NUCLEAR REGULATORY AUTHORITY, GHANA

COMPUTER SECURITY DESIGN METHODOLOGY FOR NUCLEAR FACILITY & PHYSICAL PROTECTION SYSTEMS

Nelson K. Agbemava
ICT and Computer Security Section Head
Instrumentation & ICT Department
Radiological & Non Ionizing Installations Directorate

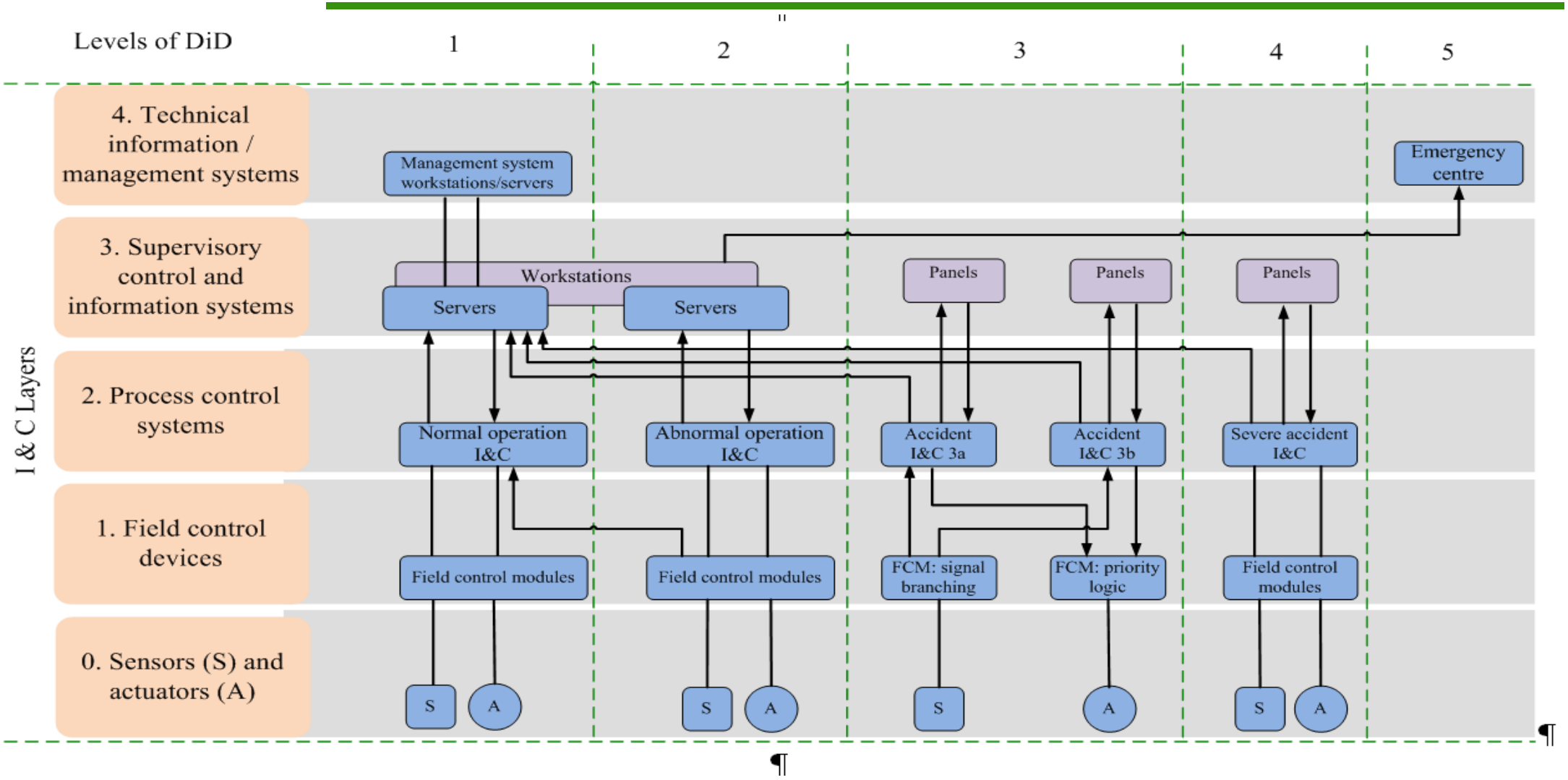
Agenda

- Background
- Nuclear Facility Industrial Control System Architecture
- ICS CYBER SECURITY LIFE CYCLE PROGRAM
- ICS Cyber Security Life Cycle
- Defence In Depth (DID) Design
- DID Architecture
- Security Controls In DID Architecture
- Conclusion

Background

- Computer security design methodology for nuclear power plant (NPP)'s industrial control system (ICS) has been discussed. The critical components of cyber security life cycle programme including the plan were discussed with the perspective of ICS. Nuclear security target set identification in relation to critical system (CS) and critical digital assets (CDS) have been discussed expressing the need to identify systems and networks associated with safety, security, emergency preparedness systems and their support systems.
- Defence in Depth (DID) approach strategies grouped zones in relation to the CS and CDA were discussed emphasizing on firewalls and their capabilities security control in DID architecture were discussed focusing on technical, operational and management control.

Nuclear Facility Industrial Control System Architecture



Safety Defence in Depth

- Five levels of *defence in depth* are discussed in Ref. [16] (See Ref. [16] for further information):

  (a) The purpose of the first level of defence is to prevent deviations from *normal operation* and the *failure* of *items important to safety*.

  (b) The purpose of the second level of defence is to detect and control deviations from *normal operation* in order to prevent *anticipated operational occurrences* from escalating to *accident conditions*.

  (c) The purpose of the third level of defence is to prevent damage to the reactor core and *releases* of *radioactive material* requiring *off-site protective actions* and to return the plant to a *safe state* by means of inherent and/or engineered *safety* features, *safety systems* and procedures.

  (d) The purpose of the fourth level of defence is to prevent the progress of, and to mitigate the consequences of, *accidents* that result from *failure* of the third level of defence by preventing accident sequences that lead to *large radioactive releases* or *early radioactive releases* from occurring.

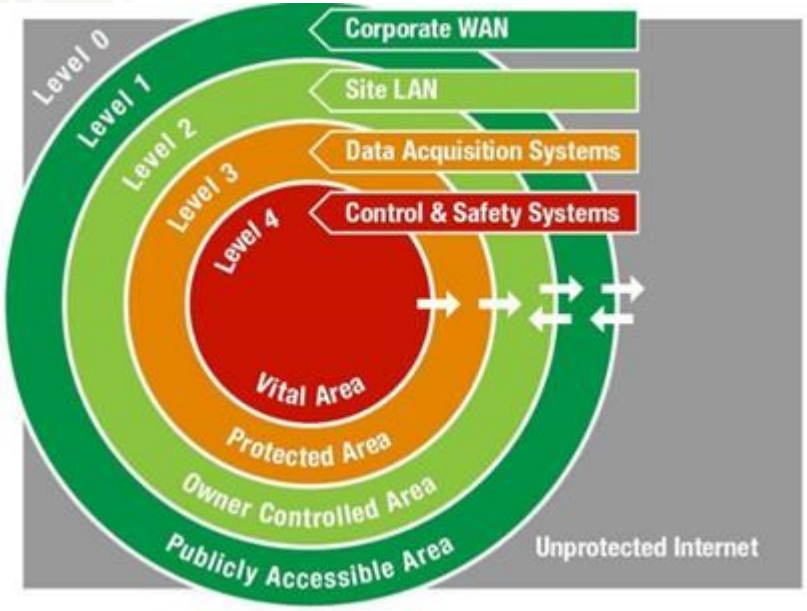
  (e) The purpose of the fifth and final level of defence is to mitigate radiological consequences of a *large release* or an *early release of radioactive material* that could potentially result from an accident.

DEFENCE IN DEPTH (DID) DESIGN

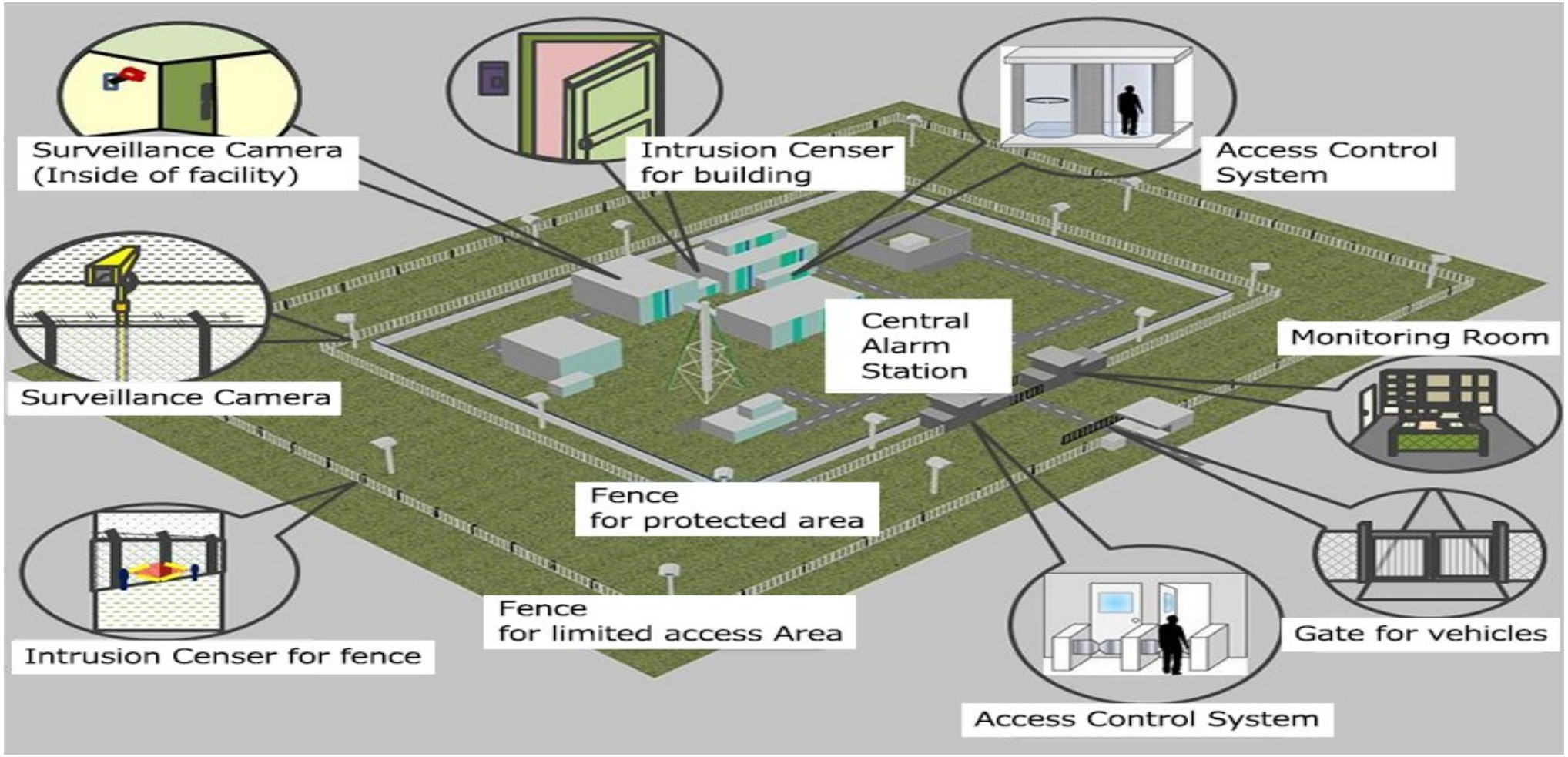
DID ARCHITECTURE (US NRC)

- Similar to the petrochemical, and other utility industries, Defense In Depth approach is adopted in the Nuclear Power Industry to protect their critical systems against any Cyber Attack. This approach splits the Nuclear Power System Architecture into 4 layers:

  - ✓Level 4 – Control and Safety System
  - ✓Level 3 – Data Acquisition Network
  - ✓Level 2 – Site Local Area Network
  - ✓Level 1 – Corporate Wide Area Network (WAN)



Concept Of Defence In Depth



Potential PPS Exposures to Cyber-Attack

- The Central Alarm Station is critical and is currently commonly implemented requiring bi-directional communication with all of the devices.
- PPS devices and networks span the entire facility site, with little or no logical separation. Dependent upon ‘air-gap’, isolation from adjacent or external networks.
- Therefore PPS design ‘breaks’ the zone model, and requires additional controls to protect against those attacks exploiting physical, portable interfaces, or local network attacks.

ICS CYBER SECURITY LIFE CYCLE PROGRAM

- All nuclear regulations and international standards mandate NPP ICS be designed from cyber security prospective in accordance with an established cyber security life cycle program.
- **CYBER SECURITY PROGRAMME (CSP)**
  - Cyber Security Programme (CSP) explains the methodology followed to achieve high assurance that all the critical systems and their digital assets have protections from the cyber-attacks. In the nuclear industry, the plan focuses on the methodology followed to achieve high assurance that the following digital systems are protected from the cyber-attacks:

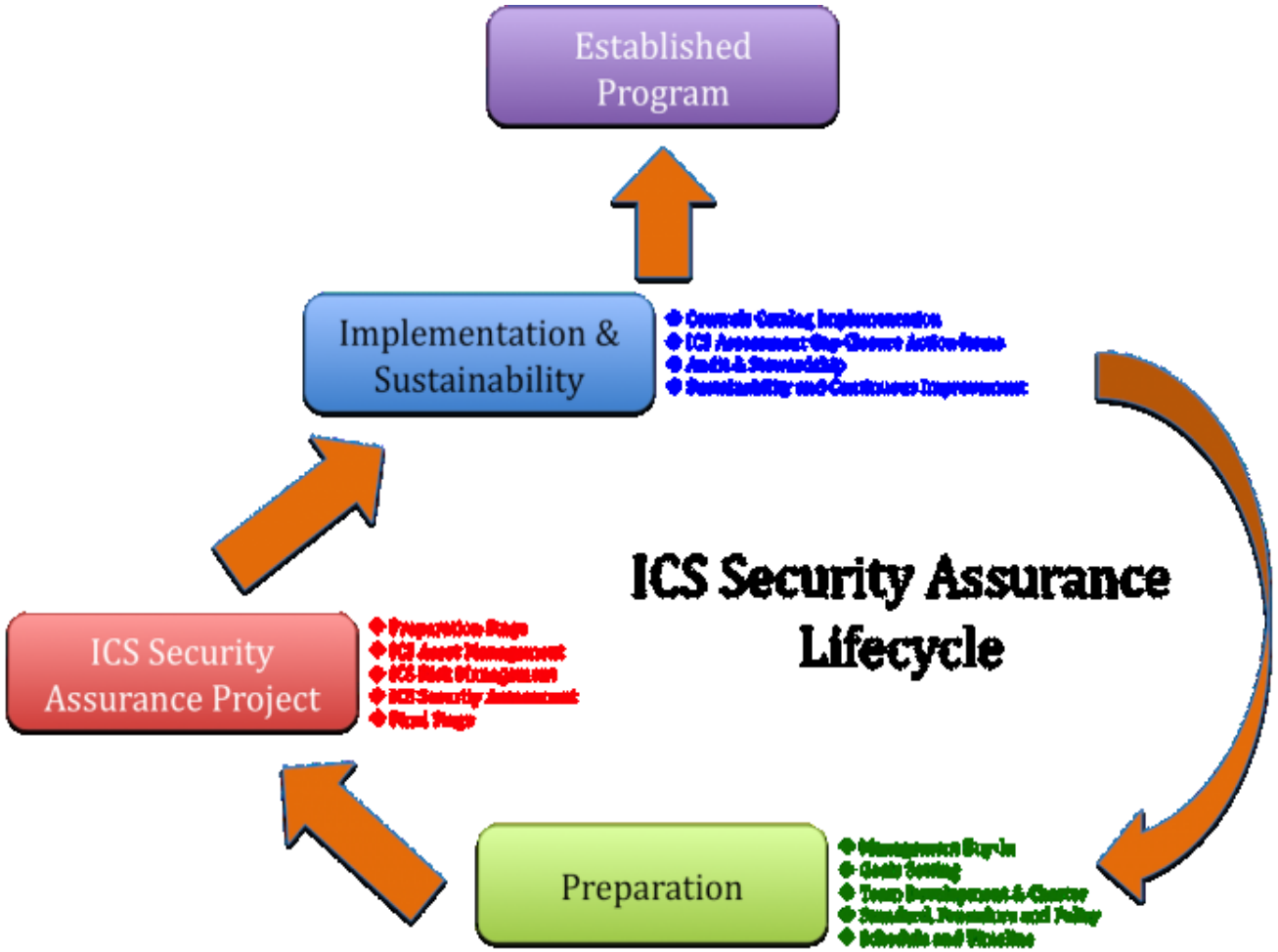
✓ Safety Systems (i.e. ICS contain components part of Safety System).

✓ Security Systems.

✓ Emergency Preparedness Systems.

✓ Systems and equipment's that support the operation of the above systems (i.e. ICS contain components which fall under this category).

ICS CYBER SECURITY LIFE CYCLE



- The CSP follows the ICS cyber security life cycle programme as show in figure 2 to put the required technical, process and management controls used to protect the identified systems against cyber-attacks [6,8]. The CSP requires regulatory approval before it can be executed in the implementation phase and also if future plan modifications are required

SECURITY CONTROLS IN DID ARCHITECTURE 1/1

In NPP DID architecture including NPP ICS DID architecture, applied on each DID layer falls under the following categories:

- **TECHNICAL CONTROLS**
  - These controls are executed through non-human mechanisms to:
    - ✓Perform Protective Measures against Cyber Attack (Such as Firewalls and System Hardening).
    - ✓Provide Electronic enforcement of polices such as Access control, One Way communication (such as data diode), and report of cyber-attacks.
- **OPERATIONAL CONTROLS**
  - These controls are executed through human mechanism and provide guarding against the insider threat. These controls vary from procedural controls such as patch management procedures to controls provided by the physical protection systems in the plant. These controls are applied across all DID architecture levels.

SECURITY CONTROLS IN DID ARCHITECTURE 1/2

- **MANAGEMENT CONTROLS**
  - These controls include risk management to manage the risks introduced by the cyber-attack and procurement controls applied during the procurement process of a CDA ensuring that the final CDA product is free of any cyber vulnerabilities. These controls are applied across all DID architecture levels. Some specific challenges in this area include the establishment and verification of Secure Development environments by vendors developing software code that will eventually be deployed in the NPP.

- **CYBER SECURITY VALIDATION AND VERIFICATION**
  - Cyber Security Validation and Verification is the final step performed on the implemented Cyber Security features in NPP ICS design before the designed or modified ICS is put online. Intensive testing is performed on the NPP ICS design or modified design including cyber testing to ensure that the designed ICS performs its function during the cyber-attack and no cyber security measures degrade the ICS performance. The validation and verification results are documented in the cyber security plan and program.

CONCLUSION

- In conclusion, the Cyber Security design for the nuclear facility ICS. The process is similar to the design process followed in the cyber security design for ICS in other industries such as petrochemical and fossil power utilities in a sense that DID concept is applied when developing the ICS architecture. The Cyber Security Design for nuclear facility ICS architecture that are followed by designer (Target Set Identification, and CS/CDA identification) before finalizing the nuclear facility ICS DID architecture.

Thank you

If you have more question, contact by

n.agbemava@gnra.org.gh