CERIAS

The Center for Education and Research in Information Assurance and Security

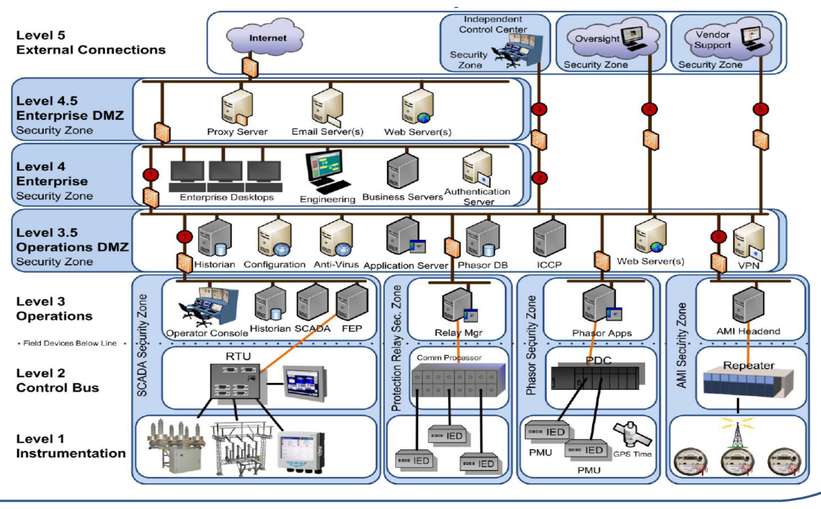
Accelerating Cyber Security Improvements for Critical Infrastructure Control Systems

J.E. Dietz, J. Lerums

1. Abstract - Despite robust cybersecurity standards and vendor solutions, U.S. critical infrastructure experienced a 20% annual increase in cyber incidents during federal FY 2015. This study introduces operational concepts for accelerating necessary cyber security improvements.

2. Motivation - Critical infrastructure control systems cyber attacks are no longer theoretical. On 12/23/14 over 200,000 Ukrainian electric customers lost power for over five hours due to a cyber-attack. As with interruption of power, disruption of industrial control systems for other critical infrastructures (e.g. water, natural gas, transportation, manufacturing) could result in potentially catastrophic and cascading endangerment to life, safety, and health.

3. Problem - Legacy industrial control systems without cyber security capabilities. Under pressure to do more with less, organizations have integrated their operational controls systems' networks with their business networks as a means of improving efficiency. This has in-turn exposed previously isolated control systems to cyber attacks.



4. Methodology - Conduct a gap analysis of what is preventing acceleration of critical infrastructure cyber security improvements by applying DoD's DOTMLPF-P methodology to a state's critical infrastructure utilities.

DOTMLPF-P		Cybersecurity	
Element	**Definition**	**Functional Area**	**Definition**
Doctrine	how missions are conducted	Procedures	processes, guidelines, standards
Organization	combination of organizations, i.e. division, air wings, fleets	Organization	organization of the public & private voluntary coalition
Training	tactical preparation	Training	degrees and/or certification
Materiel	available equipment, testers, spares, "off the shelf" items	Materiel	Industrial controls systems hardware and software
Leadership	leader's preparations at all levels to execute mission	Leadership	preparation of senior private & government executives
Personnel	availability of qualified personnel	Personnel	availability of qualified personnel
Facilities	real estate, industrial facilities	Facilities	real estate, industrial facilities
Policy	department and agency policies that affect the above	Regulations	federal and state regulations and codes that affect the above

5. Findings -

Functional Area	Definition	Cybersecurity Status of State Utilities
Procedures	processes, guidelines, standards	NIST Cybersecurity Framework and CSET provide assessment, standards and procedures
Organization	organization of the public & private voluntary coalition	State's Cybersecurity Executive Council and public and private partners
Training	degrees and/or certification	Awareness and education deficiencies noted in Lessons Learned
Materiel	Industrial controls systems hardware and software	Cybersecure vendor solutions for new and legacy systems available
Leadership	preparation of senior private & government executives	Cyber risk awarness deficiency noted in Lessons Learned
Personnel	availability of qualified personnel	Large number of small companies lacking qualified personnel
Facilities	real estate, industrial facilities	Utilities have facilities
Regulations	federal and state regulations and codes that affect the above	Regulated utilities need financial relief for cybersecurity investments

No Known Capability Gap(s)
Capability Gap(s) Being Addressed
Capability Gap(s) Unaddressed

Findings (Cont.) - Identifying gaps is necessary but not sufficient to accelerate improvements in cybersecurity. Ensuring that cybersecurity organizational roles, responsibilities, synchronization, and timing are identified and executed.

Role	Responsibilities
Boards	An organized group of individuals with designated responsibilities and authorities granted by higher authority
Bureaus	An office or department for transacting particular business
Centers	Permanent cross functional integration organizations. Focuses on supporting, direct, monitoring, assessing, and planning functions
Cells	Current, near term, and future planning elements with appropriate cross functional expertise
Working Groups	Enduring or ad-hoc cross-functional organizations formed to develop, maintain and leverage expertise from appropriate organizations and provide analysis to users
Operational Planning Teams	Cross-functional teams established to solve a single problem and in most cases are not enduring and dissolved upon task completion

Synchronization Rhythm Process Steps
1. Given objectives, establish an optimal number of cross-functional staff elements (i.e. Cells, Working Groups, or Operational Planning Teams) to support the IECoC's decision cycles. The vetting process should be decided upon by a designee acting as a "chief of staff" to ensure only required cross-functional elements are implemented, given limited time and manpower.
2. Afterwards a flow-chart diagram should be used to depict the Synchronization Rhythm events situated on the planning and execution horizons with input and output relationships shown as connections. This helps leaders and the entire cybersecurity team visualize information exchange requirements connections, critical paths of information, and how decision cycles are supported.
3. To ensure there aren't any staffing constraints, a staff matrix should be cross referenced against the Synchronization Rhythm flow chart. The cross referenced staff matrix will help the "chief of staff" or IECoC manage priorities for supporting Synchronization Rhythm events.
4. Finally, the Synchronization Rhythm events should be scheduled in calendar-style time blocks. This will support deconflicting events timing, physical space, resources, and codify the sequence of events that best support the information exchange elements of the IECoC and staff.

6. Results/Conclusion – For one state's critical infrastructure cybersecurity, standards, assessment tools, vendor solutions and facilities are sufficient. Cybersecurity organizations, training, and leadership is being addressed. There are shortfalls in qualified personnel and regulations. Accelerating cybersecurity improvements will be dependent upon execution of organizational roles, responsibilities, synchronization, and timing.

7. Future Work – Quantifying the number and types of vulnerable systems in the state's critical infrastructure utilities. Identifying gaps in organizational roles, responsibilities, synchronization, and timing necessary to accelerate improvements.

CERIAS

PURDUE UNIVERSITY