U.S. Nuclear Regulatory Commission Staff Request for Additional Information On Rolls-Royce Civil Nuclear SPINLINE 3 Platform

To date, the U.S. Nuclear Regulatory Commission (NRC) staff has made reasonable progress on the safety evaluation for the licensing topical report (LTR) on the Rolls-Royce Civil Nuclear (RRCN) SPINLINE 3 Digital Safety Instrumentation and Control Platform. However, there are a handful of areas where the NRC staff needs to ensure that it clearly understands the terminology and some very specific SPINLINE 3 Operating System Software (OSS) operations.

In addition, the NRC staff has a reasonable understanding of the NERVIA network communications from discussions during the regulatory audit performed in Grenoble, France. For the NRC staff to rely on some of the NERVIA features in its assessment of how SPINLINE 3 meets Interim Staff Guidance (ISG)-04 (ADAMS No. ML083310185), the NRC staff will need to have some of the LTR provided NERVIA communications material augmented.

Please answer the following requests for additional information on the SPINLINE3 Platform.

I. Operating System Software

1. Operating System Software

The LTR, Sections 4.4.2 and 6.1, briefly describe that the Core System Software (CSS) and the Basic Functions (BFs) are part of the OSS. However, it is not clear how the CSS and BF work. In particular the LTR does not clearly describe how the CSS manages the environment in which the OSS elements operate. Also, the LTR does not describe how the BF transfers or exchanges data between the OSS and the CSS, and the input/output modules, and then how this data is transferred and used by the application software.

RRCN submitted Document 1 207 108, “Operational System Software – Software Requirement Specification.” This document seems to make a clear distinction between the functions performed by the OSS, BF, and CSS that is not explained in the LTR. Further, it is not clear why functions or attributes explained in the LTR are not consistent with the description provided in this document. For example, Section 3 of RRCN Document 1 207 108 explains error management for the SPINLINE3 system, which states that errors are generated and reported by the CSS. However, the LTR, Section 4.4.3.6, states that the errors are generated and reported by the OSS, without referencing the CSS.

Please clarify the relationship between the OSS, BF, and CSS. Also please explain the use of configuration tables by the OSS. Note if drawings are provided, please include a description of the drawing and how the information depicted relates to operation of the SPINLINE 3 platform.

2. Platform Peripheral Boards

LTR Section 4.4.3.5.1 describes the initialization functions that the OSS performs. This section identifies the following peripheral boards: microprocessor-based peripherals, non-microprocessor-based peripherals, and configurable non-microprocessor-based peripherals. LTR Section 5.2 describes the following peripheral boards: intelligent

ENCLOSURE

peripherals, non-intelligent peripherals, configurable non-intelligent peripherals, and non-configurable non-intelligent peripherals. Please clarify the different peripheral boards terminology used in the LTR and OSS software requirement specification. Also, please include a complete list of peripheral boards and their classification.

3. Initialization Functions

LTR Section 4.4.3.5.1 describes the initialization functions that the OSS performs. This section does not explicitly state that the initialization functions should be performed in a particular order. LTR Section 5.2 states that these functions should be performed in a particular order, which does not match the order followed in the LTR. Please clarify if these functions are performed in a specific and determined order, and, if so, which is the nominal order.

4. Use of Interrupts

LTR Section 4.4.3.5.1, Sub-function 1, states that when the central processing unit (CPU) is initialized, it sets up interrupts. Other sections in the LTR (e.g., Section 6.2.3) state that interrupts are not used in the OSS for managing functions. Please explain what type of traps and interrupts are used in the SPINLINE 3 platform, and how and when they are activated. Further, if these interrupts are generic to the platform review, then describe cases, conditions, and actions taken when these interrupts are activated.

5. Self-Diagnostic Tests of the CPU Board

LTR Section 4.4.3.5.2 describes the test and self-test diagnostics for the CPU and LTR Section 5.3.1 describes UC25 board tests during operation. The OSS document states that these tests are performed over several cycles, and the operator defines how to spread these tests. The execution of these tests is not described in the LTR, although they are described in the OSS document. Please clarify how these self-diagnostic tests are performed, and what parameters are defined to spread out and perform these tests (e.g., all self-tests should be performed).

6. Electrically Erasable Programmable Read-Only Memory (EEPROM) Parameters

LTR Section 4.4.3.5.1, Sub-function 2, describes the initialization task for the EEPROM. LTR Section 5.2.6 also describes this initialization activity. However, the OSS document states that during initialization of the EEPROM this component is not accessible for a defined period. Please explain this initialization function and where the defined period is configured, and whether the EEPROM becomes available after the defined period has elapsed.

II. Communication

1. Consistency Blocks and Dual-Port Memory

LTR Section 4.5 describes the SPINLINE3 platform communications. In particular, Section 4.5.2.6 describes how data from the Station's MPC860 microprocessor is transferred to the Unit's 68040 microprocessor via writing to the Dual-Port Memory (DPM), so it can be used by the NERVIA network. This section explains that data is copied using consistency blocks. Section 4.5.4.3 goes into further detail by "DPM memories are organized [ ]." However, this section does not explain how the CBs are [ ] in the DPMs, and how [ ] when data is transmitted in the NERVIA network. Please provide further explanation regarding how CBs are used in

conjunction with the DPM – specifically, elaborate on the use of the [
].

2. DPM data control

LTR Sections 4.5.2.6 and 4.5.4.3 state that data control flags would be used to access each side of the DPM, and [
]. Section 4.5.3 states that the use of this flag is explained in Section 4.5.4.3, but this section only states that access to the buffers is controlled using a pair of data control flags. Thus, it is not clear how the data control flags work to indicate that a buffer is not available. Also, the LTR explains that in the case that one of the microprocessor is reading, the data will be written to the buffer not being accessed. It is not clear when the other buffer is updated, and how this will be indicated by the data control flags.

Then, Section 4.5.4.3 states that potential conflicts with both processors attempting to access the data control flags at the same time are managed by the Complex Programmable Logic Device (CPLD), and that this is explained in Section 4.5.3. However, Section 4.5.3 only repeats what was said in Section 4.5.4.3. Therefore, it is not clear how the data control flags and the CPLD interact and work to control access to the buffers.

Please explain how DPM and data control flags work and how they control access to the DPM's buffers.

3. Status of the DPM buffer

The LTR explains that when a microprocessor wants to read data from the DPM, it will read it from the buffer with the most recently updated data. It is not clear what flag or data is used to identify the recently updated buffer. Please explain how the status of the buffer is kept.

4. NERVIA communication

The LTR explains that the NERVIA network is a SPINLINE 3 dedicated network, which was developed based on the Open System Interconnection model of the International Standard Organization. Further, the LTR provides a general description of the frame and protocol used to transmit messages in the network. However, this information is not sufficient to understand:

a) Additional information on the NERVIA logic code and how the protocol works is necessary to evaluate points 16 and 18 of ISG-04. Specifically, the NRC staff needs information that describes the logic used to flag invalid data, network initialization and operation, network status, etc.

   For example, Section 4.5.5.2 of the LTR states that network and station description tables (e.g., Table de Description de Station) are defined for the network communication. These tables would specify the [
   ]. This section states that if there is only one station in the network, this station will transmit data.

However, if several stations are in the network, the TDS will define the [

]. For example, if there are 4 stations, the [ ] is defined for these stations to be [

].

What happens if station [ ]?

Can station [ ] defined in the TDS?

Will station [ ] initialize?

Please provide different scenarios of how events that could occur during initialization and how the stations would behave.

b) ISG-04, Staff Position 1, Point 12 contains 12 examples of credible communication faults to be considered as part of the evaluation. Table 3.7-1 of Appendix A in ISG-04 addresses each of the 12 examples. It is understood by the NRC staff that the SPINLINE 3 NERVIA network would not normally exhibit any of these errors. However, the NRC staff is attempting to conclude that the system is robust to handle such errors or that the example error is not credible for the system.

For examples 2 and 3, do the NERVIA messages contain any time-stamp or message sequence identifiers such that a repeated or out-of-sequence message would be identified by a recipient station (i.e., is the NERVIA network designed to handle and/or detect such errors)?

Alternately, is it RRCN's position that such errors are not credible for the NERVIA network?

If so, please provide additional explanation as to why these errors are not credible.

c) Additional information on the configuration of the network and definition of stations categories is needed to evaluate ISG-04 and independence between 1E and non-1E communication.

For example, how does the network know when to define a receive-only station?

Where is this marked in the TDS?

d) Additional information is necessary to evaluate determinism and independence of the NERVIA and the CPU. Specifically, when both the NERVIA and CPU are writing data to the DPM, and then how data is updated in the buffer not being updated.

e) Additional information is needed to demonstrate that network initialization is independent of station initialization and unit operation and to demonstrate that these functions are independent from the network operation. In other words,

when the SPINLINE3 platform starts, the operating system performs a series of initialization functions, including the NERVIA daughter board. Then the system starts operating and performing its functions.

It is not clear how the NERVIA network is initialized and configured. LTR Section 4.5.2.5 states that the network is initialized when the first station is powered.

Does the network have to wait for the OSS to finish configuration of this first station?

How does this work when more than one station is connected to the network?

How is the order established for them to start transmitting?

5. Reinsertion of a station in the NERVIA Network

a) LTR Section 4.5.5.2 states that when a station wants to transmit [

]. Please explain how this is indicated in the network message or frame. Is this simply reflected as “stale” data for the station that could not transmit, or is there a different method to acknowledge this occurrence?

b) Also, this section states that a [ ] waits to transmit. Please clarify if this [ ]. And if this is a NERVIA-specific [ ], please explain how this [ ] works.

6. DPM configuration

LTR Section 4.5.4.3 states that the [ ] are handled by the off-line configuration generation tool. Please clarify if this is intended to refer to the CLARISSE Workshop tool. If not, please provide a brief description of this tool.