MODELO DE PLAN PRELIMINAR DE VALIDACIÓN Y VERIFICACIÓN PARA EL SISTEMA DE PROTECCIÓN DEL REACTOR CAREM

Fittipaldi, A.[1], Maciel, F.[2]
[1] Centro Atómico Bariloche, CNEA, fittipal@cab.cnea.gov.ar
[2] Centro Atómico Bariloche, CNEA, macielf@cab.cnea.gov.ar

PRELIMINARY VALIDATION AND VERIFICATION PLAN FOR CAREM REACTOR PROTECTION SYSTEM

Abstract

The purpose of this paper, is to present a preliminary validation and verification plan for a particular architecture proposed for the CAREM reactor protection system with software modules (computer based system).
These software modules can be either own design systems or systems based in commercial modules such as programmable logic controllers (PLC) redundant of last generation.
During this study, it was seen that this plan can also be used as a validation and verification plan of commercial products (COTS, commercial off the shelf) and/or smart transmitters.
The software life cycle proposed and its features are presented, and also the advantages of the preliminary validation and verification plan.

Objetivos

Este trabajo tiene como objetivo presentar el desarrollo de un plan preliminar de validación y verificación para una propuesta de arquitectura del sistema de protección del reactor CAREM con módulos de software (computer based system).
Estos módulos de software pueden provenir ya sea de sistemas de desarrollo propio o sistemas basados en módulos comerciales tales como los controladores lógicos programables (PLC) redundados de nueva generación.
Durante este estudio se ha podido apreciar que este plan puede también ser utilizado como plan de validación y verificación de productos comerciales "de estantería" (COTS) y/o sensores inteligentes.
También se presentan el ciclo de vida de software propuesto y las características y ventajas del plan preliminar de validación y verificación.

Procedimientos

En el principio de este estudio se realizaron reuniones con expertos de la autoridad regulatoria nacional (ARN) para definir la normativa a aplicar en el sistema de protección del reactor y el sistema de supervisión y control y la metodología para realizar la validación y el licenciamiento de las arquitecturas propuestas y sus componentes asociados (sistemas comerciales "de estantería"(COTS), buses de campo, controladores lógicos programables(PLC)) para el sistema de protección del reactor CAREM.
Como parte de este trabajo también se llevo a cabo un estudio comparativo en profundidad de las normas nacionales e internacionales aplicadas en los sistemas de

protección de las centrales nucleares de potencia basados en software (USA, UK, FRANCIA, CANADA, JAPON, KOREA) [1] y documentos asociados; que hacen a la producción y ciclo de vida de software de alta confiabilidad para sistemas asociados a la seguridad en reactores nucleares.
A partir de lo anteriormente mencionado se pudo definir la normativa relevante en base a la cual podía comenzar el trabajo de definición del ciclo de vida y plan de validación y verificación del software.
Esta elección de normativa también lleva a una definición del proceso de desarrollo del software, su QA (quality assurance) y configuration management, que serán oportunamente desarrollados.

Basado en estos estudios se llevo a cabo la consolidación de un posible modelo de ciclo de vida de software. Este modelo fue concebido de tal manera que se pueda aplicar tanto para el desarrollo propio de los módulos de software como para la integración del sistema de protección con módulos de software previamente desarrollados (comerciales o no)

El modelo de ciclo de vida de software consolidado consiste en una variación sobre el ciclo de vida tomado como referencia en los documentos de la IAEA, IEC, ISA. [2,3,4]

Este consta de las siguientes fases: (ver Figura 1)

- Requerimientos del sistema de seguridad: esta fase consiste en la extracción de un conjunto completo y exhaustivo de requerimientos que debe cumplir el sistema de seguridad en el que se esta trabajando y deben surgir del análisis de comportamiento de la planta en condiciones normales de operación y en condiciones de los accidentes base de diseño y del informe final de seguridad.
- Requerimientos del sistema digital: esta fase divide las funciones entre hardware y software para permitir el desarrollo de los requerimientos individuales. Los requerimientos derivados son requerimientos de hardware, requerimientos de software y requerimientos de integración.
- Requerimientos de Hardware: son las bases para el diseño y/o validación del hardware.
- Requerimientos de Integración del sistema: son las bases para la integración del hardware y el software en el sistema digital así como para la integración del mismo en la planta.
- Requerimientos de Software: Son la base de diseño del software y debe contener todo lo necesario para el desarrollo del mismo; esto se ha dividido considerando la separación entre el llamado software de base (operativo, monitores, etc.) y el denominado software de aplicación (donde esta implementada la funcionalidad requerida del sistema).
- Requerimientos de Integración del Software: son la base para la integración del software en el caso de existir la separación antes citada (software de base, software de aplicación)
- Diseño de Software de Base: esta fase tiene tres actividades diseño del software de base, especificación detallada del módulo y diseño del módulo.
- Diseño de Software de Aplicación: esta fase tiene tres actividades diseño del software de aplicación, especificación detallada del módulo y diseño del módulo.
- Codificación de Software de Base: esta fase traduce el diseño del software de base en el lenguaje de programación.

- Codificación de Software de Aplicación: esta fase traduce el diseño del software de aplicación en el lenguaje de programación.
- Integración de Software: consiste en la reunión del software de base y el de aplicación en un código fuente en formato adecuado para ser leído y procesado por una computadora; se ejercita el software integrado por simulación estática y dinámica de entradas y salidas.
- Integración Hardware - Software: el sistema se ejercita por simulación estática y dinámica de las señales de entrada.
- Prueba de Instalación: es la prueba y validación del sistema en campo.

Este ciclo de vida del software es compatible y cumple con lo requerido por la normativa de la autoridad reguladora nacional ARN. [5]

Basado en este modelo de ciclo de vida se llevo a cabo el desarrollo de un plan de Validación y Verificación versátil capaz de abarcar las posibles variantes en la gestión de productos (documentos de salida de cada fase y eventualmente el código) de las sucesivas fases (ver Figura 1).
Este plan consiste en:

1. Verificar cada etapa del ciclo de vida del software donde fuera posible:
    - Módulos de desarrollo propio, por ejemplo: Requerimientos del software de aplicación, Diseño del software de aplicación, Codificación del software de aplicación.
    - En caso de desarrollo propio del software de base: Requerimientos del software de base, Diseño del software de base, Codificación del software de base, etc.
2. Validar por medio de pruebas, tablas, etc., aquellos módulos que no son de desarrollo propio, y/o en los cuáles no es posible llevar a cabo un proceso de verificación, por ejemplo: en el caso de PLCs ó COTS, el software de base ó el hardware.

Concluidos los puntos 1 y 2 y después de llevar a cabo el proceso de instalación del sistema y sus pruebas correspondientes, se realiza una validación final del sistema completo.

Resultados

Entre los resultados obtenidos se consolido la normativa guía a aplicar durante el proceso de desarrollo del software y el proceso de validación y verificación del mismo
También se ha definido una estructura preliminar de ciclo de vida de software capaz de abarcar tanto el desarrollo propio de módulos de software del sistema como la integración de módulos predesarrollados propios o provenientes de productos comerciales. [5]
Además, se definió un plan preliminar de validación y verificación aplicable al ciclo de vida de software previamente citado

Conclusiones

El plan preliminar de validación y verificación desarrollado al presente tiene la flexibilidad necesaria para hacer frente a las distintas posibilidades de arquitectura bajo estudio (arquitectura propia basada en COTS, buses de campo, MIL-STD- 1553, Trip Unit basada en software ó arquitectura basada en PLCs, u otras alternativas) sin comprometer la calidad e integridad del proceso de verificación y validación de las tareas del ciclo de vida del software y del sistema de protección en sí mismo.

Dado el alcance de estas tareas, se está en permanente consulta y discusión con los expertos de la autoridad reguladora nacional (ARN), a fin de consolidar un plan óptimo de V&V del sistema de protección para el licenciamiento de la planta.

Queda bajo estudio y para un futuro trabajo, el flujo detallado de documentación y definir las tareas a realizar en cada fase del ciclo de vida del software, así como también definir el proceso de desarrollo del software, su QA (quality assurance) y configuration management, que serán oportunamente desarrollados.

Referencias

1- AECB/NII/USNRC/DSIN - "Four party regulatory consensus report on the safety case for computer-based systems in nuclear power plant"
2- IAEA TRS384 – "Verification and validation of software related to nuclear power plant instrumentation and control"
3- IEC 880 – "Software for computers in the safety systems of nuclear power stations"
4- IEC 61508 – "Functional safety of electrical/electronic/programable electronic safety-related systems"
5- Norma AR 1.4.1.(draft) "Sistemas digitales relacionados con la seguridad de instalaciones relevantes"

Figuras

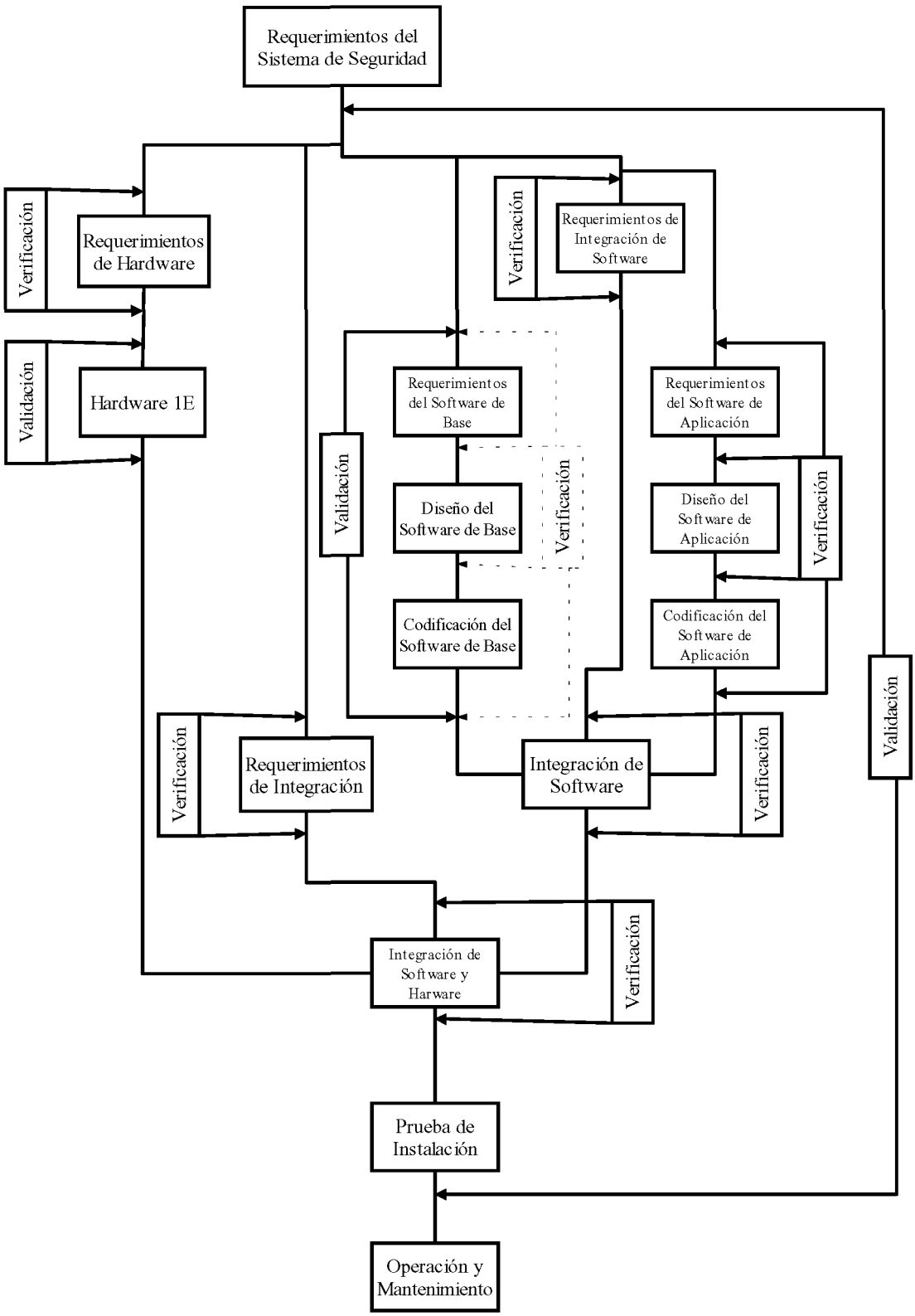

Figura 1