# U.S NUCLEAR REGULATORY COMMISSION (NRC) CYBER SECURITY OVERSIGHT PROGRAM OVERVIEW FOR THE POLISH REGULATORS

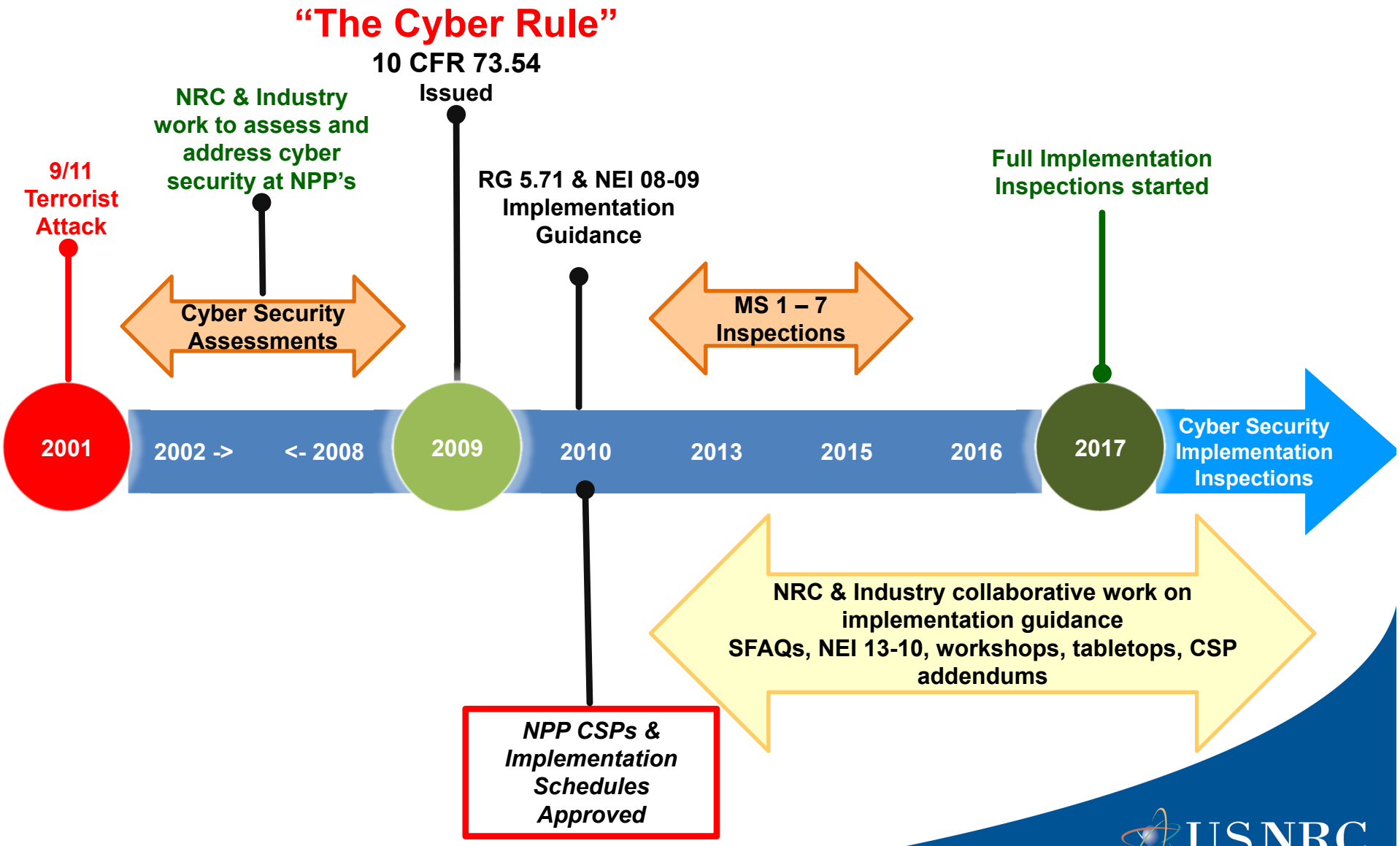
**Michael Brown, CISSP**
Michael.brown@nrc.gov
**Cyber Security Branch (CSB)**
**Division of Physical and Cyber Security Policy (DPCP)**
**Office of Nuclear Security and Incident Response (NSIR)**

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# AGENDA

- Brief History of Cyber Security at the NRC
- 10 CFR 73.54 – Cyber Rule and Guidance
- Cyber Security Full Implementation Inspections
- Cyber for the AP1000

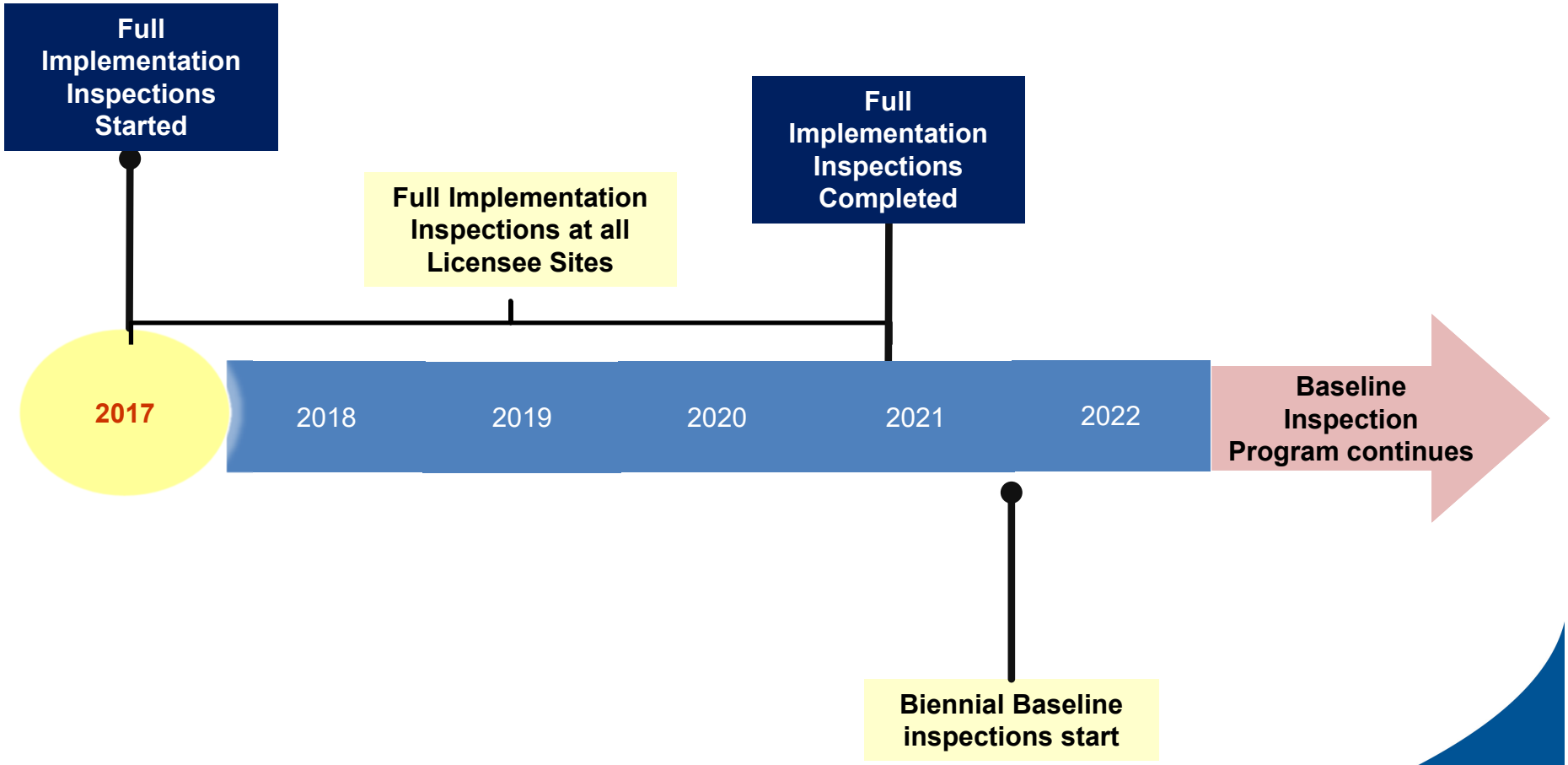
# Cyber Security Program History




U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

SM1
BM3

# Future of US NRC Cyber Security Program




U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

## Slide 4

**SM1** missing the slide number on slide 4
Sampson, Michele, 4/18/2022

**BM3** Added slide number
Brown, Michael, 4/20/2022

# 10 CFR 73.54 Protection of Digital Computer & Communication Systems and Networks

*High assurance that digital computer and communication systems and networks <u>are adequately protected against cyber attacks</u>*

Cyber Security Program Implementation Requirements at NewRx and OpRx

**Focus: <u>Prevention of Radiological Sabotage</u>**

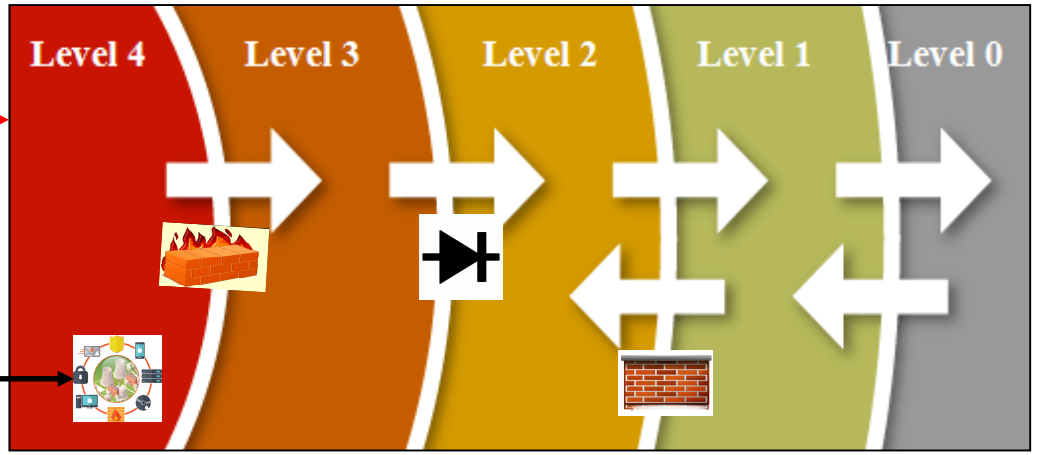
U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# 10 CFR 73.54

- **Op Rx and license applicants must have a Cyber Security Plan**
  - Protect digital computer and communication systems and networks associated with
    - Safety, Security & Emergency Preparedness (SSEP) functions
    - Support systems and equipment which, if compromised, would adversely impact SSEP functions
  - Protect from cyber attacks that adversely impact
    - Integrity or confidentiality of data and/or software
    - Deny access to systems, services, and/or data
    - Operation of systems, networks, & associated equipment

# Implementation Guidance

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls to CDAs

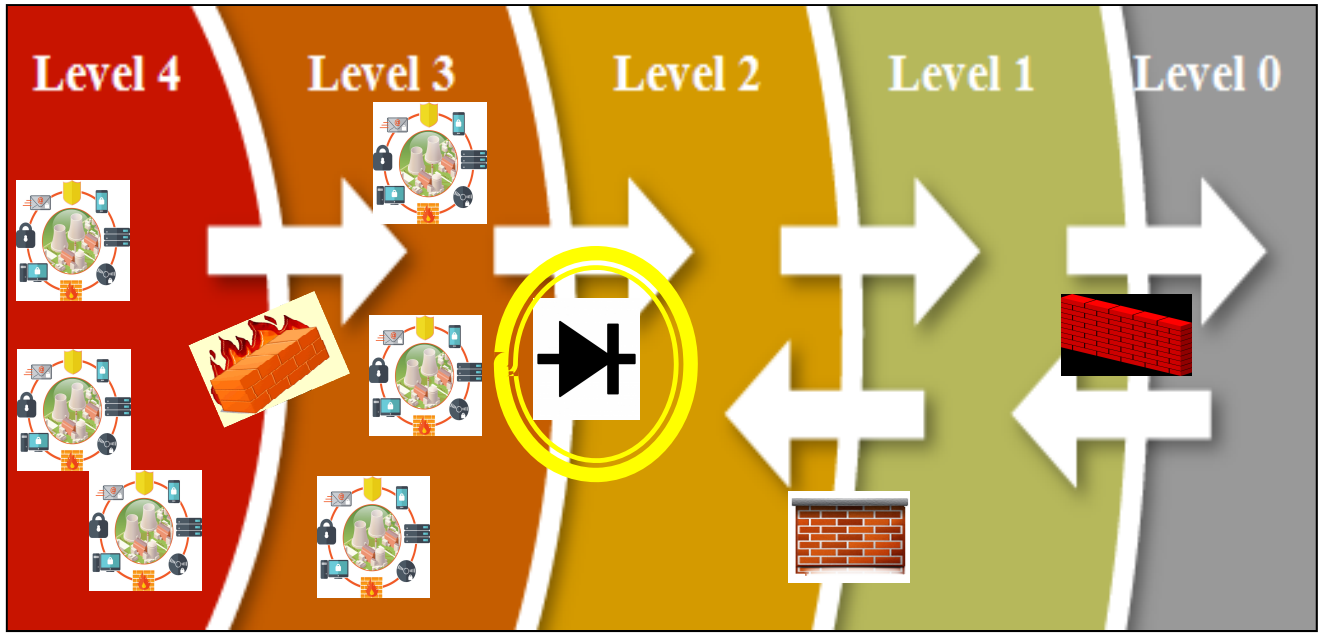



5. Cyber Security Program Must Include These Areas to Support Implementation

CYBER SECURITY PROGRAM

- Defense-in-Depth
- Security Controls NEI 13-10
- Mitigation Strategies
- Training
- Manage Cyber Risk
- Periodic Review
- Modification Evaluation
- Incident Response
- Procedures
- Records Retention

# Generic Defensive Architecture




Security / Safety Systems

Site Network

Corporate Network

Internet

One-way Deterministic Device

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# IAEA Guidance Documents

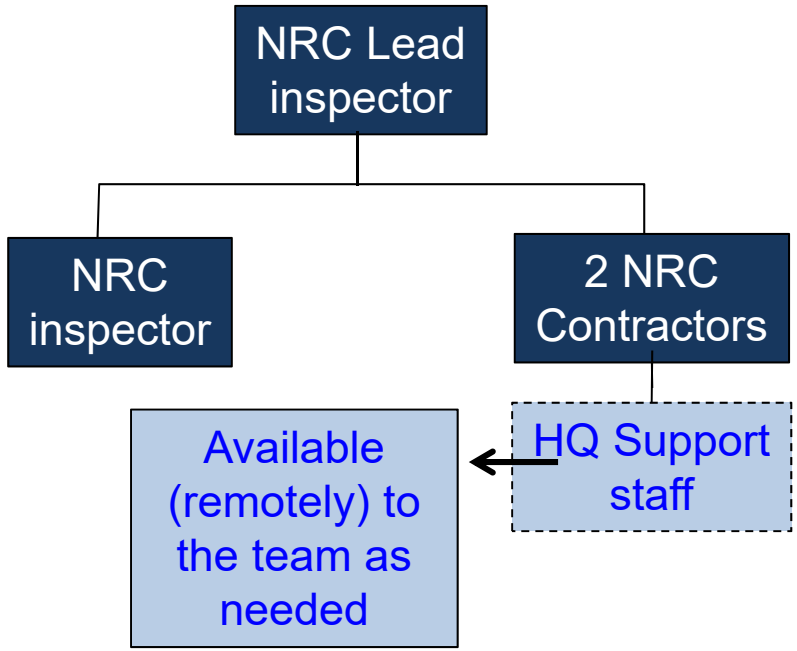
- **US nuclear plants typically use either NEI 08-09 or RG 5.71 for guidance in developing their cybersecurity programs**
- **Most International plants use IAEA guidance in developing their cybersecurity programs.**
  - IAEA Nuclear Security Series (NSS) No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities
    - Provides guidance on physical protection of facilities and transportation
  - NSS No. 23-G Security of Nuclear Information
    - Provides guidance on securing information
    - Provides different classifications for information (e.g. secret, confidential, etc.)

# IAEA Guidance Documents

- NSS No. 42-G Computer Security for Nuclear Security
  - Provides implementing guidance for computer security
  - Provides recommendations for different security levels
- NSS No. 17-T Rev 1 Computer Security Techniques for Nuclear Facilities
  - Provides technical guidance on how to setup your computer security program and the security requirements for different security levels

# Full Implementation Inspection Resources

- Inspection Procedure  IP 71130.10P
- Team Composition (4 inspectors)
  - Regional Inspector Team Lead
  - Regional Inspector
  - 2 Cyber Security Subject Matter Experts (Contractor SMEs) Inspectors
- The initial round of full implementation inspections were completed in 2021
- These inspections consisted of a week onsite followed by an offsite week, followed by a 2nd week onsite



# Inspection Procedure 71130.10P

| Programmatic | Technical |
|---|---|
| *Cyber security program & training* | *Access control/media and portable device protection:*<br>• *Policies & procedures, CDAs, Networks, Portable Media Devices,*<br>• *Controls login, authentication, wireless* |
| *Attack mitigation, incident response, and contingency planning* | |
| *Program monitoring, assessment, configuration, and change management* | *CDA and communications protection*<br>• Protocols, passwords, shared resources, Denial-of-Service protection, digital certificates, information protection, encryption, removal of unnecessary services, OS |
| *Systems/services acquisition and supply chain protection* | |
| *Review changes to the cyber security plan* | *Defense-in-depth, detection, and response*<br>• Hardware configuration, intrusion detection system, malicious code protection, monitoring tools, information flow enforcement |
| *Cyber security event reporting* | |
| *Identification and resolution of problems* | |

# Cyber Security During Construction

- NEI 08-09 Addendum 3 provides guidance on System and Services Acquisition (Supply Chain) and discusses some of the following:
  - Maintaining custody and control of device from vendor to installation
    - Many components at Vogtle were shipped without software installed and software was installed during system turnover
    - Requirements for tamper proof products or tamper seal on acquired products
  - Establishment of trusted distribution paths to ensure traceability
  - Integration of security capabilities
    - The best time to add security features is during the design and construction of a product, not as an add on after construction
  - Licensee testing
    - Licensee should always test products prior to installation

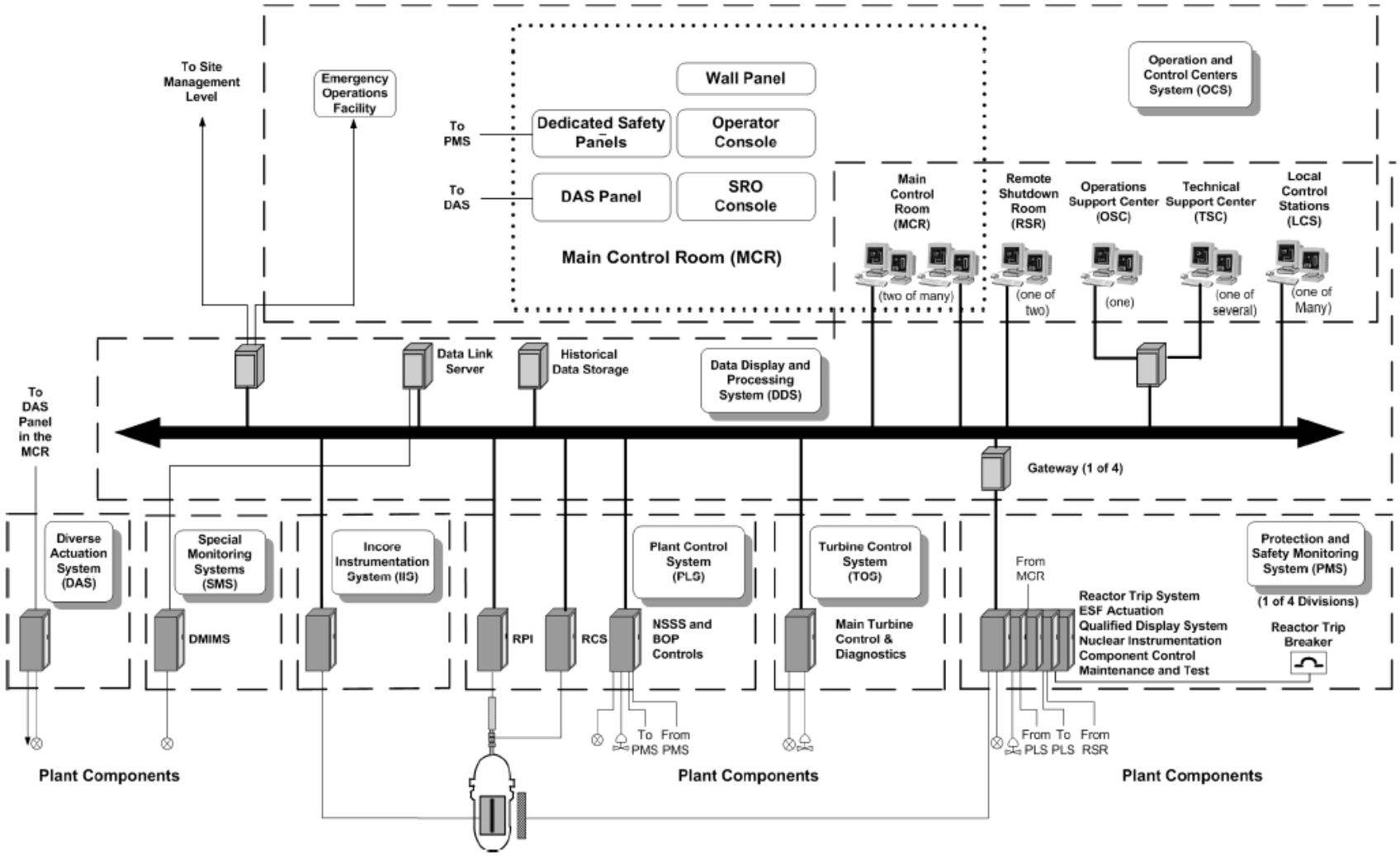
# Cyber Security During Construction

- A good practice is to store safety related and important to safety CDAs in a secured storage areas prior to their installation in the plant to minimize any unauthorized access to them
  - These areas should be access controlled to minimize unnecessary traffic to them

# Cyber Security For the AP-1000

- A major difference between the AP-1000 and current nuclear fleet in the USA is the shear number and complexity of digital components
- Most of the nuclear plants in the USA were designed in the 60s and built in the 70s and 80s.
  - The old nuclear fleet relied on relays, analog controllers (4-20ma), sensors and switches for operation
    - Analog equipment is typically not susceptible to cyber disruption – (e.g. you turn a hand switch and the rods fall into the core)
  - The AP 1000 relies on a digital network for communication
    - Much faster and more efficient, however, more susceptible to cyber disruption

# Data Highway for the AP-1000



# Picture of Current Control Room

# Picture of AP-1000 Control Room

Testing of the Westinghouse AP1000 control room simulator software in preparation for training of Vogtle 3 and 4 plant operators.

March 5, 2012

# Questions