SAND2016-8688C

Exceptional service in the national interest

Sandia National Laboratories

2016 Symposium on Secure and Resilient Microgrids

Secure Microgrid Cybersecurity Workshop Part II: R&D Gap Analysis Project

Jason Stamp, Ph.D.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY | National Nuclear Security Administration

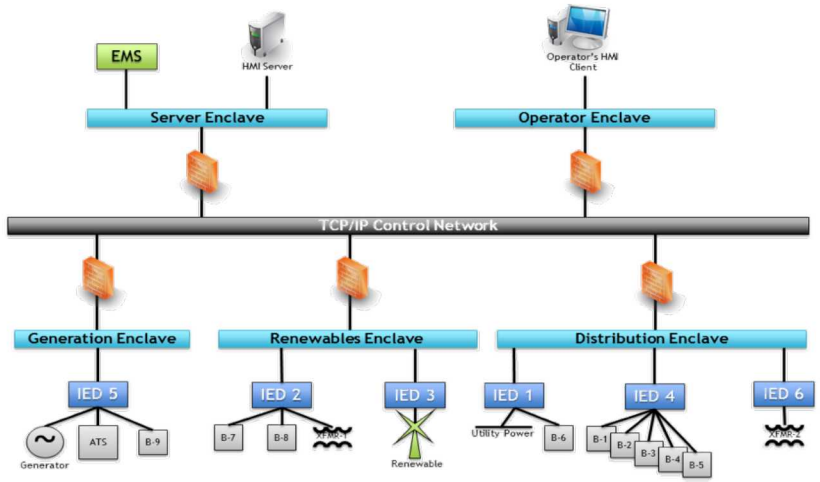
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Microgrid Cyber Security Scoping Study

Objectives & Outcomes

The microgrid cyber security scoping study will encompass industrial control systems (ICS) for energy management at critical and high-security installations including Department of Defense (DOD) facilities. The effort will use a gap analysis approach to identify opportunities for high-impact R&D investments. The primary project deliverable will be the summary of the study's methodology, results, and analysis which will be used to inform a FOA.



Life-cycle Funding Summary ($K)

Prior to FY 16	FY16, authorized	FY17, requested	Out-year(s)
-	$100K	-	-

Technical Scope

- Identify the technical challenges facing cyber security for critical installation energy, including microgrids
- Define *as-is* and *to-be* states of cyber security for critical installation energy
- Identify gaps in both the short- and long-term
- Prioritize gaps to support high-impact R&D investments unique to DOE
- Leverage stakeholder and expert input where feasible

Tasking and Personnel

Sandia National Laboratories

- Given scope is:

  “Deliver a peer-reviewed report with input from relevant stakeholders, identifying priority gaps and key milestones related to microgrid cyber security"
- Key personnel:
  - Jason Stamp (SNL)
  - Joe Cooley (MIT-LL)
  - Abe Ellis, SNL program manager
  - Erik Limpaecher, MIT-LL program manager

Clarifying Terminology

Sandia National Laboratories

- ICS (industrial control system):
  - Includes control center/HMI based on IT
  - Field devices and communications, also known as OT
  - Sensors and actuators to interact with a physical process
- "Priority gaps":
  - Important topics that are either unaddressed or severely under-addressed
  - Enables a capability (revenue based on utility data connectivity), addresses key deficiencies (operational resilience), or improves cost-benefit
  - Significant deltas between current state and desired end state possibly based on TRL, cost, and benefit

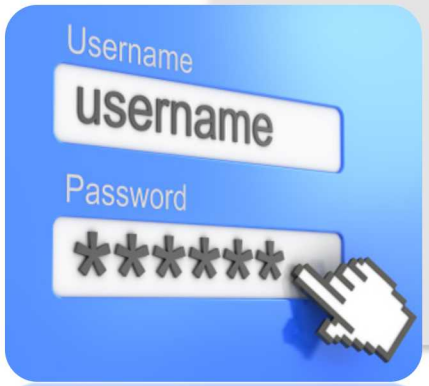
What is “Cybersecurity”?

Sandia National Laboratories

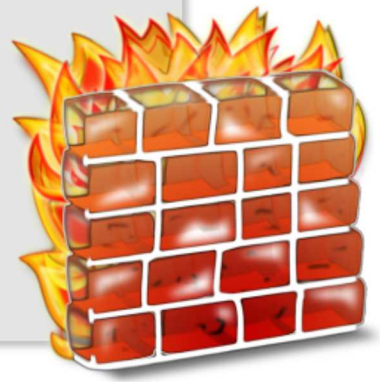
Antivirus?

Cryptography?

- **All of these AND more…**
- **Includes People, Policy, Process, Technology (P3T)**
- **Goes hand-in-hand with safety**
- **Enables a higher-level goal**
- **Cyber-design is specific to the goal**



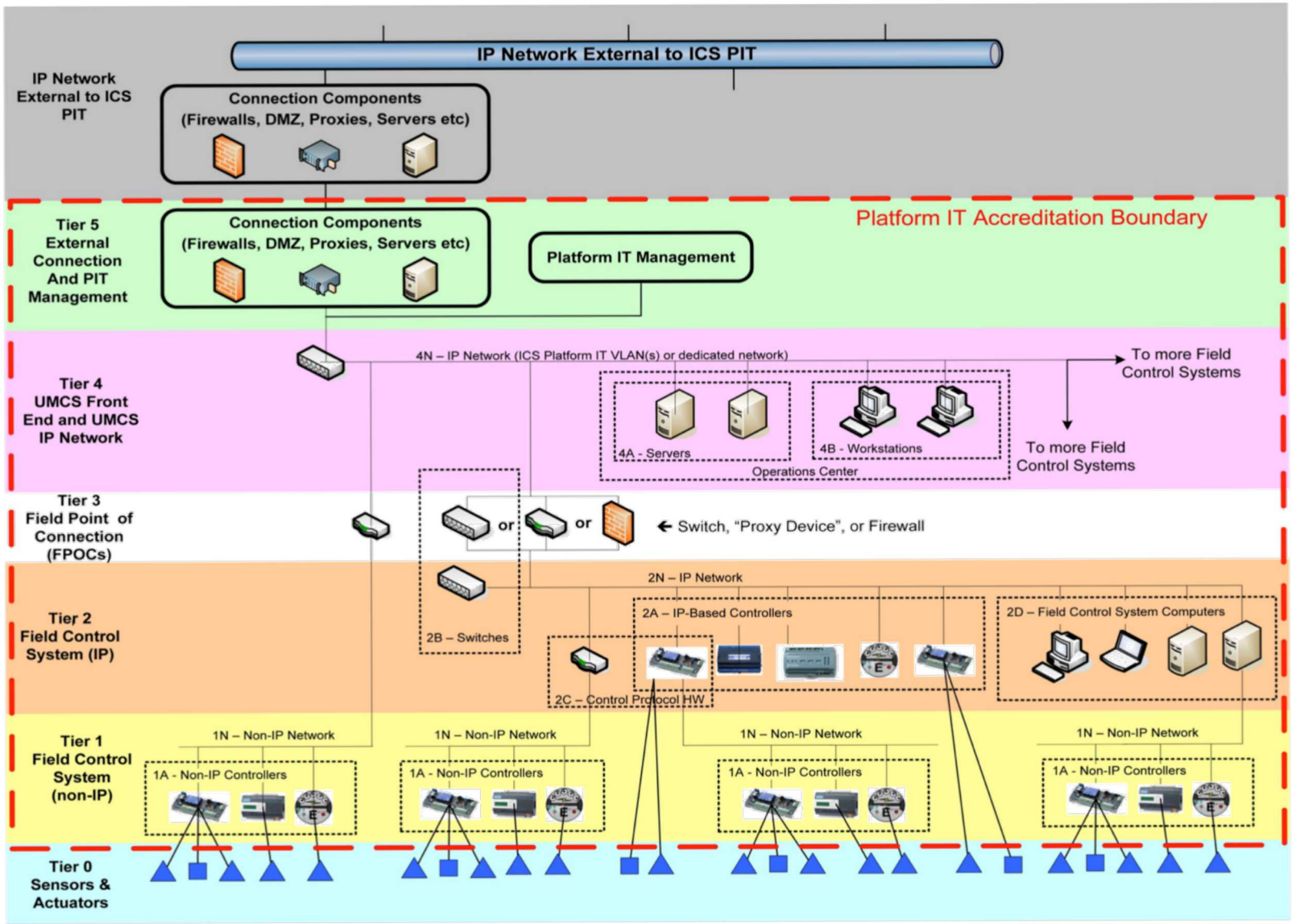
Strong password?



Firewall?

P3T: People, Policy, Process, Technology

Existing DOD ICS Terminology



Problems & Needs Addressed

Sandia National Laboratories

- There are critical cyber risks associated with ICS, including people, policy, process, and technology; for example:
  - Cyber security training for ICS is challenging for operators
  - Application-specific devices (like RTUs, PLC, etc.) include high-risk hardware and software vulnerabilities
  - ICS networking usually does not employ defense-in-depth
- ICS are a crucial element for the function of microgrids (and also other important facility energy systems)
- DOD and other government sites are adding advanced ICS along with microgrids and other energy improvements
- R&D funding and direction is spread across many US government agencies
  - NIST
  - DOD (DARPA, services, other OSD agencies)
  - DOE (CEDS, etc.)
- Proposed solution: scoping study to identify high-impact R&D opportunities for DOE

Current Practices and Their Challenges Addressed

Sandia National Laboratories

- Long-term cyber security is not well-mapped to ICS challenges and characteristics
  - Unique challenges for cyber-physical system evaluation
  - Nonstandard operating systems and hardware
  - Integration “seams” across vendors and subsystems causing unexpected behavior and threat opportunities
- Short-term cyber security concepts and R&D are constrained by legacy policies and procedures
  - Secure connections to 3rd parties for coordinated revenue operation
  - Vulnerability mitigation through patching is difficult
- This project will identify the resulting gaps in R&D for both short- or long-term ICS cyber issues for microgrids/critical installation energy

Project Significance and Impact (Quantitative Measures)

Sandia National Laboratories

- Provide the necessary foundation for targeted R&D, in the form of a FOA
- Focus on the microgrid/installation scope to enhance the applicability and impact of successful R&D
- Identify R&D that can help move beyond limitations caused by existing technology and policy (and help redefine the policy)
- Modify/adapt long-term IT security R&D to focus on the narrower application space and characteristics of ICS for the DOD set of challenges (which should illuminate high-impact R&D opportunities that may not be obvious within the general-purpose IT and ICS space)
- While this project focused on high security applications, there is valuable overlap with microgrids driven by economics, such as university campus microgrids and distribution systems in general

Technical Approach

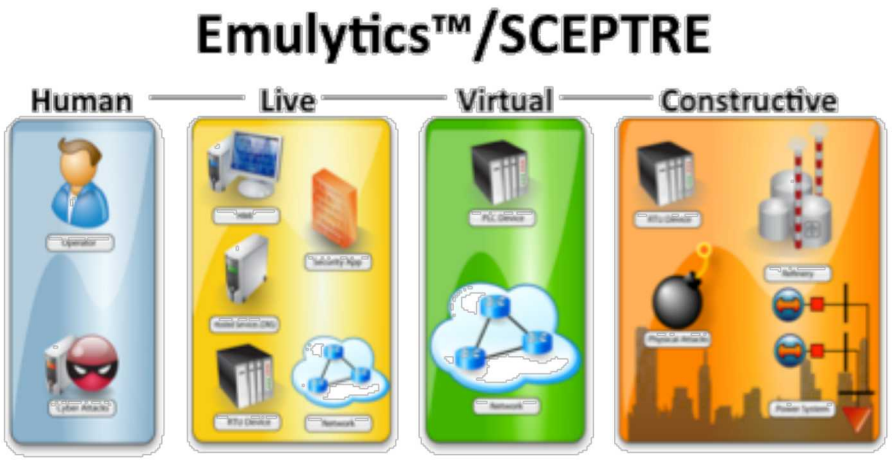
Sandia National Laboratories

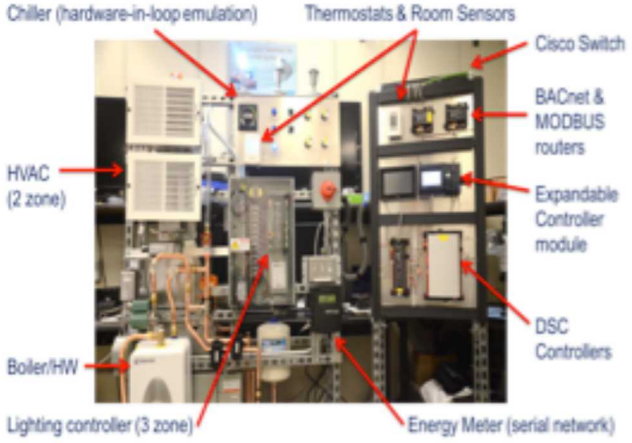
- Apply gap analysis techniques:
  - Identify the desired end-state for ICS microgrid and installation cyber security
  - Develop an estimate of the current state of R&D
  - Both must be decomposed into salient characteristics; subdivisions may be organized around necessary cyber security attributes for ICS as pertains to technical security controls
- Any differences between the desired end security state and the identified current R&D state can represent gaps
- Prioritize gaps to support the eventual project goal (identifying key R&D challenges), leveraging existing documentation from key agencies operating critical energy systems as well as stakeholder input
- Since ICS cyber security has a number of immediate pressing issues, a distinct desired end state will be described for each of the short- and long-term (each timeframe will be carefully defined)
- Short-term R&D needs will be well-suited for demonstration
  - Essential for risk evaluation prior to new capability integration (SPIDERS, JBASICS, etc.)
  - Identifying additional long-term R&D gaps
- Leverage extensive team experience to identify/prioritize gaps based on known vulnerabilities, threat scenarios, and ICS use cases
- Summarize resulting gap analysis into short- and long-term

Technical Approach

Sandia National Laboratories

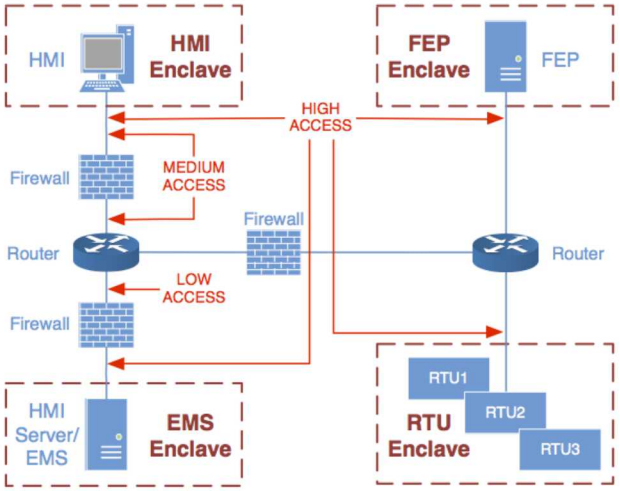
- Leveraging experience:
  - Numerous energy assessments (including ICS cyber) for DOD and other critical government installations
  - SPIDERS reference architecture (network defense-in-depth)
  - Advanced hybrid mod/sim for simulated, emulated, hardware-in-the-loop integration of devices, networking/communications, and physical systems like microgrids (SCEPTRE)

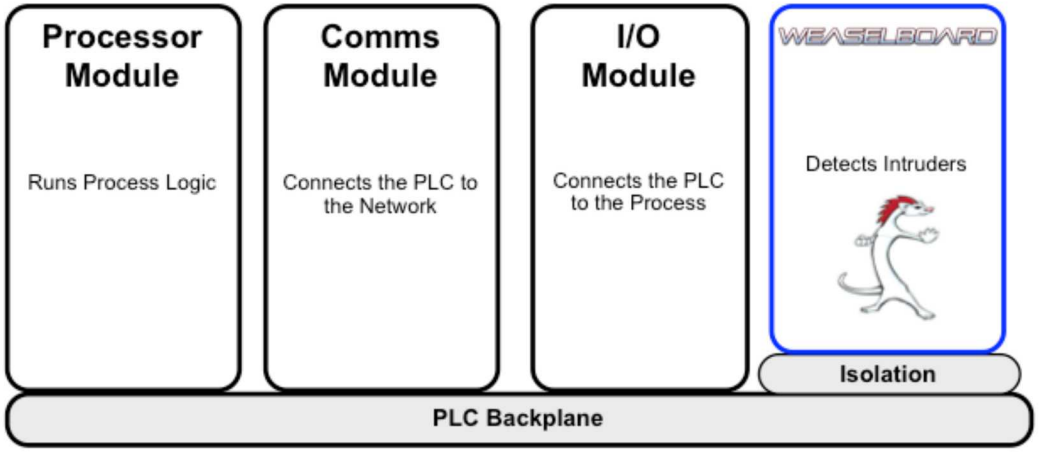




Technical Approach

- Leveraging experience:
  - SPIDERS reference architecture (network defense-in-depth) and quantitative Red Team test scoring
  - Hardware monitoring for programmable logic controller (PLC) cyber defense (WeaselBoard)
  - Security overlays for ICS systems (DOE OPSAID/ Lemnos)
  - Virtual Power System architecture for secure utility grid-integration





Architecture	Access	Compliance	Confidentiality	Integrity	Availability	Total
Flat	High	Insecure	0	0	8	8
		Hardened	9	0	14	23
Enclaved	High	Insecure	0	0	8	8
		Hardened	9	0	14	23
	Med-ium	Insecure	7	6	11	24
		Hardened	9	6	14	29
	Low	Insecure	11	6	16	33
		Hardened	11	6	16	33
Maximum Possible Score →			11	16	14	41

Red Team Scoring Results

Technical Approach

Sandia National Laboratories

- Leverage findings identified in recent DOD study to scope and prioritize near-term gap analysis
- Study scope included
  - Survey of existing DoD microgrid efforts
  - Identification of key parameters and issues
  - Preliminary cost - benefit trades
- Key findings span people, policy, process, and technology
  - Tight integration of microgrid with utility enables greater financial benefit
  - Wide variation from base-to-base, will likely drive architecture decisions
  - Limited concrete guidelines/best practices for DoD microgrids impedes metering efforts
  - New skill sets may be required to operate and maintain microgrids, staffing already thin
  - Microgrid technologies may not be mature enough to provide reliable energy security
- Refine research priorities by correlating near-term gaps with NIST RMF
  - Help posture our study to promote R&D successes

FY 2016 Performance and Results, Against Objectives and Outcomes

Sandia National Laboratories

- Technical progress is limited (the SNL team is expected to partner with MIT-LL on the work and their funding was delayed until mid-July)
- New date for deliverables is NOV 2016, leveraging FY16 funding
- Presented a number of important concepts at the DOE Microgrid research group meeting in Columbus, Ohio (late APR 2016)
  - Defining the study scope boundaries (detail on the next slide)
  - Study report outline
  - Project requirements and limitations (key takeaway is that the results of the study must be non-sensitive to suit the planned FOA)
  - Preliminary categories for the gap analysis (e.g. quantitative risk metrics, field device security, addressing operational test safety concerns, etc.)

FY 2016 Performance and Results, Against Objectives and Outcomes

Sandia National Laboratories

- Defined the study scope:
  - The application range includes microgrids and also DOD/critical government site installation energy using modern cyber controls
  - The cyber adversary target space includes ICS field devices, control center equipment, and communications/networking
  - The project covers all aspects of security lifecycle, including operation, acquisition/installation, maintenance, etc.
  - Existing and desired and states will include aspects relating to design assurance, defense, detection, reaction, and restoration
  - The R&D gaps should include current deficiencies of existing newer systems (installation energy today) and support a cyber roadmap to the microgrids and systems of tomorrow

FY 2016 Performance and Results, Against Objectives and Outcomes

Sandia National Laboratories

- Developing the description of the long-term end state
  - Leveraging a taxonomy of ICS cyber mitigations developed and presented in APR
  - Leveraging requirements identified in recent studies on installation energy
  - Laying the groundwork to align with NIST RMF
- Accumulating the necessary critical mass of background research
  - Supports the development of the desired end state (by noting key requirements from various authorities within DOD)
  - Describes the current R&D state (showing what is already identified and funded as important ICS cyber R&D)
- Finally, the team has scheduled a second key stakeholder feedback session at the upcoming SNL/EPRI Microgrid Resilience Workshop in Baltimore at the end of August

Collaborations and Technology Transfer (Including Cost-Share Info)

Sandia National Laboratories

- Project collaborator for this gap analysis is MIT Lincoln Laboratory
- Team is working weekly coordination discussions in order to finalize the complementary scopes of effort to completely cover the required analysis
- Current planning:
  - MIT-LL to have primary ownership of the short-term gap analysis, as informed by a reference architecture that defines the space for the current and desired states (short-term is also better suited for subsequent technology demonstrations), will also support long-term work
  - SNL is focusing on the long term cyber security needs for critical energy ICS, with the desired end state defined by advanced resilient controls operating in an advanced persistent threat environment, will also support short-term work

Lessons Learned (What Worked Well & What Could be Improved)

Sandia National Laboratories

- What worked well:
  - The two project collaborators have complementary experience
    - MIT-LL has strong background in technical studies for DOD capabilities and concerns, including cyber security, and familiarity with relevant technical policy/ procedures
    - SNL has extensive history supporting DOD and industry ICS cyber security technical challenges and advanced R&D as well as DOD energy analyses
  - Stakeholder input opportunities are agreeable, given the availability of DOE-sponsored events and meetings
- What could be improved:
  - Usual interagency funding delays to MIT-LL contributed to a delay in deliverables

Stakeholder Engagement Cases

Sandia National Laboratories

- Worst case:
  - Existing backups inadequate due to vulnerable civilian power
  - MG/advanced installation energy has cyber problems
    - New systems perform poorly electrically
    - Expected cost benefit does not happen
    - Operational errors are rampant
    - Certification and maintenance are inordinately difficult
- Desired state:
  - Better mission critical energy (reliability, endurance, etc.)
  - Financial and environment benefits
  - Simple enough to run for moderately qualified personnel
  - Easy monitor and maintain security

Scoping: Application

Sandia National Laboratories

- Range includes microgrids and possibly also installation energy using modern cyber controls
- Project plan:
  - Focus on the more broad case
  - Cyber problems of installation energy will overlap with microgrids meaning that R&D gaps will address both
  - Avoid tactical/operational energy issues

Scoping: Facility Applications

Sandia National Laboratories

- Range includes DOD applications or other sites with critical government missions
- Project plan:
  - Focus on both – both are important!
  - Like the previous slide, cyber security challenges overlap

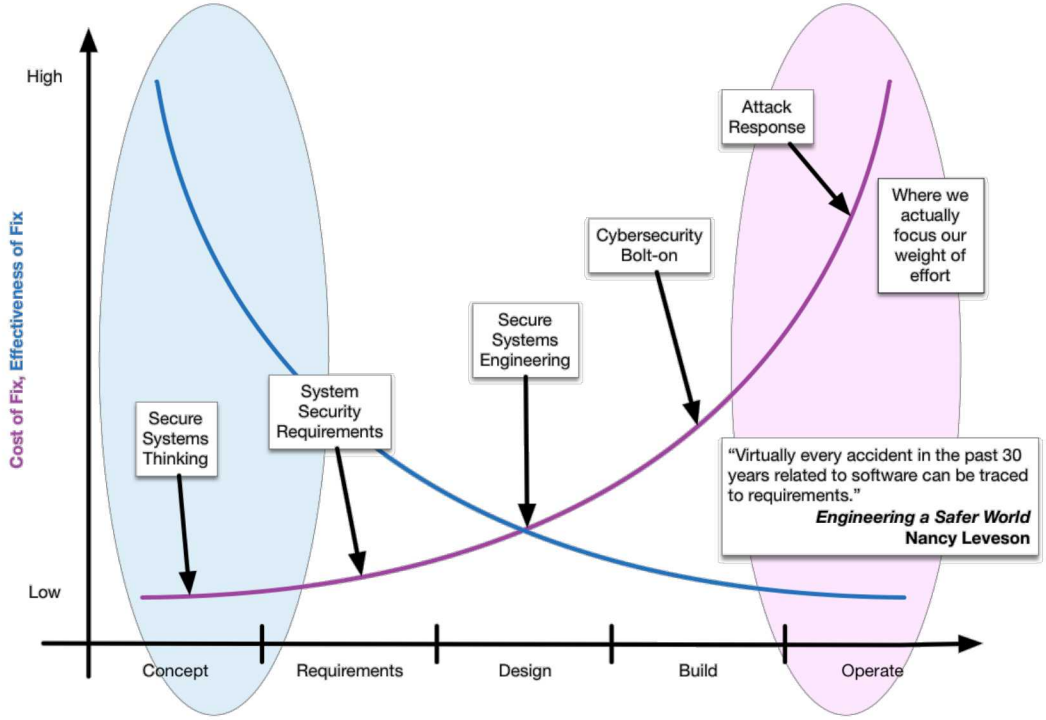
Scoping: Cyber Adversary Target Space

Sandia National Laboratories

- Range includes ICS field devices and control center equipment
- Project plan:
  - Consider high-impact/high-loss and its mapping to equipment
  - Currently, the path of least resistance for an adversary is the control center equipment
  - Field devices have more direct impact on the physical process
  - Focus on range until there is a clear motivation for one end of it
  - Consider weakness in architecture too

Scoping: Security Lifecycle

- Range includes operation, acquisition/installation, maintenance, or some combination
- Project plan:
  - Address all relevant areas
  - Covers equipment and processes
  - Results will illustrate the point that there is no single solution for the ICS cyber problem space



Scoping: Cyber Security Improvements

Sandia National Laboratories

- Range includes: design assurance, prevention, monitoring, resiliency
- Project plan:
  - All of the above, mission assurance through resilient operations across states of degradation
  - Best bang for the buck may be in addressing a process rather than a technology solution
  - Verification for secure embedded system logic (low TRL/high Impact if it is possible, large unknown and difficult to scale)
  - Non-intrusive solutions like advanced device level monitoring, DARPA LADS program, hardware in the loop modeling and simulation for testing

Scoping: ICS Age Timeline

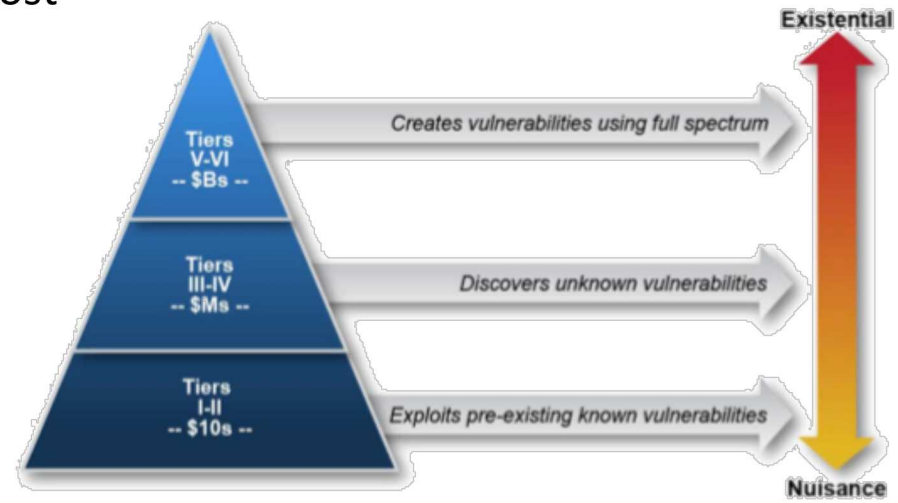
Sandia National Laboratories

- Range includes older existing systems, recent systems, near-term planned systems, and far into the future
- Project plan:
  - R&D must address current deficiencies of existing newer systems (installation energy today)
  - Provide cyber roadmap to support near-term system capabilities (microgrids of tomorrow)

Scoping: Cyber Threat Characterization

Sandia National Laboratories

- Range varies from advanced persistent threat (including nation states) to lower-level (more common) threats
- Project plan:
  - Non-state actors covers a huge amount of attack surface and risk reduction, but might be less about R&D gaps than poor design
  - Foreign state cyber operations are clearly relevant and pose high risk, but insufficiency of current systems suggest APTs are a big reach
  - Focus on mission assurance through resilient operation and by increasing adversary cost



Scoping: Facility Electrical Operating Modes

Sandia National Laboratories

- Range includes normal (utility is available), typical problem (simple outage), abnormal problem (extended utility outage)
- Project plan:
  - Include all of these, mapped to the worst-case and desired end states
  - ICS cyber security problems may cross states, like hazard controls or loss (spoofing) of communications

Tentative Report Outline

Sandia National Laboratories

I. Introduction
- A. Quick ICS cyber background
- B. Broad project goals

II. Scope
- A. Facility/ICS application space
- B. Threat model
- C. Definition of "high impact"

III. Method
- A. Determining current/future requirements
- B. Developing an R&D baseline for the scope
- C. Plans to solicit/capture stakeholder input

IV. Results
- A. Rank/sort current/future requirements
- B. Baseline for existing/planned R&D
  1. Relevant agencies and industry groups
  2. Key document sources
- C. Initial identification/ranking of R&D gaps
- D. Stakeholder feedback
- E. Final ranking of R&D gaps

V. Conclusions
- A. Summarize trends in R&D gaps
- B. Recommendations for R&D focus

Possible Categories for Existing/Planned R&D

Sandia National Laboratories

- Metrics (always on cyber lists, but it is probably not going to happen in any objective meaningful way)
- Quantitative risk assessment (includes metrics) including risk reduction recommendations
- Cyber alert integration into TTPs
- Monitoring (both for individual systems and also coordinated SA/response for multiple systems and sites)
- Protecting insecure equipment against attacks
- ICS Training support (systems and tools)

Possible Categories for Existing/Planned R&D

Sandia National Laboratories

- ICS algorithmic improvement, meaning graceful degradation (current systems can be brittle)
- Better patching/upgrading and auditing
- Effective lab testing (including virtualization)
- Safe OT&E
- Design/logic verification, deployment certification
- Supply chain and transitive trust
- ICS-specific EW issues

Stakeholder Input

Sandia National Laboratories

- List may include each service's corresponding ICS security elements as well as OSD, UCCs, and OGAs
  - Services could include AFOTEC, AFCEC, AFCYBER (maybe?), USACE (CERL/ Huntsville), ARL, ATEC, NAVFAC, ONR, COMOPTEVFOR
  - DOD/OSD could include OSD/DOT&E, DUSD(I&E), DARPA
  - UCCs could include USPACOM, USNORTHCOM, USCYBERCOM
  - OGAs could include DHS (ICS-CERT), White House, DOE (especially OE and CEDS), NIST, HS-ARPA
- Gaps may be explicit on IPLs
- Leverage existing relationships at MIT/LL and SNL where available to capture input
- Concern is that stakeholders are too "installation" and not enough "cyber" or vice versa, so focus on worst case scenarios so that everybody shares the problem

Exceptional service in the national interest

Sandia National Laboratories

2016 Symposium on Secure and Resilient Microgrids

Secure Microgrid Cybersecurity Workshop Part II: R&D Gap Analysis Project

Jason Stamp, Ph.D.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.