Integrating Controls Cyber Security with Corporate IT: A management perspective

Enzo Carrone

San Francisco, ICALEPCS 2013

U.S. DEPARTMENT OF ENERGY
Office of Science

SLAC NATIONAL ACCELERATOR LABORATORY

I could give you…

Outline (or *life in the land of standards*)

SLAC

- Progress on regulations
- Standards
- Relationships
- Communication
- Strategies

So, you want to be safe AND compliant?

SLAC

If we thought that:

We would just do Controls Engineering…

We would configure our networks as we please…

IT Department would take care of CSCS…

There would be only one guideline to refer to (à la IEC 61508/61511)…

…We are in for a rude awakening.

Evolution of regulatory landscape: EO

SLAC

Obama's Cybersecurity Executive Order (Feb 2013):

- Agencies to share information with companies
- NIST to develop a framework with industries
- Review CS regulation
- Voluntary compliance

Deadline: Feb 2014

Leadership: NIST

Evolution of regulatory landscape: CICF

SLAC

4th Critical Infrastructure Cybersecurity Framework (Sep 2013):

(a system of regulations and the means used to enforce them)

1. Core functions (activities and references);
2. Implementation tiers (guidance);
3. Framework profile (how to integrate CS functions within a CS plan).

So far:

- Guidance on what constitutes adoption of the framework not complete;
- A set of toolboxes;
- An ongoing process.

NIST SP 800-53 – IT CS Land

NIST Special Publication (SP) 800-53 (Computer Security Guide) – Rev. 4 published in April 2013

Information Security Program:

- Risk assessment
- Policies and procedures
- Subordinate plans
- Training
- Periodic testing
- ATS
- Incident response
- Continuity of Operations

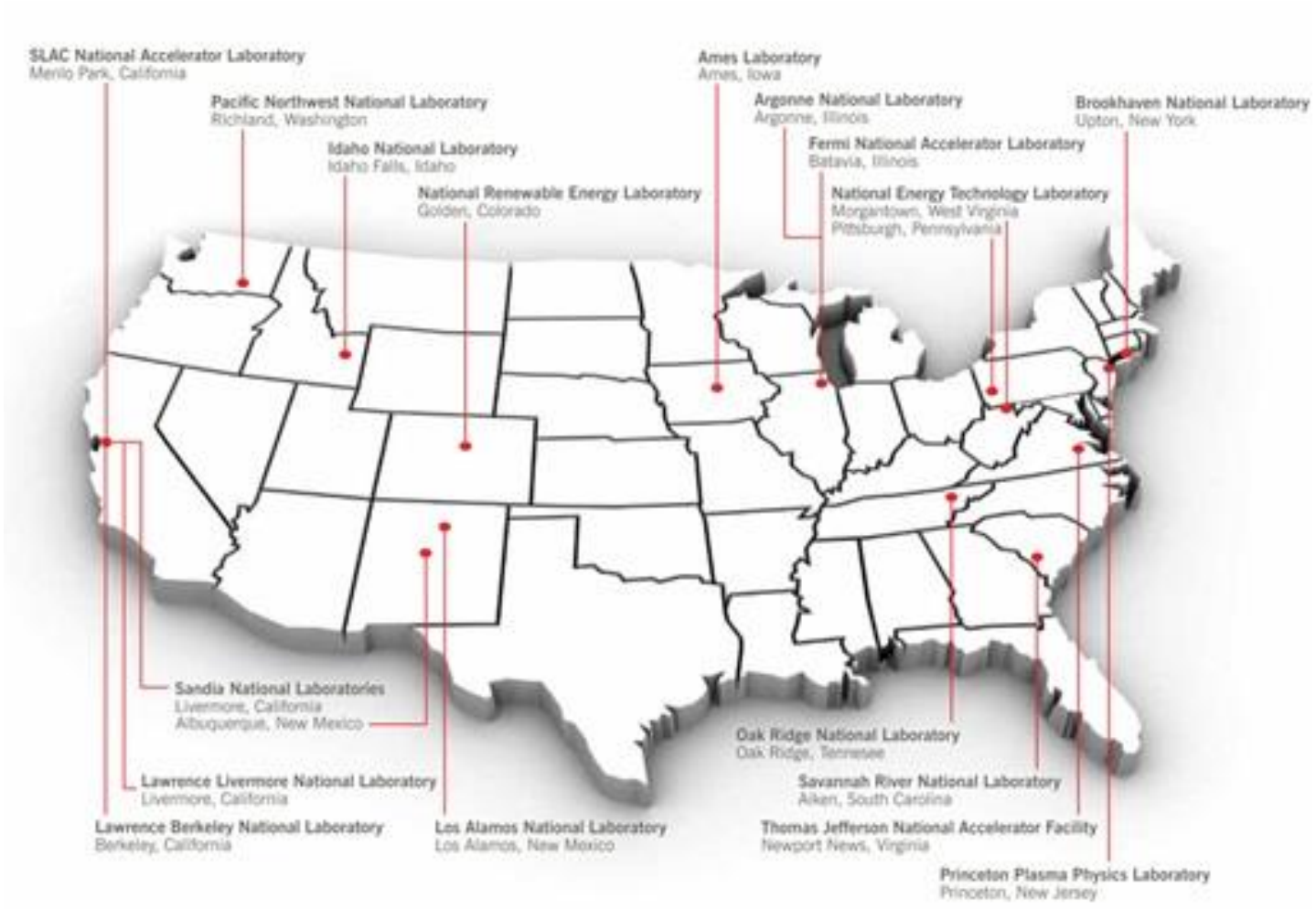
NIST SP 800-53 – Details

SLAC

Mission-Oriented: based on FIPS 199 (Federal Information Processing Standard) for Security Categorization of **Federal** Information and Information Systems: definition of **security control categories** for information systems (Confidentiality, Integrity, Availability -CIA).

Based on impact on organization's **capability to accomplish its mission** (full catalog with, e.g., access control, awareness and training, audit and accountability, authentication, maintenance, media protection and access, etc.)..

The US DOE Complex



DOE Order 205.1B

DOE O205.1B **Cyber Security Program**:

- Integrated, Enterprise-Wide
- Risk Managed Approach (vs. Controls Compliance)
- Configuration Management
- Consistent with NIST
- Line Management Accountability
- Integrated into GOCO model
- Protection of DOE information and information systems
- Mission focused
- Governance

DOE Order 205.1B – Cont'd

DOE oversight is conducted through **Contractor Assurance Systems**: this provides the *Authorization Function*.

Risk Management Approach (RMA): Framing; Assessing; Responding; Monitoring.

What do you know, you are not alone anymore!

IEC 17799 and ISA-TR99

SLAC

IEC 17799: Information Technology – **Code of practice for Information Security Management** :

High level, broad in scope, conceptual in nature and a basis to develop your own security standard and security management practices.

ISA-TR99: Integrating Electronic Security into the Manufacturing and Control System Environment:

Guidance to user and manufacturers, analyzing technologies and determining applicability to securing Manufacturing and controls.

IEC 15408 and IEC 27001

SLAC

IEC 15408 (3.1) – Information Security Management Systems (ISMS):

Framework to specify security **functional and assurance requirements** through the use of Protection Profiles. **Vendors** can implement security attributes, **testing labs** can evaluate the products.

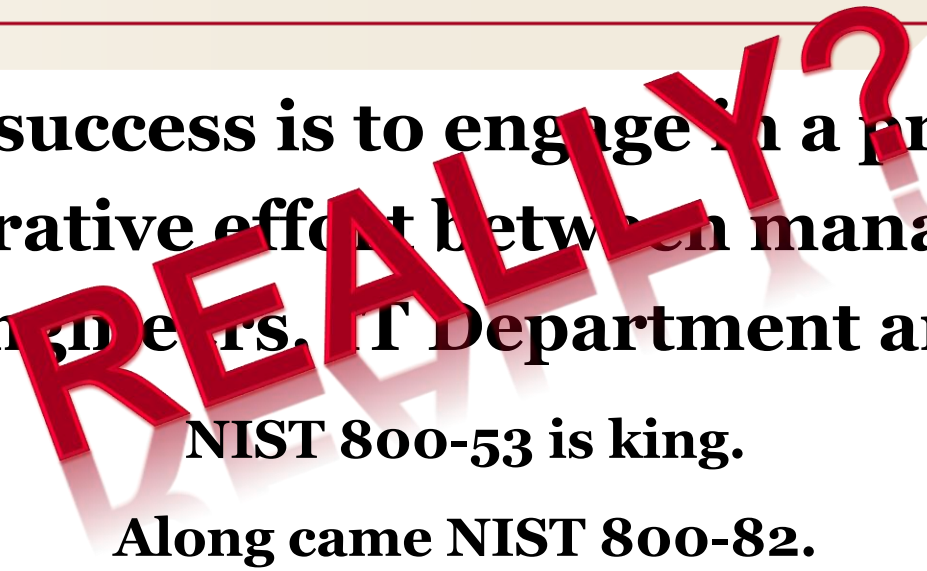
IEC 27001:2005 - Common Criteria for Information Technology Security Evaluation (aka CC):

System to bring information security under **explicit management control**:

- Policies and governance; Asset management; HR security;
- Access control; Incident management; Business continuity; etc.

Your interface with IT

Key to success is to engage in a proactive, collaborative effort between management, controls engineers, IT Department and security.



NIST 800-53 is king.

Along came NIST 800-82.

- Many times a CS team (an “enclave”) exists already.
- “Ah, we’re not sure we can share such information with you”…
- They might even tell you that it is impossible to gain access.
- You are the bridge between 800-53 and 800-82.
- You will have to provide the expertise to implement it.

NIST SP 800-82

- Latest release: **May 2013**
- "***Defense-in-depth***" strategy: layering security mechanism so that impact to one mechanism as a result of failure is minimized.
- Includes:
  - ICS policies based on DHS Threat Level;
  - Implementing multi-layer network topology;
  - Provide logical separation b/w corporate and ICS networks;
  - Use DMZ (i.e., no direct communication b/w ICS and corporate);
  - Fault-tolerant design;
  - Redundancy for critical components;
  - Privilege management;
  - Encryption.

NIST 800-82 Do we speak the same language?

SLAC

Requirement	ICS	IT
Performance	Time critical, deterministic.	High throughput. Reliable. Jitters ok.
Availability	Continuous processes. No start/stop. Planned outages, no rebooting. Redundancy.	Tolerable.
Risk Mgmt	Human safety paramount. Compliance, losses, damages. Fault intolerant.	Data integrity paramount. Priority: CI(A). Recover by reboot.
Architecture Security	Protect edge systems (PLC, DCS).	Protect assets and info (often centralized).

NIST 800-82 - Do we speak the same language? – Cont'd

Requirement	ICS	IT
Physical Interaction	Yes, certification.	Coming up (internet of things)
Time-Critical Response	Yes (e.g. HMI password shouldn't compromise emergency actions)	No
System Operations	Control Engineers are not IT. Legacy, proprietary systems (support?)	More tools available.
Resources	Limitations on CPU, third part security solutions	Plenty

NIST 800-82 - Do we speak the same language? – Cont'd

SLAC

Requirement	ICS	IT
Communications	Often proprietary	Plenty
Change Mgmt	Requires tests by vendors and re-certifications. Old OSs no longer supported.	Same
Managed Suppt	Often single vendor.	Often same challenge.
Component Lifetime	15-20 years	4 years
Access to Components	Remote, hazardous locations	Easy

Different flavors of ICS

SLAC

Towards a two-tiers approach?

For Laboratories, risk tolerance for “generic” ICS is different than for Safety Systems (ACS, BCS, MPS) or Medical Applications (protect lives, information, asset, etc.).

Somebody will have to identify boundaries and interfaces.

In highly regulated environments, once a standard is chosen, the organization is auditable against it –a big deal.

Your relationships horizon

"What employees call *politics*,

executives call *cooperation*"

CIO: Needs a CS program for the entire organization.

YOU will have to tell her how to integrate CSCS it with IT.

COO: Needs to integrate the CSCS into the CAS framework.

YOU will have to work with IT to define a reasonable, auditable, attainable approach.

Your relationships horizon – Cont'd

SLAC

Your boss: Has line management responsibility on your beloved ICS.

YOU have to keep the systems secure.

The Laboratory's **users** (internal and external, including **Operations**): Don't want CS to be in their way.

And **YOU** will be blamed.

Your vendors: In the best case, they'll be compliant to some standard.

YOU will not have access to the PLC source code, period.

A communication challenge

The CS Manager (**YOU**):

We should have a Cyber Security Assessment.

What **your engineers** hear: Cool! They are going to try and hack our boxes, bring down the network, check on its security.

What **your boss** hears: They are going to check whether our systems are secure or not (oh well, my guys are so awesome, I should not worry).

What **the IT department** hears: they are doing an assessment on control systems –fine, they are on their own (ok, sort of).

The farther from you it goes, the worse it gets…

What **your VP (or Group Leader, or ALD)** hears: The DHS is coming and they will check on how the guys in engineering do business. Better be ready.

What the **program managers** hear: the Feds are coming down to penetrate the system and will bring down the entire facility –we have to stop them! The Lab Director has to stop them right away!

…Communication happens in the mind of the listener.

Acceptance Factors

SLAC

Implementation of Cyber Security is hard:

Not much love from **users** (aka *"I need to access the machine and change the beam parameters on my iphone while I'm waiting for the traffic light to become green"* syndrome).

Not much love from **organizations removed from Engineering**: we do theoretical *[insert any hard science here*] and data analysis, we don't need all this CS controls.

Not much love from **Cost Account Managers**: Whoa! These control systems guys are so expensive! This facility has been up from *[insert any time after WWII]* without any problem…!

Acceptance Factors – Cont'd

Bottom line: You have to "**socialize**" your plans and actions: it's a **strategy** on its own which determines whether you will be successful or not.

Always **give management**:

- Enough time to digest changes;
- Enough details (it means 1/10 of what you have in mind);
- A good story for their superiors;
- A feasible training program customized across levels (executives, managers, supervisors, engineering, IT, Contractors);
- Executable plans (aggressive, but not unrealistic).

Conclusion

CSCS is getting more and more attention.

This is good.

Honing and fine-tuning our interactions with non-Controls Engineering specialists is key to grabbing this opportunity.