NRCREP Resource

From: Contratto, Robert [Robert.Contratto@ds-s.com]
Sent: Friday, February 20, 2009 2:50 PM
To: NRCREP Resource
Subject: Data Systems and Solutions Comments on DG-1190
Attachments: DSS_Comments on DG-1190_2009_02_20.doc

Dear Sirs:

Please find attached Data Systems and Solutions comments on draft Regulatory Guide DG-1190.

Sincerely,

Robert J. Contratto
Vice President, I&C Customer Business
Data Systems and Solutions
994-A Explorer Blvd.
Huntsville, AL 35806

contrattor@ds-s.com
B/Berry: +1-404-775-8190
Ofc.: +1-770-205-2206
Fax: +1-770-205-7441

12/23/08
73 FR 78856
(6)

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add = K. H. Nguyen (khn)

Comments on Draft Regulatory Guide DG-1190, December 2008

No.	Section	Paragraph	Page	Comment
1	B	3rd	3	IEEE 603, clause 6.2.3, states "Means shall be provided to implement manual actions necessary to maintain safe conditions after protective actions are completed as specified in 4.10". IEEE 603 does not require that each Class 1E component have individual component controls in the control room if they are not required to maintain the plant in a safe shutdown condition.
2	B	2nd	3	IEEE 603, clause 7.2 states "If manual control of any actuated component in the execute features is provided, the additional design features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2". It does not state the manual controls "be subject to the single-failure criterion". The wording must be changed for a Class 1E component is associated with a division or train, and the manual controls associated with that component will only be associated with the respective division or train and will not meet the single-failure criterion.
3	B	1st	3	A definition should be provided for the term "advanced analog systems". What types of platforms are encompassed by this term and what are new vulnerabilities associated with their use?
4	B	4th	3	ANSI/ANS 58.8 has always been used as a guideline for allowable operator action times following an anticipated operational occurrence (AOO) or design basis event (DBE), i.e., 5 to 10 minutes for an AOO and 20 to 30 minutes for a DBE. Is this regulatory guide essentially stating that 30 minutes must be assumed for all operator action times in the future? Why is the standard revising the existing guidance that has been used for many years?
5	B	2nd	4	It would be better if the regulatory guide only referred to Regulatory Guide 1.97, and not to a specific revision. There are no operating plants licensed to revision 4 which endorses IEEE 497-2002. Most operating plants are licensed to Regulatory Guide 1.97, revision 3.
6	B	3rd	4	Why is this regulatory guide even addressing software common cause failure (CCF) since scenarios resulting from an initiating event concurrent with a postulated software CCF are beyond design basis events? The last four sentences of this paragraph should be removed beginning with "IEEE Std 7-4.3.2-2003 ...".
7	B	1st	5	Again, this paragraph is discussing requirements following an initiating event concurrent with a postulated software CCF which is beyond a design basis event. IEEE 603 is only applicable to AOOs and DBEs. This paragraph should be removed and addressed in a D3 document, e.g, DI&C-ISG-02.
8	C	Item 1	5	Refer to comment 2 above
9	C	Item 3	6	The first sentence should be modified to state the following: "The control interfaces for manual initiation of protective actions on a plant system component basis (required to maintain safe plant

No.	Section	Paragraph	Page	Comment
				conditions) and on a system-level basis for each division should be located in the control room".
10	C	Item 4	6	This paragraph essentially requires that the component manual controls not be implemented through a software path for a digital protection system implementation. In other words, the signal prioritization between automatic and manual command signals from the protection system must be performed in the priority module (as is implemented in the relay logic of most operating plants). This requirement increases the complexity of the priority module which makes it more difficult to use FPGAs upon which to implement the logic (100% testability). I recommend that additional discussion be added to this paragraph discussing the conflicting requirements if the manual component controls are excluded from the protection system software and the increased complexity in the protection system priority logic.
11	A	2	2	The author should note that IEEE 603 is written for Design Basis Events and not Beyond Design Basis Events, which later in this draft guide becomes a dominant issue (SWCMFs).
12	A	4	2	In this area, IEEE 603 is referring to divisional level manual switches and not component level switches. Component control is only discussed if necessary for safe shutdown.
13	B	10	4	Why is the draft RG referencing a computer-based Equipment Qualification RG? Most of this paragraph deals with computer based qualification such as IEEE 7-4.3.2 and RG 1.209. These areas should be removed from the draft RG.
14	Regulatory Analysis	1 & 2	7	This draft RG has included more than the referencing of IEEE 603 and digital capabilities. It has included Beyond Design Basis Event guidance for manual initiation, actual guidance for allowed times (30 minutes), computer qualification criteria, and increased guidance for component controls,
15	Regulatory Analysis	Item 4.	8	The NRC should identify where the cost savings will be for a plant to implement this draft RG.