

## **CANDU NPP S/W Categorization Methodology for Safety, Plant Control, Monitoring & Testing Systems**

This lecture will provide some insight into the categorization methodology that should be taken into consideration for safety critical software for computerized shutdown system applications.

### **Lecture topic summary includes:**

- Purpose of the S/W Categorization Process
- Necessary Definitions
- Specification of the S/W Categories
- Categorization Process Basis
- Determining Plant System Safety Significance
- Determining S/W Failure Impact Type
- Final S/W Category Determination
- S/W Categorization 1-4 Summary

### **Supporting software categorization documents for this lecture that could be consulted for further information:**

- COG-95-264 'Guideline for Categorization of Software in Nuclear Power Plant Safety, Control, Monitoring and Testing Systems', 95 September 22
- CANDU 9 Assessment Document 69-66700-ASD-002, 'Preliminary Categorization of DCS Software'

### Purpose of the S/W Categorization Process

- ***Minimize any unnecessary reliance on S/W*** or S/W controlled systems for nuclear safety
- Ensure that S/W necessary for nuclear safety is ***clearly identified, understood and achieved***
- Select the S/W Engineering practices which ***assures the reliability and safety*** of the S/W
- Categorize S/W with respect to its ***failure effect on nuclear safety***

### S/W Categorization Process - Necessary Definitions

- ***Safety-Related System*** - A plant system that, upon failure, has the potential to impact the ***radiological safety*** of the public or plant personnel due to the operation of the nuclear power plant (NPP).
- ***Nuclear Safety-Related Functional Requirements*** - those functional requirements which ensure that the system will fulfill its role in ***achieving acceptable levels of radiological safety*** with respect to the public and plant personnel
- ***Process System*** - a safety-related plant system whose role is to contribute, directly or indirectly to the ***production of electricity***.
- ***Initiating Event*** - a malfunction of a plant system that would, ***in the absence of Special Safety System actions***, lead to a release of radioactivity which could result in doses exceeding the most restrictive regulatory dose limit for that station.
- ***Mitigating System*** - a safety-related system that has nuclear safety-related functional requirements ***to reduce the consequences of an initiating event***.

### **S/W Categorization Process - Necessary Definitions...continued**

- ***Safety System Significance*** - a classification (into *High, Medium* or *Low*) of the plant system in terms of its *importance to nuclear safety*
- ***Software Failure Impact*** - the impact of the failure of that S/W *with respect to the nuclear safety related functional requirements* of the host plant system
- ***Minimum Performance Requirements*** - the minimum amount of equipment, and the minimum functional and performance characteristics of that equipment, *necessary to achieve the plant system performance* specified in the safety analysis completed in support of that station operating license.

### Specification of the S/W Categories

- The Software Category - is represented by a ***number*** from ***1*** to ***4***
- ***Category 1*** S/W considered the **most important** to Nuclear Safety
- ***S/W Nuclear Safety Category 1*** - is also referred to as ***Safety Critical Software***
- ***Failure of Safety Critical S/W*** can result in a system with a high safety-related reliability requirement ***not meeting its minimum performance requirements*** or can result in a ***serious initiating event*** (low frequency limit) in a process system.
- ***Category 4*** S/W is to have ***no importance*** to Nuclear Safety
- ***S/W Nuclear Safety Category 2*** - Failure of this S/W can result in a ***serious process failure***, or a ***degradation in the performance of a mitigating system***.
- There is a distinct ***reduction in safety significance*** from Category 1 S/W since the ***consequences of the Category 2 S/W failure*** can still be ***mitigated*** by special safety system action.

***S/W Nuclear Safety Category 3*** - Failure of this S/W ***does not prevent*** the affected plant system from ***meeting its Nuclear Safety-related design intent*** or the affected plant system has a ***low safety significance***.

## **Categorization Process Basis**

***Fundamental Basis*** - As the *Safety Significance of the S/W decreases, less effort is required* to be expended to demonstrate that the S/W meets its requirements.

***Risk Based Approach to Nuclear Safety*** - The risk associated with the failure of a system to perform is a function of the *Probability of the failure* and the *Consequences of the failure* (the *higher the risk* associated with a failure, *the higher the assurance* must be that the S/W will not contribute to that failure).

***Acceptable levels of plant risk*** are achieved by - Designing the plant to have a *low probability of serious process failures*, and by *providing redundant mitigating systems* that minimize the consequences of serious process failures, should they occur.

## **Two Phases for the Categorization Process**

- Phase I; Determine the System's *Safety Significance*
- Phase II; Determine the *S/W Failure Impact*

## Two Phases for the Categorization Process

- Phase I; Determine the *System's Safety Significance* - This involves identifying the safety significance (as *High, Medium* or *Low*) for the plant system of which the S/W to be categorized is a part.
- *Safety Significance Determination* - The safety significance is obtained by determining the *system type* (safety-related, mitigating, process, etc) and *quantifying* the *systems reliability* requirements
- It is also important to note that *more stringent reliability requirements* due to factors other than nuclear safety may be used (i.e. *engineering judgment*, experience, etc.) to justify selecting a *more restrictive* S/W category
- *Phase II; Determine the S/W Failure Impact* - This involves *identifying* and *classifying* the *worst possible S/W failure modes* and effects in terms of *impairment of plant safety functions*.
- *Failure Impact Types* - The Failure Impact Type is identified as *Type I, II* or *III* with *Type I* representing a failure with the *greatest consequences* with respect to Nuclear Safety.

*Failure Impact Type Analysis* - The determination of the failure impact type is based on an analysis of the **role of the S/W** with respect to the *safety-related function* of the system and on the *independent mitigating provisions* within the plant system which can mitigate the consequences of the S/W failure.

### **Failure Impact Type Considerations**

- ***Assess all Failure Impacts*** - Within a plant system there can be sub-systems that perform *multiple functions*.
- The Failure Impact Assessment must *identify all possible safety-related impacts* of S/W failure on a plant system.
- For the purposes of categorization, *the most severe S/W failure impact type should be used*.
- ***Failure Impact*** - If the *worst-case* S/W failure is *not Type I*, then it is possible to *reduce the stringency* of the S/W category because **the role of the S/W within the plant system is less significant from a safety perspective than the role of the overall plant system**.

### **Definition of Plant Safety Significance values for Phase I use**

- ***Safety & Mitigating Systems Safety Significance***

**High Significance:**  $Q \leq 10^{-3}$  yr/yr (Q= unavailability req'tmt)

**Medium Significance:**  $10^{-3} < Q \leq 10^{-1}$  yr/yr

**Low Significance:**  $Q \geq 10^{-1}$  yr/yr

- ***Process Systems Safety Significance - Process System Failures***

**High Significance:**  $f \leq 10^{-3}$  occ/yr (f= event frequency limit)

**Medium Significance:**  $10^{-3} < f \leq 10^{-2}$  occ/yr

**Low Significance:**  $f > 10^{-2}$  occ/yr

- ***Monitoring/Testing Systems Safety Significance***

**High Significance:**  $Q \leq 10^{-3}$  yr/yr (Q= unavailability req'tmt)

**Medium Significance:**  $10^{-3} < Q \leq 10^{-1}$  yr/yr

**Low Significance:**  $Q \geq 10^{-1}$  yr/yr

#### **Four Steps to follow for Phase I - Determining Plant Safety Significance**

- ***1. Identify the Plant System or Systems Involved -Determine which plant systems the S/W or S/W controlled systems are a part of or interact with and determining the role of the S/W.***
- ***2. Determine the Plant System Type - Identify each role for the plant system's nuclear safety functions and determine if it is a special safety, mitigating, process or monitoring/testing system***
- ***3. Establish a Suitable Plant System Boundary -Selection of the boundary influenced by data availability by using either system unavailability requirements or the initiating event frequency limit***
- ***4. Determine the Plant System Safety Significance -High, Medium or Low***



## **Four Steps for Phase II - Determining S/W Failure Impact Type**

- **5. Identify All S/W Failure Modes & Effects** - Assess the interactions of the relevant sub-systems that comprise the plant system to determine the *possible failure impacts of the S/W* for all conceivable failure modes.
- **Credit S/W and Computer System Design Attributes** - This is *an optional additional step* to consider the possibility of S/W and computer system *design attributes for preventing or minimizing specific failure modes*.
- **6. Determine the limiting S/W Failure Impact Type** - Apply the classification criteria to determine *Type 1-3 Failure Impact Type*
- **7. Determine the S/W Category** - Use the determined the plant system S/W failure *Safety Significance* (Column data) and the *S/W Failure Impact Type* (Row Data) to find the S/W Category Matrix intersection value which is the *S/W Category* value
- **8. Determine the limiting S/W Category** - This step is necessary when the application involves *more than one system* or can be *classified as more than one type*. The *most restrictive* category should be used.
- Note that S/W categorization *can be Iterative* - An initial category may be determined and then further analysis may be initiated in order to resolve any issues which arise during the design process

### The Criteria for S/W Failure Impact for Safety or Mitigating Systems

- **Type I** - The designed *nuclear safety functions will not be available* or the **minimum performance requirements of the plant system will not be met** for some or all process system failures.
- **Type II** - The system's functional performance is *degraded* for some or all *process system failures* but the **minimum performance requirements of the plant system will be met**. Or the system's *redundancy is reduced* such that the *probability* of not meeting the minimum performance is *increased*
- **Type III** - The S/W failure has *no impact* on the nuclear safety functions of the plant system

### The Criteria for S/W Failure Impact Type for Process Systems

- **Type I** - The S/W failure can, *in the absence of safety or mitigating system actions*, directly or indirectly *cause systematic fuel failures* or *release of radioactivity* which *could result in doses exceeding* the most restrictive *regulatory dose limit* for the station
- **Type II** - The S/W failure can directly or indirectly *raise the temperature of the fuel* but *not lead to systematic fuel failures*. Or the S/W failure leads to an *increase in probability* of the *Type I consequences* of systematic fuel failure or releases (probability)
- **Type III** - The S/W failure has *no impact* on *the nuclear safety-related reliability performance* of the nuclear safety functions of the plant system

### The Criteria for S/W Failure Impact Type for Testing Systems

- **Type I** - The S/W failure can cause the *designed nuclear safety functions* under test *not to be available* or the *minimum performance requirements of the plant system under test not to be met* for some or all process system failures
- **Type II** - The S/W failure causes an *inaccurate test result* or *degrades the functional performance* of the system under test or causes a *redundancy reduction* in the system under test but the *minimum performance requirements* of the plant system *will still be met* for all process system failures.
- **Type III** - The S/W failure has *no impact* on the *test* or on the *safety-related performance of the system* under test.

**S/W Categorization tabled as a function of Safety Significance & Failure Impact Type**

System Safety Significance	Impact Type I	Impact Type II	Impact Type III
High	Cat. 1	Cat. 2	Cat. 4
Medium	Cat. 2	Cat. 3	Cat. 4
Low	Cat. 3	Cat. 3	Cat. 4

**S/W Categorization 1-4 Process Summary**

- Safety Critical S/W - The standard for Safety Critical S/W **will only be applied to Special Safety Systems** and to **Process Systems** for which the initiating event frequency is **less than  $10^{-3}$  occ/yr.**
- Reduction in S/W Rigour from **Category 1 to 2 Occurs:** If the system **Safety Significance** decreases from **High** to **Medium** while the S/W Failure Impact remains Type I, or if the Safety Significance remains High but the **Failure Impact Type** is reduced from **Type I** to **Type II**.
- **Category III Application** - If the system **Safety Significance** is **Low** and the **S/W Failure Impact Type is I** or the system has a **Medium or Low Safety Significance** and the **Failure Impact Type is II**.
- **Category IV Application:** - If the **S/W Failure Impact Type is III** (no Safety- Related Impact) the S/W is assessed as Category IV.

### **Lecture Summary - CANDU NPP S/W Categorization Methodology**

- Purpose of the S/W Categorization Process
- Necessary Definitions
- Specification of the S/W Categories
- Categorization Process Basis
- Determining Plant System Safety Significance
- Determining S/W Failure Impact Type
- Final S/W Category Determination
- S/W Categorization 1-4 Summary