Cyber Informed Engineering

Virginia Wright, Program Manager Domestic Nuclear Cyber Security

www.inl.gov

Idaho National Laboratory

INL Background

- ✓ *One in a network of 17 DOE national labs*
- ✓ *DOE's lead lab for nuclear energy*
- ✓ *A major center for National Security*

INL Vision

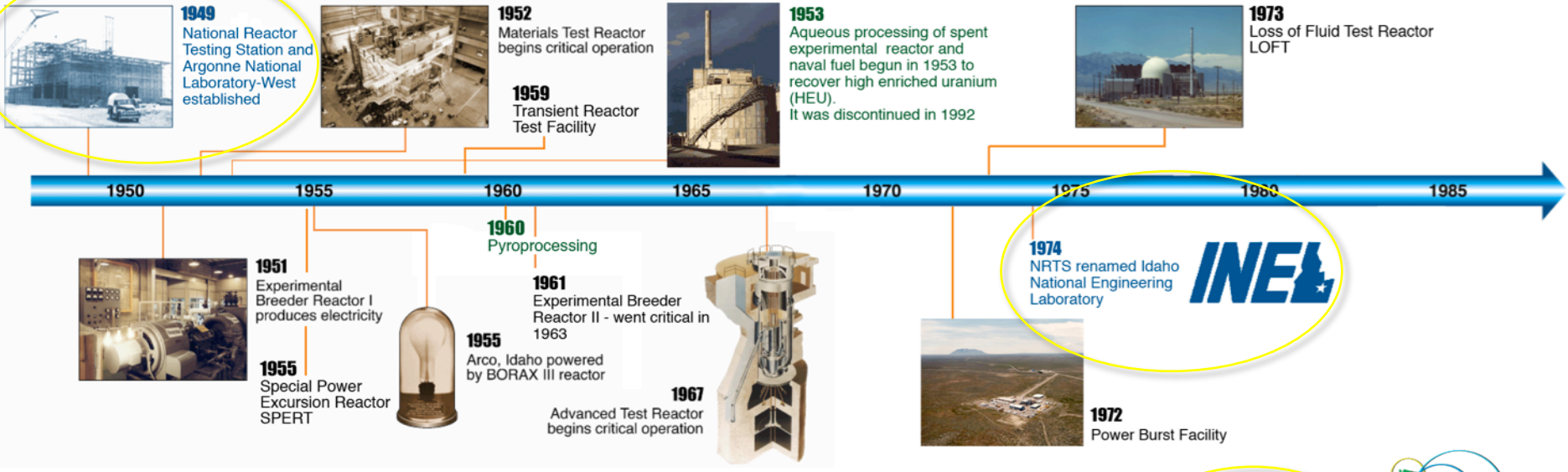
INL will change the world's energy future and secure our critical infrastructure.

INL Mission

Discover, demonstrate, and secure innovative nuclear energy solutions, other clean energy options, and critical infrastructure.

Research in the National Interest that **Maintains American Competitiveness & Security**

Our History



- Nuclear Energy in the U.S.
  - 1940' and 1950's from concept to prototype
  - 1960's from prototype to commercialization
  - 1970's an industry is launched
  - 1980's ensuring safety
  - 1990's laying the foundation for a new generation of nuclear power plants
  - 2000 & beyond a new generation of nuclear power and advanced fuel cycle technologies

Last Talk We Presented Was On Cyber Threat

- Discussed the overall threat picture and expanding adversary capabilities in cyber
- Established that digital equipment used has cyber security flaws
- Established that adversaries can take advantage of these flaws
- Established that adversaries can make these assets behave in undesired ways
- Established that airgaps and security zones are not a 100% defense

Particle Accelerators - Their Hazards and the Perception of Safety

OVERVIEW AND LESSONS LEARNED

Safety Systems Group

Kelly Mahoney, Engineering Manager for Safety Systems
TJNAF (Jefferson Lab)
mahoney@jlab.org

Jefferson Lab
Thomas Jefferson National Accelerator Facility

Current Concerns

- Controls Cyber Security
  - Greatest concern is with engineering development PCs
  - Updating to meet ISA S99, NIST SP800-82
  - Safety Systems Cyber Security Assurance Program
  - Consulting with U.S. ICS-CERT
- Threat at multiple vectors
- Vulnerable components are engineering development workstations, display systems
- Highlights malicious intent as threat
- Active (?) degradation over time
  - APT

Jefferson Lab

CERN Bulletin

News Articles | Official News | Training | Announcements | Events | Staff Association

english | français

search

Issue No. 10-11/2013 - Monday 4 March 2013

ATLAS: Now under new management
Science for a sustainable future
LS1 Report: onwards and upwards
X(3872): an exotic combination of quarks?

CYBER-ATTACKS AND THE RISKS FOR CERN

In the previous Bulletin, we discussed the cyber-risks for the accelerator complex. However, looking at the broader picture, the cyber-risks for CERN are much more diverse.

Proceedings of IPAC2012, New Orleans, Louisiana, USA WEXB03

PROTECTING ACCELERATOR CONTROL SYSTEMS IN THE FACE OF SOPHISTICATED CYBER ATTACKS*

S. M. Hartman†, Spallation Neutron Source,
Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA

CERN Bulletin

News Articles | Official News | Training | Announcements | Events | Staff Association

english | français

search

Issue No. 08-09/2013 - Monday 18 February 2013

Protons on ions bring new physics to LHCb
Success and adaptation
LHC Report: Run 1 – the final flurry
Enhanced personal protection system for the PS

HACKING CONTROL SYSTEMS, SWITCHING... ACCELERATORS OFF?

In response to our article in the last Bulletin, we received the following comment: "Wasn't Stuxnet designed to stop the Iranian nuclear programme? Why then all this noise with regard to CERN accelerators? Don't you realize that 'computer security' is not the *raison d'être* of CERN?". Thank you for this golden opportunity to delve into this issue.

HOME » NEWS » SCIENCE » LARGE HADRON COLLIDER

Hackers attack Large Hadron Collider

5 | 0 | 0 | 5 | Email

eee

The message in Greek that the hackers displayed. Click to enlarge

By Roger Highfield, Science Editor
2:30PM BST 12 Sep 2008

Hackers have mounted an attack on the Large Hadron Collider, raising concerns about the security of the biggest experiment in the world as it passes an important new milestone.

Exploit and Malware Campaigns Receiving Attention

Heartbleed

BLACK  ENERGY

Dragonfly

Shellshock
(Bash Bug)

What Consequences Result from Digital Systems Attack on Accelerators and Research Equipment?

- Damage to accelerator facilities (or engineering facilities)
- Personnel and environmental exposure
- Other safety issues
- Theft of ideas
- Data inaccuracies
- Mission disruption

Easy to Get Overwhelmed

Where should our engineering and technical staff spend their time?

CYBER INFORMED ENGINEERING

CIE Defined

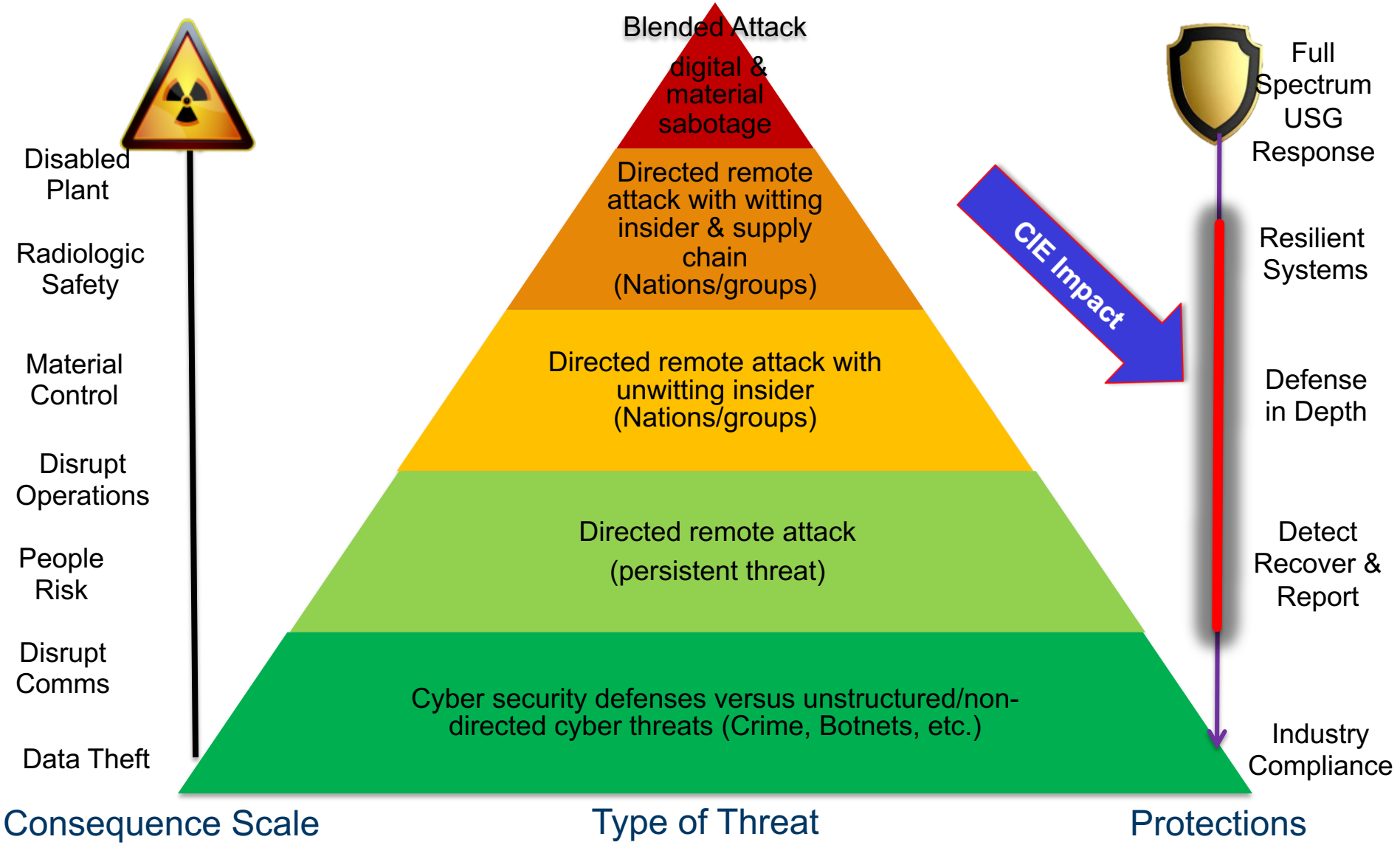
Simply Stated:

- The inclusion of cyber security aspects into the engineering process for digital systems

Expanded:

- A body of knowledge and methodology to characterize the risks presented by the introduction of digital technology towards an engineering strategy informed by an awareness of the cyber threat to mitigate such risks.

Strata of Cyber Security Threats



Why CIE?

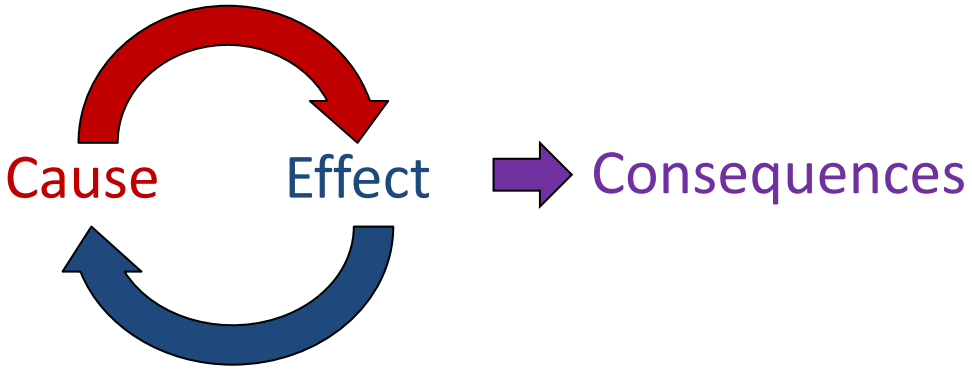
- Traditional engineering methods do not account for cyber risk
- Engineers operate in a “trusted” environment
- Belief in isolated networks
- Bolt-on cyber security solutions do not work well for digital systems used in engineering applications
- Engineering staff are unaware of the potential cyber threat to operational technology
- Not about “failure” modes, cyber attacks may make digital systems operate beyond or outside of their imagined capabilities

CIE Framework Elements

1. Consequence / Impact Analysis
2. Systems Architecture
3. Engineered Controls vs. IT Controls
4. Design Simplification
5. Resilience Planning
6. Engineering Information Control
7. Procurement and Contracting
8. Controlling Interdependencies
9. Cyber Culture
10. Digital Asset Inventories

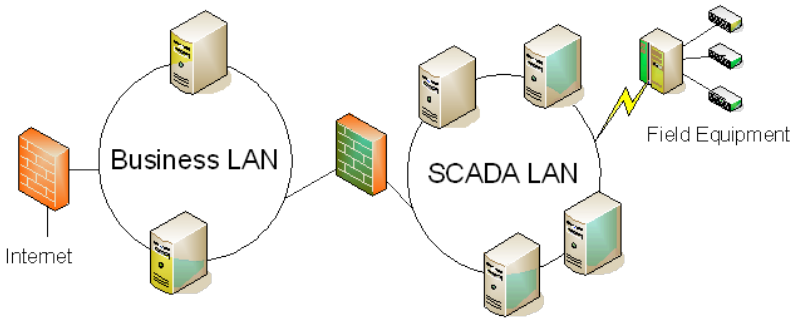
Consequence / Impact Analysis

- The key “imagineer” in the defensive process is the knowledgeable engineer
- Cyber-Physical attacks manipulate availability, integrity and confidentiality of processes using data to effect physical consequences
- Attacks can be blended - cyber and physical together
- Focus on the key adverse consequences with limited resources
- Possible adverse consequences may not have been mitigated in the engineering design process



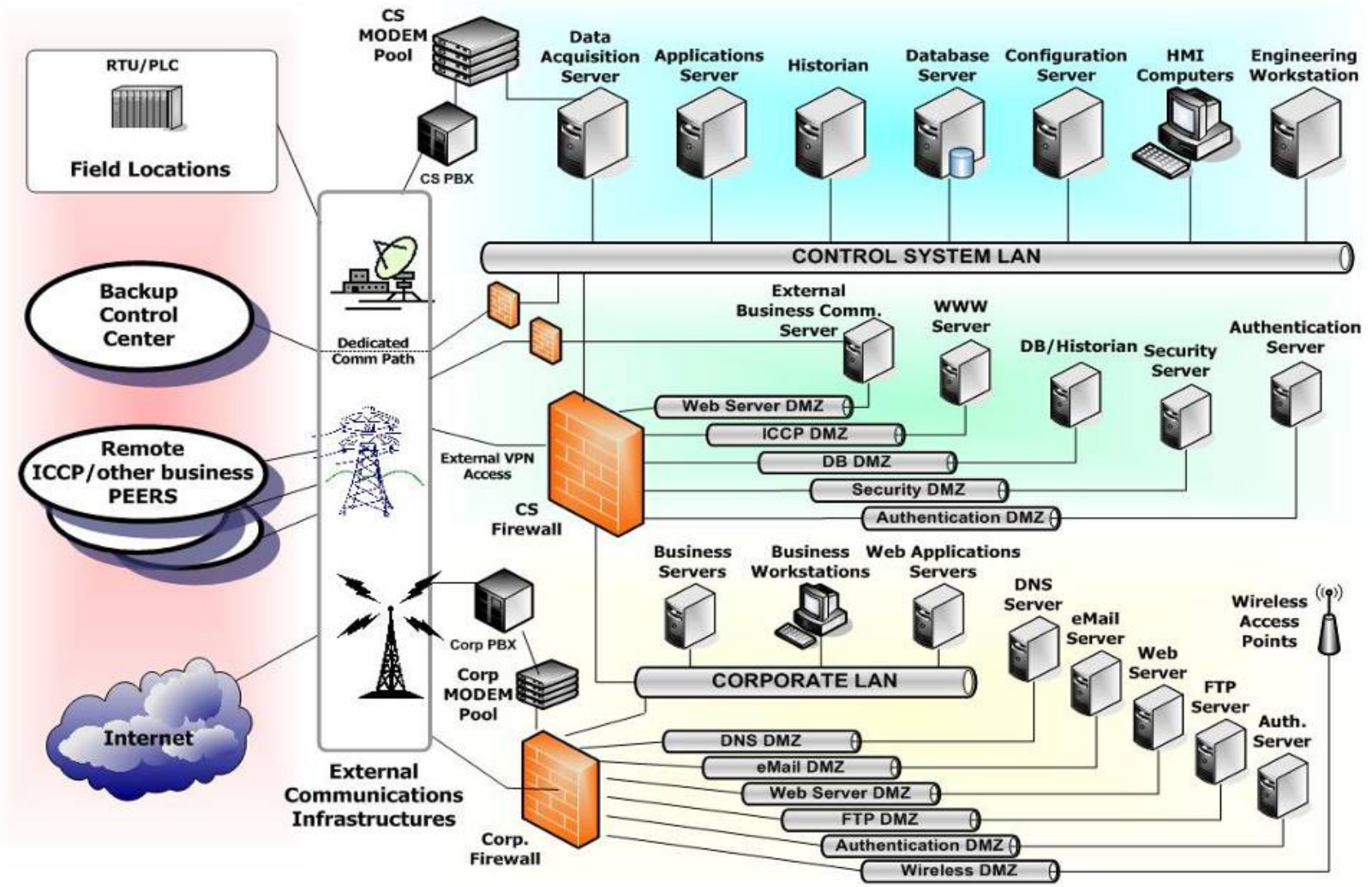
Systems Architecture

- Defines how information flows through the system
- Engineering staff know more about how data should flow than the cyber staff
- Engineering staff know:
  - what data should be protected (Confidentiality)
  - how data can be externally verified (Integrity)
  - how often data should be sampled (Availability)
  - Which data flows are most important (Availability)
- Remember that the “ideal” architectural model may not be your reality
- Cyber technology may be used to support the engineering design
  - data diodes
  - enclave network design
  - network zones,
  - virtual machines



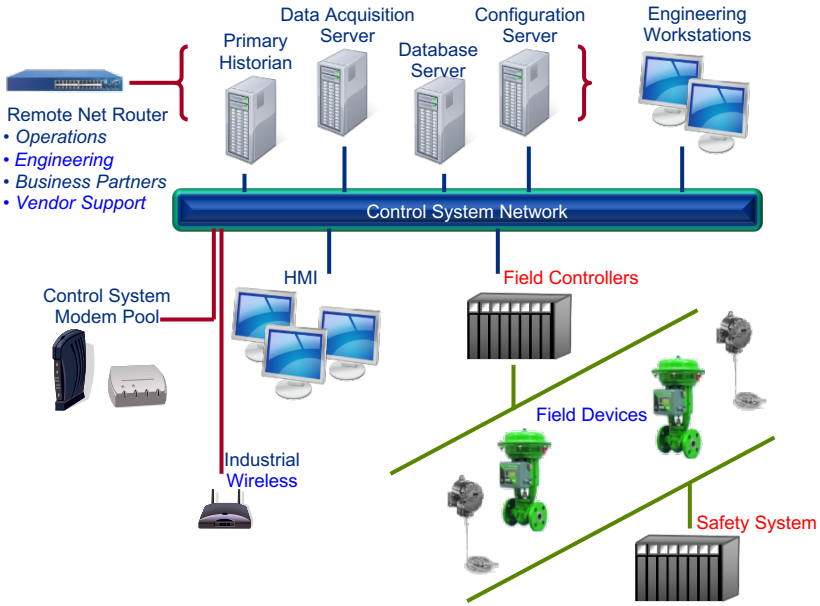
Conceptual View

Realistic View of SCADA Architecture



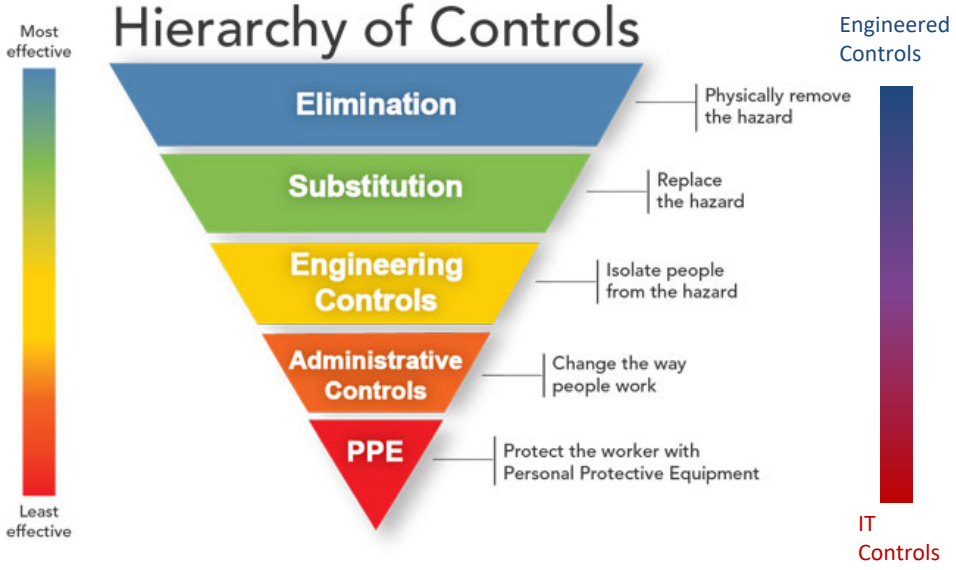
Myth of Airgaps

- **Corporate Net** connected (firewall) to ICS
- **Remote access** by engineering stations or support vendors
- **Field devices** communication ports with little or no authentication
- **Required Calibration**: laptops & handhelds
- **Wireless communications** instead of hardline networks
- **Removable media:** upgrades & backups
  - Flash drives
  - CD's
  - External hard drives
  - "periodic external connection"
- **Common Buses:** Control & Safety Systems



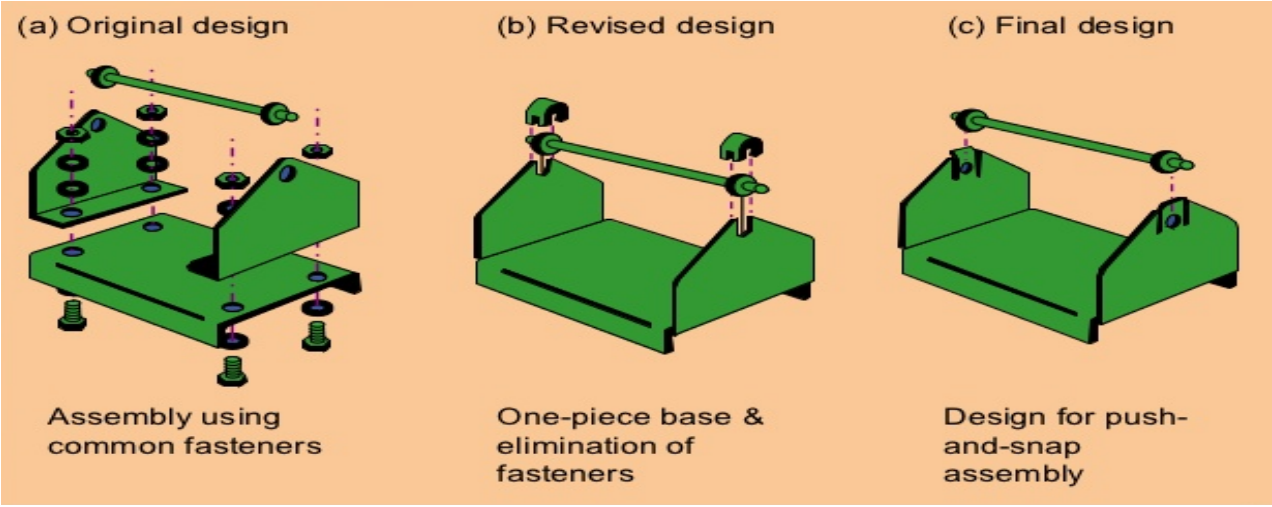
Engineered Controls vs. IT Controls

- Consider IT and Engineered controls early in the design lifecycle
- Consider how vulnerabilities can be designed out or mitigated through additional engineered controls
- Engineered controls may provide more robust protection than add-on IT controls
- Engineers should use the IT specialist as part of the requirements and design team



Design Simplification

- Reduce design to minimum necessary
  - Remember resilience
- Be aware of latent functionality
  - You may not use it, but a hacker can
- Consider non-digital technology where it fits
- Do not simplify a design into frailty
- Use ALARA (As Low as Reasonably Achievable) as a metaphor



Resilience Planning

- Vulnerabilities always exist, known or unknown
- Any digital component or system may be compromised
- Can't always stop the process and reboot
- Is there an incident response plan
  - Has it been exercised?
- Is there a cyber COOP?
  - Has it been exercised?
- How will process be affected by "resilient" operations?
- Other contingency planning (additional testing, additional systems, additional staff, etc)
- Redundancy is not resilience

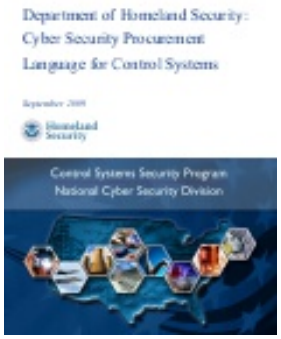
Engineering Information Control

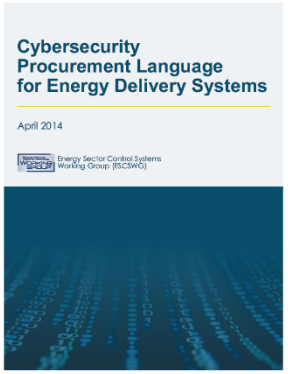
- **Who** should know **What** about your effort?
  - Engineering records
  - Drawings
  - Requirements
  - Specifications
  - Designs
  - Analysis
  - Testing

- Procurement contracts must control the vendor / integrator's sharing of these details
- Consider social media, vendor and corporate websites, conferences, etc.
- Information should be protected throughout the life of the project, not just during design and installation
- Change passwords on digital equipment when authorized users or key vendors leave the organization

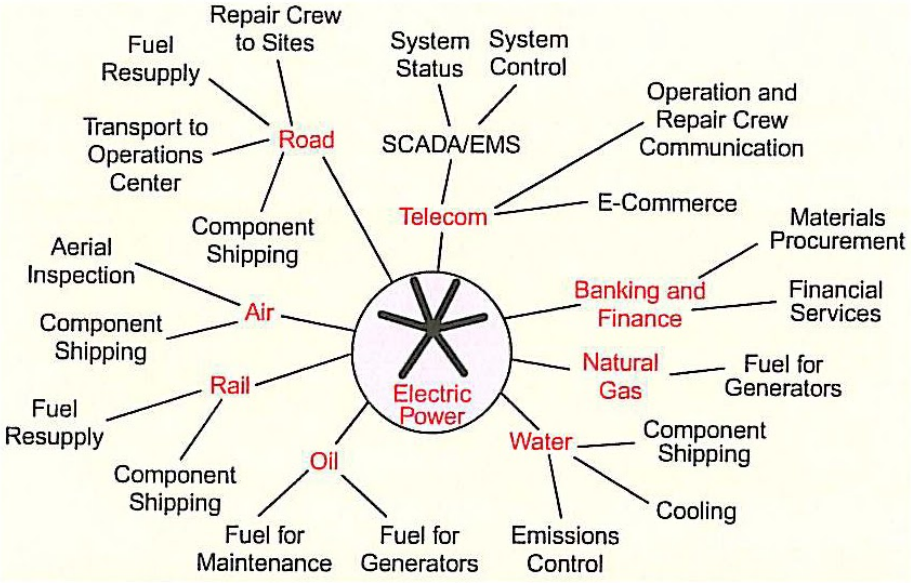
Procurement and Contracting

- Cyber security requirements must flow down to vendors, integrators, and third party contractors
  - You are only as secure as your least secure vendor
- Procurement language must specify the exact requirements a vendor must comply with as a part of the system design, build, integration, or support
- These requirements can raise procurement costs, but without them, *caveat emptor*
- Be aware of what a subcontractor puts into your network
  - You don't know where it was before today
- Consider even vendor tools such as calibration equipment or diagnostic equipment





Controlling Interdependencies



- Engineering requires many disciplines including safety, quality, maintenance, chemical, and many others
- All disciplines should share information on how cyber could affect their area of concern
- Ultimate system owner should understand risks from interdependencies
- Consider systems such as cooling, water, power, communications, etc.

Cyber Culture

- Include cyber into engineering and engineering into cyber
- Ensure entire staff is enlisted and endorses cyber security approach
- Ensure staff understand and follow process and procedures
- Even one user can lower security posture
- Always safe to take a time out

Conversations

Explicit Assumptions

Collaboration on Projects

Assessments

Scenarios

Exercises

Digital Asset Inventories

- Mechanism for organizations to track:
  - Hardware
  - Firmware
  - Software version levels of all engineering systems
  - “Gold disk” copies of software
  - Where is your restoration file for configuration data?
  - Understand every digital asset to provide protective measures
  - Could you pass an “as-built” assessment?
- How do you protect this information?

Hacking is Hard… You can make it harder

Where to begin?

1. **Consequence / Impact Analysis**
2. Systems Architecture
3. Engineered Controls vs. IT Controls
4. Design Simplification
5. Resilience Planning
6. Engineering Information Control
7. Procurement and Contracting
8. Controlling Interdependencies
9. Cyber Culture
10. Digital Asset Inventories

The opportunity to secure ourselves against defeat lies in our own hands…

Sun Tzu

Next Steps for Cyber Informed Engineering

- Framework first release, September 30th
- Revisions – Your input welcome!
- Assessment methodology (April, 2017)
- Tools and application aids (April 2017)

Virginia Wright (Ginger)
Domestic Nuclear Cyber Program Manager

Idaho National Laboratory
Virginia.Wright@inl.gov
(208) 526-7021

Idaho National Laboratory

The National Nuclear Laboratory

DOE NE Nuclear-Cybersecurity R&D

- **Mission:**
- Enable the safe, secure and reliable deployment of nuclear energy technologies by accelerating the development and integration of cybersecurity technologies and information sharing of threat/mitigation analysis and methodologies with nuclear power plants, research reactors, and fuel cycle facilities
- **Vision:**
- NE will have a global leadership role in the deployment of cybersecurity technologies into all facets of nuclear energy systems
  - Reactor protection, monitoring and control systems
  - Safety, security, and safeguards systems
  - Balance of Plant, Emergency Response and Supply Chain
  - Cradle-to-grave of nuclear/radiological materials development, use, transport, storage, and disposition

DOE NE Nuclear-Cybersecurity Program

- Current State
  - Proof of principle
  - Develop concepts for the value a future program could add
    - Initial funded research portfolio
  - Develop insights from NRC, Utilities / Asset Owners, Researchers, Laboratories regarding foundational science needs
- Future
  - Focus on developing foundational science to enable intelligent digital controls modernization
  - Planned Program Outcomes
    - Deployable cybersecure digital technologies
    - Cybersecurity standards and risk assessment methodologies for components, systems and facilities
    - Actionable information sharing forums
    - Methods for safe and secure operations, design and licensing
- Formal Program Plan under development

NE Nuclear-Cyber R&D Program

- Create effective cybersecurity frameworks for anticipatory sensors, controls, and systems that address evolving threats
- Develop new cyber-informed risk methodologies and engineering design basis for critical systems in a digital era
- Prioritize research, engineering, and technology solutions for dynamic risks, capability gaps and disruptive events

Cybersecurity R&D solutions can prepare for emerging technologies and emerging threats