Artificial Intelligence Approaches for Physical and Cyber Resilience of the 16 DHS CISA Designated Critical Infrastructure Sectors in the US Economy

Alex Dely, Contracts Manager
Advanced Air Warfare Systems Directorate
Advanced Integrated Kill Chain Architecture Directorate
Raytheon Missiles and Defense

(Co)Faculty, UA Systems & Industrial Engineering
SIE 414/514 Law for Scientists and Engineers
SIE 573 Engineering of Trustworthy Secure Systems

September 16, 2022

THE UNIVERSITY OF ARIZONA

OUTLINE: BREAD CRUMBS…..

I) The 16 NIST-DHS-NSA Critical Infrastructure Sectors

II) 16 Flavors of Artificial Intelligence, 10 AI Development and Implementation Challenges, 10 "Early Stage/Plain Vanilla" AI Use Cases in Industry"

III) Global Trends, "Technology Grand Challenges": National Academies, NSF, US and International Agencies

IV) "Grand Challenge" AI Use Case Examples in some of the 15 non-DoD CI Sectors

V) Is AI affecting the Industrial Control Systems Cyber Threat Landscape? NIST SP-800 171/172 ICS Cyber Security Guidelines

VI) A new (Southern) Arizona "AI Entrepreneurship Cluster"

I. Dept of Homeland Security’s 16 Critical Infrastructure Sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

Source: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Complex Interactions With Corresponding Government - Industry Expertise & Accountability

- Per President of the United States (POTUS) Executive Order 13636 "Improving Critical Infrastructure Cybersecurity": National Infrastructure Protection Plans to be promulgated for each sector by the designated Federal Agency in coordination with State/Local Government and Private Sector Infrastructure Operators:

- 1) Emergency Services (18,000 law enforcement agencies; 27,200 fire departments
- 2) Chemical Facilities (13,500 manufacturing plants)
- 3) Defense Industrial Base (50,000 defense contractors; 1180 Bases)
- 4) Dams (84,000)
- 5) Electrical Energy (3,300+ utilities)
- 6) Water & Wastewater Facilities (65,000+)
- 7) Public Health Facilities (5,600+)
- 8) Nuclear Reactors (99)
- 9) Food & Agriculture (30,000 Processing Plants; 2.1M farms)
- 10) Non-DoD Government Facilities (16,600 facilities; 3300 County election systems)
- 11) Critical Manufacturing (25,500 facilities)
- 12) Communications (105,000 cell towers; 550,000 miles of fiber optic cable)
- 13) Financial Services (13,000 financial institutions)
- 14) Information Technology (7,000 major data centers)
- 15) Transportation (185 ports; 19,500 airports; 15.5M trucks; 540K railroad cars)
- 16) Major Commercial Facilities (380,000+)

- **VOLUNTARY COMPLIANCE, COMPLEX INTERLINKAGES, WITH LIMITED CORRESPONDING GOVERNMENT-INDUSTRY EXPERTISE & ACCOUNTABILITY**

II. 16 Flavors of Artificial Intelligence

- Sensor Hardware/Software/Firmware in Find/Fix/Track/Target/Engage/Assess
- Collaborative Autonomy
- Supervised vs Unsupervised Learning
- Reinforcement Learning
- Symbolic AI
- Advanced Modeling and Simulation
- Advanced Heuristics
- Convolutional Neural Networks
- All-Source Intelligence Fusion
- Cognitive Amplifiers
- Design of Experiments and Bayesian Networks
- Genetic Algorithms
- Intelligent Agents
- Decision Process Optimization
- Natural Language Processing
- Ontological Reasoning

FURTHER INFO: Dr. Chertkov, Applied Math, chertkov@arizona.edu

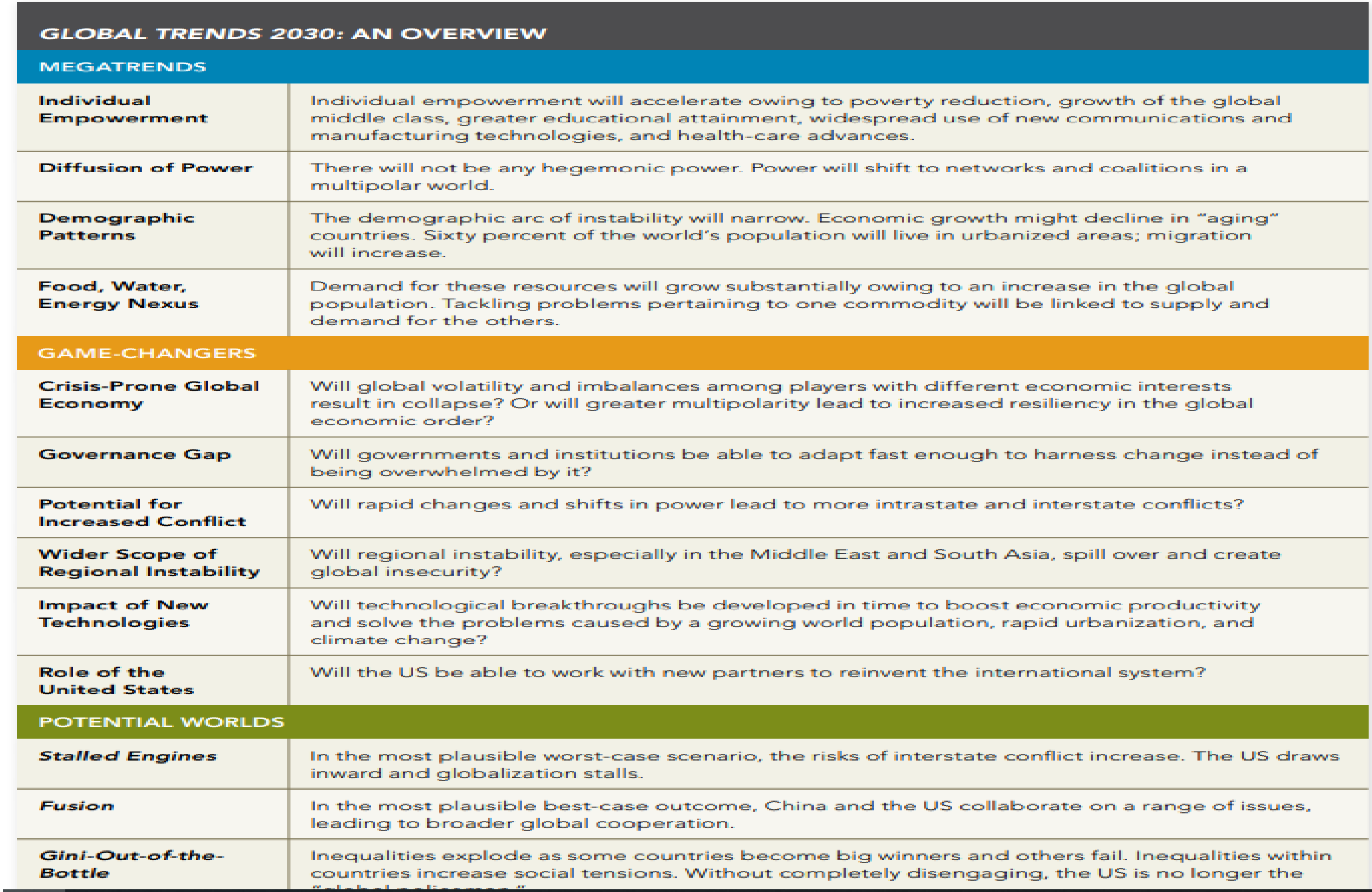
II. Top 10 AI Development and Implementation Challenges

1. Determining Right Data Set: trusted, clean, accessible, well-governed, secure
2. Biases: low quantity/quality training data with racial, gender, ethnic, etc biases. Need control frameworks to establish trust
3. Data Security and Storage: Terabyte+ training datasets for algorithm optimization
4. Computing Power + Infrastructure: extensive/expensive new processing capabilities
5. AI Integration with existing Business Systems/Processes and Staff Training
6. New Skillsets: Data Science etc.
7. Rapidly Morphing Legal/regulatory Environment: Data Privacy, etc
8. Explainability: are Models Accurate/Complete/Reliable, auditing.
9. AI Implementation Road Map
10. AI Intellectual Property Road Map

II. "Lower Value/Plain Vanilla" AI Analytics-Driven Use Cases In Industry by $ Spent (2021)

1) Supply Chain/Procurement/Logistics/Asset Tracking Optimization ("Walmart/Amazon")
2) Factory Automation/Production Scheduling/Inventory Management ("IBM/SAP")
3) Backoffice Process Optimization ("JPMorgan Chase")
4) Cyber Security Attack Early Warning ("Google/Anduril/Palantir")
5) Reliability Engineering/Defect Detection/Preventive Maintenance ("Boeing Aerospace")
6) "Digital Twins" Modeling and Simulation ("Electric Utility"
7) Autonomous Vehicles ("Tesla")
8) Robotics ("Japan")
9) Product Development ("Pfizer/Moderna"
10) Internet of Things-Telecommunications 5G-6G ("Huawei")

III. CIA Global Trends 2030 (160 pages)



GLOBAL TRENDS 2030: AN OVERVIEW	
MEGATRENDS	
Individual Empowerment	Individual empowerment will accelerate owing to poverty reduction, growth of the global middle class, greater educational attainment, widespread use of new communications and manufacturing technologies, and health-care advances.
Diffusion of Power	There will not be any hegemonic power. Power will shift to networks and coalitions in a multipolar world.
Demographic Patterns	The demographic arc of instability will narrow. Economic growth might decline in "aging" countries. Sixty percent of the world's population will live in urbanized areas; migration will increase.
Food, Water, Energy Nexus	Demand for these resources will grow substantially owing to an increase in the global population. Tackling problems pertaining to one commodity will be linked to supply and demand for the others.
GAME-CHANGERS	
Crisis-Prone Global Economy	Will global volatility and imbalances among players with different economic interests result in collapse? Or will greater multipolarity lead to increased resiliency in the global economic order?
Governance Gap	Will governments and institutions be able to adapt fast enough to harness change instead of being overwhelmed by it?
Potential for Increased Conflict	Will rapid changes and shifts in power lead to more intrastate and interstate conflicts?
Wider Scope of Regional Instability	Will regional instability, especially in the Middle East and South Asia, spill over and create global insecurity?
Impact of New Technologies	Will technological breakthroughs be developed in time to boost economic productivity and solve the problems caused by a growing world population, rapid urbanization, and climate change?
Role of the United States	Will the US be able to work with new partners to reinvent the international system?
POTENTIAL WORLDS	
Stalled Engines	In the most plausible worst-case scenario, the risks of interstate conflict increase. The US draws inward and globalization stalls.
Fusion	In the most plausible best-case outcome, China and the US collaborate on a range of issues, leading to broader global cooperation.
Gini-Out-of-the-Bottle	Inequalities explode as some countries become big winners and others fail. Inequalities within countries increase social tensions. Without completely disengaging, the US is no longer the "global policeman."

III. Global Grand Technology Challenges

Excellent lists are continuously updated by various authoritative US And International agencies/entities, such as:

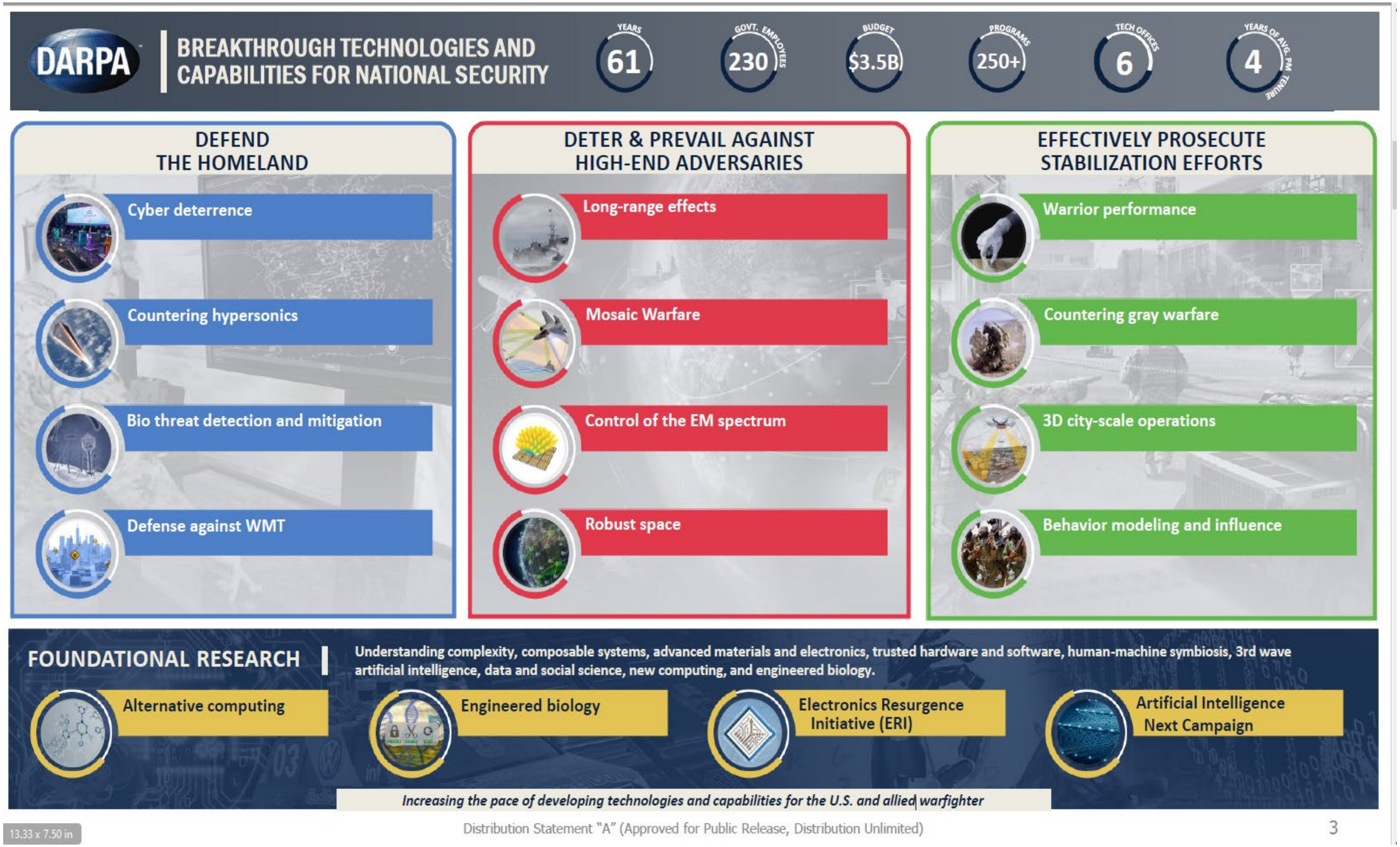
- National Academy of Engineering
- National Academy of Sciences
- National Science Foundation
- Department of Defense-DARPA
- Director of National Intelligence-IARPA, CIA
- Department of Homeland Security-HSARPA
- Department of Health & Human Services-BARDA
- Various United Nations Agencies
- World Bank
- etc

III. National Academy of Engineering “Technology Grand Challenges”

The National Academy of Engineering brought together a panel of leading people in academia, policy and business with the charge to identify a small number of grand challenges for engineering in the 21st century. This interdisciplinary group concluded that the following 14 areas would be the Grand Challenges of Engineering in the 21st century:

- Make solar energy economical
- Provide energy from fusion
- Develop carbon sequestration methods
- Manage the nitrogen cycle
- Provide access to clean water
- Restore and improve urban infrastructure
- Advance health informatics
- Engineer better medicines
- Reverse-engineer the brain
- Prevent nuclear terror
- Secure cyberspace
- Enhance virtual reality
- Advance personalized learning
- Engineer the tools of scientific discovery

III. DARPA (Defense Advanced Research Projects Agency)/"Defense Industrial Base" Sector



DARPA | BREAKTHROUGH TECHNOLOGIES AND CAPABILITIES FOR NATIONAL SECURITY

YEARS	GOVT. EMPLOYEES	BUDGET	PROGRAMS	TECH OFFICES	YEARS OF AVG. PM TENURE
61	230	$3.5B	250+	6	4

DEFEND THE HOMELAND	DETER & PREVAIL AGAINST HIGH-END ADVERSARIES	EFFECTIVELY PROSECUTE STABILIZATION EFFORTS
Cyber deterrence	Long-range effects	Warrior performance
Countering hypersonics	Mosaic Warfare	Countering gray warfare
Bio threat detection and mitigation	Control of the EM spectrum	3D city-scale operations
Defense against WMT	Robust space	Behavior modeling and influence

FOUNDATIONAL RESEARCH | Understanding complexity, composable systems, advanced materials and electronics, trusted hardware and software, human-machine symbiosis, 3rd wave artificial intelligence, data and social science, new computing, and engineered biology.

- Alternative computing
- Engineered biology
- Electronics Resurgence Initiative (ERI)
- Artificial Intelligence Next Campaign

Increasing the pace of developing technologies and capabilities for the U.S. and allied warfighter

13.33 x 7.50 in

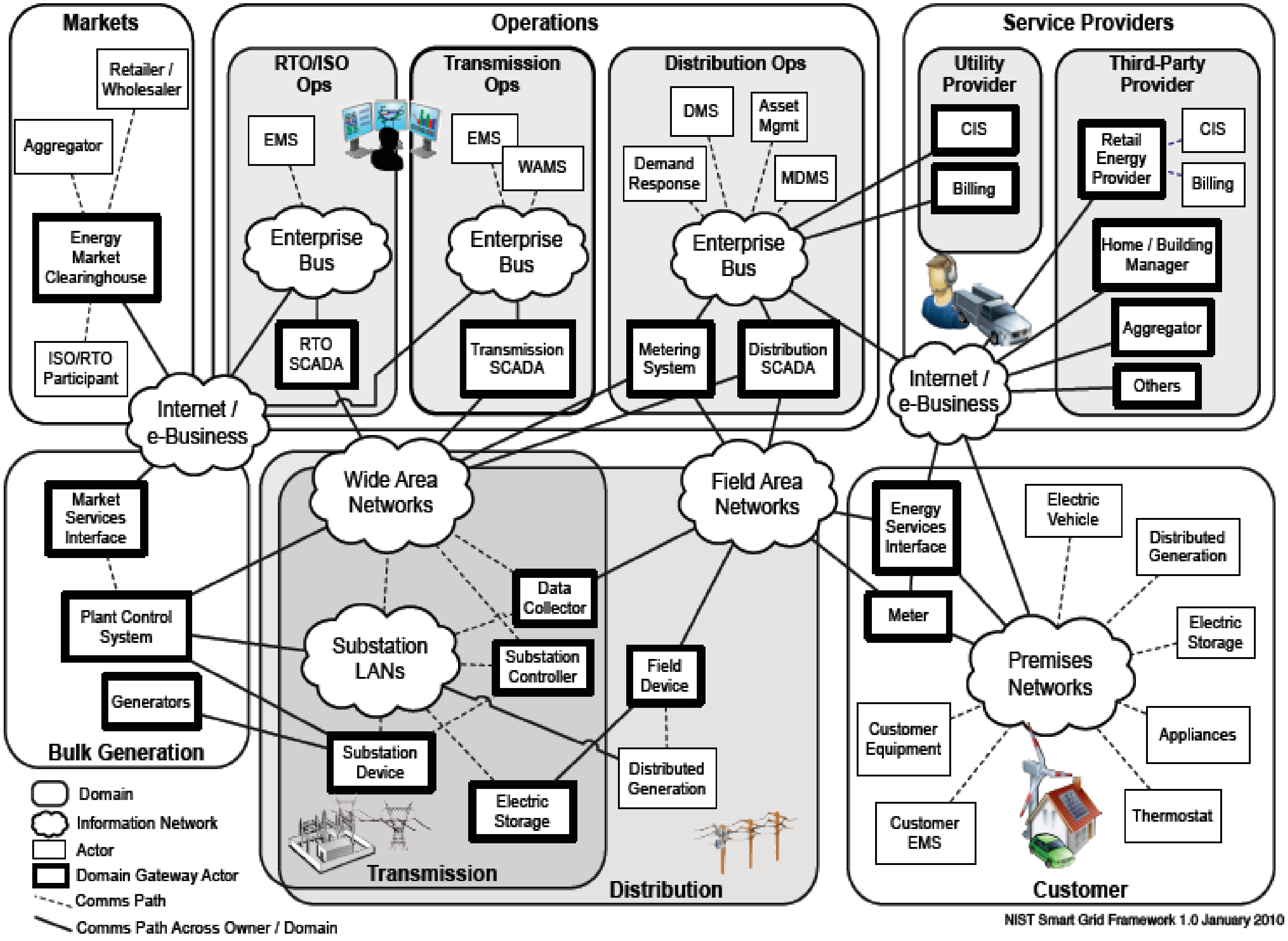
Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

3

III. Intelligence Community-IARPA ("Defense Industrial Base Sector"

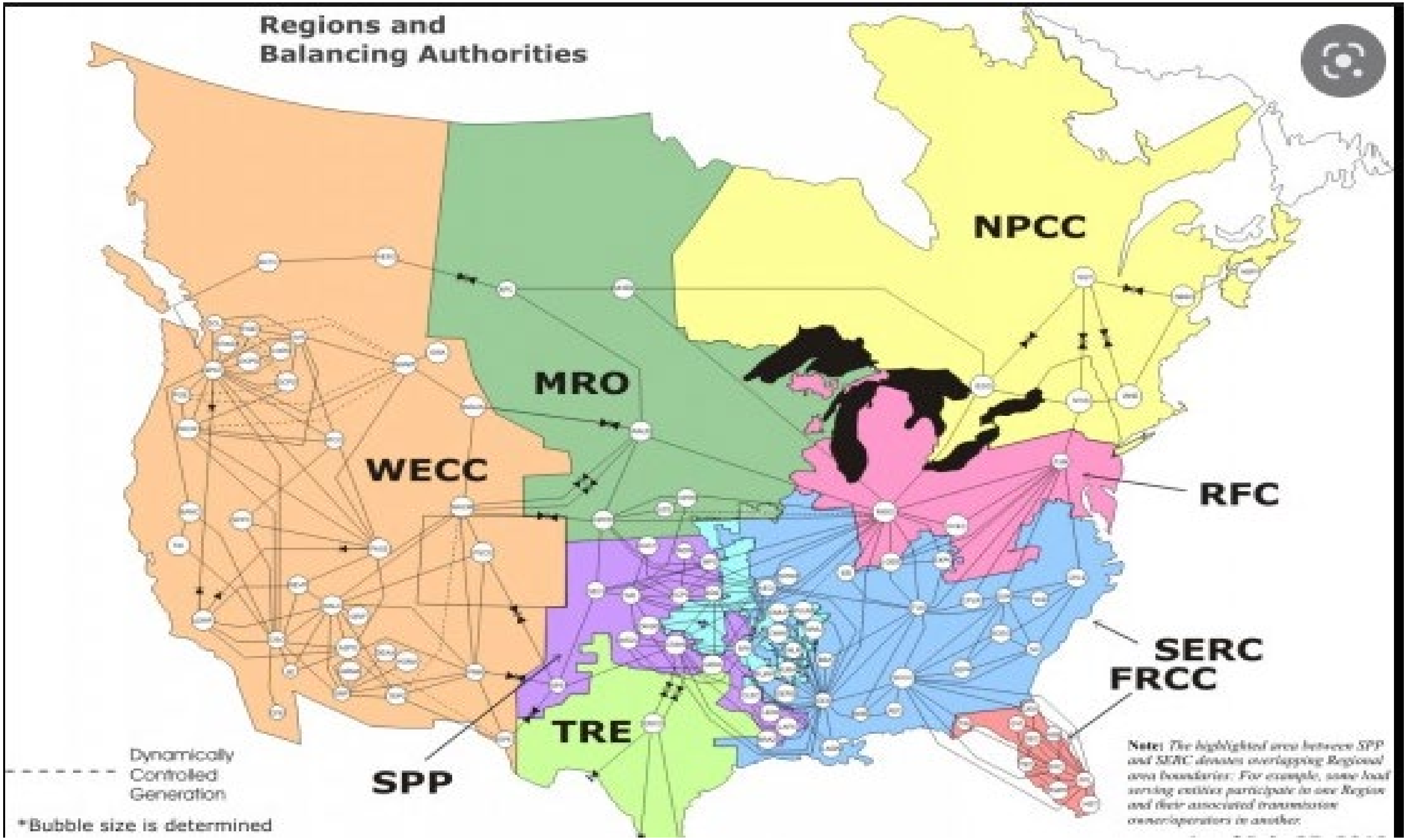
- The Intelligence Advanced Research Projects Activity invests in high-risk, high-payoff research programs to tackle some of the most difficult challenges of the agencies and disciplines in the Intelligence Community (IC).
- OUR MISSION
- IARPA's mission is to push the boundaries of science to develop solutions that empower the IC to do its work better and more efficiently for national security. IARPA does not have an operational mission and does not deploy technologies directly to the field. Instead, we facilitate the transition of research results to our IC customers for operational application.
- IARPA AND THE IC
- IARPA collaborates across the IC to ensure that our research addresses relevant future needs. This cross-community focus guarantees our ability to address cross-agency challenges, leveraging both operational and research and development expertise from across the IC, and coordinating transition strategies with our IC partners.
- AREAS OF INTEREST
- Artificial Intelligence
- IARPA is working toward breakthroughs in artificial intelligence, or AI, through a number of research programs to benefit the IC and nation.
- Quantum Computing
- As part of its mission to address some of the most difficult challenges in the IC, IARPA sponsors several applied research programs that explore the potential and possibilities in quantum computing.
- Machine Learning
- IARPA sponsors research programs and challenges that either leverage or improve Machine Learning and its applications within the IC.
- Synthetic Biology
- IARPA is investing in cutting-edge synthetic biology research that will help the IC address biothreats along with other possible applications.

IV. Sector 1 of 15 Non-DoD CI Sectors: Electrical Utility Grid Typical ICS Systems



NIST Smart Grid Framework 1.0 January 2010

IV. Sector 1 of 15: Electric Utilities NERC/FERC US Regional Interconnect Operators



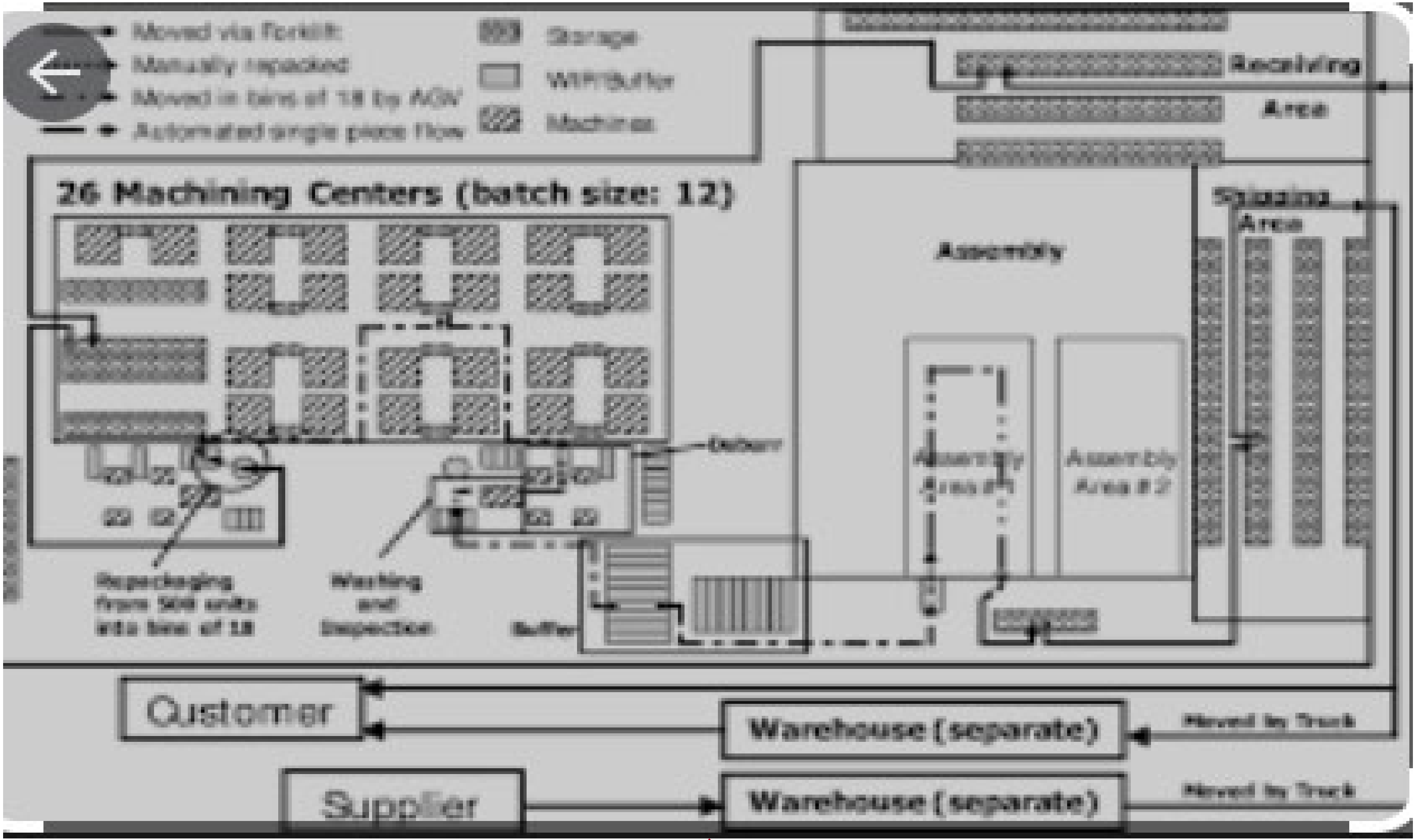
Note: *The highlighted area between SPP and SERC denotes overlapping Regional area boundaries: For example, some load serving entities participate in one Region and their associated transmission owner/operators in another.*

IV. Sector 1 Energy Utilities : Top 4 “Advanced” AI Research Applications in order of $ Allocated

1) Renewables/EV Integration and Grid Network Stability/Reliability/Availability/Safety: AC-DC Current and Picosecond 60Hz Phasor alignment throughout the system, FERC/NERC 99.9999%)
2) Grid Physical/Cyber Security (see Section V)
3) Greenhouse Gas Emissions and Carbon Capture and Storage
4) Dynamic Energy Trading and Differential Pricing

2021 Retail US Electricity Market: $ 424 Billion/Year, CAGR 8%; 3.8 Trillion Kwh, at average of $ 13.7Cents/KwH

IV. Sector 2 of 15: Critical Manufacturing



IV. Sector 2 of 15 Critical Manufacturing: Top 4 “Advanced” AI Research Applications in order of $ Allocated

1. Cloud Computing Digital Twin Process Optimization

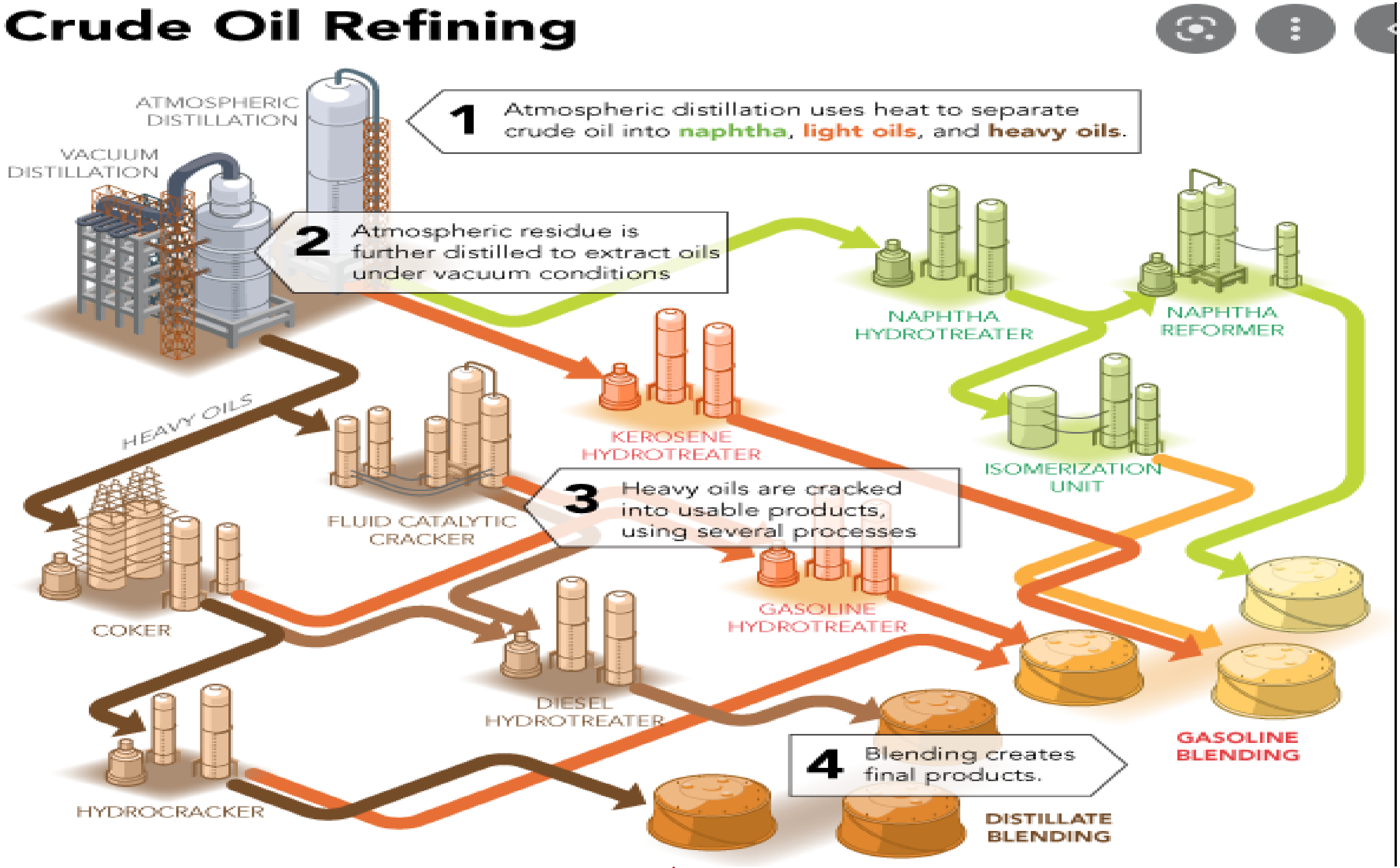
2. Autonomous Flexible Robotics in 24/7 Dark Factories

3. Edge Analytics of Quality KPIs (Yield, Quality, etc)

4. Modeling and Simulation and Additive Manufacturing of Custom Engineered Materials

Critical Manufacturing value in 2021: $ 2.7 Trillion.

IV) Sector 3 of 15: Oil/Gas/Petrochemical Facilities



Crude Oil Refining

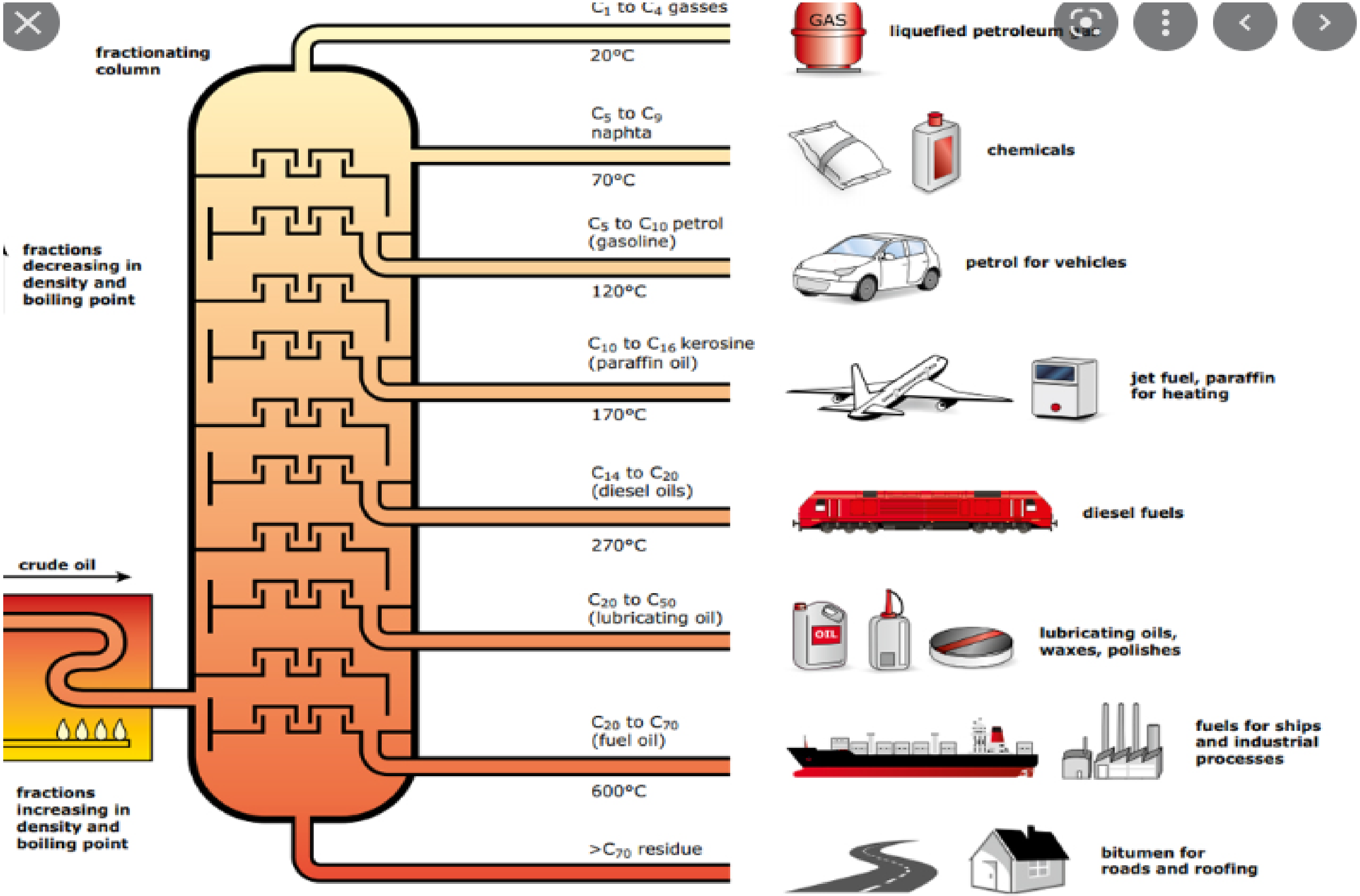
1 Atmospheric distillation uses heat to separate crude oil into **naphtha**, **light oils**, and **heavy oils**.

2 Atmospheric residue is further distilled to extract oils under vacuum conditions

3 Heavy oils are cracked into usable products, using several processes

4 Blending creates final products.

IV) Sector 3 of 15: Oil/Gas/Petrochemical Facilities


C_1 to C_4 gasses
fractionating column
20°C
C_5 to C_9 naphta
70°C
C_5 to C_{10} petrol (gasoline)
120°C
C_{10} to C_{16} kerosine (paraffin oil)
170°C
C_{14} to C_{20} (diesel oils)
270°C
C_{20} to C_{50} (lubricating oil)
C_{20} to C_{70} (fuel oil)
600°C
>C_{70} residue
fractions decreasing in density and boiling point
crude oil
fractions increasing in density and boiling point
GAS
liquefied petroleum gas
chemicals
petrol for vehicles
jet fuel, paraffin for heating
diesel fuels
OIL
lubricating oils, waxes, polishes
fuels for ships and industrial processes
bitumen for roads and roofing

IV. Sector 3 of 15 Oil/Gas Petrochemical: Top 4 “Advanced” AI Research Applications by $ Allocated

1. Subsurface Geological Assessment (Drone-based AI and Hyper Spectral, Magnetometer, LIDAR, Seismic GPR Radar, Induced Polarization, etc Sensors)

2. Refinery Digital Twins Modeling and Simulation for Asset Optimization (63% of equipment is beyond half-life of equipment expected lifetime)

3. Reduction Well Downtime ($20,000/Day/Well)

4. Carbon Sequestration (Net Zero 2030-2050 Targets: CO2 storage in existing wellfields)

Sector covers 8% or $ 1.7 Trillion/Years in US GDP

IV. Sector 4 of 15: Health Care Surgical Facilities

IV. Sector of 15: Health Care Drug Manufacturing

IV. Sector 4 of 15: Health Care: Top 4 “Advanced” AI Research Applications by $ Allocated

1. Proteomics Protein 3D Structure Optimization for DNA/RNS based Therapies

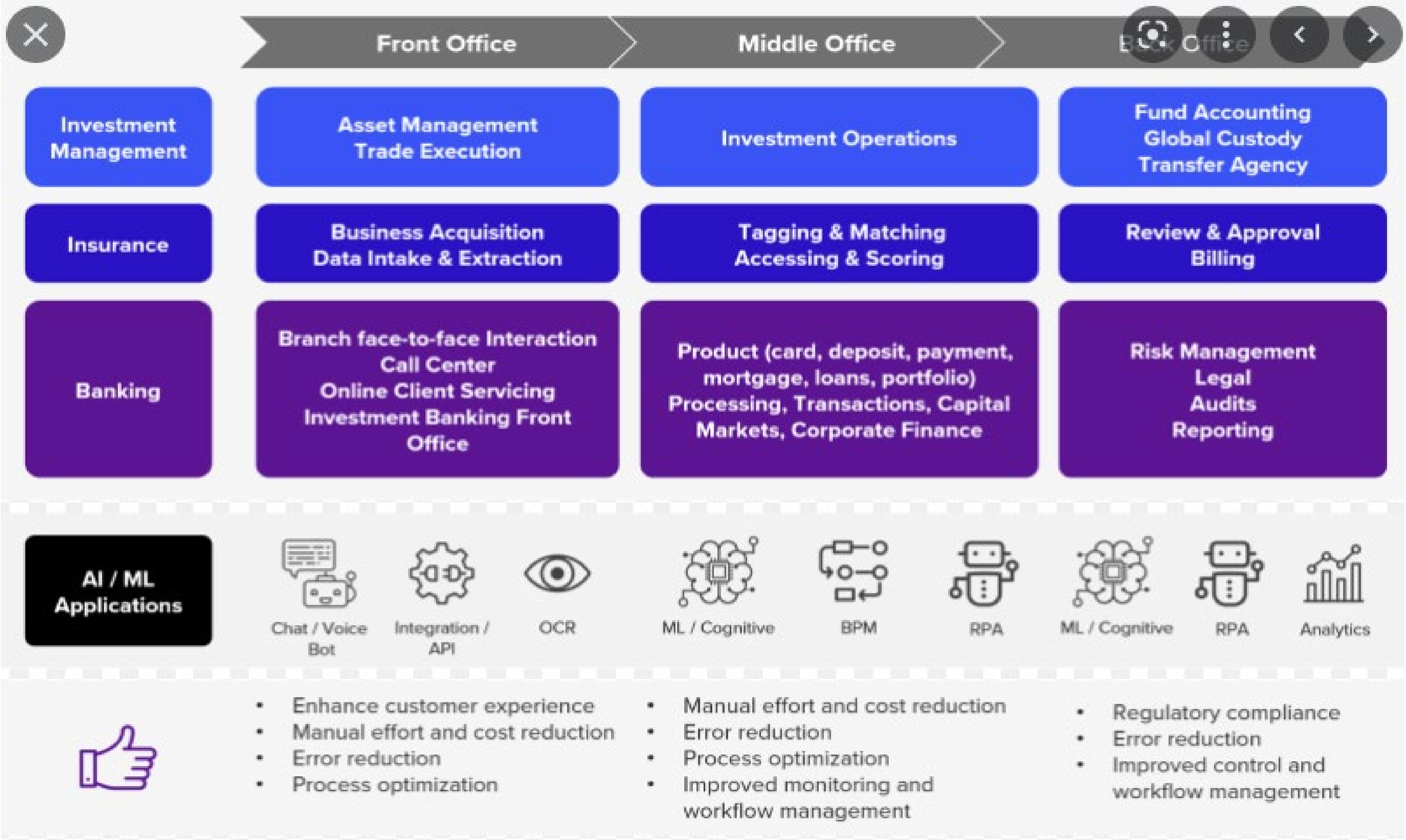
2. Global Epidemiology (Covid)

3. Medical Imaging Diagnostics (Cancer, Brain MRI, etc)

4. Acceleration of Statistically Significant Clinal Trials

Sector Impact: $ 4.4 Trillion/Year in US GDP

IV. Sector 5 of 15: Finance



	Front Office	Middle Office	Back Office
Investment Management	Asset Management Trade Execution	Investment Operations	Fund Accounting Global Custody Transfer Agency
Insurance	Business Acquisition Data Intake & Extraction	Tagging & Matching Accessing & Scoring	Review & Approval Billing
Banking	Branch face-to-face Interaction Call Center Online Client Servicing Investment Banking Front Office	Product (card, deposit, payment, mortgage, loans, portfolio) Processing, Transactions, Capital Markets, Corporate Finance	Risk Management Legal Audits Reporting
AI / ML Applications	Chat / Voice Bot Integration / API OCR	ML / Cognitive BPM RPA	ML / Cognitive RPA Analytics
👍	• Enhance customer experience • Manual effort and cost reduction • Error reduction • Process optimization	• Manual effort and cost reduction • Error reduction • Process optimization • Improved monitoring and workflow management	• Regulatory compliance • Error reduction • Improved control and workflow management

IV. Sector 5 of 15: Finance Infrastructure: Top 4 "Advanced AI Research Applications by $ Allocated

1. Global Credit Underwriting Analysis and Risk Assessment

2. Fraud Detection

3. Autonomic Personalized Financial Advisory Services

4. Cybersecure Personal Account Management and ROI Optimization

Sector Impact: 7.4% of US GDP: $ 1.5 Trillion/Year

IV. Sector 6 of 15: Transportation (Car/Train/Air/Ship)

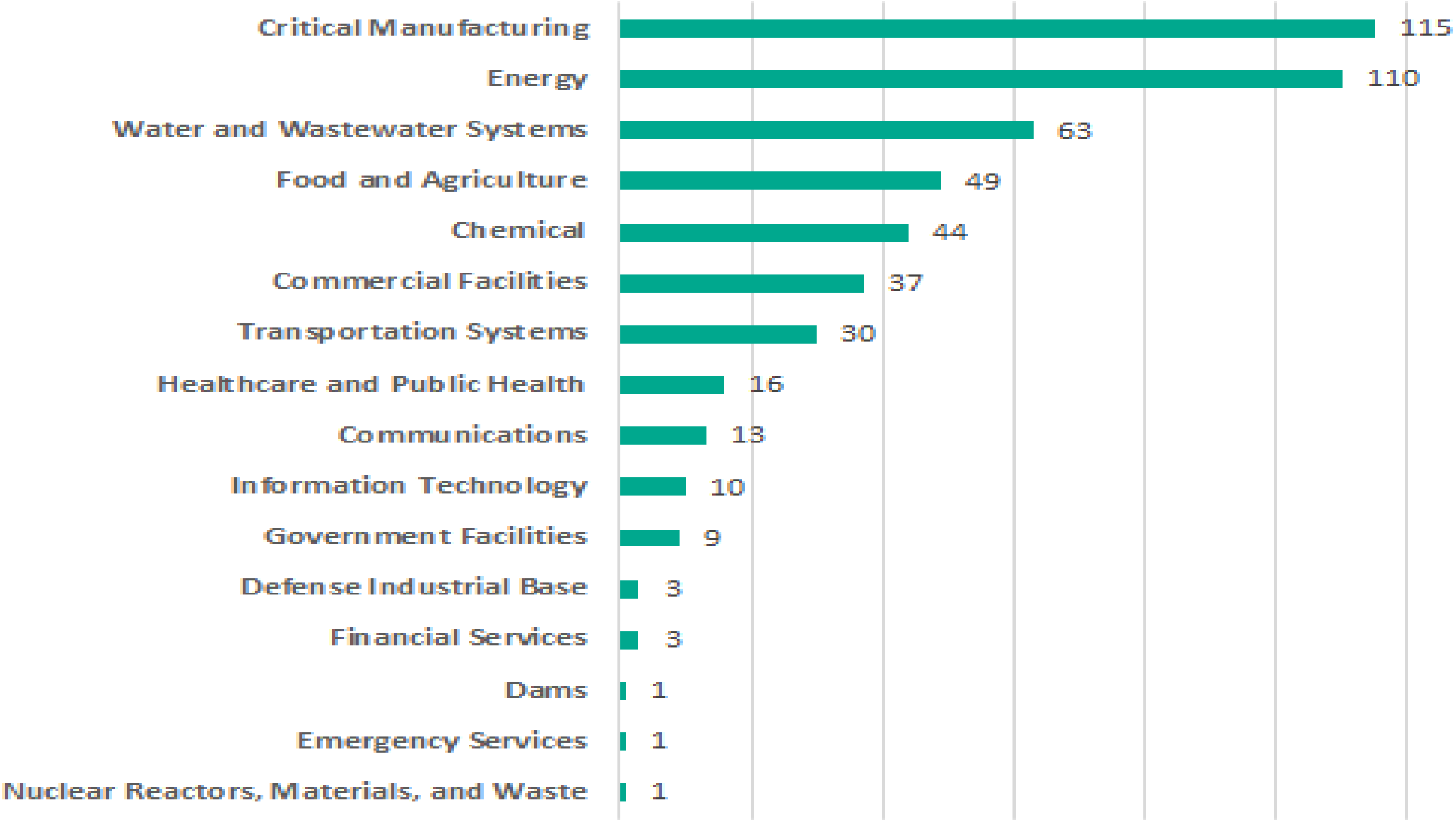
IV. Sector 6 of 15: Transportation: Top 4 “Advanced” AI Research Applications by $ Allocated

1. Self-Driving Vehicles
2. Traffic Flow Analysis and Differential Road Use Pricing
3. Computer Vision-Powered Parking Management
4. Road Condition Monitoring

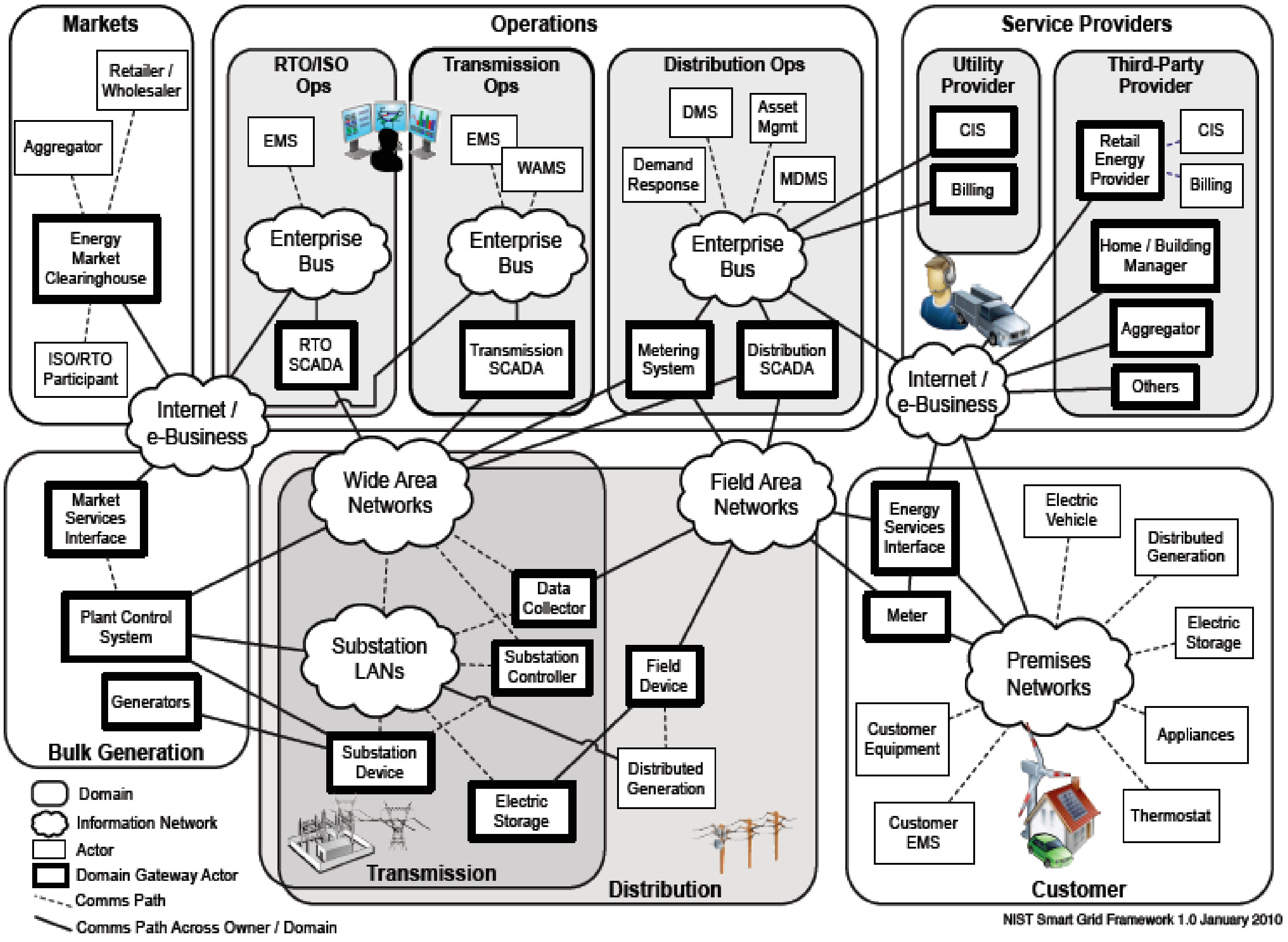
NOTE: Interesting Top 4 are all Surface Road focused, ie
applications in Air/Rail/Ship lagging

Sector Impact: 5.4% of US GDP: $ 1.24 Trillion/Year

V. ICS Cyber Incidents Per Year per Critical Infrastructure Sector

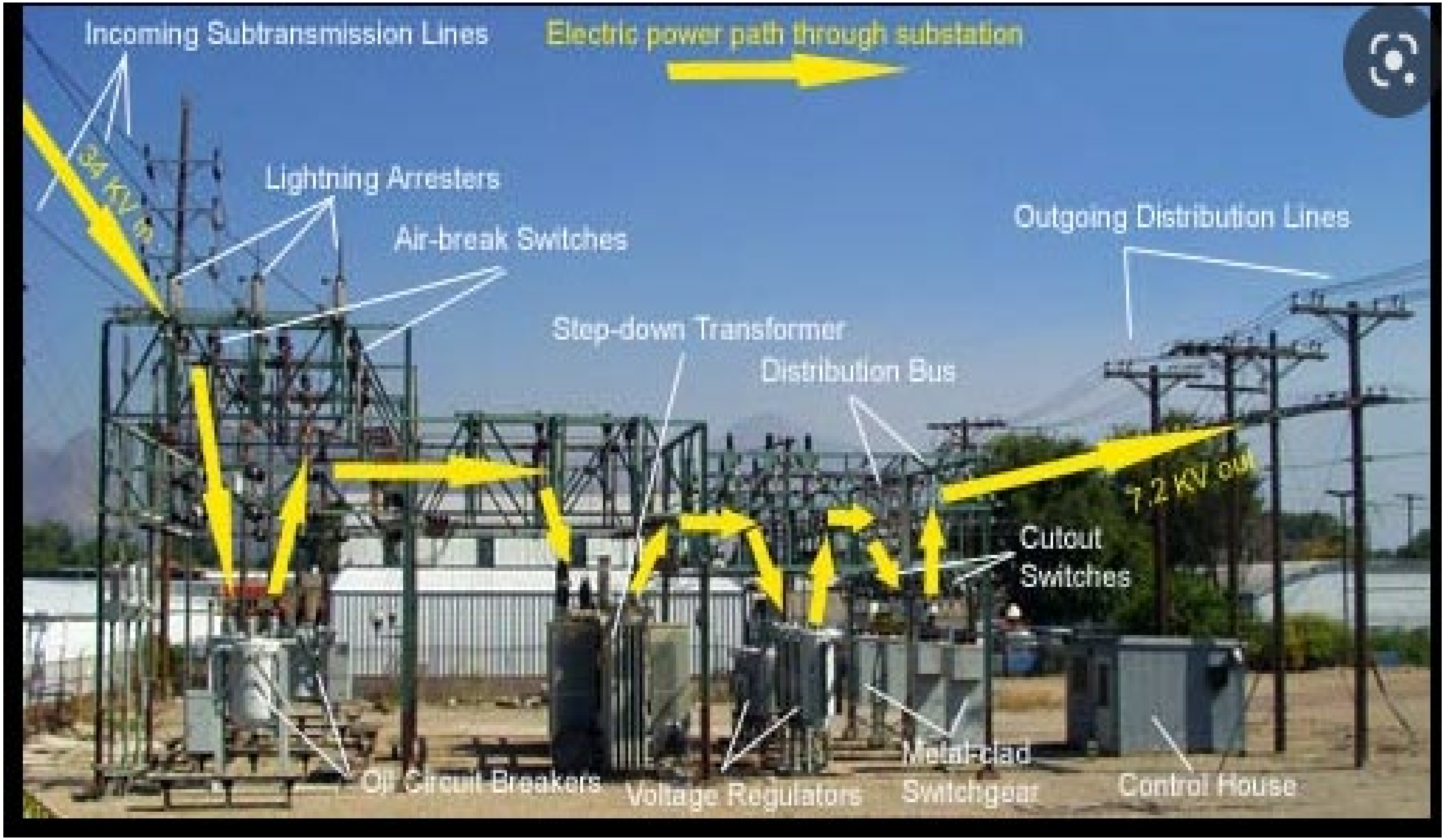


V. Increased Cyber Security Risks Example: Electrical Utility Grid Typical ICS (Industrial Control Systems)

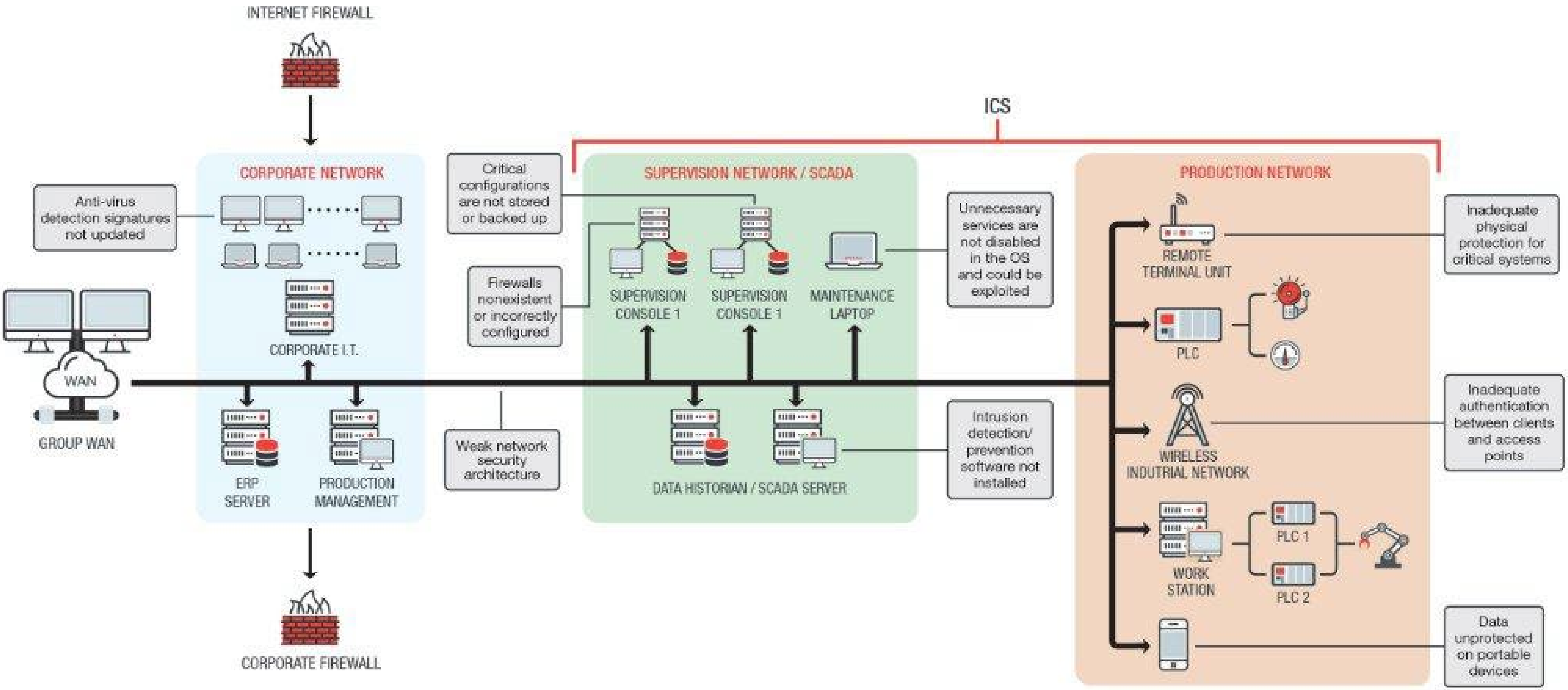


NIST Smart Grid Framework 1.0 January 2010

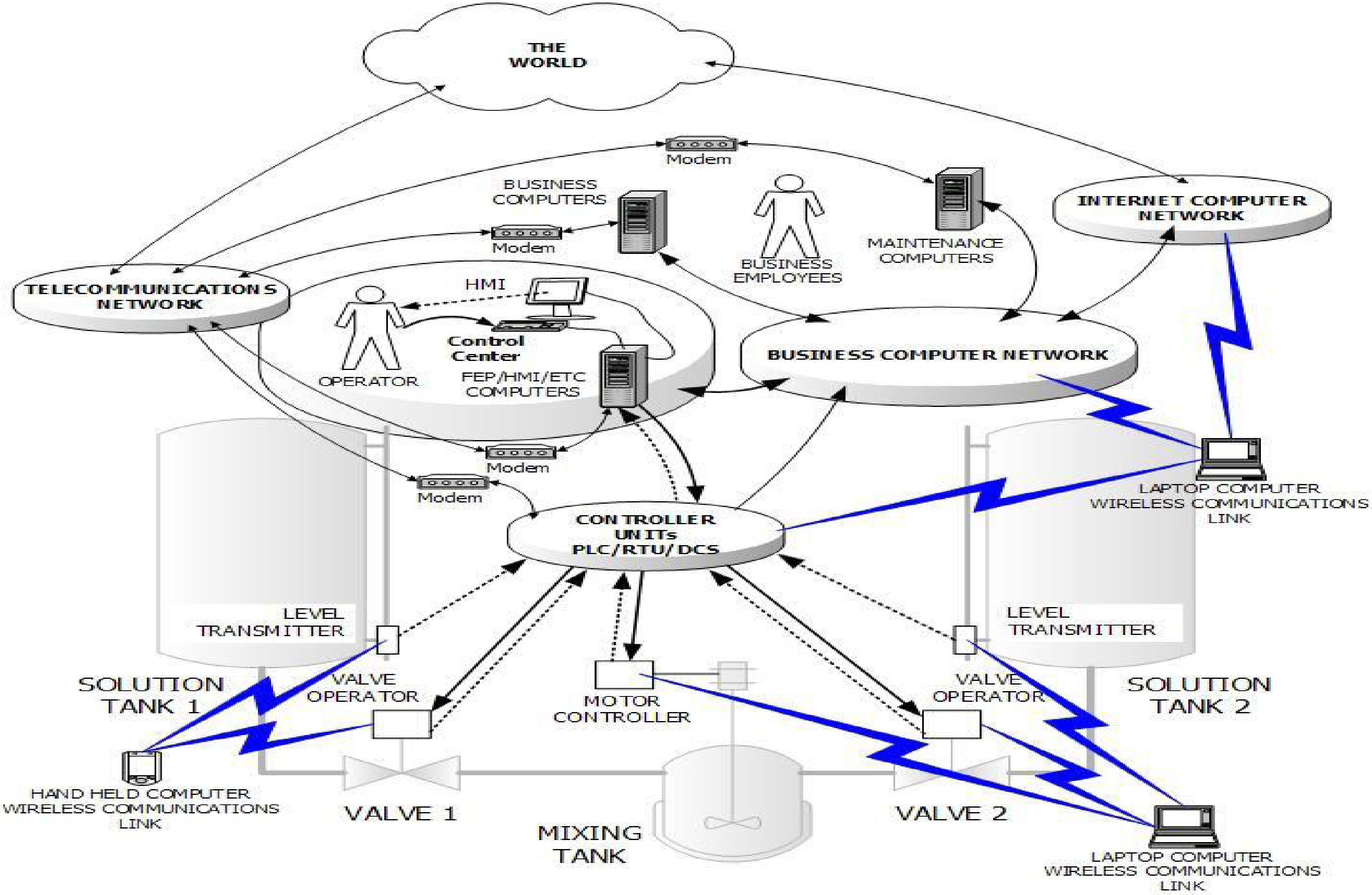
V. Typical Electrical Substations Layout



V. ICS Threat Landscape


INTERNET FIREWALL
ICS
CORPORATE NETWORK
Anti-virus detection signatures not updated
Critical configurations are not stored or backed up
SUPERVISION NETWORK / SCADA
PRODUCTION NETWORK
Unnecessary services are not disabled in the OS and could be exploited
Inadequate physical protection for critical systems
REMOTE TERMINAL UNIT
Firewalls nonexistent or incorrectly configured
SUPERVISION CONSOLE 1
SUPERVISION CONSOLE 1
MAINTENANCE LAPTOP
PLC
CORPORATE I.T.
WAN
GROUP WAN
ERP SERVER
PRODUCTION MANAGEMENT
Weak network security architecture
DATA HISTORIAN / SCADA SERVER
Intrusion detection/ prevention software not installed
WIRELESS INDUTRIAL NETWORK
Inadequate authentication between clients and access points
WORK STATION
PLC 1
PLC 2
Data unprotected on portable devices
CORPORATE FIREWALL

V. Typical ICS System Cyber Vulnerability Surfaces



V. ICS Strengths and Vulnerabilities

STRENGTHS:

1) **High Degree of Availability**

   Redundant control servers/historians/control center LANs; diverse WAN communication paths; backup control systems

2) **High Degree of Authorization**

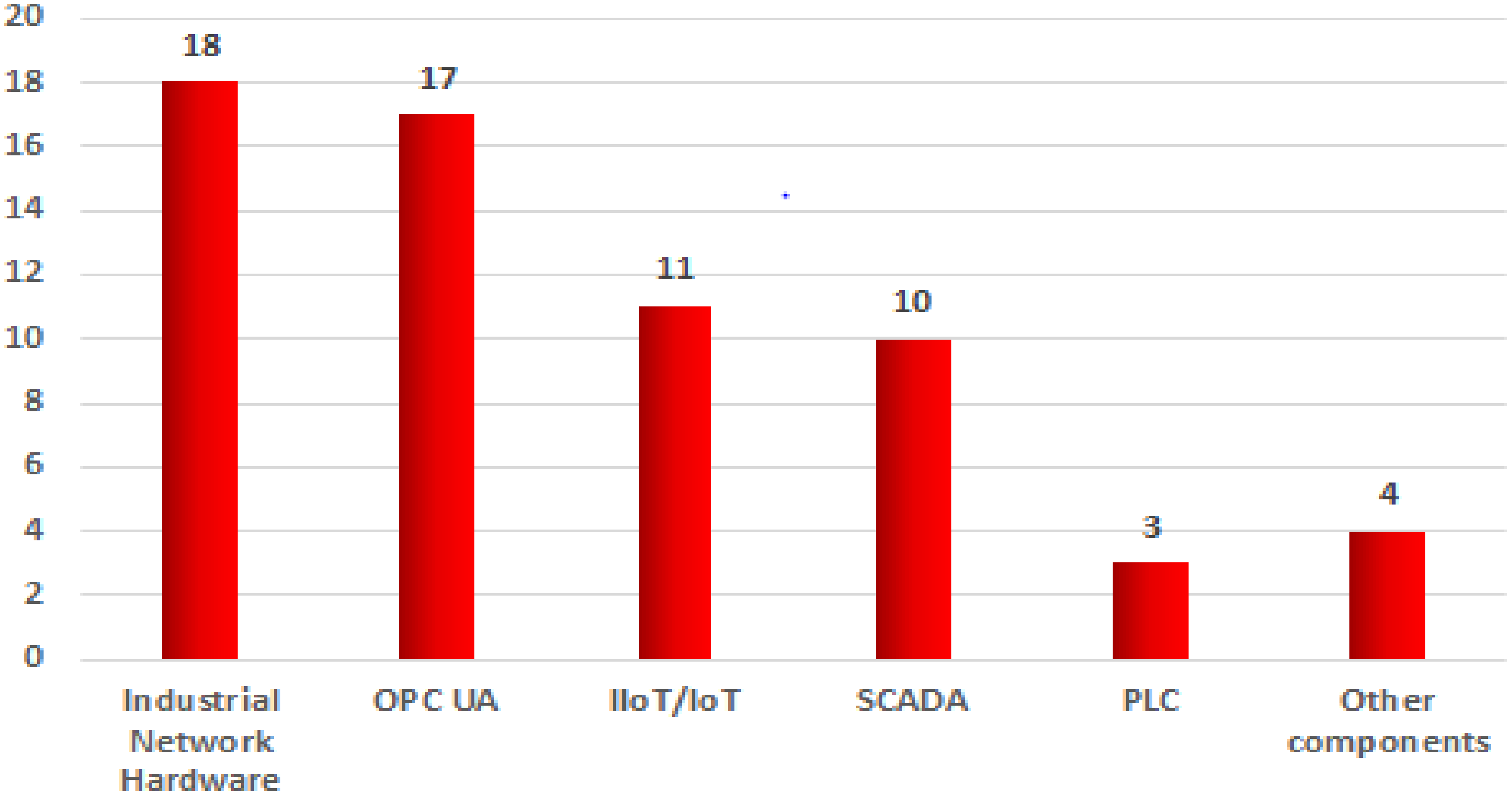
   Commands from/to anywhere, can be automated for emergency, can be issued remotely; high level of command integrity; high level of trust

WEAKNESSES:

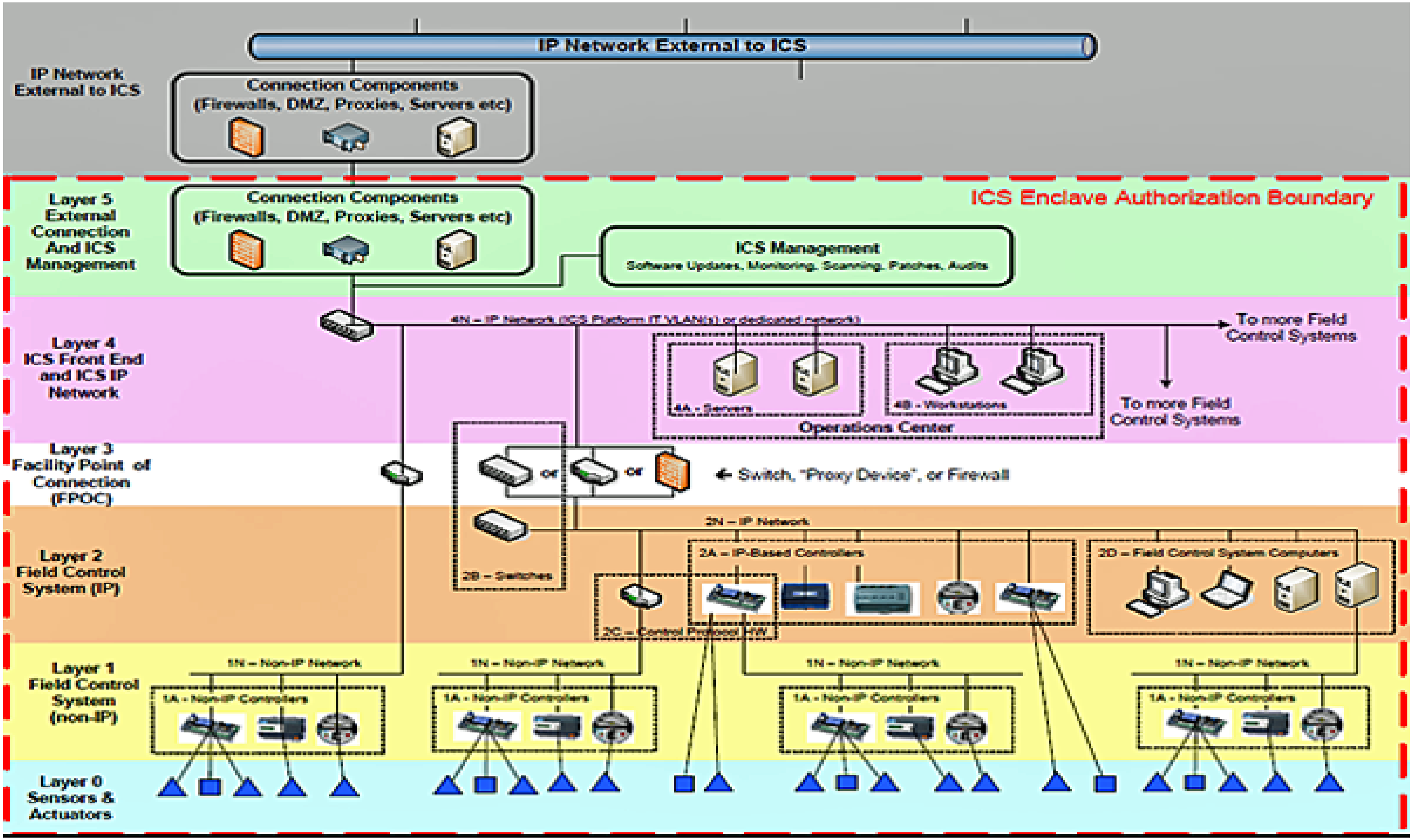
1) **General**: Often many thousands of remote access points, often in legacy and proprietary hardware decade(s) old, with limited access control, open communications protocols, default passwords, limited/no firewalls, non-resilient design architectures, etc

2) **Complex Systems dynamically reconfiguring in space/time**
3) **Reliance on mostly offshore suppliers**
4) **Technical documentation freely available on Internet**
5) **Many control systems based on old MS Windows and UNIX based OS's**
6) **Almost NON-EXISTENT trained OT Systems cyber security work force**

V. ICS Vulnerability Surfaces by ICS Subsystem Category



V. NIST Recommended ICS System Layers 0-5


IP Network External to ICS
IP Network External to ICS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Layer 5 External Connection And ICS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
ICS Enclave Authorization Boundary
ICS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Layer 4 ICS Front End and ICS IP Network
4N – IP Network (ICS Platform IT VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Layer 3 Facility Point of Connection (FPOC)
or
or
Switch, "Proxy Device", or Firewall
Layer 2 Field Control System (IP)
2N – IP Network
2B – Switches
2A – IP-Based Controllers
2C – Control Protocol HW
2D – Field Control System Computers
Layer 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
Layer 0 Sensors & Actuators

VI. Formation of a New Arizona “AI Entrepreneurship Cluster”

Critical Infrastructure Investments, Inc (CII) is a Tucson headquartered technology investment firm interesting in structuring companies and projects that will utilize appropriate Artificial Intelligence/Machine Learning approaches to address existential challenges to optimized Critical Infrastructure operations. CII is a founding sponsor of the **Arizona AI Entrepreneurship Cluster (AAEC).**

AAEC will focus Software Composable AI Instantiations in Space/Air/Ground/Under-Ground/Water Sensor Hardware/Software/Firmware and Signal Processing/Predictive Analytics. for near term use in:

A) Optimizing Energy, Food, Water Nexus
B) Optimizing Green Minerals Exploration and Processing
C) Optimizing Cyber Resilience and Reliability/Availability/Safety of critical Value Chain elements in any Critical Infrastructure sectors

PLANNED AI CLUSTER ADMINISTRATION:

A) Technology Advisory Board: Build Technology and IP Roadmaps to guide Cluster resources focus. Membership is open to all Affiliated Members.
B) Business Capture Management Team: i) Lead/Participate in the Proposal process leading to capture substantive Contracts/Grants for/with Cluster Member; ii) Act as voice of the Cluster in the local and (inter)national community. Membership is open to all Affiliated Members.

NOTIONAL AI CLUSTER AFFILIATION FEE (per Calendar Year)

Private Sector Firm: Revenue <$1M: $ 500; $1-5M: $ 750; $ 5-10M: $ 1,000; >$ 10M: $ 2,500
University Department/Center: $ 1,000; Government Agency/NGO Ally: $ 1,000
Technical/Professional Services Provider: $ 500

BACKUP

IV. Industrial Control System (ICS) Major Types

Industrial Control System (ICS) is any system that controls physical processes (such as energy generation, transmission, and distribution; petroleum refining and processing; chemical processing; oil and gas pipeline operations), and falls into one of 4 broad categories:

i) Supervisory Control and Data Acquisition (SCADA)
ii) Distributed Control (DCS) including Programmable Logic Controllers (PLC) and Field Programmable Gate Arrays/Embedded Electronics (FPGA))
iii) Manufacturing Execution Systems (MES)

SCADA is a system that collects data from various collection devices that monitor and/or control any process and consolidates this data at one/more central servers for visualization and actionable control.

DCS is a system to control continuous or batch-oriented processes consisting of functionally and/or geographically distributed controllers (often microprocessor based) and input/outputs interconnected via non-IT networks for communications and analog/digital monitoring and high speed motion control.

MES is a computerized system used in manufacturing, to track and document the transformation of raw materials to finished goods.

Typical ICS Subsystems

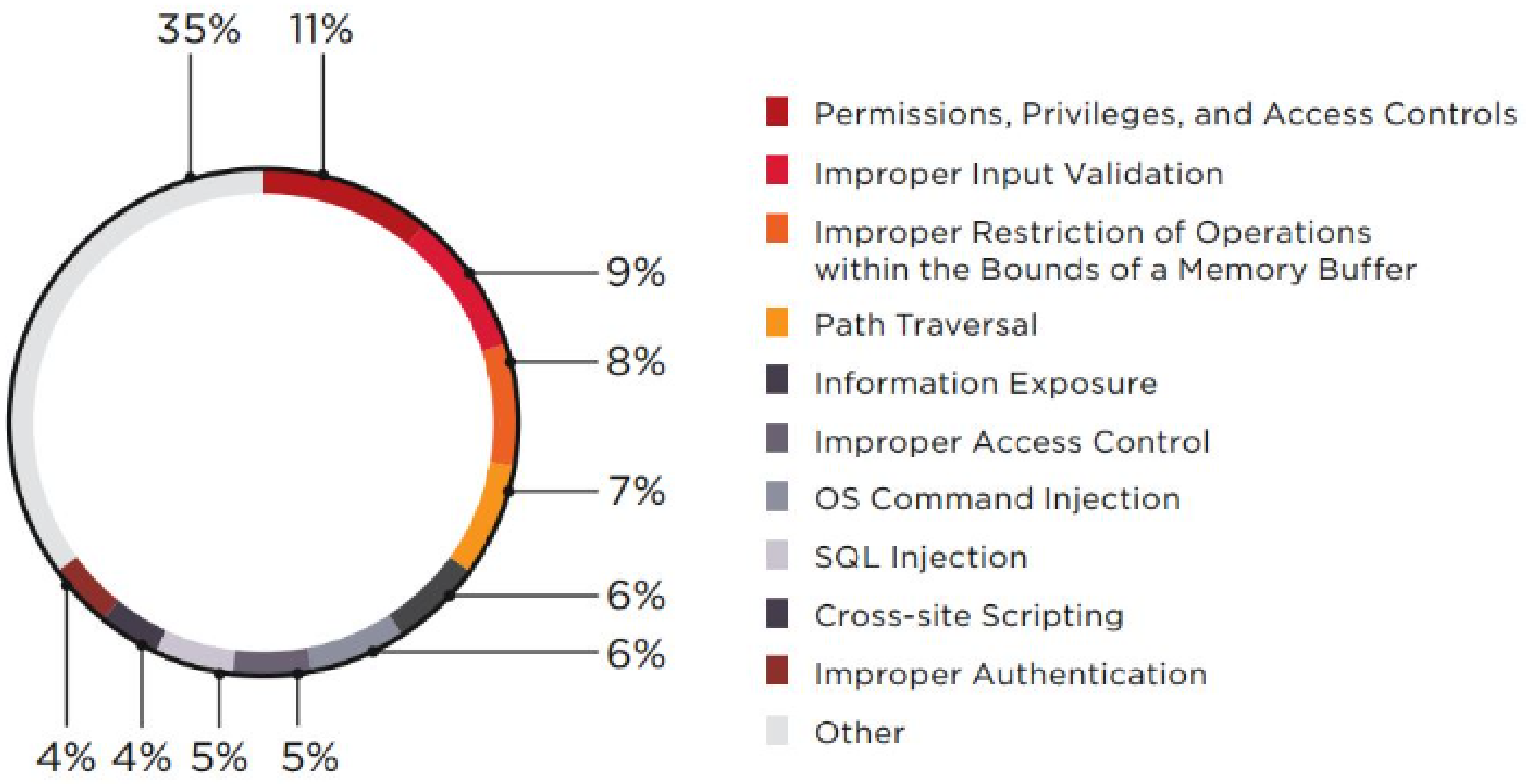
1) **Servers:**
   - Control Server
   - Input/Output Server
   - SCADA Server or Master terminal Unit (MTU)
   - Data Historian

2) **Controllers (RTU, PLC, etc)**
   - Power Supply
   - Communications Module
   - Control Processor
   - Sensors and other Input Modules
   - Actuators and other Output Modules

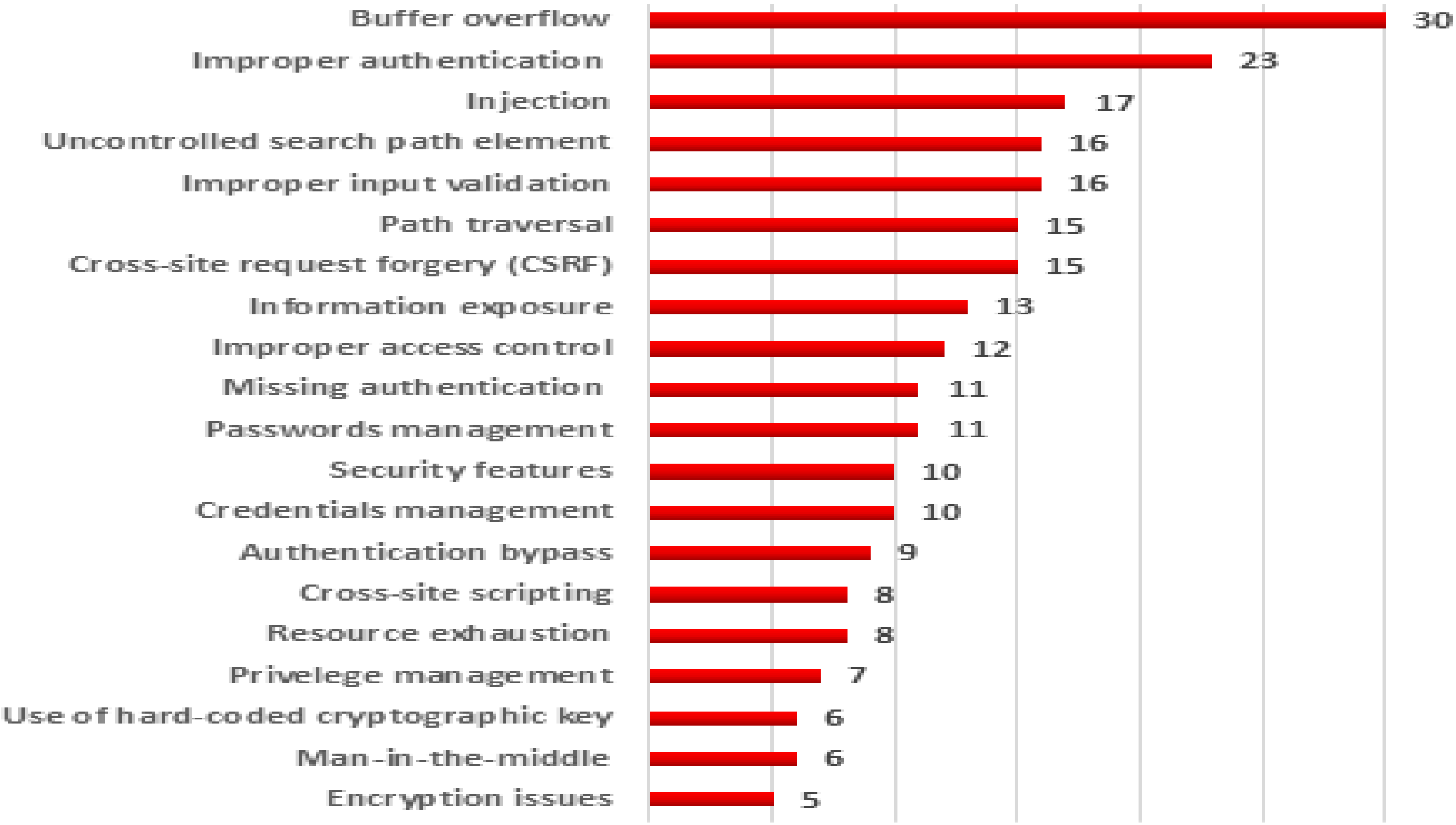
3) **Human Machine Interfaces**

4) **Safety Instrumentation System (**in parallel to and separate from the normal process control system)

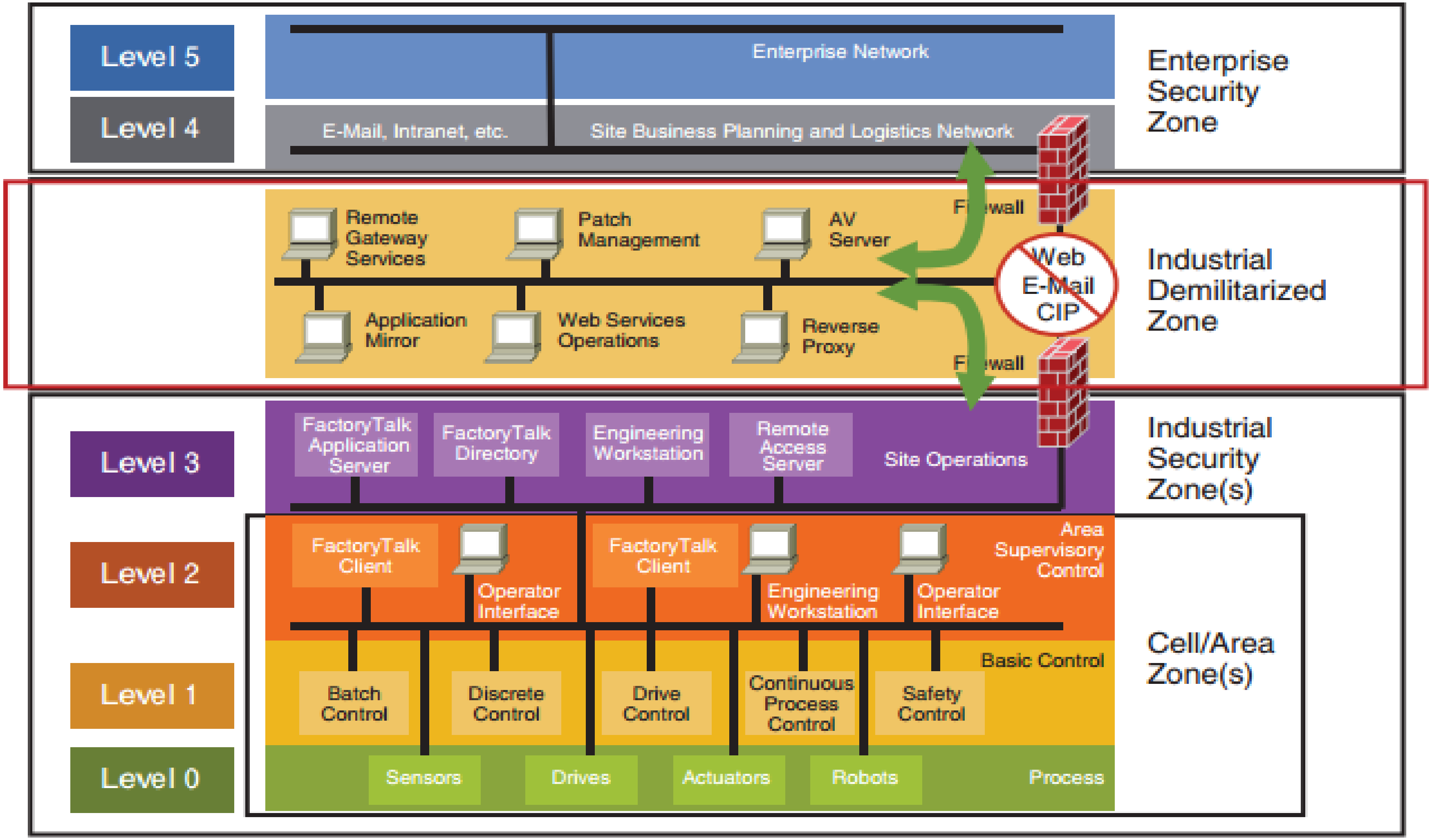
ICS Vulnerabilities by Attack Mechanism



ICS Vulnerability by Attack Mechanism II



Information Technology vs Operational Technology Segregation



NIST ICS Security Governance Documents

1) NIST Special Publication 800-82 Rev 2 “Guide to Industrial Control System Security (247 pages)

Also: 2) NIST Special Publication 800-53 rev 4 “Security and Privacy Controls for Federal Information Systems and Organizations” (462 pages)
3) NIST Special Publication 800-160 “System Security Engineering- Multidisciplinary Approach to Engineering Trustworthy Secure Systems”
4) NIST Framework for Improving Critical Infrastructure Cybersecurity
5) NIST 800-37: Risk Management Framework for Information Systems and Organizations: Systems Life Cycle Approach”

SP 800-82 Major Topics:
Ch 2: Overview of ICS Systems
Ch 3: ICS Risk Management and Assessment
Ch 4: ICS Security Program Development & Deployment
Ch 5: ICS Security Architecture
Ch 6: Applying Security Controls to ICS

NIST SP 800-82 Chapter 5 Security Architecture

5.1 Network Segmentation and Segregation

5.2 Boundary Protection

5.3 Firewalls

5.4 Logically Separated Control Network

5.5 Network Segregation Elements:

1. **Dual-Homed Computer/Dual Network Interface Cards**
2. **Firewall between Corporate and Control Network**
3. **Firewall and Router between Corporate and Control Network**
4. **Firewall with DMZ between Corporate and Control Network**
5. **Paired Firewalls between Corporate and Control Network**

5.6 Recommended Defense-in-Depth Architecture

5.7 General Firewall Policies

5.8 Recommended Firewall Rules for Specific Services:

1. **Domain Name Systems (DNS)**
2. **Hypertext Transfer Protocol (HTTP)**
3. **FTP and Trivial File Transfer Protocol (TFTP)**
4. **Telnet**
5. **Dynamic Host Configuration Protocol (DHCP**
6. **Secure Shell (SSH)**
7. **Simple Object Access Protocol (SOAP)**
8. **Simple Mail Transfer Protocol (SMTP)**
9. **Simple Network Management Protocol (SNMP)**
10. **Distributed Component Object Model (DCOM)**
11. **SCADA and Industrial Protocols**

NIST SP 800-82 Chapter 5 Security Architecture (continued)

5.9 Network Address Translation (NAT)

5.10 Specific ICS Firewall issues:

- Data Historians
- Remote Support Access
- Multicast Traffic

5.11 Unidirectional Gateways

5.12 Single Points of Failure

5.13 Redundancy and Fault Tolerance

5.14 Preventing Man-in-the-middle Attacks

5.15 Authentication and Authorization Implementation Considerations

5.16 Monitoring, Logging and Auditing

5.17 Incident Detection, Response and System Recovery

NIST 800-82 Chapter 6 Applying Security Controls to Industrial Control Systems

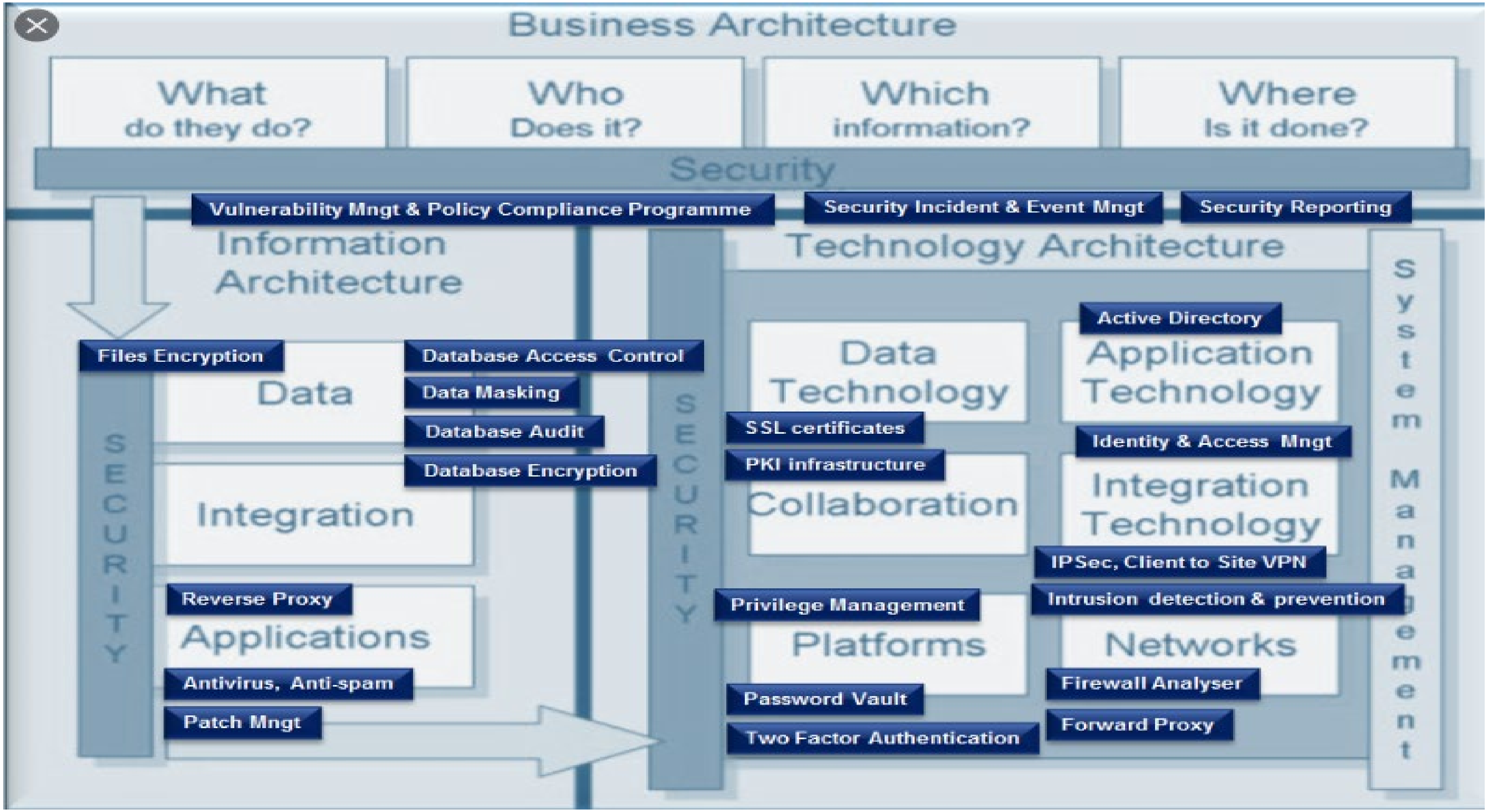
6.1 Executing the Risk Management Framework Tasks for ICS:

Step 1: Categorize Information Systems
Step 2: Select Security Controls
Step 3: Implement Security Controls
Step 4: Assess Security Controls
Step 5: Authorize Information System
Step 6: Monitor Security Controls

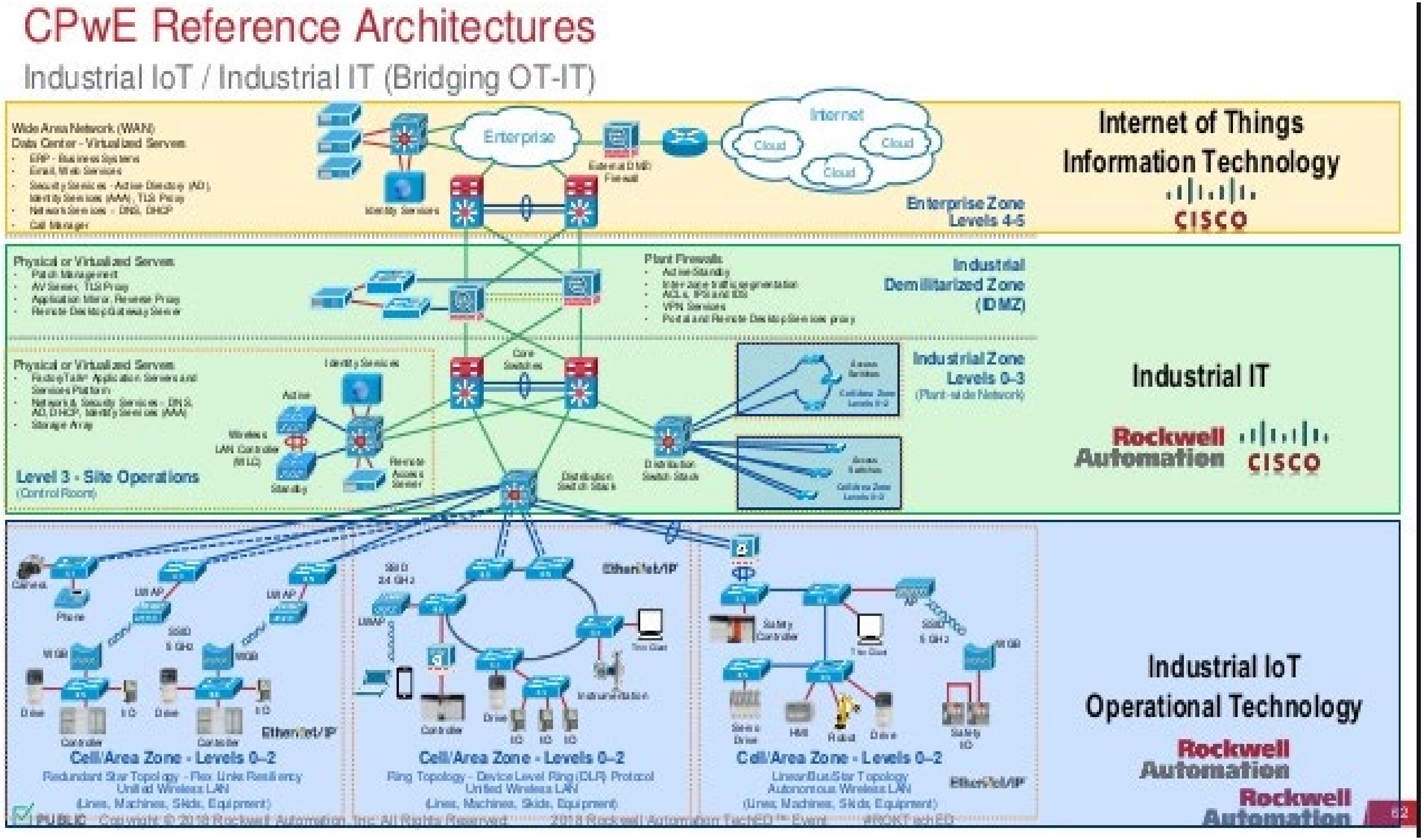
6.2 Guidance on the Application of Security Controls to ICS:

1) Access Control
2) Awareness and Training
3) Audit and Accountability
4) Security Assessment and Authorization
5) Configuration Management
6) Contingency Planning
7) Identification and Authentication
8) Incident Response
9) Maintenance
10) Media Protection
11) Physical & Environmental Protection
12) Planning
13) Personnel Security
14) Risk Assessment
15) System and services Acquisition
16) System and Communications Protection
17) System and Information Integrity
18) Program Management
19) Privacy Controls

NIST Security Architecture



Industrial Internet of Things



CPwE Reference Architectures

Industrial IoT / Industrial IT (Bridging OT-IT)

Wide Area Network (WAN)
Data Center - Virtualized Servers
- ERP - Business Systems
- Email, Web Services
- Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
- Network Services – DNS, DHCP
- Call Manager

Physical or Virtualized Servers
- Patch Management
- AV Server, TLS Proxy
- Application Mirror, Reverse Proxy
- Remote Desktop Gateway Server

Plant Firewalls
- Active/Standby
- Inter-Zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Physical or Virtualized Servers
- FactoryTalk® Application Servers and Services Platform
- Network & Security Services - DNS, AD, DHCP, Identity Services (AAA)
- Storage Array

Level 3 - Site Operations
(Control Room)

Enterprise Zone
Levels 4-5

Industrial
Demilitarized Zone
(IDMZ)

Industrial Zone
Levels 0–3
(Plant-wide Network)

Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)

Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)

Internet of Things
Information Technology
CISCO

Industrial IT
Rockwell Automation CISCO

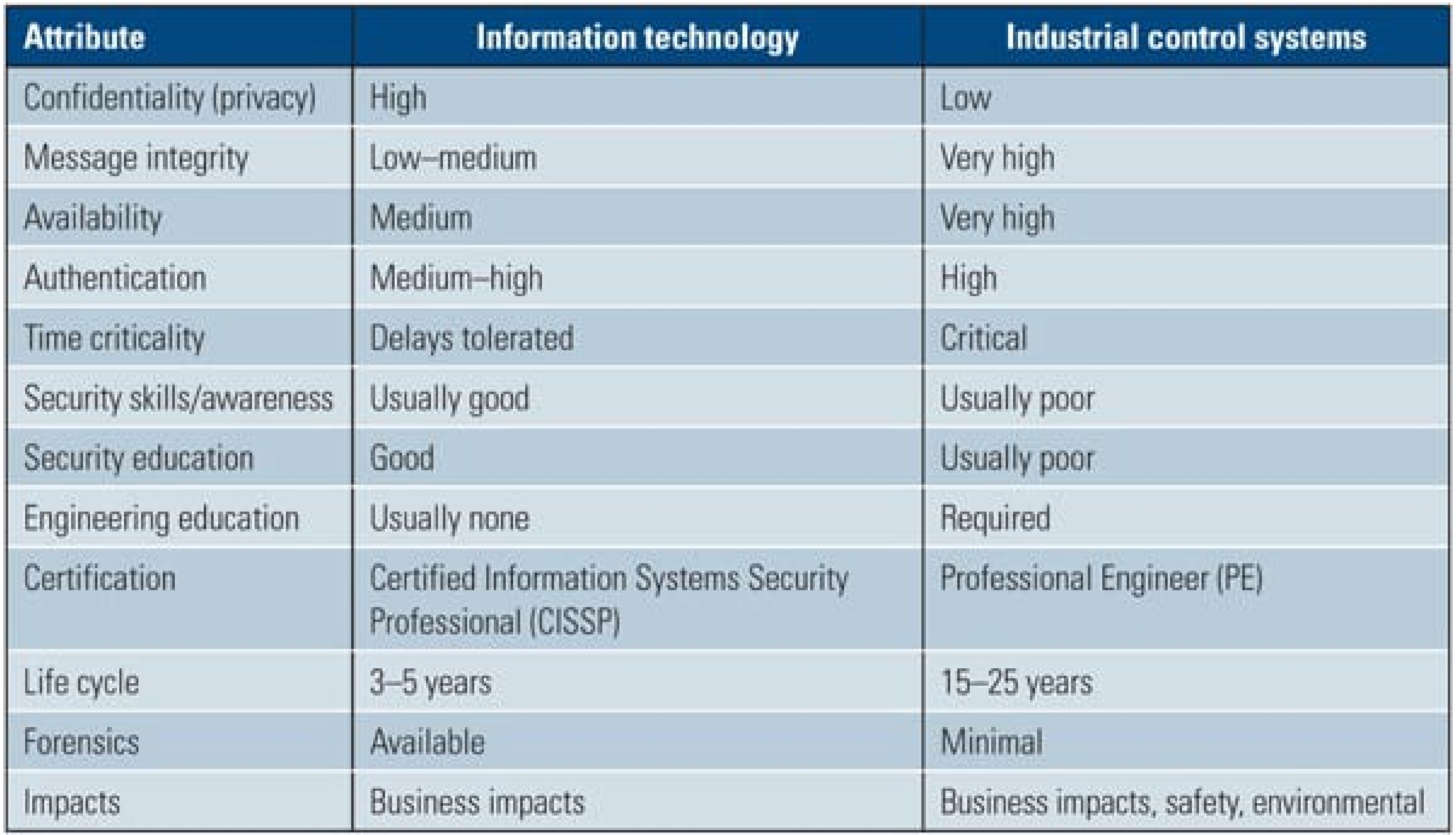
Industrial IoT
Operational Technology
Rockwell Automation

Rockwell Automation

PUBLIC Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved. 2018 Rockwell Automation TechED™ Event #ROKTechED

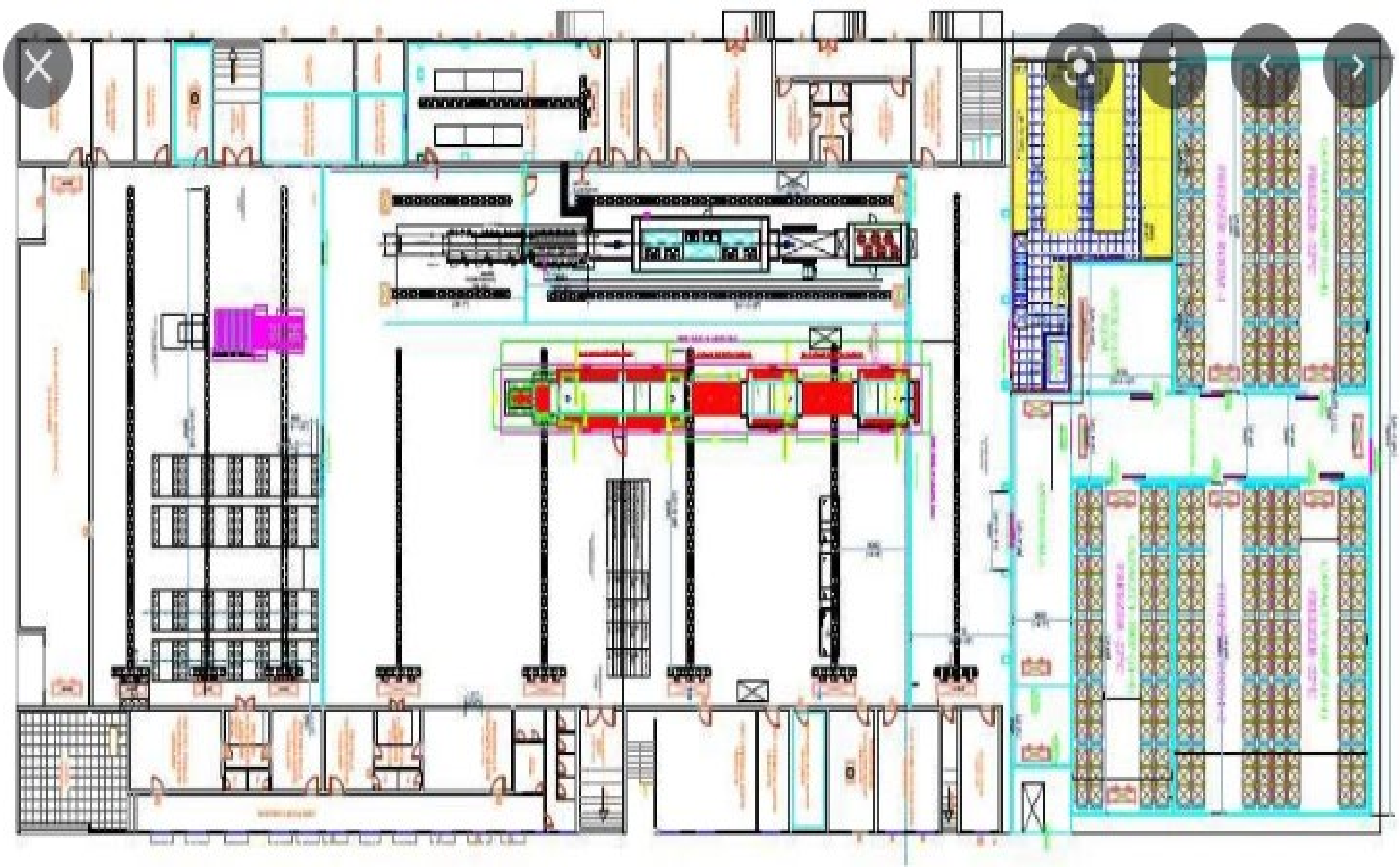
62

IT vs OT/ICS System



Attribute	Information technology	Industrial control systems
Confidentiality (privacy)	High	Low
Message integrity	Low–medium	Very high
Availability	Medium	Very high
Authentication	Medium–high	High
Time criticality	Delays tolerated	Critical
Security skills/awareness	Usually good	Usually poor
Security education	Good	Usually poor
Engineering education	Usually none	Required
Certification	Certified Information Systems Security Professional (CISSP)	Professional Engineer (PE)
Life cycle	3–5 years	15–25 years
Forensics	Available	Minimal
Impacts	Business impacts	Business impacts, safety, environmental

IV. Sector 7 of 16: Food and Agriculture



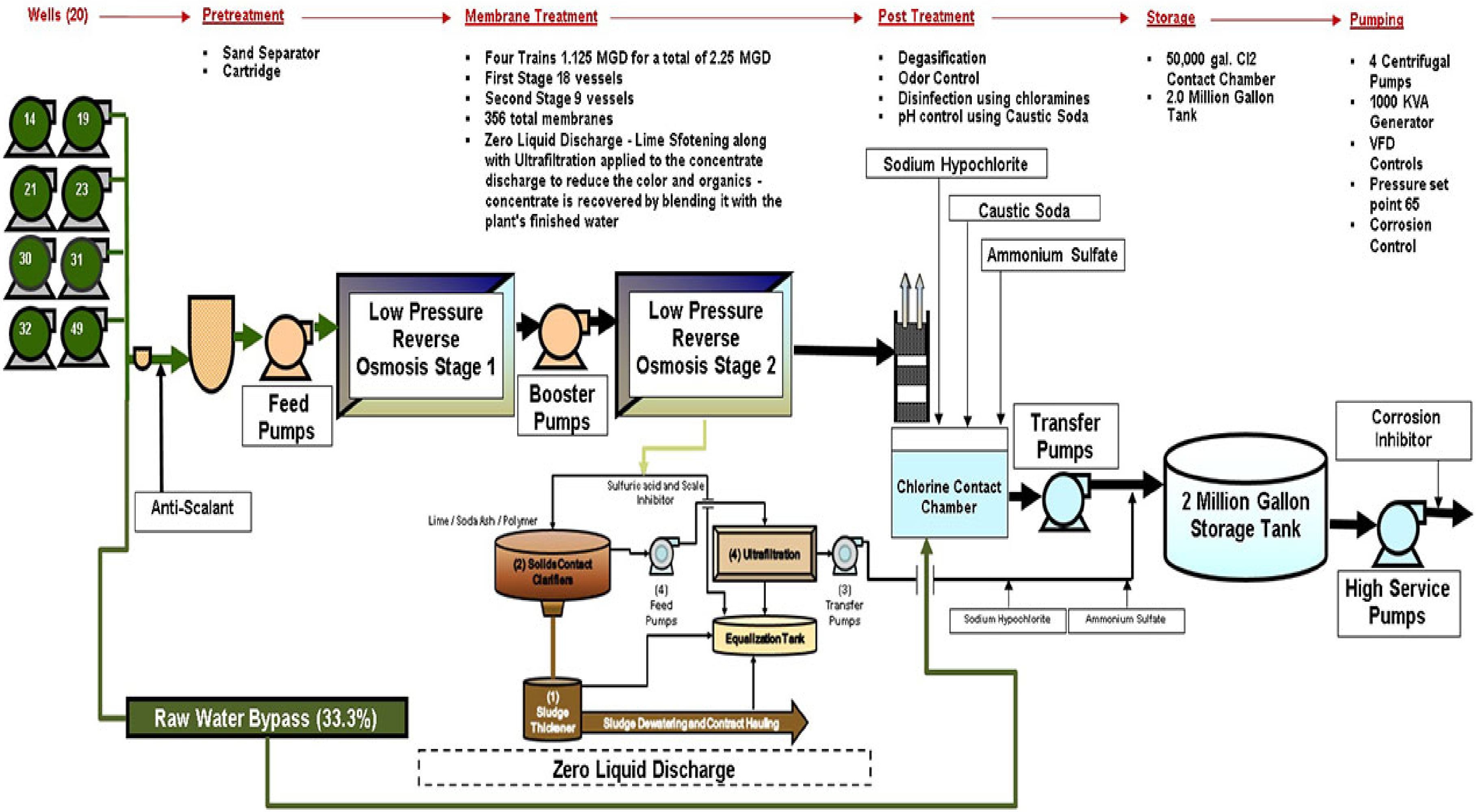
IV. Sector 7 of 16: Food and Agriculture: Top 4 “Advanced” Research Applications by $ Allocated

1. Processing Plant Food Safety Validation at Cellular Level
2. Drone-based Crop/Soil/Livestock Health Monitoring and Autonomic Response
3. Automated Spraying and Weeding
4. Predicative Analytics on Crop Yield vs Weather

Sector Impact: 5% of US GDP or $ 1.1 Trillion/Year

IV. Sector 8 of 16: Water and Wastewater Utilities

City of Palm Coast Water Treatment Plant #2



Wells (20) → Pretreatment → Membrane Treatment → Post Treatment → Storage → Pumping

Pretreatment

- Sand Separator
- Cartridge

Membrane Treatment

- Four Trains 1.125 MGD for a total of 2.25 MGD
- First Stage 18 vessels
- Second Stage 9 vessels
- 356 total membranes
- Zero Liquid Discharge - Lime Sfotening along with Ultrafiltration applied to the concentrate discharge to reduce the color and organics - concentrate is recovered by blending it with the plant's finished water

Post Treatment

- Degasification
- Odor Control
- Disinfection using chloramines
- pH control using Caustic Soda

Storage

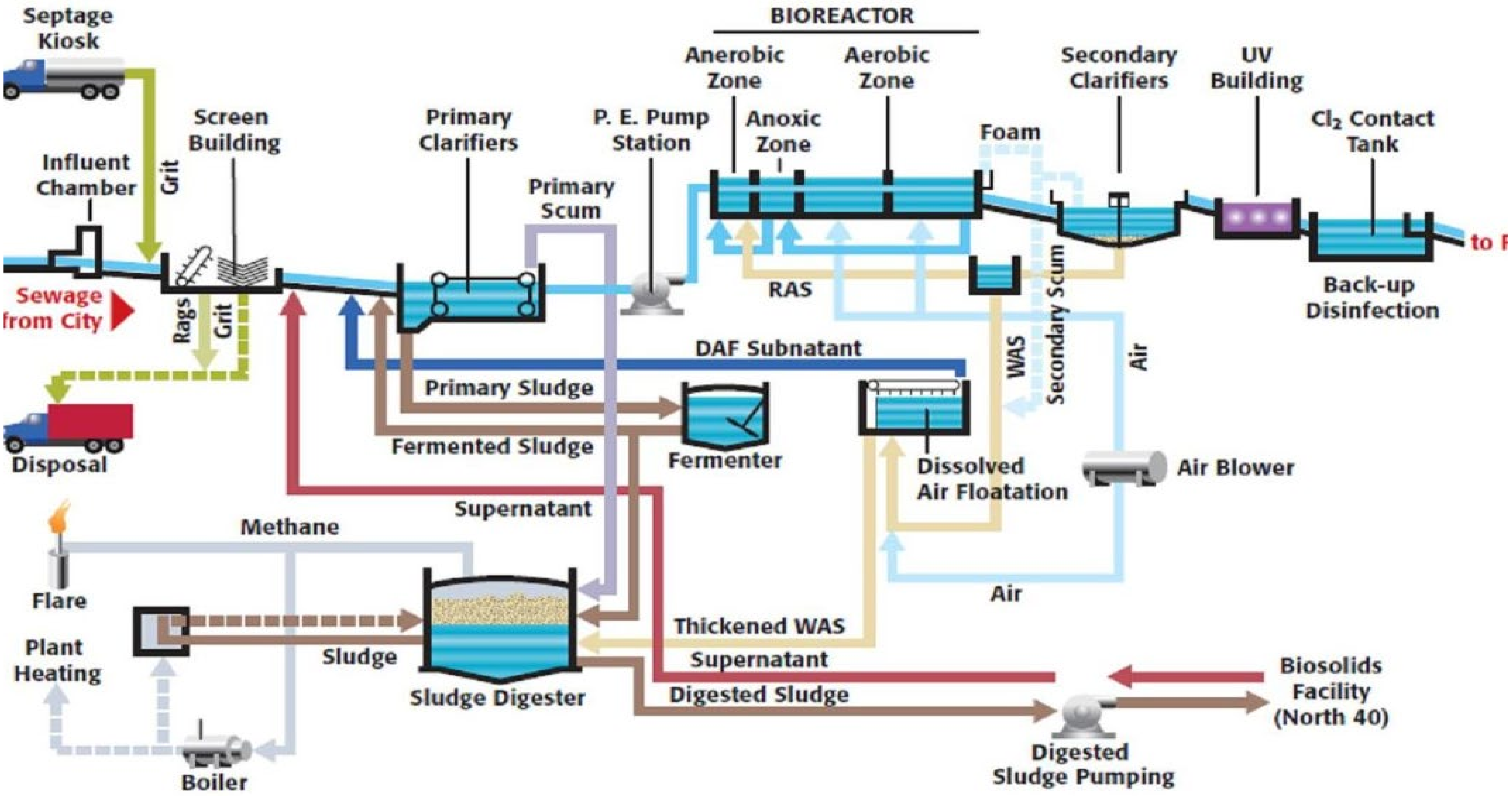
- 50,000 gal. Cl2 Contact Chamber
- 2.0 Million Gallon Tank

Pumping

- 4 Centrifugal Pumps
- 1000 KVA Generator
- VFD Controls
- Pressure set point 65
- Corrosion Control

IV. Sector 8 of 16: Water and Wastewater Facilities

Biological Nutrient Removal



IV. Sector 8 of 16: Water and Wastewater: Top 4 “Advanced” AI Research Applications per $ Allocated

1. Smart Water Grid: Preventive Remote Equipment/Pipe Fault Monitoring and Remediation

2. Early Warning of Outages and Disaster Recovery Optimized Restart of Services Throughout Distribution System

3. Optimize SCADA Data to Optimize Energy Use Throughout the Water Infrastructure

4. Workforce Institutional Knowledge Base Maintenance

Sector Impact: 16& of US GDP / $ 3.7 Trillion/Year

IV. Sector 9 of 16: Emergency Services

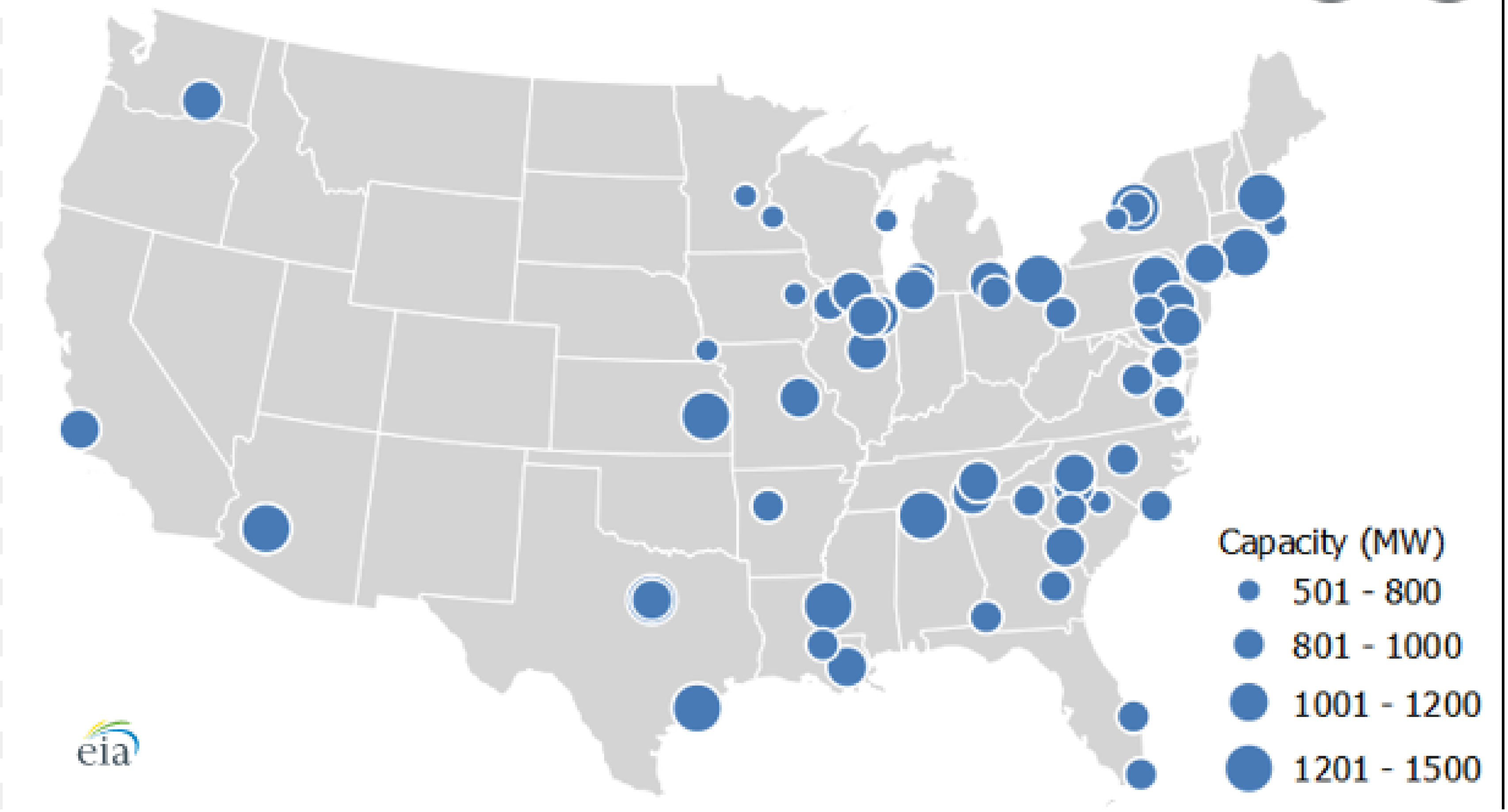
IV. Sector 9 of 16: Emergency Services: Top 4 "Advanced" AI Research Application by $ Allocated

1. Prioritized Response to Climate Change Events (Flood, Fire, Hurricane, Drought, etc) Based on Human Life and Economic Impact Severity
2. Automated Integration of National/State/Local Emergency Services Providers
3. AI-Autonomous 24/7 Dispatch Systems and Robots
4. Prediction Models of People Flows in Various Emergencies

Sector Impact: EMS Services Budgets: $ 80 Billion/Year
Natural Disaster Impacts: $ 306 Billion/Year
56% of Americans cannot cover a $1,000 urgency

Sector 10 of 16: Nuclear Facilities

U.S. installed nuclear capacity by reactor
megawatts (MW)



Sector 10 of 16: Nuclear Facilities: Top 4 “Advanced” AI Research Application per $ Allocated

1. Digital Twin for Advanced Modeling and Simulation
2. Nuclear Safety Analysis and Accident Management
3. Intelligent Prognostics and Health Management of Plant Equipment
4. Reactor Automatic Control and Autonomous Operation

Sector Impact: 19% of US Power Generation (843 Billion/KwH/year)

Sectors 11-12 of 16: Major Government and Commercial Facilities

Sectors 11-12 of 16: Major Facilities: Top 4 “Advanced” AI Research Applications per $ Allocated

1. Optimization of Space Development and Utilization Planning

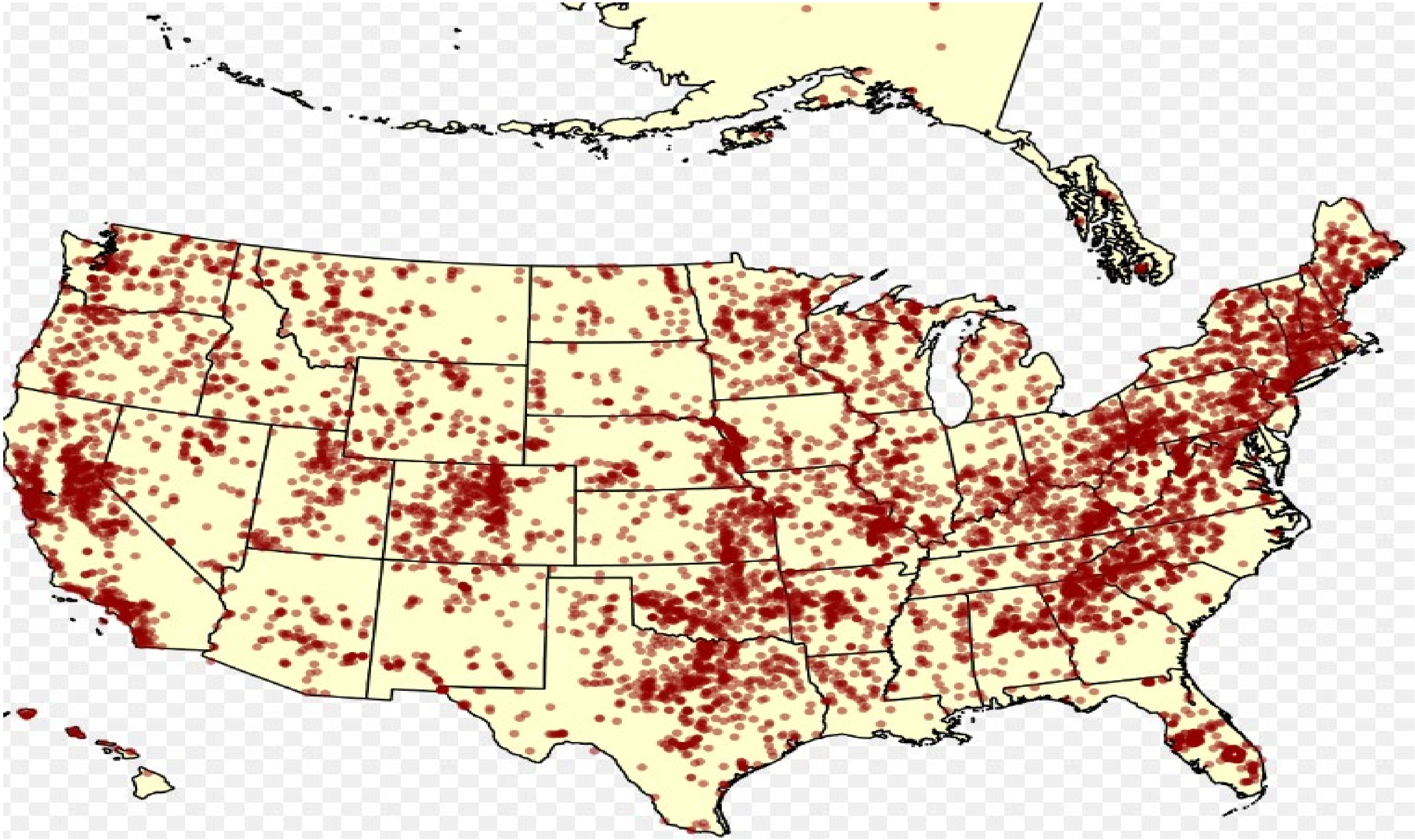
2. Terrorist Attack Scenario Planning

3. Predictive Analytics for Equipment and Utilities Usage Minimization

4. Optimization of Human Relations/Facilities Management/Information Technology

Sectors Impact: Facilities Management: $ 1.5 Trillion/Year

IV. Sector 13 of 16: Dams



Sector 13 of 16: Dams: Top 4 “Advanced” AI Research Applications per $ Allocated

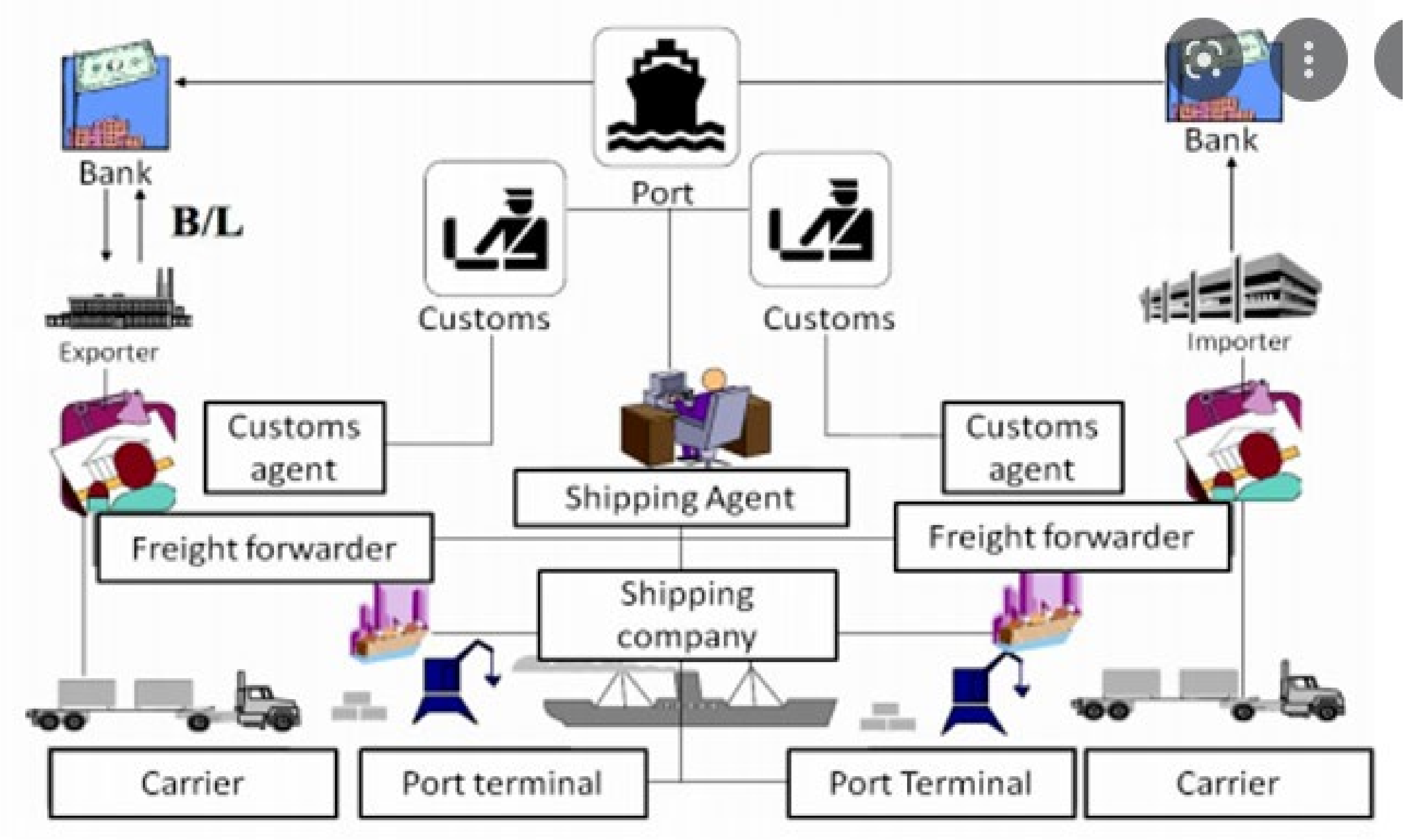
1. Remote Autonomous Monitoring for Man-made and/or Natural Negative Dam Integrity Incidents

2. Optimizing Dam Safety Protocols and Preventive Maintenance

3. Digital Twin Modeling and Simulation for Optimized Water/Energy Demand

4. Personnel and Downstream Population Safety and Evacuation Scenario Planning

Sector 14 of 16: Shipping



Sector 14 of 16: Shipping: Top 4 “Advanced AI Research Applications per $ Allocated

1) Terrorist Attack Scenario Planning and Adaptive Route Rescheduling

2) Autonomous Ships and Port Operations

3) Organizing Containers Positioning. On-Ship and In-Port for Schedule Agility and Optimizing Fuel Consumption and Emissions Reduction

4) Route Optimization Forecasting

Sector Impact: 11 Billion Tons/Year

Sector 15 of 16: National Monuments

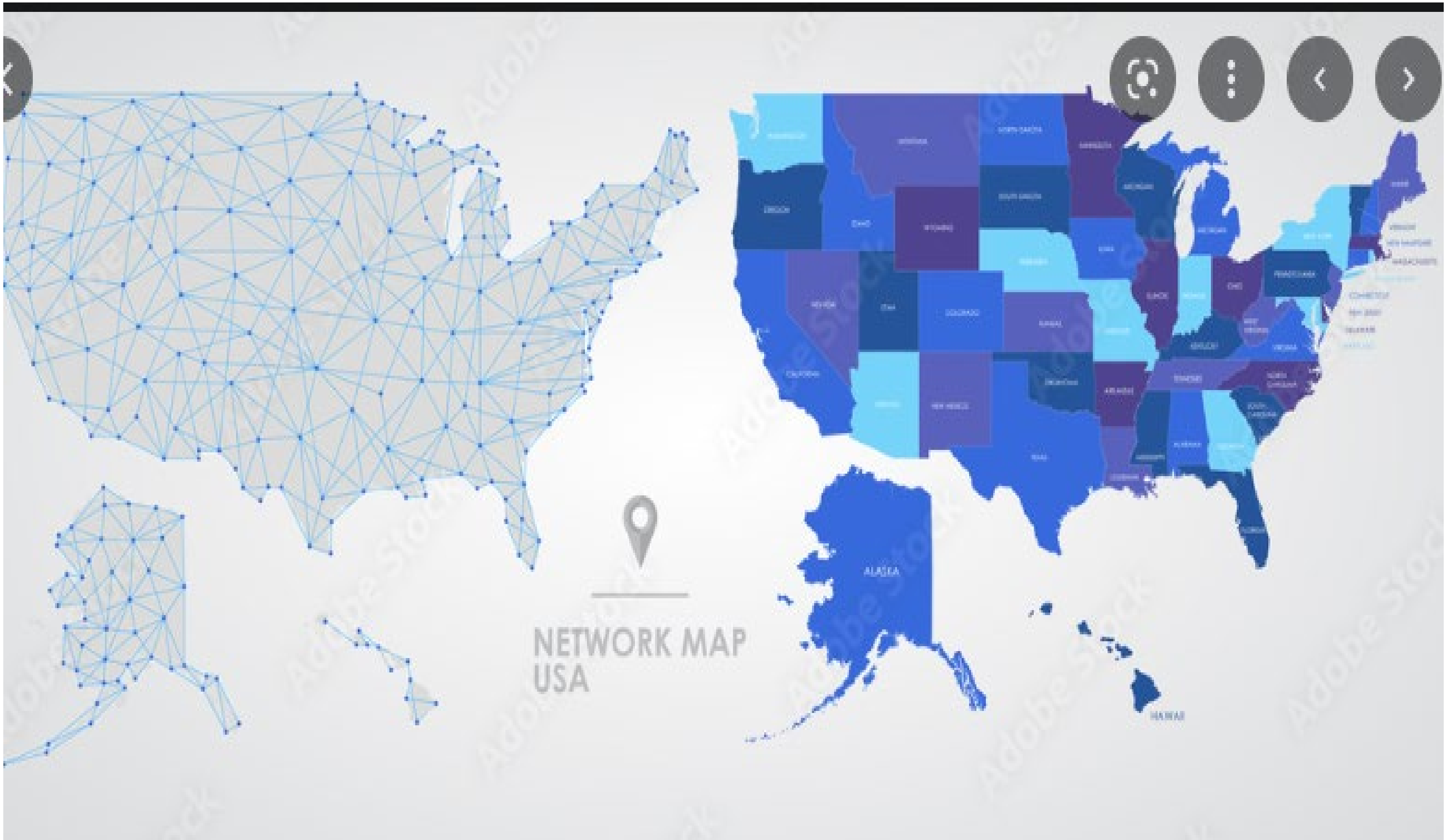
Sector 15 of 16: National Monuments: Top 4 “Advanced” AI Research Applications by $ Allocated

1) Digital Twin to Preserve Cultural Heritage and Culturally Sensitive Deep Education/Learning

2) Large Scale Historical Simulator based on Digitized Museum/etc Archives and Using Semi-Automatic Scanners, Robotic Page-Turners, Automatic Handwriting Recognition Systems

3) Satellite/Drone-Based Architectural Heritage Preservation

Sector 16 of 16: Telecommunications/Information Technology



Sector 16 of 16: Telecommunications/Information Technology: Top 4 “Advanced” AI Research Applications per $ Allocated

1) Digital Twin for Network Optimization per Quantity/Quality of Network Traffic

2) Terrorist Attack Scenario Planning

3) Robotic Process Optimization (Billing/Data Entry/Workforce Management/Order Fulfillment/Identity Authentication etc)

4) Fraud Prevention

Sector Impact: $ 1.5 Trillion/Year, growing at 30%/Year