**Cyber Security Design Methodology for Nuclear Power Control & Protection Systems**

**By Majed Al Breiki – Senior Instrumentation & Control Manager (ENEC)**

## 1. INTRODUCTION

In today's world, cyber security is one of foundational design attributes that are necessary in any integrated Industrial Control System (ICS) design process. A standard design approach is to identify significant cyber security risks in the ICS Architecture and implement cyber security protection layers to mitigate these risks in the ICS Architecture in accordance to known International Standards or Guidelines (i.e. ISA 99, INPO 10-008, NIST standards, and US Nuclear Regulatory Commission Guideline 5.71). A majority of these standards consider embedding the DID (Defense In Depth) approach in the ICS architecture design as a reasonable approach to protect the ICS from cyber security attacks.

For an ICS in a Nuclear Power application, the DID approach is a key aspect adopted to augment the cyber security protection layers within the Nuclear ICS Architecture. The design requires multiple analysis to be performed during nuclear power plant design process (i.e. such as target set analysis, Critical System/Digital Asset identification ) before the system designer can adopt the DID approach when defining the Nuclear Power ICS Architecture. The design and implementation processes are carried out under a Cyber Security Life Cycle Program and may vary between control and protection systems.

In this article, Cyber Security design process and its implementation in the Nuclear Power ICS Architecture are explained. A complete Nuclear Power ICS cyber security life cycle program is described and how the DID approach is sequenced in this life cycle is explained.

## 2. NUCLEAR POWER PLANT OPERATION PRINCIPLE

Figure 1 shows typical schematic diagram for a pressurized nuclear power plant. The plant operates utilizing the nuclear fission principle [1] to generate thermal power within the Nuclear Reactor in the containment building. Thermal power is carried out by the pressurized primary water into a steam generator in the containment building to heat the secondary water in the steam generator to its boiling temperature.

At boiling temperature of the secondary water, the steam is generated in the steam generator and used to drive the Turbine Generator generating electrical power (Electricity).

[1] Fission Principle: nuclear fission is either a nuclear reaction or a radioactive decay process in which the nucleus of an atom splits into smaller parts (lighter nuclei). The fission process often produces free neutrons and photons (in the form of gamma rays), and releases a very large amount of energy even by the energetic standards of radioactive decay.

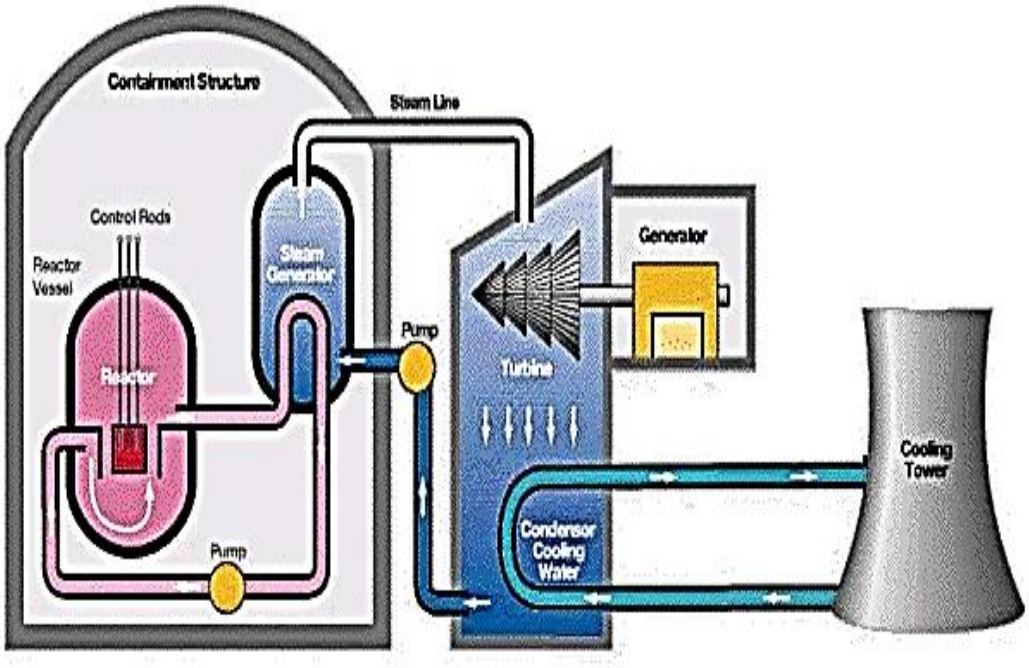


Figure 1: Nuclear Power Plant

Wasted steam is then flown to a condensor where its temperature is cooled down by a condensar cooling water producing condensed water (Secondary Water). The condensed water is pumped into a steam generator where its heated by the primary water using the thermal power (generated from the Nuclear fission process in nuclear reactor) to generate the steam and the cycle repeats itself again.

The above operation is monitored and controlled by Instrumentation and Control (I&C) system together with the plant personnel operation. Through its various constituent elements (e.g. equipment, modules, subsystems, redundancies, systems, etc.), the plant I&C system senses basic parameters, monitors performance, integrates information, and makes automatic adjustments to plant operations as necessary. Also, it responds to failures and off-normal events, thus ensuring goals of efficient power production and safety.

Essentially, the purpose of I&C systems at a Nuclear Power Plant (NPP) is to enable and support safe and reliable power generation. Figure 2 shows a typical Nuclear Instrumentation & Control Architecture (high level schematic).

To accomplish the power production objective, Nuclear ICS monitors and controls hundreds of plant parameters, such as power, power-density, temperatures, pressures and flow rates, within the design limits. Also, it controls the energy flow from the reactor core to the generator within the design limit. Furthermore, it safely shuts down the NPP and keeps the reactor cooled down during abnormal design events to prevent the nuclear radiation release into atmosphere. Therefore, it is crucial that the ICS is designed to withstand cyber and environmental (such as Flooding & Seismic) attacks and still be able to perform the control and protection of the Nuclear Power Plant in safe and efficient manners. Section 3 provides

general description of the NPP ICS architecture and section 4 explains its Cyber Security life cycle program.

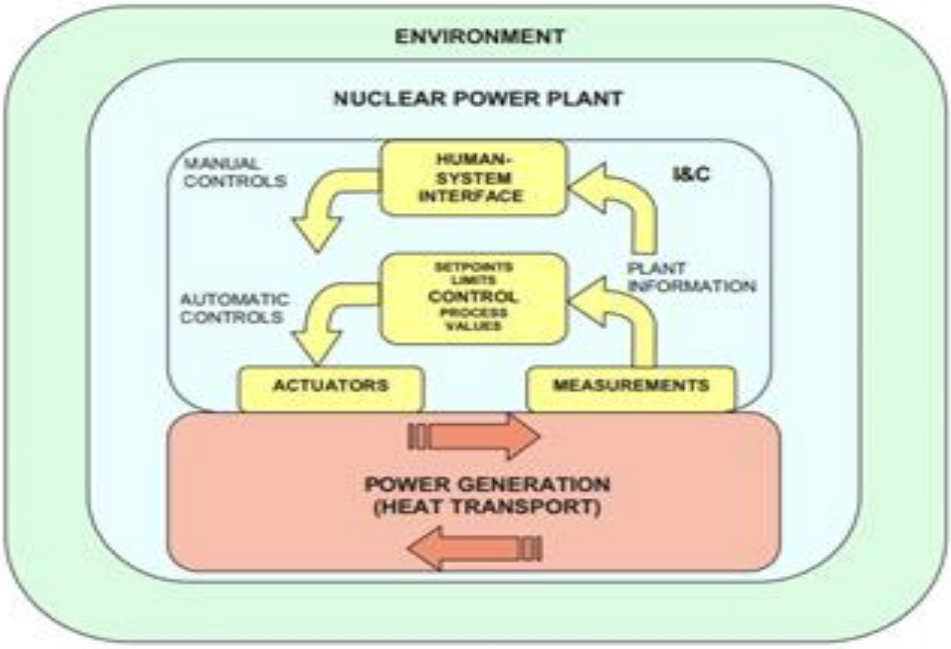


Figure 2: NPP Instrumentation & Control Architecture High Level schematic[2].

## 3. NUCLEAR INDUSTRIAL CONTROL SYSTEM ARCHITECTURE

In a typical NPP, ICS architecture consists of non-safety and safety systems. The non-safety system is a distributed computer system comprising number of remote control nodes distributed across the NPP and communicating among each other and with the Human Machine Interface (HMI) through redundant real time data network. It also supports communicating with third party systems and Operation Maintenance Corporate Systems (OMS) utilizing open protocols such as Object Embedding Linking Process Control (OPC), fieldbuses and Modbus-TCP. Furthermore, the operator can monitor and manually control the NPP processes via HMI consoles connected in the non-safety system. Through Interface gateways, the safety system communicates with the non-safety system to display the safety critical information on the non-safety HMI.

On the other hand, the safety system is often a channelized Programmable Logic Control (PLC) based system containing a number of PLC nodes segmented across the NPP to align with safety components in the process system and communicating with in a safety channel via the redundant real time data safety network or in between safety channels by dedicated high speed links. These PLCs and its cabinets are designed to with stand seismic events, environmental events and cyber security attack and still be able to safely

[2] IAEA Nuclear Energy Series Report No. NP-T-3.12

shutdown the reactor and maintain reactor core cooling to avoid the fuel rod damage which could lead to the radioactive release to the environment. Both the ICS safety and non-safety system software is developed following a software life cycle in line with the software life cycle defined in international standards such as IEEE Standard 1074 or ISO/IEC 12207. Figure 3 shows a typical NPP ICS Architecture.

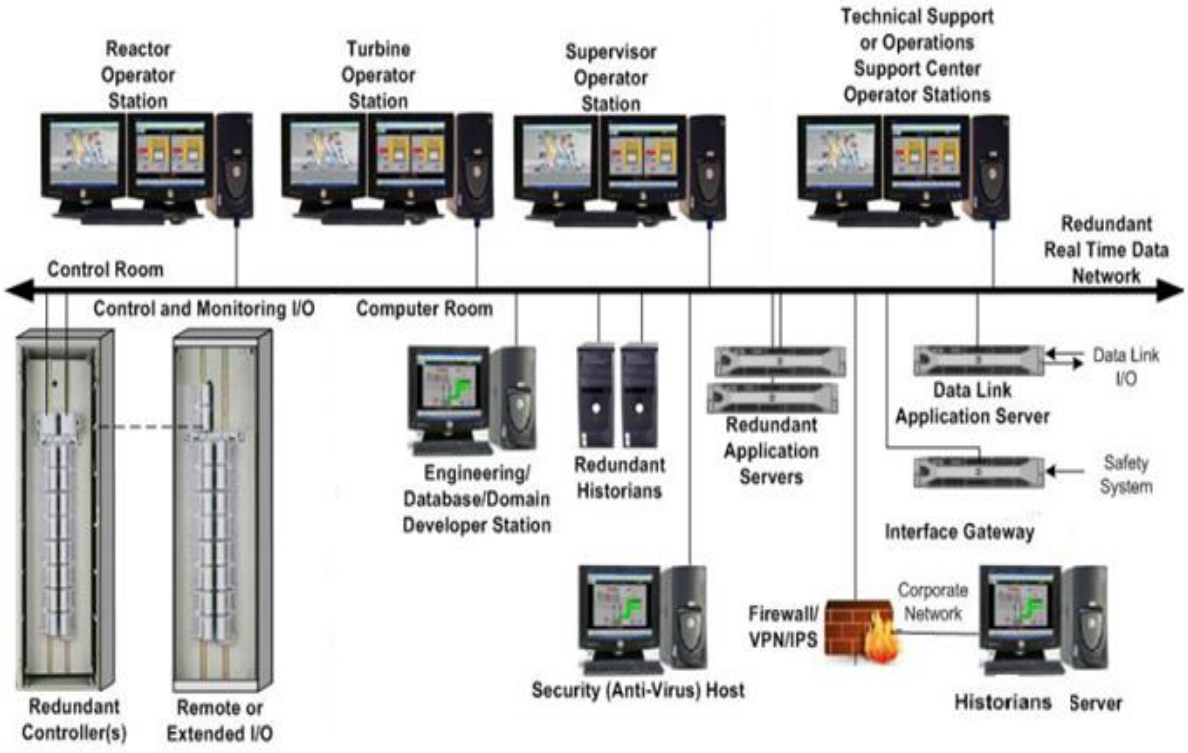


Figure 3 typical NPP ICS Architecture.

## 4. NPP 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. Figure 4 shows the program's components and the following sub-sections provide description of these components.

### 4.1 CYBER SECURITY PLAN (CSP)

Cyber Security Plan (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).

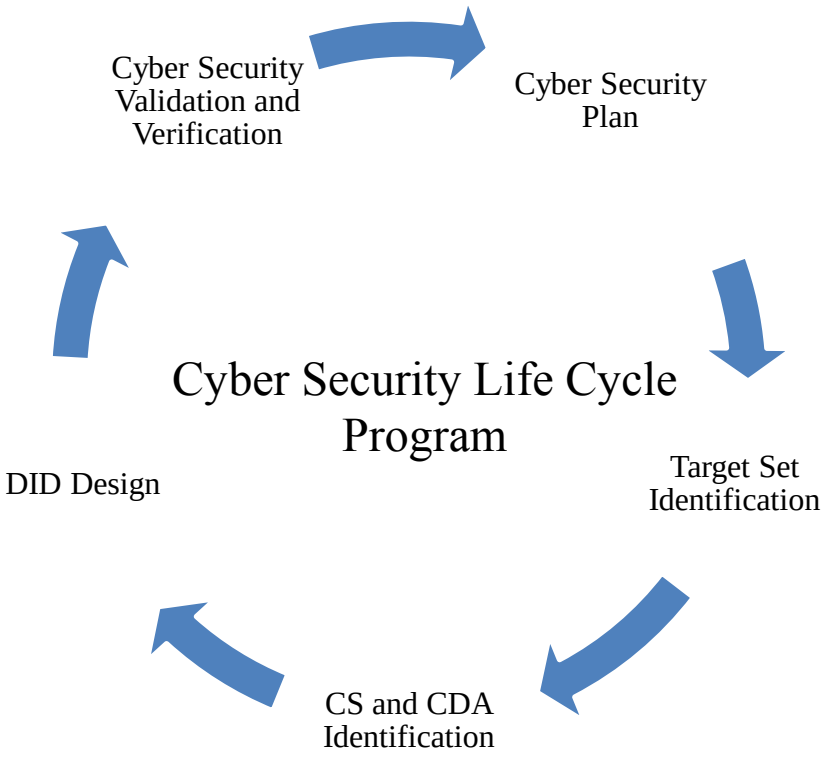


Figure 3 NPP ICS Cyber Security Life Cycle Program.

The Cyber Security Plan (CSP) focuses on the activities followed to put the required technical, process and management controls used to protect the identified systems against the cyber-attack. The CSP requires regulator's approval before it can be executed in the implementation phase and if future plan modifications are required.

## 4.2 TARGET SET IDENTIFICATION

Target set is defined as list of equipment's and elements within the nuclear power plant which if attacked physically or by cyber methods could result in nuclear sabotage[3]. These sets are identified through a well-structured approach outside the scope of this white paper to explain (see NEI 10-04, NEI 13-05 or USNRC RG 5.81). The result of this

[3] Nuclear Sabotage terminology used to indicate the radioactive material release to the environment and public.

identification process is the list of critical systems and assets that require protection against cyber-attack as explained in the next section.

## 4.3 CRITICAL SYSTEM (CS) AND CRITICAL DIGITAL ASSETS (CDA) IDENTIFICATION

In the Nuclear Industry, Critical System (CS) is defined as systems and networks associated with Safety, Security, Emergency Preparedness (SSEP) Systems, and their support systems. For NPP ICS, CS mainly consists of safety systems and non-safety systems which their malfunction will affect the operability of the safety system or create an unnecessary actuation of those safety systems. Components and Equipment within a CS that contain digital electronics (uP, FPGA, SoC, etc) are considered Critical Digital Assets (CDA). The identification of these systems and assets are the first step towards defining the total scope of application for cyber security measures within the NPP ICS Architecture.

In the CS identification process, each system including the ones part of the target sets is evaluated to determine if its function is related to SSEP System, or supporting system for any of these systems. If its function is related to SSEP systems or their supported systems then the system is considered a CS and all the digital components within the CS are considered CDA.

The above process is done for each system installed in NPP and the results are documented in the Cyber Security Plan.

Figure 3a and 3b summarize the CS and CDA identification process utilized in the Nuclear Power Plant Design.

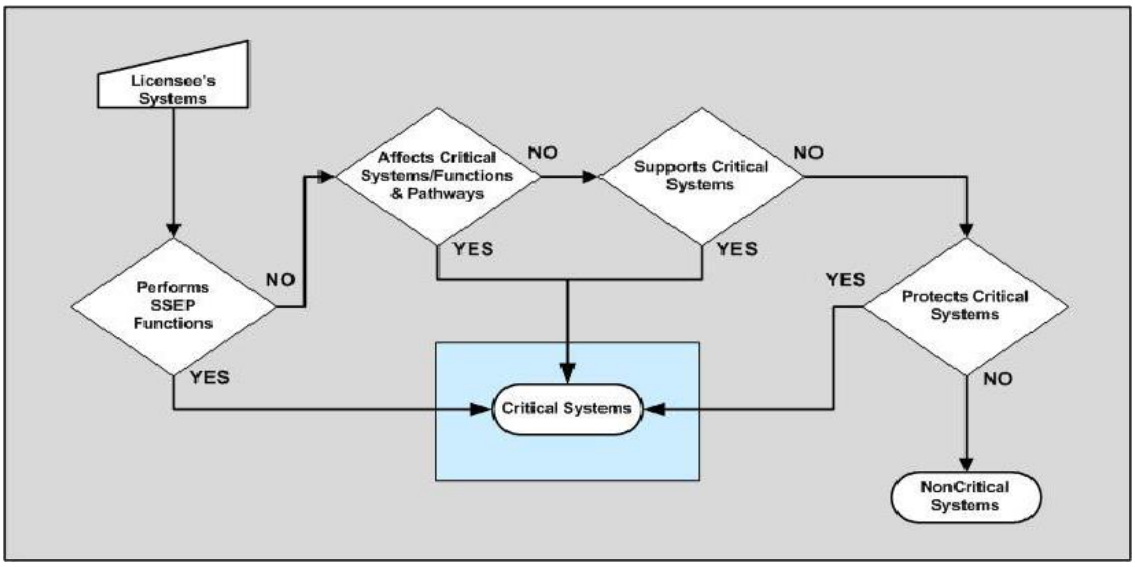


Figure 3a CS Identification Process.

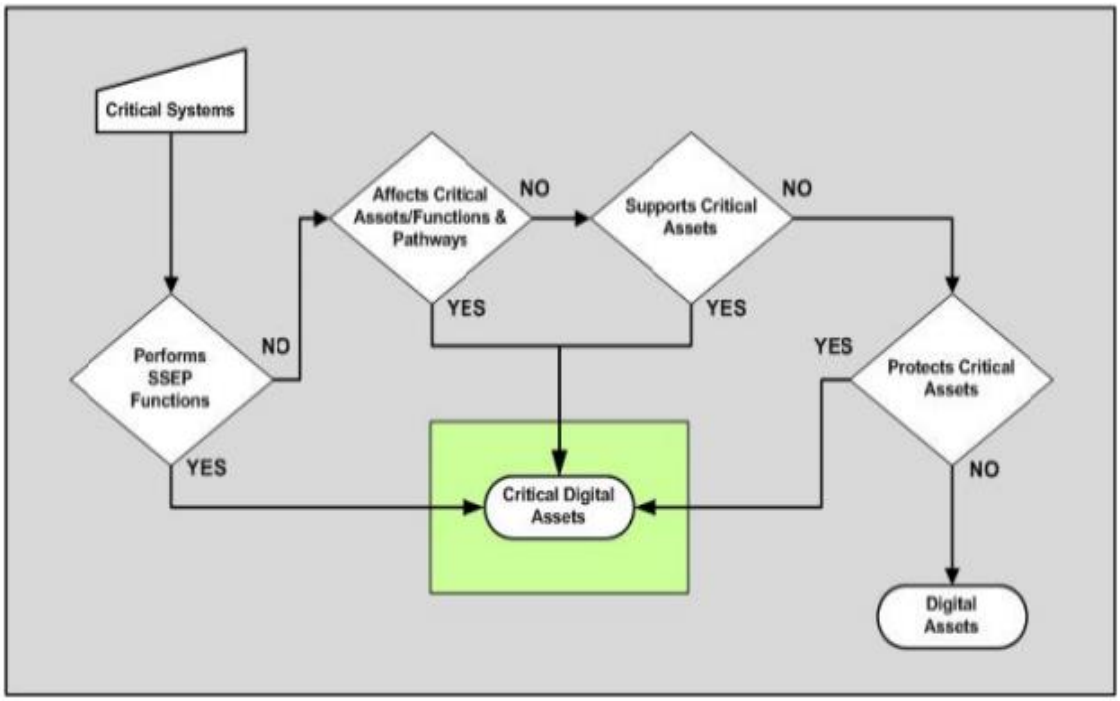


Figure 3b: CDA Identification Process.

## 4.4 DEFENCE IN DEPTH (DID) DESIGN

### 4.4.1 DID ARCHITECTURE

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)

At certain layers and for any interfaces between Level 1 & 2 strict security measures such as data flow restriction, Deep Package Inspection, and system hardening are applied as needed. Management controls are applied on CDAs in Layer 1, security measures on CDAs in Level 2 and 3 are a mixture of technical controls (adopting firewall, and System Hardening as example) and operational controls applied to protect these CDAs against the cyber-attack. One very important aspect of all security measures applied is that they must not affect the CS' primary capability to perform its SSEP function.

The NPP ICS contains CDAs that perform their required safety function or support to the system with the SSEP functionality. The components within these CDAs performing these functions will be located in level 4 whereas components within these CDAs performing the data acquisition from the SSEP systems will be located in level 3. The data flow between

level 4 and level 3 will be restricted to uni-directional communication from level 4 to level 3 only. All the communication between NPP ICS and the OMS (Operation Maintenance Systems) will be done through level 2 and it will also be uni-directional communication. Figure 4 explains high level of NPP ICS DID Architecture diagram.

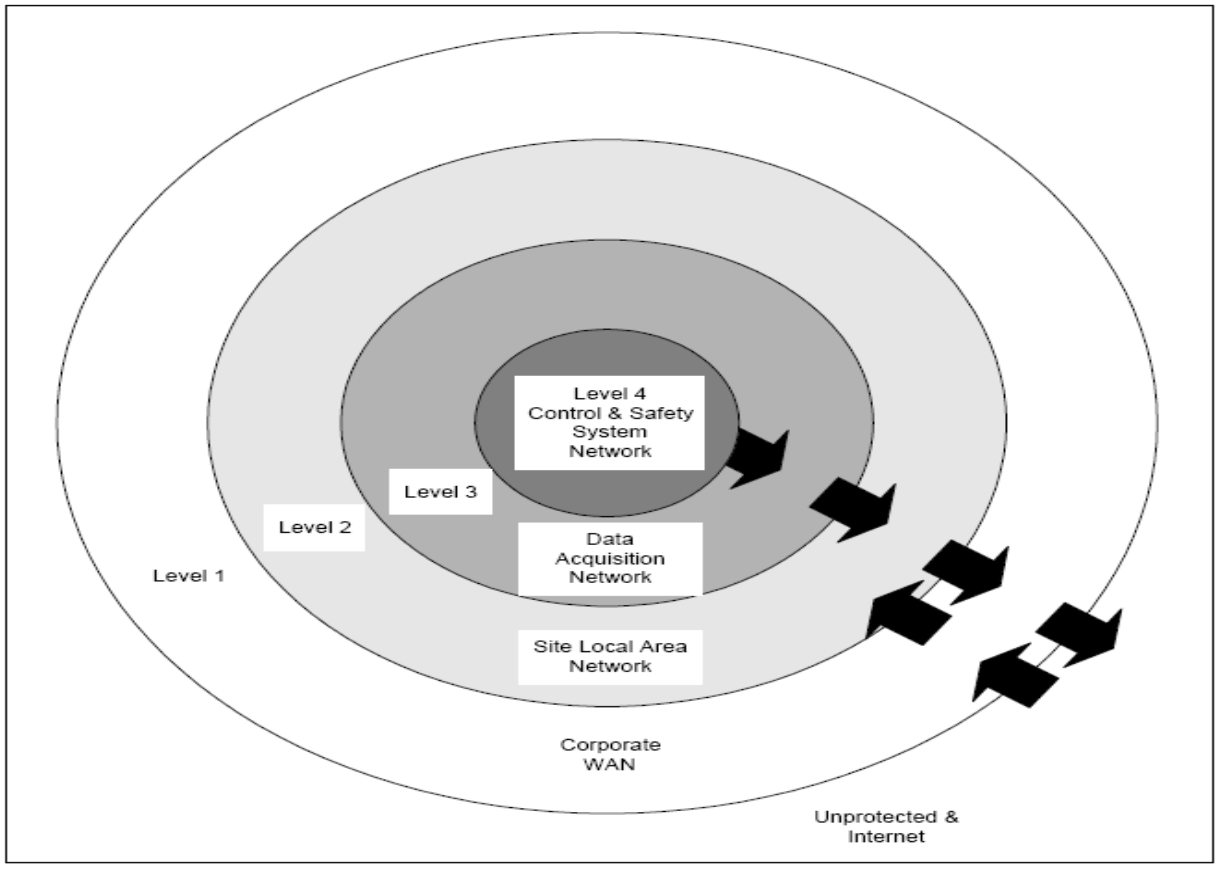


Figure 4 High level NPP ICS DID Architecture diagram.

## 4.5 SECURITY CONTROLS IN DID ARCHITECTURE

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

### 4.5.1 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.

These controls are applied across all layers of DID architectures and the specific type is determined based on specific application and design philosophy. For example, the

communication between layers 4 and 3 and between layers 2 and 3 is uni-directional communication achieved through data diode to prevent external intrusion, while internal threats and cyber-attack prevention is achieved by other technical controls such as access control, and system hardening.

Certain communication between layers 2 and 1 is bi-directional communication with technical controls used to perform protective measures against cyber-attack along with access control for electronic enforcement of policies.

There are also special considerations for safety systems and any technical controls included in those safety systems. Safety system software is typically certified and closely controlled for all safety functions in the NPP. Any future changes to those safety systems (i.e. additional firewalls, software patches, intrusion detection monitoring software) all required that software to be re-certified for use in the NPP. It is important when applying cyber security technical controls these challenges and software requirements be taken into consideration during the cyber security design phase.

### 4.5.2 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.

### 4.5.3 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.

## 5. 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.

## 6. CONCLUSION

In conclusion, the white paper has explained the summary of the Cyber Security design for the NPP 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. This paper has also demonstrated the additional steps in the Cyber Security Design for NPP ICS architecture that are followed by designer (Target Set Identification, and CS/CDA identification) before finalizing the NPP ICS DID architecture.

About the Author:

Mr. Al Braik is Senior Instrumentation & Control Manager within the Engineering Department in Emirates Nuclear Energy Cooperation. He holds Master of Science and Bachelors of Science in Control System. Also, he holds TÜV Rheinland certified Functional Safety Engineer since 2011 and Green Belt Six Sigma from Institute Quality Federation. His interests are cyber security, wireless system, fieldbus, advanced control systems, and Integrated Control System design. He already had published articles in journals such as "wireless control in offshore facilities" in Oil & Gas journal, and "Can Virtualization be adopted in control system?" in the control engineering magazine.