U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

LESSONS LEARNED USING DIGITAL I&C INTERIM STAFF GUIDANCE WORKSHOP

APPLICATION OF ISG-4 DURING WOLF CREEK AND OCONEE REVIEWS

Paul Loeser
Instrumentation & Controls Branch
Office of Nuclear Reactor Regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Review of ISG 4

- ISG 4 is concerned with the communications aspect of Highly-Integrated Control Rooms.

- This ISG is divided into three sections:

  - Section 1 - Interdivisional Communications – This section has 20 staff positions concerning the communications between redundant channels and between the safety-related system and non-safety systems.

  - Section 2 - Command Prioritization – This section has 10 staff positions concerning combining of safety-related and non-safety actuation signals to control a safety-related actuation device.

  - Section 3 - Multidivisional Control And Display Stations – This section has staff positions concerning operator workstations, safety-related and non-safety, used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division.

Application of ISG 4 to the Wolf Creek FPGA-based MSFIS System

- **Section 1 - Interdivisional Communications**
  - **The MSFIS does not have interdivisional communications, so no review was needed.**
  - **The only safety to non-safety communications was with the ALS Service Unit, and this could only be done on one channel at a time when the ASU is attached to the channel via a USB cable and the channel is in bypass.**
  - **Due to physical restrictions, the FPGA or non-volatile memory can only be modified when the board is removed from the chassis.**
- **The staff determined, with minimum review effort, that the MSFIS meet all requirements of section 1, Interdivisional Communications, of ISG 4.**

Application of ISG 4 to the Wolf Creek FPGA-based MSFIS System

- **Section 2 – Command Prioritization**
  - **The MSFIS does not use a priority logic module, and does not receive actuation signals from non-safety sources.**
  - **MSFIS receives actuation commands from two sources, automated actuation commands from the SSPS, and manual valve control signals from the operator control panel. These are both safety-related sources, and both perform the safety function of closing the isolation valves. The manual "open" command will be ignored while the automated actuation command from the SSPS is present.**
- **The staff determined, with minimum review effort, that the MSFIS meet all requirements of section 2, Command Prioritization, of ISG 4.**

Application of ISG 4 to the Wolf Creek FPGA-based MSFIS System

- **Section 3 - Multidivisional Control And Display Stations**
  - **The MSFIS does not use multidivisional control and display stations.**
  - **The only workstation used to modify, monitor, or maintain the MSFIS is the ALS Service Unit, and it is only connected to one MSFIS channel while that channel is in bypass and not performing its safety function.**
- **The staff determined, with minimum review effort, that the MSFIS meet all requirements of section 3, Multidivisional Control And Display Stations, of ISG 4.**

Lesson Learned from the application of ISG 4 to the Wolf Creek FPGA-based MSFIS System:

Simple system without interchannel or non-safety to safety communications can be reviewed for compliance with the guidance of ISG 4 with minimum effort and no effect on the review schedule.

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 1 – Interdivisional Communications**
  - **The Oconee system has communications between the safety-related channels and between the safety-related channels and non-safety systems.**
  - **Staff Position I requires that the safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. In the Oconee system, each channel normally receives sensor data and status from the other three channels.**
    - **The staff had to review the 2nd Min / Max function block and coding of that function block to determine what happens if the communications is lost, to verify that each safety channel was capable of accomplishing its safety function without this communication.**
    - **This took significantly more review time and extended the time required for the review.**
    - **Lesson Learned: Sufficient detail should be provided with the LAR to demonstrate conformance with this criteria.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 1 – Interdivisional Communications (continued)**
  - **Staff Position 3 requires that 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, that safety systems should be as simple as possible, and that functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system.**
    - **The Oconee system challenges this position. The system is very complex!**
    - **Interchannel communications is not necessary to perform the safety functions, but does enhance reliability. (i.e.; the system could have been designed to not need this communications.)**
    - **The Oconee RPS/ESPS system does not satisfy this criteria, and the staff was required to spend significant additional time to review the additional communications and determine its acceptability. This had the effect of delaying the approval LAR.**
    - **Lesson Learned: In those cases where a system does not meet ISG criteria, sufficient detail should be provided with the LAR for the staff to verify the acceptability of the system. In this instance, this included the failure modes and effects analysis of all external communications within a channel.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 1 – Interdivisional Communications (continued)**
  - **Staff Position 4 requires that the communication process itself should be carried out by a communications processor separate from the processor that executes the safety function.**
    - **The TXS has a communications module which can be attached to the safety processor.**
    - **It was not initially clear to the staff if this communications module contained a separate communications processor, or how the exchange of data between the communications module and the safety processor was done.**
    - **After review, the staff determined that there was a separate communications processor, and that the exchange of data was via dual ported memory with dedicated memory locations. Therefore, the Oconee system satisfies this criteria, however, this determination took additional staff review time and effort.**
    - **Lesson Learned: Sufficient detail on the communications processor and how it works should be provided with the LAR.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- Section 1 – Interdivisional Communications (continued)
  - Staff Position 6 requires that the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.
  - After review, the staff determined that the required handshaking and acknowledgement are performed by the communications processor, not the safety processor. The safety processor does not accept interrupts, but at one point in the safety software execution loop, the content of the shared memory is read into local memory. Therefore, the Oconee system satisfies this criteria.
  - To make this determination, the staff had to look at the internal coding of the communications functions blocks and the overall safety software execution loop. This review took significant additional time and effort.
  - Lesson Learned: Sufficient detail on the exact message formats and how they are handled should be provided with the LAR.

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 1 – Interdivisional Communications (continued)**

  – **Staff Position 7 requires that only predefined data sets should be used by the receiving system, with predefined message format and protocol, including message identification, status information, data bits, etc. in the same locations in every message.**

  - **In order to make this determination, the staff had to examine each type of message used in the system. The staff also had to examine the communications function blocks to determine what would happened if corrupted messages were received. In some instances, this required examination of the code within the function block.**

  - **The Oconee system satisfies this criteria, however, this review took significant additional time and effort.**

  – **Lesson Learned: Sufficient detail on message format and contents, including exact bit assignment, should be provided with the LAR.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 1 – Interdivisional Communications (continued)**
  - **Staff Position 9 requires that incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor, and that these memory locations should not be used for any other purpose.**
    - **The staff determined that the TXS design satisfies this criteria. The memory locations used are determined when the software is compiled, and are not changeable without re-compiling.**
    - **Reaching this determination took additional staff time and effort.**
  - **Lesson Learned: Sufficient detail on the shared memory, including memory location maps, should be provided with the LAR.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 1 – Interdivisional Communications (continued)**

  – **Staff Position 10 requires on-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment, and that a keylock switch either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic.**

    - **The system does not meet this requirement. The keylock sets a software bit, and does not open or interrupt a physical connection.**

    - **The staff had to spend significant additional time and effort to understand the software operation and how this was affected by the key switch. The staff also needed to review potential failures of both the key switch and the software. This review required an additional site visit to review and understand the actual code involved with the key switch, and what changed within the software when the key switch was in different positions.**

  – **Lesson Learned: Whenever a system does not meet ISG requirements, the exact details on what the system is and how it works should be provided with the LAR to allow the staff to assess the alternative design.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 2 – Command Prioritization**
  - **The Oconee TSX Based RPS/ESFS System does not use a priority logic module**
  - **For RPS, existing relay logic functions are used for voting and input of non-safety signals.**
  - **For ESFS, a TXS based voter is used for voting and input of non-safety signals.**
  - **The staff has determined that the system complies with the guidance of section 2 of ISG 4.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 3 - Multidivisional Control And Display Stations**

  - **The primary issue here was that all four channels of the Oconee RPS/ESFS system are connected to the non-safety Service Unit via the Monitoring and Service Interface (MSI).**

  - **The Service Unit has continual communications with all safety-related channels to request information for display.**

  - **The Gateway PC is continually connected to all channels via the MSI.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 3 - Multidivisional Control And Display Stations**

  - **Staff position 3.1.3, bullet 2 requires that a non-safety work station not affect the operation of safety-related equipment, and should only be able to bypass a safety function, suppress any safety function, or bring a safety function out of bypass condition unless the affected channel division has itself determined that such action would be acceptable.**

  - **The staff determined that while the service unit can bypass a channel and take the channel out of bypass, this was only possible when the key switch was in the appropriate position. A single failure would only affect one channel.**

  - **The same is true of suppressing the safety function of each channel. This could be done only when the key switch was in the appropriate position, and only to one channel at a time.**

  - **The staff is satisfied that this design is acceptable and complies with this criteria. However, reaching this determination took significant staff time and effort, and affected the overall review schedule.**

  - **Lesson Learned: Sufficient detail should be provided with the LAR to show compliance with the ISG.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 3 - Multidivisional Control And Display Stations (Continued)**
  - **Staff position 3.1.3, bullet 2 (continued)**
  - **Since the Gateway is continually connected to all channels via the MSI, Areva and Oconee installed a "Port Tap" which provides a one way out connection. The Gateway is unable to send anything to the MSI.**
  - **The internal workings of the "Port Tap" were proprietary, and gaining sufficient information about this device for the staff to determine that the connection was one-way required significant staff and vendor time and effort.**
  - **Lesson Learned: Vendors should insure that if proprietary equipment is used to show compliance with an ISG, sufficient detail is provided to the staff to show that use of that equipment is appropriate. The proprietary design information should have been procured with the hardware and supplied with the LAR.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Section 3 - Multidivisional Control And Display Stations (Continued)**
  - **Staff position 3.1.5, Malfunctions and Spurious Actuations, requires that the workstation be designed such that malfunctions must be consistent with the assumptions made in the safety analysis of the plant. A malfunction of the workstation must not cause the safety system to prevent actuation or provide spurious actuations.**
  - **Reaching this determination required the staff to examine the inner workings of the MSI and communications channels, including a review of the actual coding of the applicable function blocks. This was necessary since an understanding of the method used by the internal workings of the function blocks to prevent propagation of failures in the Service Unit was necessary to reach this determination.**
  - **This required significant staff time and effort, and affected the overall review schedule.**
  - **Lesson Learned: Sufficient detail concerning the effects of malfunction within the multidivisional control and display stations should be provided with the LAR.**

Application of ISG 4 to the Oconee TSX Based RPS/ESFS System

- **Conclusion**

  - **The interchannel and non-safety to safety communications used by the Oconee TXS based RPS/ESFS system required additional staff time and effort.**

  - **The system has not yet been approved, and additional questions may come up.**

  - **The communications complexity could have been avoided with a different design.**

- **Lesson Learned – Whenever the proposed system does not meet the ISG guidance, sufficient detail on what the system is and does needs to be provided to the staff to allow a determination that system is acceptable. In those cases where compliance with ISG guidance is not obvious, the staff needs to understand the system well enough to verify compliance. The licensee engineers may wish to ask themselves whether this level of detail would be sufficient for them to reach the determination of compliance.**

CONCLUSION

- **ISG 4, Communications, has been successfully used for two reviews.**
- **In the simpler system with little communications, review was fast and easy.**
- **In the more complex system with significant amounts of communications, review to verify compliance with the ISG criteria and gain a good understanding of alternative designs to ascertain reasonable assurance that the design is safe took much more time and effort, and affected the overall review schedule.**
- **In either review, ISG 4 successfully provided review guidance which the staff was able to use to determine the acceptability of the communications.**