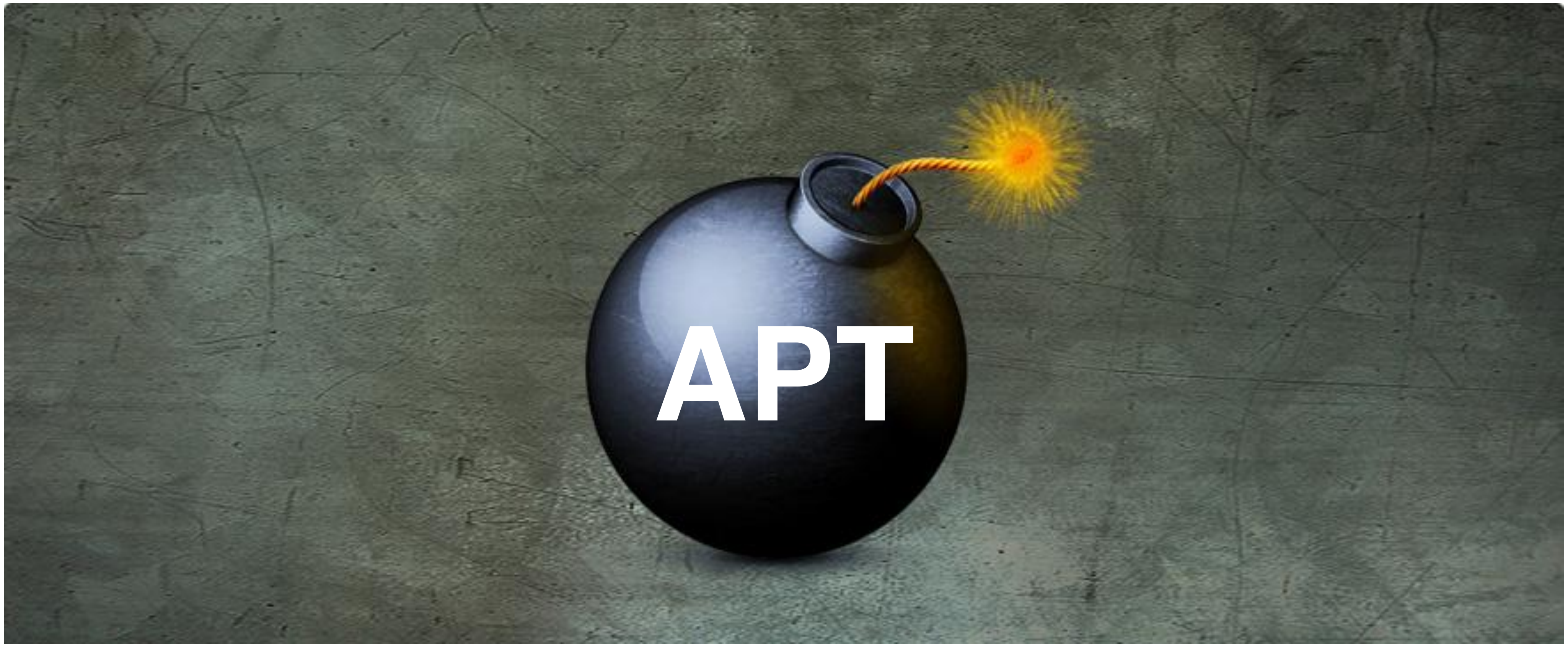
And what else is on your enterprise network?

BAYSHORE NETWORKS

www.bayshorenetworks.com

And what else is on your enterprise network?



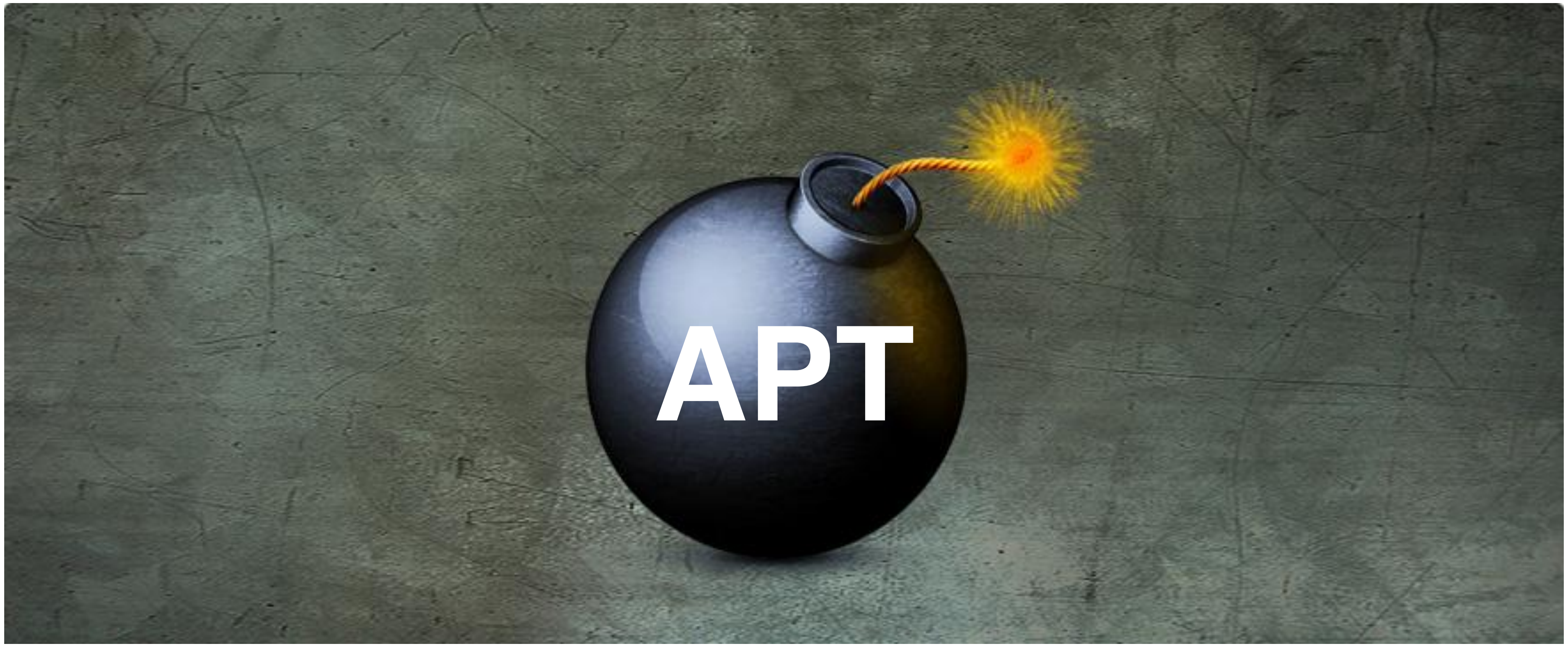


What do we know about these bad guys?

They're determined, knowledgeable and well-resourced

They're learning your protocols and your gear

...And they're in your network **now.**

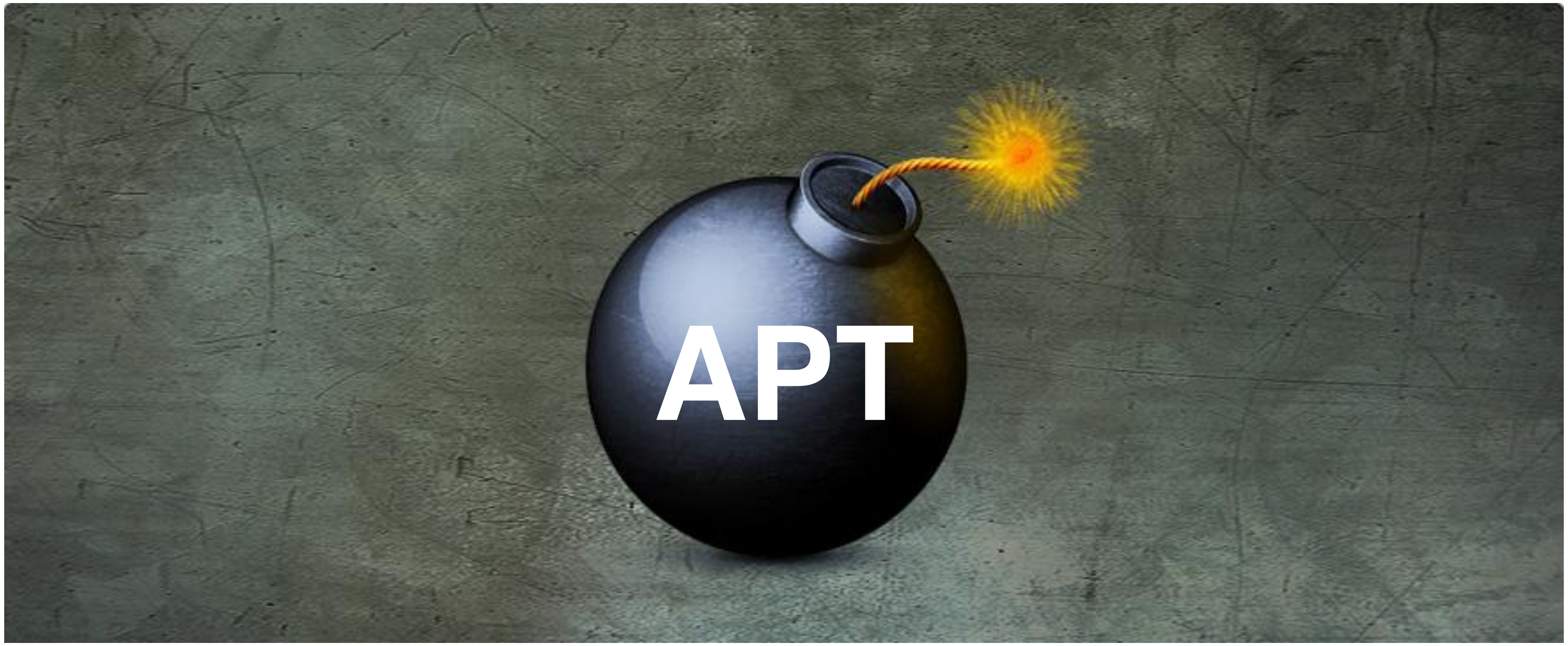


What are their objectives?

Recon

Data exfiltration

Cyberattacks



NOW you should be scared.

A **disconnect** between need and action

A **disconnect**
between need and action

Is there a technical response?

Is there a technical response?

Lock your doors

Follow OWASP recommendations

Consider unidirectional flows

Use SCADA gateways

Who are the bad guys?

Who are the bad guys?

...Not so much

Who are the bad guys?

...Yup, these guys and their buddies

Who are the bad guys?

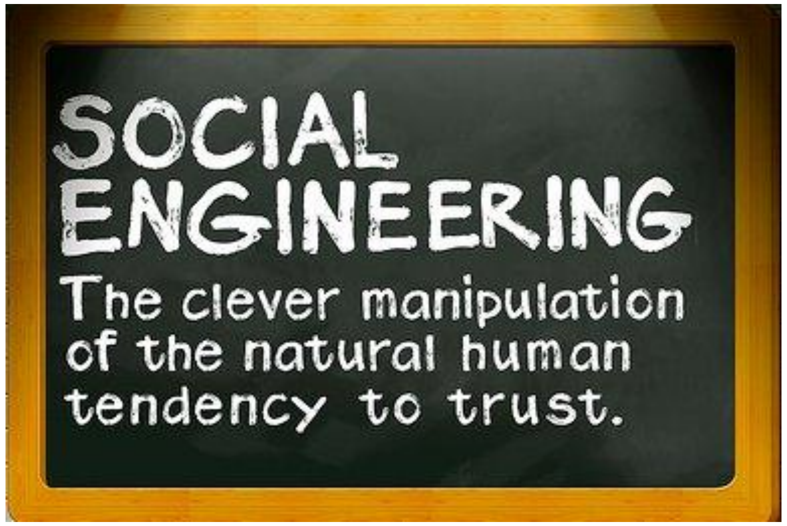
...These guys too.

Who are the bad guys?

You worry about the ones you don't know are there.

Who are the bad guys?

You worry about the ones you don't know are there.



SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

...There's an app for that

SCADA Gateways

SCADA Gateways

Firewall?

...depends on your definition

SCADA Gateways

Essential Features...

SCADA Gateways
Essential Features...

A protocol-aware network filter...

Level-7 Firewall

...That can enforce policy

deny modbus.write-register[100] > 8000

SCADA Gateways

Operational Models

SCADA Gateways

Operational Models

In-line (blocking)

Out-of-band (advisory)

SIEM integration and threat-intelligence

SCADA Gateways

Deployment Models

SCADA Gateways
Deployment Models

"I don't want another box in my ICS enclave!"

SCADA Gateways
Deployment Models

No, but the threat starts from the enterprise network

SCADA Gateways
Deployment Models

No, but the threat starts from the enterprise network

...deploy the SCADA gateways there.

But you also may need field deployments

SCADA Gateways

Configuration and Management

SCADA Gateways

Configuration and Management

Automatic Learning is a MUST

Capital-equipment vendors must integrate it

Behavioral analysis is a critical future capability

SCADA Gateways

Behavioral analysis is a critical future capability

What does that mean?

SCADA Gateways

Behavioral analysis is a critical future capability

Heuristic baselining

...Let the systems tell you what "normal" is

SCADA Gateways

Behavioral analysis is a critical future capability

Heuristic baselining

Big-data Analytics

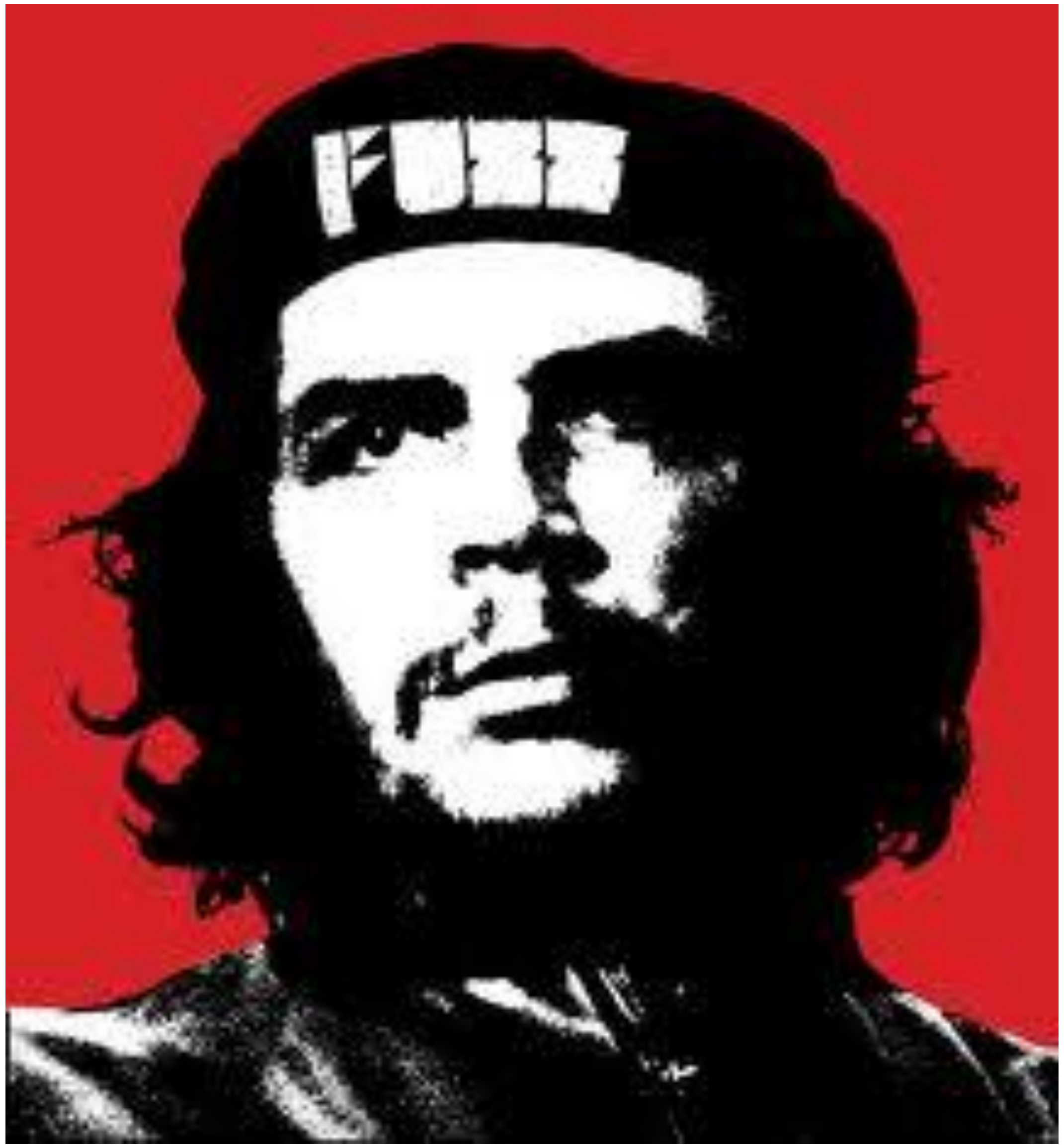
hadoop

H·BASE

accumulo™

Pre-announcing the SCADA Fuzzer!

Pre-announcing the SCADA Fuzzer!



Pre-announcing the Bayshore SCADA Fuzzer!

An open-source tool...

...Assists in pen testing and vulnerability assessment

Pre-announcing the SCADA Fuzzer!

An open-source tool...

...Assists in pen testing and vulnerability assessment

Native support for multiple protocols

Modbus/TCP

DNP3

Bacnet/IP

Profibus

Pre-announcing the SCADA Fuzzer!

An open-source tool...

...Assists in pen testing and vulnerability assessment

Recon Phase

Scans ports and interrogates for native responses

Doesn’t depend on well-known ports

Fingerprints

enumerates IDs, detects specific devices

Pre-announcing the SCADA Fuzzer!

An open-source tool...

...Assists in pen testing and vulnerability assessment

Attack Phase

Intelligent fuzzing

Mutating vectors

Known working exploits

Input from honeypots to big-data database

BAYSHORE NETWORKS

Pre-announcing the SCADA Fuzzer!

An open-source tool...

...Assists in pen testing and vulnerability assessment

Developed by the lead developer of OWASP's WS Fuzzer!

Wrapping up...

What **will** we do about the cyberthreat?

What **will** we do about the cyberthreat?

Near term, not much.

...Business and organizational reality intrudes

What **will** we do about the cyberthreat?

Meanwhile, the danger level is very high, and getting higher.

☠

What **will** we do about the cyberthreat?

Action Items

What **will** we do about the cyberthreat?

Action Items

Vulnerability assessments

Capital-equipment vendor support

Best-practices formulation

The costs and risks are too high to go it alone

What **will** we do about the cyberthreat?

The Players

What **will** we do about the cyberthreat?

The Players

Capital-equipment vendors

DIB companies

Regulators

Industry Groups

What **will** we do about the cyberthreat?

The Process

What **will** we do about the cyberthreat?

The Process

Negotiating the Rules

Federally-funded pilot projects

What **will** we do about the cyberthreat?

The Technology

What **will** we do about the cyberthreat?

The Technology

Technology matters **tremendously**,
because we're in a race

What **will** we do about the cyberthreat?

The Technology

Technology matters **tremendously**, because we're in a race

SCADA Gateways

Heuristic baselining

Behavioral Analytics

What **will** we do about the cyberthreat?

Legislation

What **will** we do about the cyberthreat?

Legislation

Several bills in the House

Lieberman-Collins and McCain in the Senate

Whose jurisdiction?

...This could be the year

What **will** we do about the cyberthreat?

Bottom Line

What **will** we do about the cyberthreat?

Bottom Line

We’re now in a very high risk position

Where enterprises were five years ago

What **will** we do about the cyberthreat?

Bottom Line

We’re now in a very high risk position

The road ahead is straightforward but slow

What **will** we do about the cyberthreat?

Bottom Line

We're now in a very high risk position

The road ahead is straightforward but slow

Meanwhile, the clock is ticking...