ENERGY DIVISION OPERATION TECHNOLOGY FOUNDATION AND PROCESS

U.S. Army Engineering and Support Center, Huntsville

July 2017

IN ACCORDANCE WITH - EO 13636 IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

US Army Corps of Engineers

U.S.ARMY

AGENDA

BLUF: The purpose is to convey and provide visual concepts of the architecture for implementing energy resilience and security solutions

SLIDE 1 –	Pillars of energy resiliency and security success
SLIDE 2 –	Installation level operational environment
SLIDE 3 –	DoD architectural framework for medium/high voltage systems
SLIDE 4 –	Difference between information technology and operational technology
SLIDE 5 –	Difference between energy information management and the Army Metering Program
SLIDE 6 –	Repeatable process for energy solutions

BACK-UP SLIDES

BACK-UP 1 –	DoD Architectural Framework (medium and high voltage energy solutions)
BACK-UP 2 –	DoD Architectural Framework (low voltage solutions) Building Automation Framework
BACK-UP 3 –	Risks of applying IT solutions to OT systems
BACK-UP 4 –	IT and OT Comparison

FOUNDATION OF ENERGY RESILIENCE AND SECURITY

EEAP

CUP OEI ESPC

REM EIM PPA UESC ERCIP

Four Pillars of Success

DoD Architectural Framework

-Provide a starting point of design; build in engineering and security enhancements
-Optimize design/network
-Building in energy security and resiliency
-Common operational view

E.O. 13693
DoD CIO
Clinger-Cohen Act

Energy Information Management

-Security and continuous monitoring
-Manage critical infrastructure
-Informed decision making
-Visualize environment
-Trouble-shooting
-Standardized database

E.O. 13693
DFARS 252.204-7012
NIST SP 1800-7a,b,c
IEC 61850

Cyber Security

-Risk Management Framework
-Continuous monitoring
-Type accreditation and standardization

E.O. 13636
DoDI 8510.01
NIST SP 800-37
NIST SP 800-82
NIST SP 800-161
NIST SP 800-171

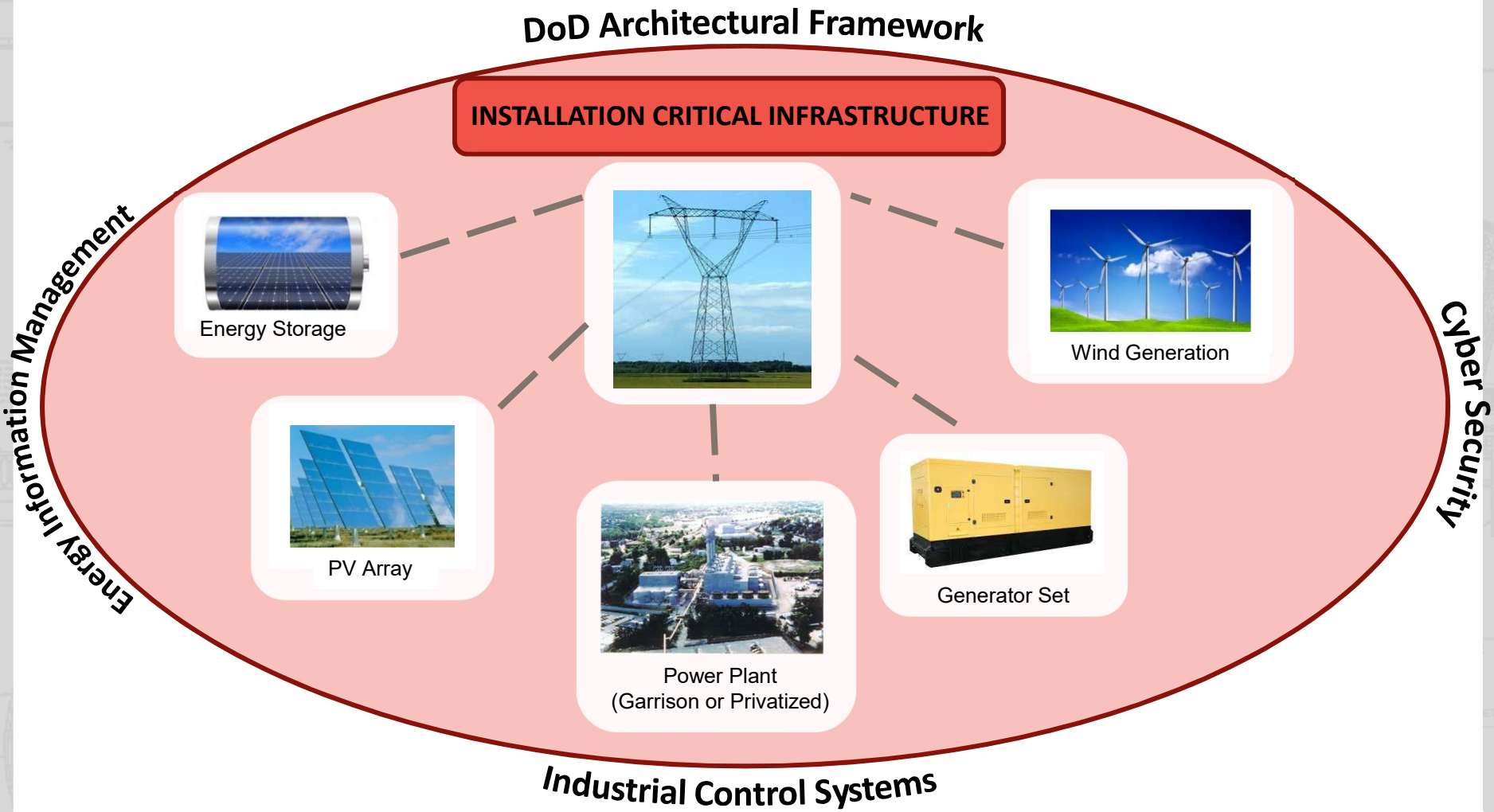
Industrial Control Systems

-To use the right tools/equip.
-Speed, accuracy, and reliability
-Assure life safety

EO 13636
UFC 3-500 series
UFC 4-010-06
IEC 62443
IEEE Std 242
IEEE Std 37.1
ANSI-NETA
IEEE 1547/2030
(mandatory)

Resiliency, Security, Safety, and Mission

OPERATIONAL ENVIRONMENT



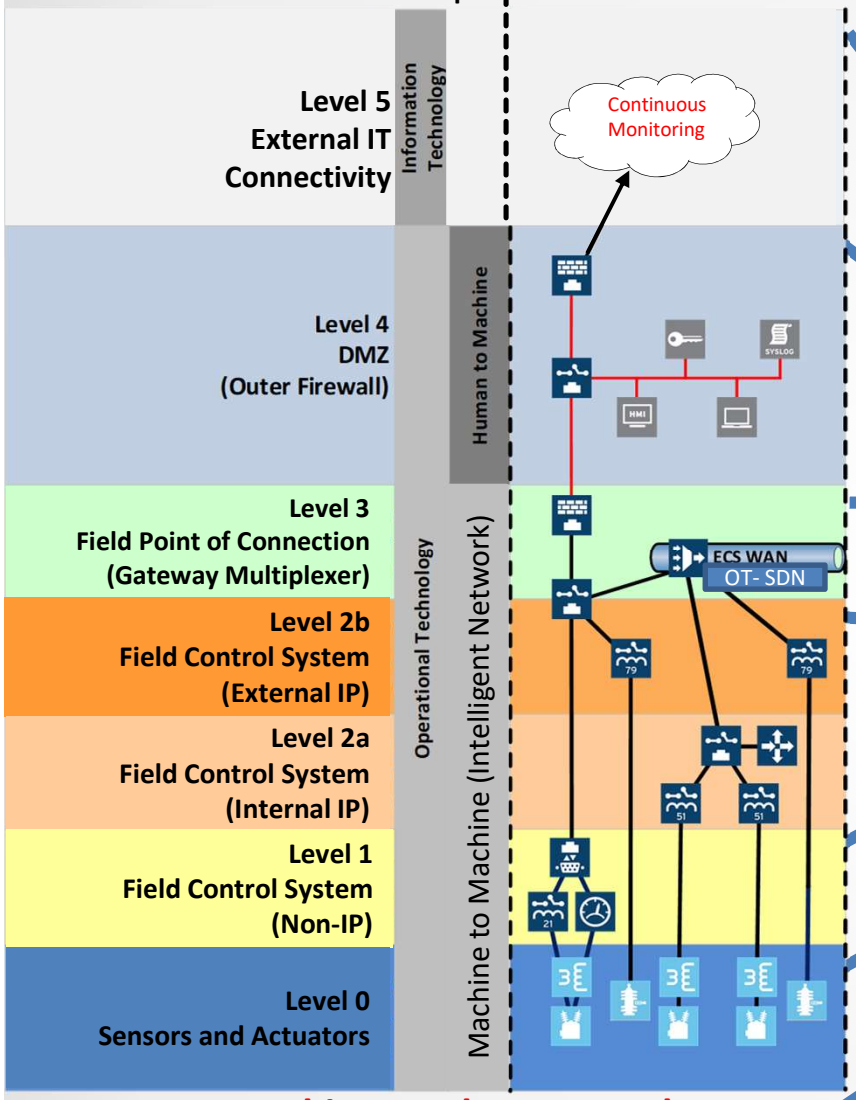
US Army Corps of Engineers

U.S.ARMY

Executing for Resiliency and Energy Security

Energy Control System

Defense-in-Depth Levels



DoD Architectural Framework

Medium and High Voltage

Cyber Security

Energy Information Management

DoDAF Defense-in-Depth NIST SP 800-82		Cyber Security
		Provides compliancy, continuity of ops, and training
Level 5	External Boundary	Risk Management, Interconnection Agreement
Level 4	NIST Standard	Publish and Subscribe for Data Accessibility
Level 3	NIST and IEEE Requirement	Segregates Human to Machine (Human Interaction) from Machine to Machine (Intelligent Automation)
Level 2	Resiliency, Security, and Safety	Pre-Engineer Traffic
Level 1	IEEE Standards	Protection of Serial Devices with no Ethernet
Level 0	Sensors	Signal sensing equipment and actuators

Industry Control Systems

Legend

Non-Embedded OS: Authentication, Syslog Server, HMI, Computer

Embedded OS: Ethernet Firewall, Ethernet Switch, Ethernet to Serial, Multiplexer, Ethernet Encryptor, Radio Encryptor, PAC/PLC, Distance Relay, Motor Relay, Overcurrent Relay, Recloser Relay, Differential Relay, Meter

Power System Components: AC Generator, Tranformer, Switching Gear, Circuit Breaker, Recloser, Wind Turbine, Photovoltaic, DC Cell, DC/AC Invertor

SLIDE 3

OPERATION TECHNOLOGY VS INFORMATION TECHNOLOGY CONTINUUM

Control Systems

Industry defines as Industrial Control System

Industrial Controls (Utility, Process) (sub-microseconds) | Local Controls (BAS) (Seconds/microseconds)

Government delineates (NIST SP 800-82)

Operational Technology

Industrial Control Systems (high speed)
Mission Critical
Mission Essential
Higher safety risk threshold (high & medium voltage)

Building Automation Systems (lower speeds)
Mission Support
Lower safety risk threshold (low voltage)

Information Technology

Operational Technology

- ❑ Real-time response critical
  - Precision timing/(IEEE 1588)teleprotection (IEC 61850)
- ❑ Response to human and other emergency critical
- ❑ Control physical world (energy distribution)
- ❑ Medium and high voltage systems
  - Micro-Grids
  - Power Generation Systems
  - Energy Distribution System
  - Power Plants
  - Generator Sets
  - Wind Generation
  - PV Array
  - SCADA system
  - Water energy plants
  - Industrial control systems (ICS)
- ❑ Complex Networks

***UFCs and UFGSs *are not fully* developed

Information Technology

- ❑ Non Real-time performance
- ❑ Less critical emergency interaction
- ❑ Low voltage systems
  - UMCS (a control system but not an ICS)
    - NIST SP 800-82 rev2 2.5 (p 2-17) (control system classification)
    - UFC 4-010-06 (p 25) (geared towards building control/BAS)
    - UFGS 23 09 00 3.2.5.2 (UMCS requires seconds/microseconds), IEEE 1588 (ICS requires sub-microseconds) (precision timing)
  - EMCS
  - Metering (EEDRS)
  - Unit level Building Automation Systems (BAS)
- ❑ Manage Data
- ❑ Standard communications protocols

***UFCs and UFGSs *are* developed

of Engineers

U.S.ARMY

ENERGY INFORMATION MANAGEMENT AND METERING ENVIRONMENTS

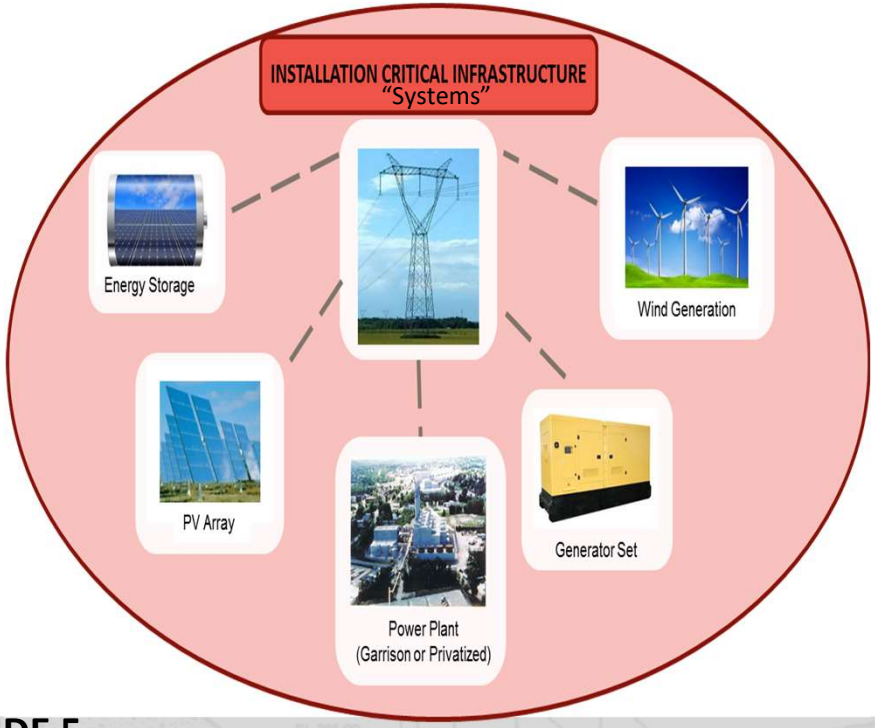
Energy Information Management

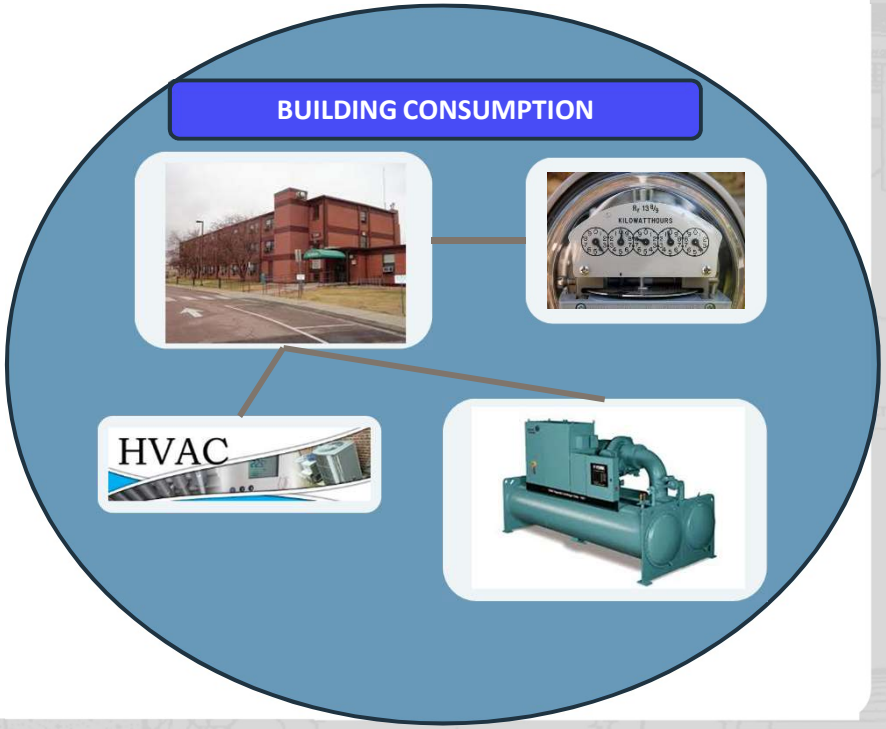
-Systems/system-of-systems
-Security, resiliency, and monitoring of critical infrastructure
-Visualization of a complex system environment
-Power quality monitoring
-Critical to life, safety, and health
-Integrates OT and IT

Army Metering Program

-Facility energy use (building consumption)
-Energy use intensity
-Communication speeds are slower
-Not critical to life, safety, and health

*Foundational to meeting EO 13636, and forms the basis for standardization of an OT output





PROCESS FOR ENERGY SOLUTIONS

INPUTS

- Executive Order
- Programs
- Unified Facilities Criteria
- Institute of Electrical and Electronics Engineers
- National Institute of Science and Technology

COMMON FOUNDATION FOR REPEATABLE ENERGY SOLUTIONS
Department of Defense Architectural Framework
Industrial Control System
Energy Information Management
Cybersecurity
Safety Integration Program

Resiliency

Security

OMB Goals (Why):
- Interoperability
- Cost Savings
- Competition
- Innovation
- Tech Refresh (LCCA)
- EO 13693 Planning for Federal Sustainability in the Next Decade
- EO 13636 Improving Critical Infrastructure Cybersecurity

(What)
Base Contract
RFP, PWS
SOW
ECMs

Approaches (How):
- Modular Design
- Defined Interfaces
- Standard Process
- Accessible Data
- Open Interfaces
- IP Rights
- Inclusion of stakeholders
- OMB Circular No. A-130 Managing Information as a Strategic Resource

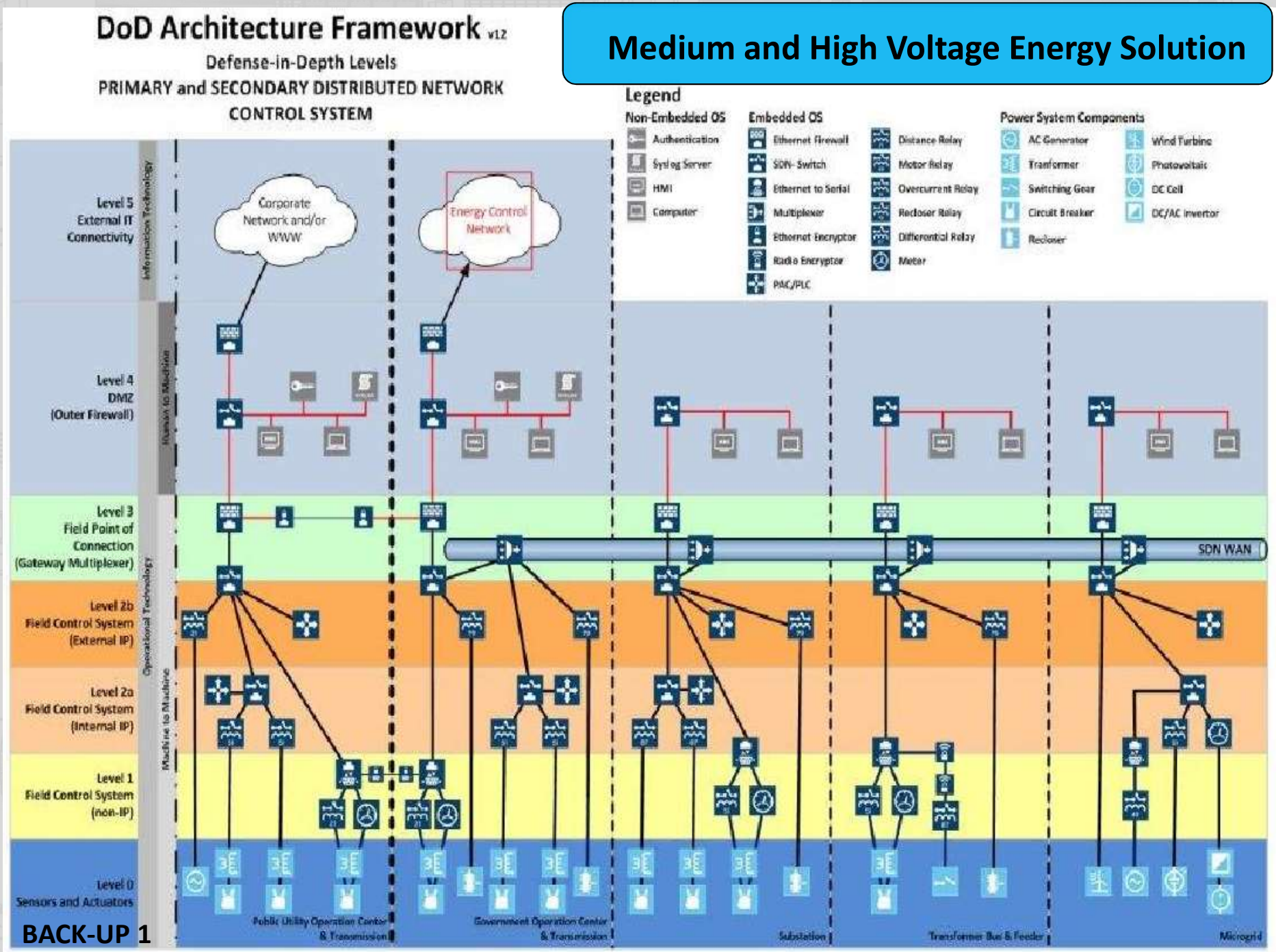
Output:
Deliver cyber secure comprehensive integrated energy security resiliency solutions
Visualize environment to make decisions, troubleshoot, and manage critical infrastructure

BACKUP

US Army Corps of Engineers

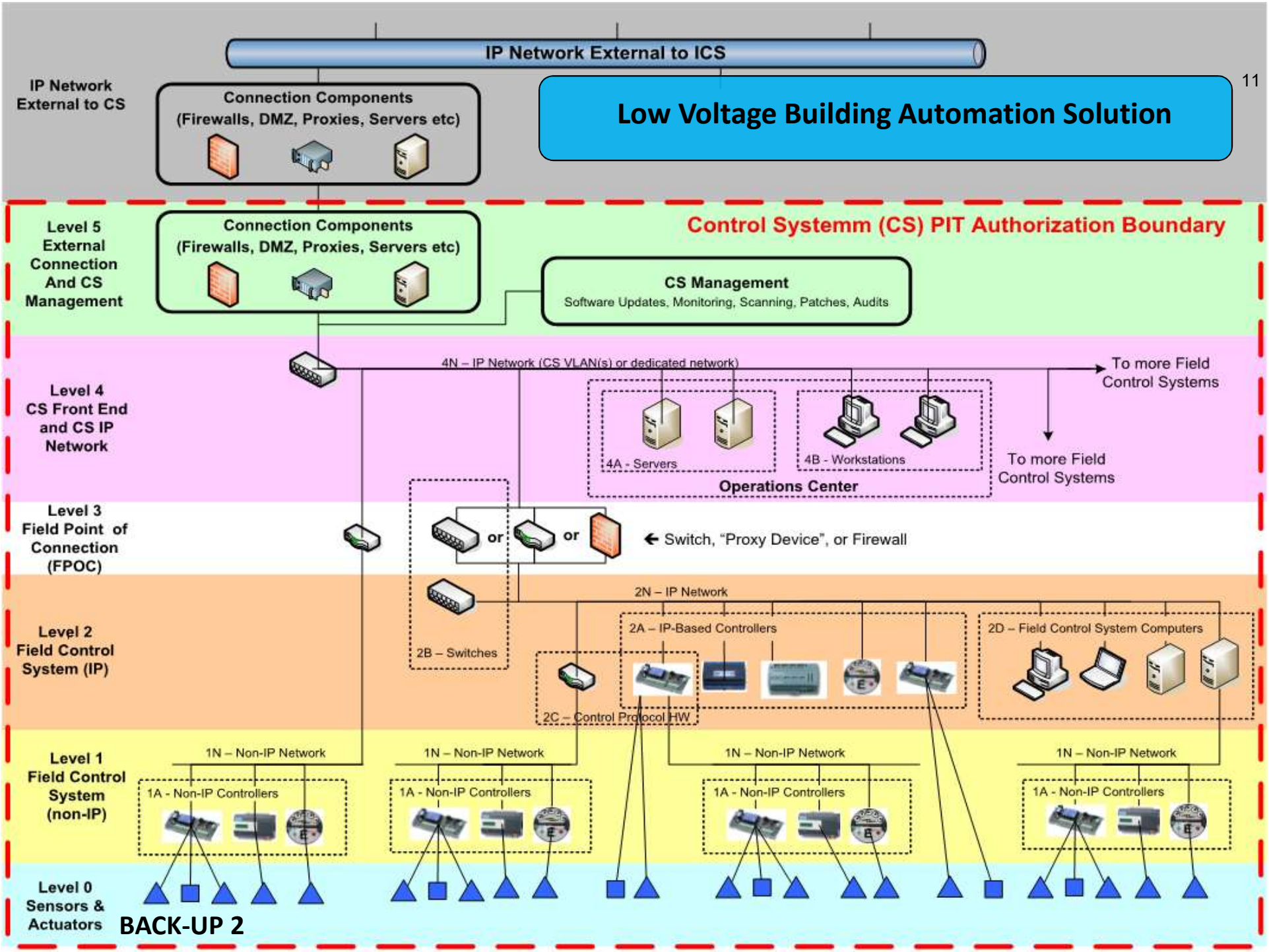
U.S.ARMY

Medium and High Voltage Energy Solution



BACK-UP 1

Low Voltage Building Automation Solution



BACK-UP 2

OPERATION TECHNOLOGY VS INFORMATION TECHNOLOGY RISKS

Risks of Applying IT Solution to OT System

- Negative Impacts to Mission
  - Inferior design; IT systems not designed for operational high speed environment
  - IT lifetimes have shorter life spans, 3 to 5 years compared to 10 to 15 for OT

- Decreased Security
  - Compromise data system versus operational systems
  - Networks are complex and sometimes require the expertise of control engineers
  - Less efficient system, easily hacked

- Increased Risks to Safety
  - Life safety response slower or non existent with IT systems
  - Fault tolerance is essential with OT, even momentary downtime is unacceptable, unlike IT
  - Higher chances of accidents or safety incidents

IT VS OT

	Information Technology	Operational Technology
Scope & Ownership	Information Technology (IT) covers the spectrum of systems that support corporate functions like Finance, HR, Supply Chain, Order Management, Sales, etc. More often than not, these functions and their processes tend to have commonality across industries.	Operational Technology (OT) covers the spectrum of systems that deal with the physical transformation of products and services. **They are task-specific systems,** are highly customized for industries and **considered mission-critical.** They typically fall under the domain of Engineering.
End-Point	In the world of Corporate IT, the end-point being managed is often a human (whose job tends to be information-intensive) using a computing device (that has been relatively homogeneous until the recent and growing BYOD [bring your own device] trend.)	In the world of OT, the end-point being managed is often a physical asset such as pumps, motors, conveyors, valves, forklifts, etc., where these "things" come in all shapes, sizes, level of complexity, versions and vintage.
Focus	The software applications that make up the IT portfolio are people-centric in the sense that they help people "make money" by managing and coordinating the higher-level processes and transactions of the business.	In contrast, most of the software applications in OT's portfolio are "thing-centric" in the sense that they help "make product" by controlling the physical equipment with a great deal of precision (and safety), where the human's role is supervisory (as automation increases.)
Architecture	Besides being pervasive in our personal lives, IT is a relatively standardized world, and that is far more homogeneous than OT.) IT also tends to adapt far more quickly to multiple computing trends, from PCs to Internet to mobility, all of which have broadly shaped today's Corporate IT strategy.	In contrast, OT is filled with silos of proprietary architectures because of its task-specific nature. For example, a refinery is designed so it can run continuously for 5+ years before it is shut down for maintenance. In other words, reliability can often trump innovation, open architecture, interoperability, etc.

US Army Corps of Engineers

U.S.ARMY