Rolls-Royce

SPINLINE 3 Digital Safety I&C Platform

- NERVIA Network
- Testability

January 07, 2010
Non-proprietary

Overview of the Presentation

- NERVIA Network
  - Protocol
  - Data exchange
  - Media
  - Layout of network components
  - Behavior in case of some typical failures
  - Reliability
  - Answers to questions listed in Section 4 of Appendix of NUREG/CR-6082
- Testability
  - Fault detection strategy
  - Self-tests
  - Tests and self-tests coverage
  - Self-tests results signalization
  - Self-tests results and process application
  - Periodic tests
  - Tests performed by the Operational System Software (OSS)

Rolls-Royce

NERVIA Network

NERVIA Safety Network - Protocol (1/3)

NERVIA Safety Network - Protocol (2/3)

NERVIA Safety Network - Protocol (3/3)

NERVIA Safety Network - Data Exchange (1/6)

NERVIA Safety Network - Data Exchange (2/6)

NERVIA Safety Network - Data Exchange (3/6)

NERVIA Safety Network - Data Exchange (4/6)

NERVIA Safety Network - Data Exchange (5/6)

NERVIA Safety Network - Data Exchange (6/6)

NERVIA Safety Network - Media

NERVIA Safety Network - Layout of Network Components

NERVIA Safety Network - Reliability

NERVIA Safety Network - Behavior in Case of Typical Failures (1/3)

NERVIA Safety Network - Behavior in Case of Typical Failures (2/3)

NERVIA Safety Network - Behavior in Case of Typical Failures (3/3)

NERVIA Safety Network - Answers to Questions in NUREG/CR-6082 Appendix, Section 4 (1/5)

a) Is it an event-based or state based system?

NERVIA is based on a cyclic and deterministic protocol. The communication between the NERVIA stations and units is asynchronous. NERVIA is a state-based system.

b) Is there an accurate picture of the layout?

The detailed architectures with the connection of each unit on the networks are shown in each individual system description.

c) Are the data rates known between all nodes of the architecture? Are they known for upset and error conditions?

- The data rates between all nodes of the architecture are based on the network cycle time. This cycle time is constant even in case of failure of a Station.
- The cycle time is fixed and defined from the definition of the data sent on the network during the design phase.
- The consistency of data transmission is verified.

NERVIA Safety Network - Answers to Questions in NUREG/CR-6082 Appendix, Section 4 (2/5)

d) Is the message mix known? Is it known for upset and error conditions?

The messages mix is predefined during design. It is not sensitive to upset condition. It is monitored against error conditions

e) Are the timing and delay requirements known?

Timing and delay Requirements are expressed in detailed requirements of the systems. The response time of the system is defined by theoretical model and verified on the equipment during the equipment validation in the factory.

f) Is the system "deterministic" and the effects of error recovery accounted for?

- The protocol is deterministic. Even in case of errors, the cycle time is constant.
- If there is any error, the operational system software of the receiver invalidates the data as long as the error remains. The application software processes invalid data.

NERVIA Safety Network - Answers to Questions in NUREG/CR-6082 Appendix, Section 4 (3/5)

g) Is the actual link capacity including interface, operating system and protocol performance effects being quoted, or is the vendor basing calculations on raw media bandwidth?

The cycle time includes the timing of reception and transmission processing, and is used to determine the actual link capacity.

h) What are the media requirements?

- Electric cable inside cabinets: Shielded Foil Twisted Pair (SFTP), Category 5 Class D (IEEE 802.3i-1990)
- Fiber optic 62.5/125 (10BaseFL) between cabinets.

i) Does the design meet independence requirements?

The architecture and the use of fiber optic allow the requirements of electrical and physical independence to be met.

j) What are the communications error performance requirements?

NERVIA Safety Network - Answers to Questions in NUREG/CR-6082 Appendix, Section 4 (4/5)

k) What are the protocol requirements? What services should the protocol provide?

Main requirements: Determinism of exchanges, no sensitivity to load, static configuration, asynchronous from processing (no dead lock), reliability of exchanges
Main service: cyclically update a set of data among UNITS of the network

l) Is the medium proprietary? Are the protocols proprietary?

The medium is an off-the-shelf product.
The protocol is a “timed based token bus protocol
The software is proprietary software developed by RRCN.

m) Is there theoretical support for performance and reliability?

- Reliability: A reliability analysis enables identification of the failure modes and evaluates the corresponding failure rates of each component involved in a board or module. Detailed reliability data for the network components have been computed according to IEC 62380
- Performance: the scan time of each network is fixed and computed during design from the data exchanged

NERVIA Safety Network - Answers to Questions in NUREG/CR-6082 Appendix, Section 4 (5/5)

n) Is there experimental support for performance and reliability?

Detection of failed components is supported by system self-tests. Then repair is limited to replacement of electronic cards and the cabling is facilitated by use of connectors. Restoration of NERVIA networks after identification of any failure of an electronic component is simple and not time consuming.

o) Is there an installed base? If proprietary, how many suppliers support the medium and the protocol software?

- The NERVIA network is already installed in French N4 NPPs (4 units), Fessenheim and Bugey NPPs (6 units), Kozloduy NPPs, Qinshan NPPs, Tihange NPP, Ignalina NPP, Dukovany NPPs (4 units).
- The lower layers of the protocol are standard Ethernet provided by the Freescale MPC860 Communication Processor. The upper layer of the protocol is provided by RRCN proprietary software.

p) Is there a good match between nodes processors, networks controllers and operating system and protocol stack?

The NERVIA network is already installed in safety systems of NPPs. This long-term installation and operation allows us to claim that there is a good match between all elements of the ***SPINLINE 3*** system

Rolls-Royce

Testability

Testability - Fault Detection Strategy

Testability - Self-tests

Testability - Test and Self-test Coverage (1/2)

Testability - Test and Self-test Coverage (2/2)

Testability - Self-test Results Signaling

Testability - Self-test Results & Process Application

Testability - Periodic Tests

Testability - Tests Performed by the OSS (1/2)

Testability - Tests Performed by the OSS (2/2)