Typical Design Guide Features - Annunciation as an Example

This lecture will present some of the key features for a **HFE Design Guide** by considering the Annunciation Design Guide as an Example. The consideraations for implementing a pant ageing management program will also be reviewed.

Scope for the Design Guide

- The **Annunciation Design Guide** (DG) provides designers with the project **rationale** and **rules** necessary to specify **consistent alarms** in a format for **standardized** implementation by the HSI's designers.
- Assist designers to **identify the need** for an alarm
- Define hardwired alarms (i.e. so called **'hard' alarms**)
- Define computerized alarms (i.e. so called **'soft' alarms**)
- Provide guidance on **'Handswitch (HS) Off-Normal'** annunciation
- Provide a **summary of alarms** related to the subject design activity

Expected Work Outputs resulting from using this Design Guide:

- A **request form** documenting each **Hard** Annunciation identified
- A **request form** documenting each **Soft** Annunciation identified
- A **summary** of all requested alarms for this design application

Identifying The Need for an Alarm

The potential alarm condition is checked sequentially by the designer as follows to determine if it satisfies the definition of a particular **annunciation type**.

- Check to see if the conditions warrant **specifying a Hard Alarm**
- Check to see if the conditions warrant **specifying a Soft Alarm**
- Check to see if the conditions warrant **specifying a HS Off-Normal Alarm**
- Does this candidate meet the definition for an alarm (**is it an Alarm?**)

Assess the annunciation as a Hard Alarm Candidate

By asking the designer to consider the following questions, **any positive response** will indicate the potential need for a **Hard Alarm** specification.

Could this application provide an alarm which:

- Directly indicates special **safety system actuation**?
- Directly indicates the **requirement** for a special safety system actuation?
- Indicates potential **margin reductions** for Critical Safety Parameters?
- Supports operator **credited safety actions** from the Probabilistic Safety Assessment?
- Indicates a potential **challenge to safety related** systems and support systems, particularly upon loss of the computerized HSI?
- Indicates a potential **threat to plant equipment** upon loss of the computerized HSI?

Assess the condition as a Soft Alarm Candidate

- The annunciation application is next considered as a possible **Soft Alarm** candidate regardless of whether it was already selected as a hard alarm or not.

- That is to say, most hardwired alarms will also be displayed as computerized alarms except for those which do not satisfy the software categorization requirements (i.e. the alarm which indicates the failure of the computerized system).

By asking the designer to consider the following questions, **any positive response** will indicate the potential need for a **Soft Alarm** specification.

Could this application provide an alarm which:

- Indicates **successful performance** of a system, subsystem or component for the specified operating region.
- Indicates **unsuccessful performance** of a system, subsystem or component for the specified operating region.
- Indicates the **health** (i.e. ability to complete the design mission) of a system, subsystem or component.
- Indicates the **health of support functions** for a given system, subsystem or component.

Assess the condition as a HS Off-Normal Alarm Candidate

- Finally, the annunciation application is considered as a possible **HS Off-Normal** alarm candidate only if it has **not been previously selected** as a Hard or Soft alarm.

By asking the designer to consider the following questions, **any positive response** will indicate the potential need for a **HS Off-Normal Alarm** specification.

Could this application provide an alarm which:

- Indicates MCR control panel handswitch position logic that requires operators to be alerted to **HS off-normal** positions (i.e. Not Auto, Transfer Blocked, etc.)
- Indicates conditions for **remote panels** that require alerting the main control room?

Not an Alarm Candidate

- If the above process has been completed for the candidate alarm and the entire review was **negative** (i.e. not a **hard** alarm AND not a **soft** alarm AND not a **HS Off-Normal** Alarm), then this candidate should not be considered further for annunciation purposes - but the documentation should be filed.
- If the designer thinks that the initially proposed Hard alarms that appear rejected could be of importance, then these alarms should be documented as such and sent to the control centre HSI designer with an appropriate explanation (i.e. experience or **judgment based recommendation**).

Completing the Hard Alarm Request Form to Define Hard Alarms

- The designer should check that all **Hard alarm** candidates are considered **essential** for the operator in the absence of the computerized HSI.

The designer must then complete the **Hard Alarm Request Form** to:

- Specify the **purpose** of the alarm
- **Assign a window** identification number (i.e. physical location)
- Propose the window **message content**
- **Cross-Reference** the related **Soft alarm** identification number
- List the associated **reference information** for this Hard Alarm.
- Add this new Hard alarm to the **Alarm Summary List**

Purpose of the Hard Alarm

- Briefly document the **rationale** for selecting this hard alarm. The rationale can just be a specific statement of the checklist question which **identified the need** for this alarm.

- The designer should consider if the alarm purpose could change dependent upon the **current operating region** of the plant.

- **Any special conditions** associated with the purpose of the alarm should be stated on the request form.

Hard Window Alarm Identification Number

- Each Hard Alarm must be assigned a **unique annunciation number** which allows database tracking.

- The method used in CANDU 9 is a **six digit number** preceded by **W** for window.

- The first three digits are from the host **system identification number** (SIN) while the last three numbers are the **unique alarm serial number** for that system.

- **W- SIN - 123**

Completing the Hard Alarm Request Form ....continued

Proposed Hard Alarm Message Content

- Designers should include a **suggested message** for the hard alarm window on the form.
- The message text is to be written without acronyms or abbreviations but appropriate acronyms can be included in parentheses.
- The final alarm message will be prepared by the control centre HSI designer with the agreement of the system designer.
- As a minimum for each alarm, the system designer must **identify the associated component** or subsystem (i.e. Heat Transport Pumps) and the **consequences** of this alarm (i.e. one PHT pump is not running so a Reactor Stepback is initiated)

Hard/Soft Alarm Cross-Referencing

- The system designer must specify the **associated logical set of parameters** and **values** that can turn the window **ON** signifying that the alarm condition is true.
- The provision of a **formula** or a reference to the associated **logic diagram** is acceptable.
- The system designer must also record **the associated computerized alarm identification numbers** that represent the same component conditions.

Hard Alarm Reference Information

- The system designer must provide additional reference information necessary to **define and understand** the **alarm and alarm context**.
- Provide the **complete System Identification Number**
- Provide the **associated elementary** wiring drawing identification number.
- Provide the **instrument loop number** within which the alarm devices reside.

Add this new Hard alarm to the Alarm Summary List

- Once the new **Hard Alarm** has been **fully defined**, the **alarm number** and **alarm purpose** should be added to the **Alarm Summary List**.

Defining Soft Alarms

- The designer should **confirm** that the proposed alarm is a **Soft alarm** and then to further categorize the alarm as a **Fault** or **Status** alarm.
- **Fault Alarm** - the **failure** of a process, system or component **to perform as required** for the plant situation (i.e. pump motor trip)
- **Status Alarm** - the **change in the control mode** for the plant or the change in state of a process, system or component in response to a change in the operating state of the plant (i.e. Reactor Stepback Initiated)

The designer must complete the **Soft Alarm Request Form** to:

- **Confirm Soft** Alarm Candidate and assign alarm type (**Fault** or **Status**)
- Assign a Soft Alarm **Identity Number**
- List the associated **reference information** for this Soft Alarm.
- Propose the Soft Alarm **message content**
- Describe the **expected operator response** to this alarm
- Add this new Soft alarm to the **Alarm Summary List**

Confirm Soft Alarm Candidate and assign alarm type (Fault or Status)

By asking the designer to consider the following questions, **any positive response** will indicate the potential need for a **Soft Fault Alarm** specification.

Could this application provide an alarm which identifies:

- A challenge to **operational goals**?
- Or requires a PSA **Safety Credited Action** by the operator?
- A change in, or potential challenge to, **system function** inconsistent with the operating situation?
- Changes in process conditions that represents a **departure from the expected** process value for the operating situation?
- Potential **violations of the Operating Policies** and Procedures?
- **Equipment failure** or loss of functionality?

If the alarm was confirmed as a **Soft Fault alarm**, the remainder of the Soft Alarm request form would be completed. Otherwise, the candidate alarm would be **checked** further to identify if it was a **Soft Status alarm**.

Confirm Soft Alarm Candidate and assign alarm type (Fault or Status)...continued

Assuming the designer did not obtain a positive Soft Fault confirmation, then the candidate alarm is checked further to see if it could be a Soft Status Alarm. By asking the designer to consider the following questions, **any positive response** will indicate the potential need for a **Soft Status Alarm** specification.

Could this application provide an alarm which identifies:

- A successful **automation action** in response to disturbances or failures?
- Successful **changes in equipment state** or control modes fundamental to the basis of the plant state.
- Successful **changes in plant/system mode**?

Not a Soft Alarm Candidate

- If the above process has been completed for the candidate soft alarm and the entire review was **negative** (i.e. not a **Soft Fault** alarm AND not a **Soft Status** alarm), then this soft alarm candidate should be rejected and documented as not being considered further for annunciation purposes.
- If the designer thinks that the initially proposed alarms that appear rejected could be of importance, then these alarms should be documented as such and sent to the control centre HSI designer with an appropriate explanation (i.e. allow experience or judgment recommendations).

Assign a Soft Alarm Identity Number

- Each Soft Alarm must be assigned a **unique annunciation number** which allows database tracking.
- The method used in CANDU 9 is a **six digit number** just like the hard alarm identity (system identification plus serial number) but this is **preceded by four characters** to identify the alarm source (i.e. AI, DI, Control Program) and is **trailed by three qualifier characters** (i.e. LOW, VHI, IRR, etc.)
- **SGLC - SIN - 123 - LOW**

Confirm Soft Alarm Candidate and assign alarm type (Fault or Status)...continued

List the associated reference information for this Soft Alarm.

- The system designer must provide additional **reference information** necessary to **define and understand** the **alarm and alarm context**.
- Provide the complete **System Identification Number**
- Provide the associated elementary wiring drawing identification number.
- Provide the **instrument loop number** within which the alarm devices reside.

Defining the Soft Alarm

- Briefly document the **rationale** for selecting this **type** of soft alarm. The rationale can just be a specific statement of the checklist question which **identified the need** for this alarm.
- The designer should consider if the alarm purpose could change dependent upon the **current operating region** of the plant.
- **Any special conditions** associated with the purpose of the alarm should be stated on the request form (i.e. can the alarm be **soft jumpered**?).
- The data **source** of the soft alarm and the scan interval required should be stated.
- The soft alarm **setpoint** should be stated as well as the recommendation for **tunable parameter range limits**.
- The **consequences** for the plant when this alarm occurs
- Designers should include a **suggested text** for the soft alarm message on the form.
- The **message text** is to be written without acronyms or abbreviations but appropriate acronyms can be included in parentheses.
- The final alarm message will be prepared by the control centre HSI designer with the agreement of the system designer.

Confirm Soft Alarm Candidate and assign alarm type (Fault or Status)...continued

Describe the expected operator response to this alarm

- The probable cause, resultant automatic actions and the **necessary operator actions** and **checks** must be recorded for each soft alarm.

- If the response is dependent on the **operating region**, the designer should note this fact and attach a more detailed **operating region response** explanation.

Soft/Hard Alarm Cross-Referencing

- The system designer must specify the **associated logical set of parameters and values** that can initiate the soft alarm signifying that the alarm condition is true.

- The provision of a **formula** or a reference to the associated **logic diagram** is acceptable.

- The system designer must also record **the associated hard alarm identification numbers** that represent the same component conditions.

Add this new Soft alarm to the Alarm Summary List

- Once the new **Soft Alarm** has been **fully defined**, the alarm number and alarm purpose should be added to the **Alarm Summary List**.

Defining Handswitch Off-Normal Alarms

- The Handswitch Off-Normal annunciation provides a warning to the operator if a panel **handswitch** is placed in an **unexpected** or incorrect position.
- This type of alarm is required for those applications where the incorrect position of the handswitch can have a direct and **potentially immediate influence** on the safety, reliability or production capability of the generating station.
- The operator is made aware of this condition by a **local alerting feature** located on the control panel.
- The designer is required to submit a memo to the control centre HSI design team requesting the annunciation, describing the functions and logic of the handswitch, identifying the **Off-Normal positions** and their **associated potential consequences** for plant operations.

Remote Annunciations

- **Local field panel annunciations** may be required for the same reasons as described for hard MCR alarms.
- The designer is required to submit a memo to the control centre HSI design team requesting the provision of local field annunciation using the same information identified in the Hard Alarm request Form
- Where it is necessary for the control room staff to be alerted to the actuation of alarms at local field panels, the system designer is requested to submit a memo to the control centre HSI design team requesting MCR **annunciation for remote field annunciations**.

Typical Annunciation Design Guide Contents

- This summary presents a **suggested table of contents** that could be provided by a sample Annunciation Design Guide to assist in the development of such a design guide for a specific project application.

1. **Scope** of the Design Guide
2. Identifying the **Need for an Alarm** (Hard, Soft, Off-Normal)
3. **Confirming** a Hard Alarm
4. **Defining** a Hard Alarm (purpose, ID, inputs, reference & message)
5. **Confirming** a Soft Alarm
6. **Defining** a Soft Alarm
7. Describe the **expected operator responses** to an alarm
8. Specifying a **Handswitch Off-Normal** Alarm
9. Specifying **the need for Remote Annunciation**

Appendices:

Appendix A Hard Alarm Request Form

Appendix B Soft Alarm Request Form

Appendix C Summary of Alarms (ID Number and Purpose)

Plant Ageing Design Guide Considerations

The purpose of this lecture is to introduce the concepts needed to implement an effective ***ageing management program*** for a major project to ensure that the ***plant life goal*** is achieved successfully

- These ***ageing considerations*** could be used to form the basis of a design guide so as to be able to implement the necessary design features within the project life-cycle.

- Related topics for consideration would include ***design***, ***procurement***, ***construction***, ***commissioning***, ***operation***, ***maintenance*** and ***replacement/refurbishing***.

- There are two aspects that need to be addressed by an ageing management program - ***safety performance*** and ***general performance*** capability.

- Safety performance addresses the need to ensure that the plant continues to ***meet all of the defined safety requirements*** throughout the specified plant life.

- General performance capability relates to the ability of the plant to continue ***operating economically*** over the desired life of the facility.

Requirements Related to Plant Ageing

- The project ***design life must be defined*** - for example 40 years operation.

The key project components can be classified as follows for ***replacement consideration***:

- **Critical, non-replaceable** components - take the project design life into account. Assurance of component life will be supported by condition monitoring, inspection, and maintenance.
- **Critical, replaceable** components - design provisions (such as lay-down areas, routing path access, craning, etc.) are made to allow for planned component replacement.
- **Non-Critical, non-replaceable** components that can be designed for the plant life expectancy
- **Non-Critical, replaceable** components

General Regulatory Requirements

- Nuclear regulatory requirements require NPP's to develop and maintain an ***ageing program*** to ensure that the conditions for the facility licensing basis are always satisfied.

The ***NPP ageing program*** should be ***auditable*** and provide ***effective management of ageing degradation***:

- Of any component which could ***increase the probability*** or ***consequence*** of process system failures.
- Of any safety support or other safety related system that could ***reduce the reliability*** or ***effectiveness*** of a special safety system
- That could cause key system parameters such as pressure drop, flow or heat transfer rates to change to the extent that ***limits assumed*** in the ***safety analysis are exceeded.***
- Detailed ***safety and performance design requirements*** must be derived for each system in the design requirement documents for the critical system, structure or component (SSC).
- Potential ageing degradation mechanisms that may impact the critical SSC should be reviewed, identified, addressed and documented within the design cycle.

General Design Methodology

- ***Identification*** of Critical systems, structures and components (SSC).

- Critical SSC are those that if failed will have a **major impact** on the **plant safety, long term reliability** and **life of the plant.**

A component is classified as **critical** if it meets one or more of the following conditions:

- **Safety and Environmental Protection** - Failure results in an inability to meet licensing requirements in terms of public safety, worker safety or environmental protection.
- **Plant Reliability** - failure could lead to a long forced outage reducing plant reliability
- **Cost** - the cost of refurbishment or replacement is significant

A component is classified as ***non-critical*** if the SSC ***do not directly impact plant safety or plant reliability*** and hence can be replaced or maintained during the maintenance call-ups or regular scheduled outages.

Component Selection Process for Ageing Considerations

A ***systematic examination*** of all systems, structures and components from safety and performance perspectives must be completed in order to select those components that should be considered for ageing:

- Does the plant system or structure contribute to ***plant safety or performance*** - to provide a short list of systems and structures for further component evaluation.
- Would the failure of the component result in ***plant incapability and/or impairment*** of the ***system's availability or safety related functions***
- Does ***Ageing Degradation*** have the potential to cause failure or impairment of identified components
- Are current ***inspection and maintenance plans adequate*** for timely detection of significant ageing degradation?

Classification of Critical SSC's

- All the critical SSC's identified in the selection process must be categorized as either a ***Replaceable*** or ***Non-Replaceable*** component.
- ***Replaceable Components*** - are those components which ***cannot be economically designed to function for the entire design life*** of the plant and for which the replacement activity is feasible.
- ***Non-Replaceable Components*** - are those components whose failure will cause ***significant economic cost including significant lost production revenue***. These should be designed for the entire life of the plant.

General Design Provision

Designers will need to ***incorporate appropriate provisions*** for the applicable ageing mechanism. The following illustrative list of ***general design considerations*** is used to decide the appropriate design features or activities needed to achieve the required design life:

- Review ***performance requirements and experience*** for that component for other similar operating facilities
- Determine ***required and achievable design life*** duration and ***replacement frequency.***
- Define component ***storage conditions*** and 'shelf' life
- Determine the optimum design approach to ***meet performance and design life requirements***.
- Provide ***optimal environment*** and choose proper materials
- Try to ***standardize on the materials*** selected (elastomers, lubricants, etc.) where practicable in order to reduce the types required.
- Provide corrosion, wear and ageing ***allowances*** in the specification
- Specify the design life and the design ***mission conditions***
- Identify ***the methods of coping with ageing effects*** over the life of the plant.
- Specify ***necessary qualification and assurance programs***
- Specify necessary ***inspection, testing and maintenance activities*** and their frequencies.
- Ensure ***plant layout*** and equipment arrangement allows ***inspection, maintenance and replacement access***, including transportation routing
- Design for ***on-line in-situ maintenance*** where practicable
- Specify any special monitoring, inspection or maintenance ***tools and equipment***
- Ensure recommended ***replacement parts and procedures*** are specified to facilitate station configuration management.
- Consider potential ***obsolescence*** of equipment and spare parts and document accommodating strategies
- The design should include features or instrumentation which can assist in ***estimating the remainder of useful operating life***.
- Identify those SSC's which are ***safety-related*** and must comply with the safety design guides.
- Identify SSC's that suffer ***undue ageing*** and initiate related ***R&D activities*** to improve the performance.

Ageing Management Program

The design information must be used by the operations organization to prepare and implement an ***auditable plant ageing management program*** that should address the following aspects:

- An ***in-service inspection program.***
- Effective ***monitoring of ageing degradation*** in the SSC's
- Preventive maintenance program that ensures ***timely refurbishment*** or ***replacement of components*** prior to their failure to function at the required level of performance and reliability.
- An ***environmental qualification program*** that provides assurance that the plant components that must function under harsh conditions will do so at any time during their design lives.
- A ***component performance monitoring process*** that provides valid data on component failure rates for updating reliability reports and probabilistic risk assessments.
- ***Operating practices and maintenance programs*** that are designed to effectively control the rate of ageing degradation or to mitigate the effects.
- Periodic ***reviews of major process systems operating characteristics*** for comparison with safety analysis assumptions.
- A formal periodic ***audit of the on-going ageing management program***