DRS

DEFENSE SOLUTIONS

DRS-2010-0204
April 5, 2010

Document Control Desk
US Nuclear Regulatory Commission
Washington, DC 20555

Subject: Topical Report Pre-submittal Power Point Presentation –
PLµS 32™Compliance with Interim Staff Guidance 4 Highly-Integrated
Control Rooms – Communications Issues Presentation to US NRC March
2010

Reference: a) NRC Project Number 778
b) DRS-CCI letter to Document Control Desk, DRS-2010-0123, "Topical
Report Pre-submittal Power Point Presentation – PLµS
32™Compliance with Interim Staff Guidance 4 Highly-Integrated
Control Rooms – Communications Issues Presentation to US NRC
March 2010," dated March 3, 2010

Ladies and Gentlemen:

Reference b) was provided to the Document Control Desk with three (3) attachments:
001 Request For Withholding From Public Disclosure & Affirmation of Affidavit
002 DRS-2010-0123 Attachment 2-P PLµS 32™ Compliance with Interim Staff Guidance
4 Highly-Integrated Control Rooms (Proprietary Markup Version)
003 DRS-2009-0123 Attachment 3-NP PLµS 32™ Compliance with Interim Staff
Guidance 4 Highly-Integrated Control Rooms (Non-Proprietary Markup Version)

Attachment 002 and 003 inadvertently contained non-proprietary information that was
requested to be redacted. Attached to this letter is a replacement copy of attachments 002
and 003 to replace the previous version. Please make this correction.

If you have any questions or comments regarding this response, please contact the

undersigned at (203) 731-9506 (David.Kulp@DRS-DefenseSolutions com).

Sincerely,

David A. Kulp
Senior Programs Manager
21 South Street
Danbury, CT 06810
203.731.9506
DKulp@DRS-DS com

cc: Ms. Stacey Rosenberg, Mr. Eric Bowman, USNRC (w/o enclosures)

Attachments:
001 Request For Withholding From Public Disclosure & Affirmation of Affidavit
002 DRS-2010-0123 Attachment 2-P PLµS 32™ Compliance with Interim Staff Guidance 4 Highly-Integrated Control Rooms
003 DRS-2010-0123 Attachment 3-NP PLµS 32™ Compliance with Interim Staff Guidance 4 Highly-Integrated Control Rooms

DRS Consolidated Controls, Inc.

AFFIDAVIT

I, David A. Kulp, being duly sworn, depose and state as follows:

1. I am Senior Programs Manager, Nuclear Controls, DRS Consolidated Controls, Inc. (DRS-CCI), and have been delegated the function of reviewing the DRS-CCI proprietary information sought to be withheld from public disclosure in connection with the pre-submittal review of the PLµS 32 Distributed Control System and I am authorized to apply for its withholding on behalf of DRS-CCI.

2. The information sought to be withheld is contained in the Attachment 2-P to DRSPCT letter DRS-2010-0123 D. A. Kulp to NRC, *Topical Report Pre-submittal Power Point Presentation - PLµS 32™ Compliance with Interim Staff Guidance 4 Highly-Integrated Control Rooms – Communications Issues Presentation to US NRC March 2010.* For pages containing DRS-CCI proprietary information, the page is marked with "Proprietary Information: Trade Secrets Submitted under 10 CFR 2.390" on the first page and at the top of the specific page.

3. In making this application for withholding of DRS-CCI proprietary information, DRS-CCI relies upon the exemption from disclosure set forth in the NRC regulations 10 CFR § 2.390 and in conjunction with the DRS-CCI application for withholding accompanying this Affidavit.

4. Some examples of categories of information which fit into the definition of proprietary information are:

    a. Information which discloses process, method, or apparatus, including supporting data and analyses, where prevention of its use by DRS-CCI competitors without license or contract from DRS-CCI constitutes a competitive economic advantage over other companies in the industry;

    b. Information, if used by a competitor, would reduce its expenditure of resources or improve its competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

    c. Information which reveals cost or price information, production capacities, budget levels, or commercial strategies of DRS-CCI, its customers, its partners, or its suppliers;

    d. Information which reveals aspects of past, present, or future DRS-CCI customer-funded development plans or programs, of potential commercial value to DRS-CCI;

e. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection;

f. Information obtained through DRS-CCI actions which could reveal additional insights into nuclear safety-related digital control system equipment design processes, qualification processes and regulatory proceedings, and which are not otherwise readily obtainable by a competitor.

Information to be withheld is considered to be proprietary to DRS-CCI based on the reasons set forth in paragraphs 4a., 4.b., and 4.f. above.

5. The information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by DRS-CCI, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by DRS-CCI, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties, including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are set forth in paragraphs 6 and 7 following.

6. Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge.

7. The procedure for approval of external release of such a document typically requires review by the Product Line Lead, Contracts Manager, Program Manager or other equivalent authority, and by the Legal Department, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside of DRS-CCI are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.

8. The information identified in paragraph 2, above, is classified as proprietary because it contains product design information. DRS-CCI has expended significant resources in both time and money in the development and qualification of this control system.

Disclosure of information in this document would cause substantial harm to the competitive position of DRS-CCI, as there are other competing companies who wish to qualify digital control systems for safety-related applications in nuclear power plants.

Competing firms could use our experience, approaches and technical information to facilitate their own qualification efforts and/or product design without compensating DRS-CCI.

9. Public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of DRS-CCI because it would enhance the ability of a competitor to provide similar designs of digital control systems using similar approaches, equipment or licensing approaches.

STATE OF CONNECTICUT
COUNTY OF FAIRFIELD

)
) ss   Danbury, CT
)

David A. Kulp, being duly sworn, deposes and says:

That he has read the foregoing affidavit and the matters stated herein are true and correct to the best of his knowledge, information and belief.

Executed at Fairfield, Connecticut, this ___5___ day of _Apr:1_ ~~2009~~ 2010 DaK

David A. Kulp
Senior Programs Manager
DRS Consolidated Controls, Inc.

Sworn to and subscribed before me this _5th_ day of _April_ ~~2009~~ 2010 vm

Notary Public,
State of Connecticut
Commission Expires _3-31-2015_

Affidavit Page **3** of **3**

PLµS 32™ Compliance with Interim Staff Guidance 4 Highly-Integrated Control Rooms— Communications Issues

U.S. Nuclear Regulatory Commission

March 2009

Project Number: 778

DRS-2010-0123 Attachment 3-NP

DRS
DEFENSE SOLUTIONS

- PLµS 32™ has been designed and developed to meet ALL of the requirements for a safety control system in a nuclear power generating station

- During a meeting at the NRC in October 2009, the NRC asked questions regarding the use of a communications network as part of the PLµS 32™ system

- This presentation is designed to address the NRC questions and provide further explanation on the performance and features of the PLµS 32™ communications

- Identify the methods in which the PLµS 32™ system complies with Interim Staff Guidance 4

- PLµS 32™ system design is an innovative approach to safety communications
  - The communications scheme is like nothing else in the industry
  - Complexity has been eliminated
  - Collisions have been eliminated
  - Deterministic worst case timing is guaranteed
  - There are NO tokens
  - Division Isolation is maintained
  - Multi-Divisional Control and Display Stations do NOT exist
  - Safety to non-safety communications links are ONE WAY only

3

- There are four basic components involved in communications within the PLμS 32™ system.
    - Network Interface Module (NIM)
    - Communications Interface Module (CIM)
    - Bridge Transfer Module (BTM)
    - Control-I/O Module
- Each of these components have been developed to meet the requirements for use in a US Nuclear Power Generating Plant

- Each of these components performs specific tasks within the communications scheme
  - NIM: Controls communications within a cabinet, and within a Division
  - CIM: Is responsible for controlling interdivision communications
  - BTM: The Gateway to the Non-Safety equipment
  - Control-I/O Module: Communicates with the NIMs, performs the safety functions
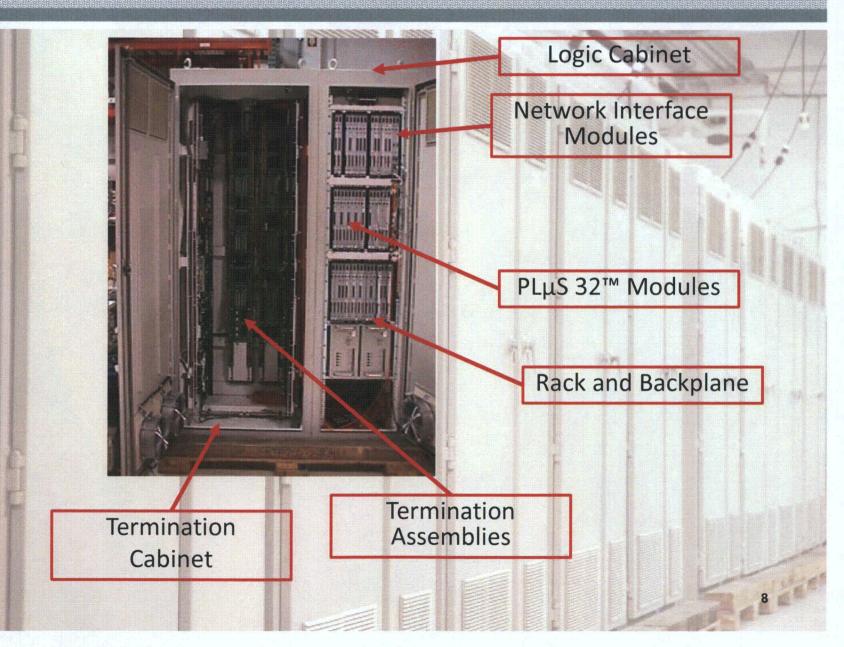
COMMUNICATIONS

How Does PLµS 32™ Communicate?

DRS
DEFENSE SOLUTIONS

- The PLµS 32™ system has several layers of communications
  - Within a Safety Cabinet
  - Within a Safety Division
  - Safety Division to Safety Division
  - Safety System to Safety System
  - Safety Division to Non-Safety Equipment
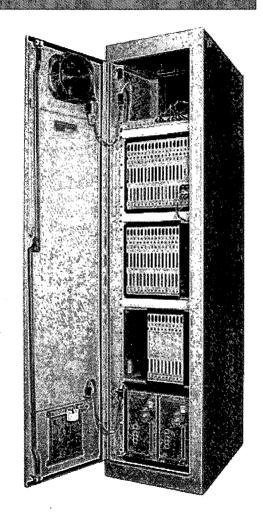- The following presentation will address each of these in detail

7

PLµS 32™ Cabinet Configuration Overview

Logic Cabinet

Network Interface Modules

PLµS 32™ Modules

Rack and Backplane

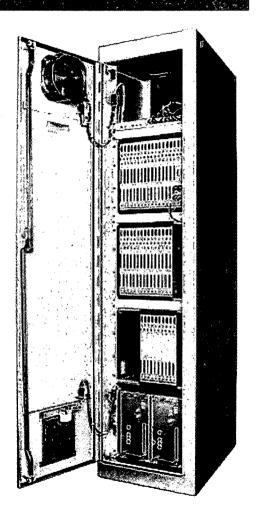Termination Cabinet

Termination Assemblies

- Two Basic Cabinet Types
  - Logic Cabinet
  - Termination Cabinet
- Logic Cabinets
  - 3 Logic Racks for 48 Modules
    - 2 NIMS per Cabinet
  - 1 Power Supply Rack
    - Redundant Supplies
    - Independent Power Sources
  - EMI Filters for Each Power Feed

- **Termination Cabinet**
  - Separate Cabinet for EMI Control
  - Termination Assemblies for Field Wiring and Relay Mounting
    - Analog and Digital Designs
    - Plug Connector Interface Cables Between Termination Assemblies and Racks
    - Relays and Fusing all on Termination Assembly
    - All Field Inputs and Outputs are connected to the Control-I/O Modules through the termination cabinets

- The PLµS 32™ system uses the term interlock to refer to any data (analog or digital) that is communicated from one module in the system to another module in the system

- Interrupts: the PLµS 32™ system uses interrupts in the Control-I/O Module software for communications only

- Channel: Channels includes the equipment from the transmitter, through the I/O module to the point the signal is compared to a setpoint to generate a single channel trip signal. A channel is contained within a division. The PLuS 32 system rarely uses this term.

- Division: Contains all of the logic for a channel and receives the signals to generate the coincident logic for initiating a safety related actuation function. The division contain the logic to insure the safety related actuation signal can align and complete the safety function. A division receives channel trip signals from all divisions

- Concept of Replicated Memory
  - Similar to Dual Ported Memory
  - 512K Bytes Total Network Shared Memory
  - Replication of the Shared Memory is performed by the ASIC on the PERFORM Net Node
  - The NIM Microprocessor is not involved in the performance of the replication of the data
  - All Nodes Have Access to Read all Shared Memory of the Network
  - Hardware Based Node Numbers used to Identify Cabinet and Restrict Write Access

COMMUNICATIONS

Within a Safety Cabinet

DRS

DEFENSE SOLUTIONS

COMMUNICATIONS

Within a Safety Division

DRS

DEFENSE SOLUTIONS

DRS

COMMUNICATIONS

Safety Division to Safety Division

DRS
DEFENSE SOLUTIONS

- The only communications between safety divisions is for:
  - Voter Logic
  - Bypass Status
- There are only 2 ways to communicate between safety divisions:
  - Hardwired
  - Through the Communications Interface Module (CIM)

- Hardwired communications are used for small quantities of individual digital or analog data
- All hardwired data is isolated from one division to the other
- This method is cabling intensive

94

DRS

COMMUNICATIONS

Safety System to Safety System

DRS
DEFENSE SOLUTIONS

- Hardwired communications are used for small quantities of individual digital or analog data

- All hardwired data is isolated from one system to the other

- This method is cabling intensive

COMMUNICATIONS

Safety Division to Non-Safety Division

DRS
DEFENSE SOLUTIONS

DRS

113

INTERIM STAFF GUIDANCE #4

Compliance

DRS DEFENSE SOLUTIONS

- ISG 4 is divided into 3 sections:
  - interdivisional communications
  - command prioritization
  - multidivisional control and display stations
- Each of these sections will be discussed in detail

Italics text is from ISG 4
Green text is DRS-CCI Response

1. *A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE 603. It is recognized that division voting logic must receive inputs from multiple safety divisions.*

- The communications network within each division is independent and isolated from the other divisions within the system. The only communications input into a Division are through redundant Communications Interface Modules (CIM). The only data items transferred into a division are the voter and bypass data needed to perform the safety functions.

- CIM to CIM communications is used to provide voting logic inputs between safety divisions

127

2. *The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.*

- All communications inputs from one safety division to another occur via CIM to CIM communications links

- The logic performed on the safety processor is designed to ensure that the safety functions can be performed in the event of a loss of data from another division

3a. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system.

- During the application of the PLµS 32™ system, the CIMs are configured to transmit and receive **ONLY** the data that is essential in the performance of safety applications from one division to another

- It is the responsibility of the Applications Design Engineers to ensure that the safety logic diagrams meet this requirement

3b. *Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.*

- During the application of the PLµS 32™ system, the CIMs are configured to transmit and receive **ONLY** the data that is essential in the performance of safety applications from one division to another

- It is the responsibility of the Applications Design Engineers to ensure that the safety logic diagrams meet this requirement

4a. 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. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B.

- Communications from one safety division to another are performed by the CIMs.

- The safety application processing is not directly affected by CIM communications errors or malfunctions.

4b. *Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.*

132

5. The cycle time for the safety function processor 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 function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

6. *The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.*

- Communications from one safety division to another are performed by the CIMs.

- The safety application processing is not directly affected by CIM communications errors or malfunctions.

7. *Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.*

- Each CIM contains an EPROM that is programmed with its own unique data sets that will be sent to or received from another division.

8. *Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.*

- Communications between safety divisions are processed completely by the CIMs .

- Communications between a safety division to non-safety division is processed completely by the BTMs or for smaller data sets the CIMs.

- The safety application processing is not directly affected by CIM or BTM communications errors or malfunctions.

9. *Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.*

*   PERFORM Net memory has well defined mapping for each safety controller used within the system.

*   Each safety application defines the locations for required interdivisional data.

*   The CIMs store incoming data to locations defined by its EPROM program. These locations are directly related to the applications programmed into the safety processors.

137

10. *Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.*

- PLμS 32 safety applications are designed such that no application parameters are modifiable on-line.

- Application code is programmed into EPROM devices which cannot be modified while installed in the safety processor.

11. *Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.*

- The application processing within a PLµS 32 safety processor is based upon a user defined FID. Application execution sequencing does not change based on any received messages.

- PLµS 32 Interdivisional communications provides transfer of application data. The PLµS 32 system architecture does not support transfer of instructions or commands between divisions.

12a.   *Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:*

- *Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.*
- *Messages may be repeated at an incorrect point in time.*
- *Messages may be sent in the incorrect sequence.*
- *Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.*
- *Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.*

- Standard PLµS 32 system design practices do not allow data from non-safety equipment to pass into the safety system.

12b. *Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:*

- *Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.*

- *Messages may be inserted into the communication medium from unexpected or unknown sources.*

- *Messages may be sent to the wrong destination, which could treat the message as a valid message.*

- *Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.*

- *Messages may contain data that is outside the expected range.*

- *Messages may appear valid, but data may be placed in incorrect locations within the message.*

- *Messages may occur at a high rate that degrades or causes the system to fail (i.e.,broadcast storm).*

- *Message headers or addresses may be corrupted.*

- Standard PLµS 32 system design practices do not allow data from non-safety equipment to pass into the safety system.

13. *Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.*

14. *Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.*

- All interdivisional communication is processed directly through the CIMs located in the affected divisions.

- CIMs provide single direction, point-to-point communications.

15. Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

16. *Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)*

145

17. *Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.*

- The PLµS 32™ system has been qualified to EPRI TR-102323 and MIL-STD-461D/MIL-STD-462D.

18. *Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.*

- The CIM cards are designed to provide point-to-point communications with another CIM. The CIM design is devoted entirely to the transfer of interdivisional data does not contain any unnecessary functionality.

19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

20. *The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.*

1. *A priority module is a safety related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system
- The priority module will not be part of this topical report

2. *Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system

- The priority module will not be part of this topical report

3. *Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state."), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal "safe state:" the valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system

- The priority module will not be part of this topical report

4. *A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system

- The priority module will not be part of this topical report

5. *Communication isolation for each priority module should be as described in the guidance for interdivisional communications.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLμS 32™ system
- The priority module will not be part of this topical report

6. *Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Standard 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system
- The priority module will not be part of this topical report

7. *Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system
- The priority module will not be part of this topical report

8. *To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system

- The priority module will not be part of this topical report

9. *Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system
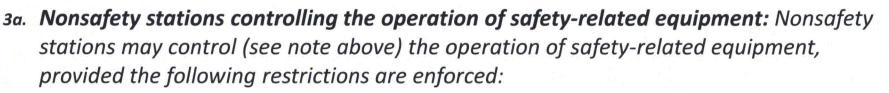- The priority module will not be part of this topical report

10. *The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.*

- The implementation of a priority module and its associated functions are a part of the overall plant system architecture and are outside of the scope of the PLµS 32™ system
- The priority module will not be part of this topical report

1. **Nonsafety stations receiving information from one or more safety divisions:** *All communications with safety-related equipment should conform to the guidelines for interdivisional communications.*

- Standard PLµS 32 system design practices do not allow non-safety operator workstations to communicate with safety equipment.

- Each PLµS 32 safety-related VDU is configured to communicate with only one division.

2. ***Safety-related stations receiving information from other divisions (safety or nonsafety):*** *All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.*

- Each PLµS 32 safety-related VDU is configured to communicate with only one division.

3a. ***Nonsafety stations controlling the operation of safety-related equipment:** Nonsafety stations may control (see note above) the operation of safety-related equipment, provided the following restrictions are enforced:*

- *The nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.*

- *A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment. In addition:*

  - *The nonsafety station should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable.*

- The PLμS 32 system architecture does not include a hardware Priority Module.

- Standard PLμS 32 system design practices do not include control of safety equipment by non-safety equipment.

3b. Continued

- *The nonsafety station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)*

- *The nonsafety station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.*

- Standard PLμS 32 system design practices do not include control of safety equipment by non-safety equipment.

4a. *Safety-related stations controlling the operation of equipment in other safety-related divisions: Safety-related stations controlling (see note above) the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that control the operation of safety-related equipment.*

    – *A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.*

- Each PLµS 32 safety-related VDU is configured to communicate with only one division.

- Control for each safety-related division is provided by VDUs within the division.

4a. Continue

- A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition:

  - The extra-divisional (that is, "outside the division") control station should be able to bypass a safety function only when the affected division itself determined that such action would be acceptable.

  - The extra-divisional station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)

  - The extra-divisional station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.

- Each PLμS 32 safety-related VDU is configured to communicate with only one division.

- Control for each safety-related division is provided by VDUs within the division.

5. **Malfunctions and Spurious Actuations:** The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, include but are not limited to the following:

   – Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station.

   – Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor.

- Each PLµS 32 safety-related VDU is configured to communicate with only one division.

DRS

168