Joseph G. Murray
Nuclear Program Manager
Invensys Process Systems
15345 Barranca Parkway
Irvine, CA 92618
U.S.A

19 January 2007

William E. Kemper, Chief
Instrumentation and Electrical Engineering
Office of Nuclear Regulatory Research
NRC

Re: Review and response to NEI submitted draft on Communications

Mr. Kemper:

On behalf of Invensys Process Systems, I have reviewed the NEI draft document dated 12/6/2006 entitled:

"White Paper, Communication Between Redundant Safety Divisions and Between Safety and Non-Safety Systems"

Invensys would like to submit the following comments on this document and also give our recommendations as to a course of action towards moving to completion on the topic of safety communications.

First, we would like to say that Invensys agrees with NEI in their summary statements:

"With digital I&C technology, judicious communication between redundant safety divisions and between safety and non-safety systems can provide reliability and safety enhancements that were not achievable when currently-operating plants were designed, using the analog technology of the day. Advanced plant designs include varying degrees of communications between redundant safety divisions and between safety and non-safety systems to validate signals and ensure high reliability. To enable nuclear plants to capture these benefits, NRC-approved guidance is needed to establish clear requirements and acceptance criteria whereby such communications can be designed and utilized, while maintaining reasonable assurance that they will not degrade safety functions through unintended behaviors or inadequately managed failure modes."

Invensys believes that the benefits from cross divisional safety to safety communications and non-safety to safety communications are great and can add overall reliability to, and availability of, the digital safety systems. Invensys also believes that there are acceptable ways to ensure the quality and safety of the communications while maintaining the integrity of the safety division independence as required by the GDC and IEEE-603.

Invensys has no comments on the NEI White Paper sections on "Background", "Definitions", "Detailed Requirements in IEEE std. 603-1998", and "Applicable Regulatory Documents" and treats them as statements of fact.

Invensys has only a single comment on the section entitled "Precedence for Communications Between Redundant Safety Divisions and Between Safety and Non-Safety Systems". Our comment is that the only examples of precedence that should be accounted for are ones that deal in digital systems communications as understood today. These examples should not include relay logic "communication".

Within the section entitled "Benefits of Communications Between Redundant Safety Divisions and Between Safety and Non-Safety Systems", Invensys agrees with the stated benefits as they are related only in terms of modern definitions of digital communications. However, the listed benefit as pertaining to the charging pump controls does offer demonstration of the benefits that are attainable using non-safety controls to operate safety equipment.

Within the section entitled "Design Criteria", Invensys agrees with the information provided with the following exceptions.

Invensys believes strongly that IEEE Std. 7-4.3.2-2003, Annex E is inadequate in providing guidance to safely design and establish safe communications. In this we agree with the statement in Reg. Guide 1.152, Revision 2, section B, subparagraph (e), which states that Annex E provides insufficient guidance.

NEI offers four additional design practices made by subject matter experts and suggests their addition to Annex E to help ensure high quality communications. Invensys agrees that these suggestions would help to ensure high-quality communications, however we still believe that the standard would give insufficient guidance and would allow for the prospect of approval of designs that have no mitigation for certain credible communications failures.

NEI next discusses and suggests a series of steps that should apply if the "non-safety related workstation" approach is used. These items are as follows:

"• All safety functions must be able to be performed solely by safety-related structures, systems, and components.

• Isolation provisions must provide both electrical and data isolation as required by IEEE Std.

7-4.3.2-2003 and Regulatory Guide 1.152, Revision 2.

•Safety-related accident monitoring instrumentation must be provided per the requirements of IEEE Std. 497-2002 and Regulatory Guide 1.97, revision 4.

•Additional non-safety-related accident monitoring instrumentation must be provided per the requirements of IEEE Std. 497-2002 and Regulatory Guide 1.97, revision 4. If the design and qualification requirements applicable to this portion of the accident monitoring instrumentation are met by the non-safety-related workstation, the workstation can be the sole indication for these additional non-safety-related parameters."

Invensys agrees with the first two items and has no comments on the final two items. Invensys would add the following statements as applicable to non-safety related workstation communications to safety systems purposes of control of safety equipment:

• All non-safety system communications to safety systems must be on physically separate communication links so that there is no mixing of safety and non-safety messages on the same physical link. (In this, Invensys deviates from the discussions of IEC 61784-3 further on in this document, in that Invensys feels that the risks posed by cyber-security issues are too great and separating communication links would add a layer of protection from outside interference through the non-safety system.)

• All credible failures of the non-safety system communication link to the safety system shall be analyzed for to ensure that there can be no interference to the safety system safety functionality.

• Non-safety inputs into safety system shall not be able to disrupt or in any way prevent a safety function from going to completion when called upon, either through failure modes or through deliberate action (i.e., no ability to stop a safety pump from a non-safety workstation communication link when it has been started as a result of a safety system action.)

• Non-safety inputs into a safety system change the SR/NSR protocol from a read-only to a read/write in the safety processor. This adds great importance to the application of cyber-security issue within the confines of the safety system and must be taken into account.

NEI then makes the following statement:

"The requirements of IEEE Std. 7-4.3.2 (subject to the enhancements suggested above) are judged sufficient to ensure that all safety functions can be performed when a design includes a workstation that controls both safety-related and non-safety-related systems and components."

Invensys disagrees with this position. A stated above, we still find that IEEE Std. 7-4.3.2, even with the NEI suggested enhancements, is insufficient. Invensys believes that the existing guidance, and the existing guidance enhancements, as recommended by the NEI working group, would not mitigate the existing confusion on the subject matter and could lead

to confusion by licensees and regulators during regulatory review. This then leads to the prospect of the approval of designs that do not account for credible failures, or rejections of designs that that are per the guidance yet may or may not have designed in methods for mitigation of credible failures.

Invensys would like to call to your attention the slide presented by Mr. Mike Waterman during the 12/12/2006 meeting. In it there is a graph of a guideline which shows the methods to developing guidance and procedures. As a part of the process, the staff looks for input from other industries, other U.S. regulations, and Foreign Regulations,

Within that context Invensys would like to offer as guidance for safety related communications the work that has been performed on this topic by the International Electrotechnical Commission, (IEC). IEC has generated guidance on this topic through the issuance of subject related documents, and most recently by the issuance of a draft document that is now finishing the review and comment cycle.

The original documents that discussed safety communications was developed for the Rail industry. An example is IEC 62280-2, *Railway applications – Communication, signaling and processing systems – Part 2: Safety-related communication in open transmission system.* The document that Invensys feels has the most applicable guidance to the nuclear industry in the realm of safety communications is IEC 61784-3 (Draft) *Digital Data Communications for Measurement and Control – Part 3: Profiles for Functional Safety Communications in Industrial Networks.*

This document is the culmination of some years of work by a working group consisting of member of academia, governmental association and regulators, vendors, safety network organizations and end-users. Invensys has a member on this working group, along with other vendors such as Toshiba, Mitsubishi, Rockwell and Siemens. Within this draft document are discussions of credible failures and recommended mitigating methodologies. These mitigating technologies effectively become part of a "safety communication layer" on top of the bus structures. Within the listing of credible failures are types of concerns that would not be addressed within the confines of either the existing Annex E of IEEE 7-4.3.2 or the NEI recommended enhancements.

An example of the credible failures and possible mitigating methodologies that are presented by IEC are listed below:

---

**Communication errors**

**Corruption**

Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference.

NOTE 1 Message error during transfer is a normal event for any standard communication system, such events are detected at receivers with high probability by CRC frame check sequence calculations and the frame is ignored.

NOTE 2 Most communication systems include protocols for recovery from message errors, so these messages should not be classed as 'Loss' until recovery or repetition procedures have failed or are not used.

NOTE 3 If the recovery or repetition procedures take longer than a specified deadline, a message is classed as 'Unacceptable delay'.

NOTE 4 In the very low probability event that multiple errors result in a new message with correct frame structure (addressing, length, CRC, etc...), the message will be accepted and processed further. Evaluations based on a message sequence number or a time stamp may result in fault classifications such as Unintended repetition, Incorrect sequence, Unacceptable delay, Insertion.

### 1.1.1 Unintended repetition

Due to an error, fault or interference, old not updated messages are repeated at an incorrect point in time.

NOTE 1 Repetition by the sender is a normal procedure when an expected acknowledgment/response is not received from a target station, or when a receiver station detects a missing message and asks for it to be re-sent.

In some cases, the lack of response can be detected and the message repeated with minimal delay and no loss of sequence, in other cases the repetition occurs at a later time and arrives out of sequence with other messages.

NOTE 2 Some fieldbuses use redundancy to send the same message multiple times or via multiple alternate routes to increase the probability of good reception.

### 1.1.2 Incorrect sequence

Due to an error, fault or interference, the predefined sequence (e.g. natural numbers, time references) associated with messages from a particular source is incorrect.

NOTE 1 Fieldbus systems may contain elements that store messages (e.g. FIFOs in switches, bridges, routers) or may use protocols that may alter the sequence (e.g. by allowing messages with high priority to overtake those with lower priority).

NOTE 2 When multiple sequences are active, such as messages from different source entities or reports relating to different object types, these sequences are monitored separately and errors may be reported for each sequence.

### 1.1.3 Loss

Due to an error, fault or interference, a message is not received or not acknowledged.

### 1.1.4 Unacceptable delay

Messages may be delayed beyond their permitted arrival time window, e.g. due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied (e.g. FIFOs in switches, bridges, routers).

NOTE In underlying fieldbuses using scheduled or cyclic scans, message errors may be recovered in several ways,

a) immediate repetition

b) repetition using spare time at the end of the cycle

c) treat the message as lost and wait for the next cycle to receive the next value

In case a) all the following messages in that cycle are slightly delayed,

in case b) only the re-sent message gets a delay.

Cases a) and b) are not normally classed as an Unacceptable delay.

Case c) would be classed as an Unacceptable delay unless the cycle repetition interval is short enough to ensure that delays between cycles are not significant and the next cyclic value can be accepted as a replacement for the missed previous value.

### 1.1.5 Insertion

Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity.

NOTE These messages are additional to the expected message stream, and because they do not have expected sources, they cannot be classified as Correct, Unintended repetition, or Incorrect sequence.

#### 1.1.6 Masquerade

Due to a fault or interference (most likely intentional), a message is inserted that relates to an apparently valid source entity, so a non-safety relevant message may be received by a safety relevant participant, which then treats them as safety relevant.

NOTE Communication systems used for safety-related applications may use additional checks to detect Masquerade, such as authorised source identities and pass-phrases or cryptography.

#### 1.1.7 Addressing

Due to a fault or interference, a safety relevant message is sent to the wrong safety relevant participant, which then treats reception as correct.

### 1.2 Deterministic remedial measures

#### 1.2.1 General

This subclause lists measures commonly used to detect deterministic errors and failures of a communication system, as contrasted to stochastic errors like message corruption due to electromagnetic interference.

#### 1.2.2 Sequence number

A sequence number is integrated into messages exchanged between message source and message sink. It may be realised as an additional data field with a number that changes from one message to the next in a predetermined way.

#### 1.2.3 Time stamp

In most cases the content of a message is only valid at a particular point in time. The time stamp may be a time, or time and date, included in a message by the sender.

NOTE 1 Relative time stamps and absolute time stamps may be used.

NOTE 2 Time stamping implicitly requires the time base to be synchronized. For safety applications, synchronization needs to be monitored.

#### 1.2.4 Time expectation

During the transmission of a message, the message sink checks whether the delay between two consecutively received messages exceeds a predetermined value. In this case, an error has to be assumed.

EXAMPLE

Time-slot-oriented access method:

The exchange of messages takes place within fixed cycles and predetermined time slots for every participant.

Optionally: Every participant shall send his data within its time slot even if there is no value change (this is an example of cyclic communication).

To identify a participant who did not transmit within its associated time slot, a source identification is added.

#### 1.2.5 Connection authentication

Messages may have a unique source and/or destination identifier that describes the logical address of the safety relevant participant.

### 1.2.6 Feedback message

The message sink returns a feedback message to the source to confirm reception of the original message. This feedback message has to be processed by the safety communication layers.

NOTE Some fieldbus specifications use the term “echo” or "receipt" as a synonym.

EXAMPLE

This returned feedback message may contain only a short acknowledge, or may also contain the original data, thus enabling the source to check the correct reception by comparing sent and received data.

### 1.2.7 Data integrity assurance

The safety-related application process shall not trust the data integrity assurance methods if they are not designed from the point of view of functional safety. Therefore, redundant data is included in a message to permit data corruptions to be detected by redundancy checks.

NOTE Communication systems used for safety-related applications may use methods such as cryptography to ensure data integrity, as an alternative to typical methods such as CRCs.

### 1.2.8 Redundancy with cross checking

In safety-related fieldbus applications, the safety data may be sent twice, within one or two separate messages, using identical or different integrity measures, independent from the underlying fieldbus.

In addition to this, the transmitted safety data is cross-checked for validity over the fieldbus or over a separate connection source/sink unit. If a difference is detected, an error shall have taken place during the transmission, in the processing unit of the source or the processing unit of the sink.

When redundant media are used, then common mode protection should be considered using suitable measures (e.g. diversity, time skewed transmission)

### 1.2.9 Different data integrity assurance systems

If safety relevant (SR) and non-safety relevant (NSR) data are transmitted via the same bus, different data integrity assurance systems or encoding principles may be used (different CRC algorithms, different generator polynomials), to make sure that NSR messages cannot influence any safety function in an SR receiver.

NOTE Having an additional data integrity assurance system for SR messages and none for NSR messages is acceptable.

---

Invensys feels that this document can be of great use by the NRC in developing guidance for safe communication in safety to safety and non-safety to safety communication regulation. Invensys would like to see the NRC use applicable portions of the work performed by the IEC in NRC revisions and generation of new regulatory documents.

In summary, the Invensys position in the question of digital communications in safety related systems is that there are no insurmountable issues. Invensys feels that the regulations need to be enhanced to take into consideration the information and methodologies provided by IEC in their work on Safety Communications. The regulations as they are today and the NEI

suggested enhancements do not raise the level of guidance high enough to prevent the possible approval of designs that have not taken into account credible failure modes nor will they prevent the continuation of the present confusion on acceptability or unacceptability of communications design.

In addition to this, Invensys believes that in the area of NSR to SR communications, the enhancements offered above by Invensys, in addition to the use of the IEC 61784-3 information should be used. Also, NSR to SR communications introduces new pathways for cyber-security intrusion concerns, so this issue must be adequately addressed in NSR to SR communications.

Regards,

Joseph G. Murray
Nuclear Program Manager
Invensys Process Systems
15345 Barranca Parkway
Irvine, CA 92618, U.S.A
+1.949.885.0854 Desk
+1.949.374.1858 Cell
+1.949.753.9101 Fax
www.InvensysNuclear.com