IAEA – Safety Demonstration of Advanced Water Cooled Nuclear Power Plants

Session: Digital I&C Systems

Topic: Defence in Depth & Diversity – Challenges related to the I&C Architecture

Pickelmann Johannes / Gregory Droba
AREVA NP / GE Hitachi

Johannes.pickelmann@areva.com / gregory.droba@ge.com

June 2017, Vienna
Overview

The position paper, “Defense-in-Depth and Diversity – Challenges related to the I&C architecture”, is the second in this series and is a continuation of, and builds upon, the work done in the “Safety classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties”

It documents the discussions of the WNA CORDEL DICTF members on the specific challenges they face in the application of Defense-in-Depth and Diversity techniques to I&C activities.
The approach of the paper is to:

- Define the current landscape by compiling and comparing Defense-in-Depth and Diversity terminology and definitions used in different regions,
- Tabulate the challenges in defining Defense-in-Depth and Diversity, and
- Identify and recommend potential solutions.
Terminology Landscape

• Work of a previous WNA paper, Troublesome Key Words For Safety Classification Of I&C Systems In Nuclear Power Plants, provided the basic data to do the more focused assessment of the key words “Defense-in-Depth” and “Diversity” to understand the landscape.

• The IAEA dictionary terminology was adopted for all other terminology to have a standard frame of reference and focus.

• It was agreed to adopt the terminology of diversity attributes from NUREG/CR-6303 and NUREG/CR-7007.
Challenges

• The terms and manner in which Defense-in-Depth and Diversity are used differ between regions.

• The quantitative aspect of DiD&D assessment will rely on some subjective or qualitative aspect, which ultimately will be accepted or rejected based on the strength of the argument made for the selections, and the argument may not stand when reviewed by different auditors or regulating bodies.

• The subjective aspects of DiD&D assessment results in ambiguous or incomplete rules relating to how quantification is achieved, and can make the achievement of “Done” difficult to obtain.
Challenges (Cont)

• The guidance with respect to attributes used to assess diversity may be out of date with respect to the way technology is designed, developed, implemented and maintained.

• Implementation of regulatory guidance in a global market is challenging. The approach of DiD&D, driven by different regulations, varies across regions of the world. Implementation of a single regulatory guidance can often be interpreted, or misinterpreted several ways, and the attempt to apply multiple regional regulation to a single product can aggravate the issue.
## Comparison of different DiD approaches

<table>
<thead>
<tr>
<th>IAEA Levels [IAEA SSR-2/1]</th>
<th>WENRA / EPRI Levels $^{1/2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td>Objectives</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Prevent deviations from normal operation and the failure of items important to safety.</td>
</tr>
<tr>
<td>2</td>
<td>Detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.</td>
</tr>
<tr>
<td>3</td>
<td>Escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop.</td>
</tr>
<tr>
<td>4</td>
<td>Mitigate the consequences of accidents that result from failure of the third level of defense in depth</td>
</tr>
<tr>
<td>5</td>
<td>Mitigate the radiological consequences of radioactive releases that could potentially result from accidents.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

$^{1}$ WENRA RHWG (2013). Safety of New NPP Designs

$^{2}$ EPRI (2014). Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support Acceptance in Multiple International Regulatory Environment
Digital upgrades face the following challenges:

- The original design basis and architecture may be lost or it wasn’t controlled or updated with the plant maintenance and modernization. This might require cost reverse engineering to re-establish the design basis and architecture prior to any upgrades.
- The application of modern DiD&D regulatory requirements may invalidate parts of the existing design basis or architecture, and may require larger measures than just replacement to upgrade.
- Even smaller instrument or system upgrades require some sort of DiD&D analysis, which faces all the same challenges of regulator guidance and quantification.
Recommendations

- Use of the terminology “D3” has the effect of amalgamating two distinct concepts into a single concept to casual readers.

- The term “Defense-in-Depth” or DiD should be separated from “Diversity”, or when appropriate, specified as DiD&D to emphasize that the two are separate concepts that must work together.

- The definitions used by the IAEA with regards to the two terms “Defense-in-Depth” and “Diversity” appear to be the best and don’t conflict with other organizational definitions and would be the recommended definitions that all organizations should adopt.
Recommendations (Cont)

• The current diversity attributes used by most organization appear to be those defined by NUREG/CR-6303. NUREG/CR-7007 supports the conclusion that these attributes should be re-visited, updated, and modernized as well-defined attributes support clear completion criteria of the DiD&D analysis.
Recommendations (Cont)

• The terms “levels of defense” and “echelons of defense” are different definitions that are sometimes used to try and relay the same concept. However, interchanging these terms adds confusion in a globalized industry. The IAEA uses the “levels of defense” and this term is widely accepted and understood as by organizations using the term “echelons of defense”. The term “echelons of defense” should be discontinued in place of the IAEA definition of “levels of defense”.
Recommendations (Cont)

Additional research into specific issues pertaining to DiD&D Challenges should be done centered around key questions and challenges of:

• The challenges of upgrading and modernizing existing NPPs

• More work is required to evaluate the interaction of DiD and particularly the manner in which Diversity criteria interact so that the completion criteria is recognized and agreed to by those performing and those evaluating the DiD&D as “done”.
Measures for Independence

Management of Postulated Initiating Events (AOO / DBA / DEC – plus maintenance) leads to the request for ...

...in case of single failure scenario

**Redundancy**

requires to consider...

... in case of systematic failure scenario

**Defence-in-Depth**

requires to consider...

... managed by combination of ...

**Independence**

**Separation**

**Diversity**

**Separation means are ...**

**Electrical Isolation**

**Physical Separation**

**Functional Independence**

**Functional Diversity**

**Design Diversity**

**Signal Diversity**

**Equipment Manufacturer Diversity**

**Software Diversity**

**(selection of) Diversity means are ...**

**Independence of Communication**

**Equipment Platform Diversity**

**Human / Life-cycle Diversity**

**Logic Processing Equip. Diversity**

**Logic Diversity**

Gregory Droba / Joh. Pickelmann
END OF PRESENTATION

Thank you for your attention