Safety I&C System Platform Requirements Technical Report

- Introduction
- Proposed Table of Contents
- Detail Requirements (Examples)

Introduction

Status of Platform Requirements TeR (APR1400-Z-J-NR-14002)

- **NRC letter comments (Dec. 19, 2013)**
  - "The application did not provide sufficient information for the critical characteristics, such as deterministic performance and the software development process of the safety I&C system platform."
- **KHNP plan proposed at the 13th PARM (Feb. 11, 2014)**

TS

**** New regulatory guidance : RG 1.152, IEEE Std. 7-4.3.2, DI&C-ISG-04, etc.***

Introduction

Status of Platform Requirements TeR

- **NRC Major Feedbacks and Comments**

TS

Introduction

Objective of This Meeting

- **Present revised table of contents based on;** **TS**

- **Present excerpts from two sections in detail for NRC review and comment.**
  - Section 4.4, “Platform integrity characteristics requirements”
  - Section 4.5, “Communications independence requirements”

Table of Contents

Table of Contents of TeR

SCOPE

Scope of the Platform

TS

Table of Contents

4.0 Technical Requirements

- **4.1 Platform Requirements**
  - Hardware Requirements
    - General Redundancy Requirements
    - Modules (Processor, Input, Output, Communication, WDT)
    - Safety VDU
  - Software Requirements
    - System Software
    - Application Software
    - Software Tools

Table of Contents

4.0 Technical Requirements (Cont'd)

- **4.1 Platform Requirements (Cont'd)**
  - Diagnostics and Self-Test Requirements
    - Processor Module
    - Input / Output Module
    - Serial Data Link
    - Safety System Data Network
    - Watchdog Timer
  - Safety VDU
  - Electrical Requirements

Table of Contents

4.0 Technical Requirements (Cont'd)

- **4.2 Software Development Process Requirements**
  - Software Management Plan
  - Software Development Plan
  - Software QA Plan
  - Software Integration Plan
  - Software Installation Plan
  - Software Maintenance Plan
  - Software Training Plan
  - Software Operations Plan
  - Software Safety Plan
  - Software Safety Verification and Validation Plan
  - Software Configuration Management Plan
  - Software Test Plan

Table of Contents

4.0 Technical Requirements (Cont'd)

- **4.3 Environmental Qualification Requirements**
  - Qualification Program
  - Environmental Qualification
  - Seismic Withstand Testing
  - Electromagnetic Compatibility Testing (i.e., EMI/RFI, SWC)

Table of Contents

4.0 Technical Requirements (Cont'd)

- **4.4 Platform Integrity Characteristic Requirements (Example)**
  - Response Time
  - Deterministic Performance
  - Failure Modes and Effects Analysis
  - Reliability and Availability Analysis
- **4.5 Communications Independence Requirements (Example)**
  - Communications with Safety Channels
  - Communications with Non-safety Systems
  - Staff Guidance in DI&C-ISG-04

Table of Contents

4.0 Technical Requirements (Cont'd)

- **4.6 Secure Development and Operational Environment Requirements**
  - Concept Phase
  - Requirement Phase
  - Design Phase
  - Implementation Phase
  - Test Phase
- **4.7 Commercial Grade Dedication Program**
  - Scope
  - Review Plan
  - Review Report

Table of Contents

4.0 Technical Requirements (Cont'd)

- **4.8 Requirements for IEEE Std. 603-1991**
  - Clause 4, "Safety System Designation"
  - Clause 5, "Safety System Criteria"
  - Clause 6, "Sense and Command Features - Functional and Design"
  - Clause 7, "Execute Features – Functional and Design"
  - Clause 8, "Power Source Requirements"
- **4.9 Requirements for IEEE Std. 7-4.3.2-2003**
  - Clause 5, "Safety System Criteria"

Detail Requirements (Example)

4.4 Platform Integrity Characteristic Requirements

- **Response Time**
- **Deterministic Performance**
- **Failure Modes and Effects Analysis**
- **Reliability and Availability Analysis**

Platform Integrity Characteristics Requirements

Response Time

- **NRC Guidance**
  - To meet the requirements of GDC 20, 21, 23 and 25, SRP BTP 7-21 provides the following guidance:
    - *"Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture so that the entire system meets its timing requirements."*
    - *"Timing requirements should be satisfied by design commitments."*

Platform Integrity Characteristics Requirements

Response Time (Cont'd)

- **Platform Requirements**
  - The overall response time shall be deterministic*.
  - The overall response time shall be demonstrated by allocating a timing budget to all components in the signal path.
  - The overall response time from input exceeding its trip setpoint to the resulting output actuation shall be 100 millisecond (ms) or less under the configuration of section 4.2.3.2 in EPRI TR-107330.
  - The overall response time shall be determined by combining the response time of individual components in control processes.
  - Analog Input module shall have a response time of 20 ms from reading a 0-1 V, 0-10 V or 4-20 mA signal to putting the value on the backplane for processor.

*Deterministic : As used in this TeR, the property of a program which assures that it will be completely executed within a specific time frame.

Platform Integrity Characteristics Requirements

Response Time (Cont'd)

- **Platform Requirements (Cont'd)**
  - Analog Input module shall have a response time of 100 ms from reading a thermocouple or resistance temperature detector signal to putting the value on the backplane for processor.
  - Digital Input module shall have a response time of 8 ms from reading a contact input to putting that value on the backplane for processor.
  - Digital Output module shall have a response time of 12 ms from time the function processor completes its execution cycle to when the state changes at the digital output.
  - Serial Data Link (SDL) shall have a response time of 13 ms from putting a value in one Processor to receiving that value in another processor.
  - The overall response time shall consider the effects of any input filtering on the response.

Platform Integrity Characteristics Requirements

Response Time (Cont'd)

- **Platform Requirements (Cont'd)**
  - Testing and analytic justification shall show that the system meets response times for a selected subset of system loads, conditions, and design basis events.
  - When calculating response times, two scan times shall be assumed to cover the case where the input achieves a trip value just after the scan of the application program starts.
  - The overall response time shall include any self-diagnostic and redundancy implementation features including any redundant processor synchronization, processor-to-processor communication and execution of the associated algorithms.
  - Platform vendor shall provide all supporting data for response time analysis.

Detail Requirements (Example)

4.4 Platform Integrity Characteristics Requirements

- Response Time
- **Deterministic Performance**
- Failure Modes and Effects Analysis
- Reliability and Availability Analysis

Platform Integrity Characteristics Requirements

Deterministic Performance

- **NRC Guidance**
  - SRP Chapter 7, Appendix 7.1-C, Section 6.1, *"Automatic Control," advises the evaluation should confirm the system's real time performance is deterministic and known.*
  - SRP BTP 7-21 requires that the following design practices for computer-based systems should be avoided.
    - *Non-deterministic data communications*
    - *Non-deterministic computations*
    - ***Interrupts***
    - ***Multitasking***
    - *Dynamic scheduling*
    - *Event-driven design*

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Platform Requirements**
  - Software processing in Function Processor (FP) and communication between Communication Processors (CPs) shall be deterministic.
  - System software and application software shall read all inputs, process all logics, and send all outputs within its cycle time.
  - System software shall initiate cyclic safety application execution using a precision interval timer with a 10 ms or faster interval.

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Platform Requirements (Cont'd)**
  - If multi-tasking is used, safety application programs shall be assigned higher priority than other supporting programs.
  - FP shall update its hardware watchdog timers cyclically.
  - System software and application software shall not perform dynamic memory allocation.
  - The following shall not prevent FP from continuing to execute safety function.
    - Input/output failures in I/O modules
    - Input/output failures in communication modules
  - Safety application program's priority shall be based on program cycle time (Faster cycle time means higher priority).

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Platform Requirements (Cont'd)**
  - Hardware watchdog timer shall detect when the execution time is exceeded.
  - All communication interfaces shall be conducted by CP, functionally isolating communications from FP.
  - No communication error shall inhibit the safety application programs performing their safety functions within the designed execution cycle.
  - Indication of system error status shall be available to the application software, along with methods to detect and recover from errors.

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Platform Requirements (Cont'd)**
  - The response time requirement shall be met with any latency time attributed to:
    - Providing synchronization (CPU Redundancy)
    - Detecting errors
    - Recovery from errors

- **Exceptions to NRC guidance in Platform**
  - Multi-tasking.
  - Pre-defined interrupt for multi-tasking.

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Requirements for interrupt and multitasking justification** TS

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Requirements for interrupt and multitasking Justification (Cont'd)** TS

Platform Integrity Characteristics Requirements

Deterministic Performance (Cont'd)

- **Requirements for interrupt and multitasking Justification (Cont'd)** **TS**

Detail Requirements (Example)

4.4 Platform Integrity Characteristic Requirements

- Response Time
- Deterministic Performance
- **Failure Modes and Effects Analysis**
- Reliability and Availability Analysis

Platform Integrity Characteristics Requirements

Failure Modes and Effects Analysis

- **NRC Guidance**
  - *RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," describes an acceptable method for the single-failure criterion to the platform.*
  - *RG 1.53 endorsed IEEE Std. 379-2000, Clause 5.5 identifies Failure Mode and Effects Analysis (FMEA) as a method to address common-cause failures when performing analysis to demonstrate the single-failure criterion has been met.*
- **Regulatory Criteria**
  - *IEEE Std. 603 Clause 5.1, "Single-Failure Criterion" endorsed "IEEE Std. 352 and IEEE Std. 577 provide guidance for reliability analysis.*

Platform Integrity Characteristics Requirements

Failure Modes and Effects Analysis (Cont'd)

- **Platform Requirements**
  - Platform vendor shall identify the built-in system diagnostics to support system level FMEA.
  - Platform vendor shall identify failure modes (including communication) that should be handled by system level FMEA.
  - Platform vendor shall provide sufficient detail of the potential failures and the effects of those failures.

Detail Requirements (Example)

4.4 Platform Integrity Requirements

- Response Time
- Deterministic Performance
- Failure Modes and Effects Analysis
- **Reliability and Availability Analysis**

Platform Integrity Characteristics Requirements

Reliability and Availability Analysis

- **Regulatory Criteria**
  - IEEE Std. 603-1991 Clause 4.9
    - Requires the identification of *the methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative of quantitative reliability goals that may be imposed on the system design.*
  - IEEE Std. 603-1991 Clause 5.15
    - States that *for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved, and that IEEE Std. 352-1987 and IEEE Std. 577-1976 provide guidance for reliability analysis.*

Platform Integrity Characteristics Requirements

Reliability and Availability Analysis (Cont'd)

- **NRC Guidance**
  - RG 1.152
    - *The acceptance of the reliability of computer systems is based on deterministic criteria for both hardware and software.*
    - *The NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for the reliability of digital computers used in safety systems.*
    - *Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of computer systems.*

Platform Integrity Characteristics Requirements

Reliability and Availability Analysis (Cont'd)

- **Background**
  - Determination of the reliability of a safety system is an application-specific activity that requires an assessment of a full system design.
  - The evaluation against this requirement is limited to consideration of the reliability characteristics of the platform and its components.
  - Two probabilities calculated include:
    - The characteristic of an item or system expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.(reliability as defined by EPRI TR 107330)
    - The degree to which a system or component is operational and accessible when required for use. Often expressed as a probability. (availability as defined by IEEE 610.12-1990(R2002).

Platform Integrity Characteristics Requirements

Reliability and Availability Analysis (Cont'd)

- **Platform Requirements**

TS

Platform Integrity Characteristics Requirements

Reliability and Availability Analysis (Cont'd)

- **Platform Requirements (Cont'd)**

TS

Detail Requirements (Example)

4.5 Communications Independence

- **Communications with Safety Channels**
- **Communications with Non-Safety Systems**
- **Staff Guidance in DI&C-ISG-04**

Communications Independence

Communications with Safety Channels

- **Platform Requirements**

TS

Communications Independence

Communications with Safety Channels (Cont'd)

- **Platform Requirements**

TS

Communications Independence

Communications with Safety Channels (Cont'd)

- **Platform Requirements**

TS

Detail Requirements (Example)

4.5 Communications Independence

- Communications with Safety Channels
- **Communications with Non-Safety Systems**
- Staff Guidance in DI&C-ISG-04

Communications Independence

Communications with Non-Safety Channels

- **Platform Requirements**

TS

Detail Requirements (Example)

Communications with Non-Safety Channels (Cont'd)

- Communications with Safety Channels
- Communications with Non-Safety Systems
- **Staff Guidance in DI&C-ISG-04**

Communications Independence

Staff Guidance in DI&C-ISG-04

- **Regulatory Criteria**
  - IEEE Std. 603-1991 Clause 5.6, *"Independence," requires independence between*
    - *Redundant portions of a safety system*
    - *Safety systems and the effects of design basis events*
    - *Safety systems and other systems*
- **NRC Guidance**
  - SRP Chapter 7, Appendix 7.1-C, Section 5.6, *"Independence," provides acceptance criteria for this requirement*
    - *Physical independence*
    - *Electrical independence*
    - *Communications independence*

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **NRC Guidance**
  - DI&C-ISG-04 contains staff positions on four areas of interest:
    - *Interdivisional communications*
    - *Command prioritization*
    - *Multidivisional control and display stations*
    - *Digital system network configuration*
  - DI&C-ISG-04 addresses *"Systems with platform which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the 20 positions described in DI&C-ISG-04."*

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **Section 1 Requirements Specific to Platform and System**

DI&C-ISG-04 Positions	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Platform Requirements TeR				O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O
Safety I&C System TeR	O	O	O		O		O	O		O	O	O	O				O	O	O	O

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **NRC Guidance**
  - Position 4 : "*The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information….*"

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **Platform Requirements**

TS

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **Platform Requirements**

TS

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **NRC Guidance**
  - Position 5 :
    - *"The cycle time for the safety FP should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the FP assuming worst-case conditions for the transfer of access from the communications processor to the FP. Failure of the system to meet the limiting cycle time should be detected and alarmed".*

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **Platform Requirements**

TS

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **NRC Guidance**
  - Position 6 :
    - *"The safety FP should perform no communication handshaking and should not accept interrupts from outside its own safety division".*
- **Platform Requirements** TS

Communications Independence

Staff Guidance in DI&C-ISG-04 (Cont'd)

- **All of the platform related requirements for ISG-04 positions will be described in the TeR.**

Plan for Further Meeting

Path Forward

- **Plan for the PARM in August**
  - Present draft TeR
  - Get additional feedbacks from NRC
- **Plan for the Pre-application Audit in October**
  - Present final TeR
  - Confirm NRC acceptability

Discussions

Table of Contents and Detail Requirements of TeR

- Completeness
- Level of depth
- Requirements expectation
- Confidence