

62-76  
52412

MAY 24 1983

MEMORANDUM FOR: Roger J. Mattson, Director, DSI, NRR  
FROM: Themis P. Speis, Director, DST, NRR  
SUBJECT: DRAFT CRGR PACKAGE ON A-30, DC POWER

The DST review of the draft CRGR package on Generic Issue A-30, DC power, has turned up problems at two levels. Within the defined scope of A-30, there are problems with the CRGR package. See Attachment 2 for details. Of broader concern are problems with the A-30 scope. We feel that significant safety problems may be falling into the crack between A-30 and USI's A-17, A-44, A-45, and A-47. The concern is sketched below. See also Attachment 1 for details.

The essence of the technical concern is this: A-30 deals almost exclusively in reliability problems associated with the design and operation of safety related DC power supplies. It does not deal with the systems integration aspects of the allocation of powered loads to DC buses, in particular with the accident sequence vulnerabilities associated with the possibility that control and instrumentation power supply faults could, in some plants, cause 1) a serious initiating event (e.g., loss of offsite power at Robinson 1972, or small LOCA at Crystal River 1980), 2) defeat a division of active engineered safety features, and 3) blind or partially blind operators to what is happening in the plant (Rancho Seco-1978, Zion 1977). See also Attachment 1. The issue touches on Systems Interactions A-17, Station Blackout A-44, Decay Heat Removal, A-45, and Safety Implications of Control Systems, A-47. The A-47 program does consider non-safety related power supplies for control systems. A-17 and A-45 address parts of the issue. However, there is no one program at present that appears to address all of the aspects of the significance to risk of accident sequences as precipitated by I&C power supply failures, noted above.

NUREG-0666 concluded that all plants, including OR's, should be required to treat loss of any one I&C bus as a DBA and require that the core survive an additional single active failure. The CRGR package for A-30 dismisses this recommendation of NUREG-0666 with what we believe to be an inadequate discussion.

Frank Rowsome met with Les Rubenstein and others on Friday, May 6, to discuss the concerns. They concluded that the scope problem is real and warrants priority attention.

Of M-7  
CRGR  
x RD-7-21

~~8306030487~~ ~~830524~~  
CF SUBJ  
DLM-7CRGR CF

ALS

OFFICE							
NAME							
DATE							

MAY 24 1983

After consideration of possible options, DST recommends that the current A-30 effort be concluded as planned and that a new generic issue be developed to pick up the related issues.

The new generic issue should be developed in accord with Office Letter 40, be prioritized, and resources allocated as appropriate. DST and DSI should collaborate in developing the scope of this issue. We also recommend that the CRGR package on A-30 indicate that we are pursuing this approach. Other suggestions on improvements to the CRGR package are contained in Attachment 2.

Contact Frank Rowsome (X28016) for additional information.

FRANK H. ROWSOME

*for* Themis P. Speis, Director  
Division of Safety Technology  
Office of Nuclear Reactor Regulation

Attachments:  
As stated

cc w/attachments:

- F. Rowsome
- F. Schroeder
- A. Thadani
- W. Minners
- G. Sege
- K. Kniel
- Z. Rosztoczy
- A. Marchese
- A. Rubin
- F. Coffman
- L. Rubenstein
- W. Houston
- F. Rosa
- W. Butler
- O. Parr
- M. Srinivasan
- A. Gill
- H. Thompson/D. Ziemann, DHFS

DISTRIBUTION:

- ~~Central File~~
- AD/T R/F
- DST R/F
- T. Speis

OFFICE	AD/T: DST	D: DST <i>FHC</i>	AD: GR: DST	C: GIB <i>KK</i>			
NAME	Frowsome/LLM	TPSpeis	FSchroeder	KKniel			
DATE	5/20/83	5/23/83	5/23/83	5/23/83			

Attachment 1:

Scope Problems with the draft A-30 Package

By construing A-30 too narrowly, we believe the proposed CRGR package misses the boat. The draft transmittal memo (Denton to Stello) describes the problem as follows: "The major areas of concern relating to the adequacy of safety-related DC power supplies stemmed from the dependence of shutdown cooling systems required for decay heat removal on DC power systems which normally meet the single failure criterion, and the potential for a sudden gross failure of these power supplies and thereby resulting in the shutdown cooling systems' inability to adequately cool the reactor core."

As exemplified by the control and instrumentation (C&I) bus fault events at H. B. Robinson, Zion, Rancho Seco, and Crystal River, we think the principal safety issue is as follows:

- 1) A C&I power supply fault can cause a critical challenge to standby ESF's, i.e., cases including trips, loss of main feedwater, loss of offsite power, and/or small LOCA.
- 2) The same C&I power supply fault could defeat some of the ESF's called upon to mitigate the initiating event, both core cooling systems and containment cooling systems.
- 3) The same C&I power supply fault could blind or partially blind the operators to the status of the plant.

The CRGR package, as it is now constituted, largely neglects the role of C&I power supply faults in causing serious initiating events and in blinding the operators; it treats the issue as though only item 2 above were the concern.

The element of the draft amendment to the SRP, Appendix 8A-3, which would partially cover this ground is element 6A, which is not recommended for any plant in the CRGR package and for which a benefit/cost assessment is missing in Enclosure 3. It calls for studies to verify that plants can take the loss of any safety related DC bus together with a single failure in the safe shutdown equipment. Some such safety analysis for OL's, including the effects of fault propagation and lost instrumentation we believe to be very important.

Some partial examinations of these issues followed from the Crystal River event of 1980 (NUREG-0667) and the Oconee event of 1979 (IE Bulletin 79-27). Nowhere does the CRGR package mention either, much less discuss what elements of the safety issues these early treatments may have left unexplored or unrectified.

Operating experience is treated in Section 2 of Enclosure 4. It mentions only the Zion event. We believe there have been dozens of events, of which the most significant were H. B. Robinson (1972), Zion (1976), Rancho Seco (1978), and Crystal River (1980). Only one of these appeared in the Precursor Study, NUREG/CR-2497. It ranked in the top three precursors. Two were missed outright and one occurred after the period studied. Had they been included, we think DC bus faults would have shown up as the most important generic category of severe accident vulnerabilities. We think it essential to survey this experience base, in the CRGR paper as well as in the underlying research, to develop the shape of the problem and the scope of the regulatory response. We believe that this approach would yield a different set of recommendations.

For these, and many other less serious reasons sketched in Attachment 2, we believe that the CRGR package needs a major overhaul and/or a follow-up program. For more information contact Frank Rowsome, X28016.

## Attachment 2:

### DST Comments on CRGR Package for Generic Issue A-30, DC Power Systems

#### I. Transmittal Memo, draft Denton to Stello

##### A. Paragraph 2, "major areas of concern"

The problem is construed too narrowly. DC faults are significant as triggers for initiating events such as loss of offsite power (e.g., Robinson, 1972) or small LOCA (Crystal River, 1980, and reactor coolant pump seal damage at Robinson, 1972). It is also a problem as it can blind operators to plant status (Rancho Seco, 1978 and Zion, 1976). If we decide to proceed with A-30 as is, the package should reference these broader concerns and the program to address them.

##### B. Paragraph 3 Related Issues

Systems Interactions, A-17, clearly has a bearing because of the functional dependencies upon DC power and the possible induced operator error due to faulted instrumentation. There is no mention of A-17 in the memo. [This may be moot if A-30 is given the narrow scope implicit in the draft package].

#### II. Enclosure 1, Summary of GI A-30 Resolution Documents and Reports

##### A. Relevant material omitted:

IE Bulletin 79-27 on fault effects of control and instrumentation bus faults, and licensee responses.

##### B. Preventative maintenance

Almost all of the more serious severe accident precursors entailing DC bus faults were caused by maintenance. Some care, and some coverage in the text should be given to considerations of attendant risks associated with more frequent maintenance.

##### C. Heavy dependence on NUREG-0666

This NUREG did a thorough analysis of a few stylized, hypothetical designs. I&C power supplies are commonly in the AE scope and show great variation from plant to plant. Neither the benefit/cost analysis nor the identification of needed fixes should depend so heavily on an analysis of a not-necessarily representative design. More emphasis should be placed upon LER's directly, and fashioning a requirement for plant specific analyses to be performed by licensees to obtain the dual benefit of 1) greater licensee familiarity with the weaknesses of his plant, and 2) identification of fixes that are truly cost effective and applicable to the subject plant.

D. Regulatory implementation

Ratchet by SRP amendment is convenient but this approach has been criticized as too cavalier and lacking strong legal foundation. If a thorough address is given to the possibility that plants may need retrofits to reduce undue vulnerability, rulemaking might be more appropriate. [Perhaps defer this to the follow-up program].

E. "Options", p. 5 et seq

The so-called "options" are sometimes treated in the CRGR package as purely regulatory options, sometimes as design variants, and sometimes as regulatory options applicable to certain design variants. This is highly confusing. The package should clearly distinguish between design differences among the plants as they are now and the regulatory options under consideration for each category of design or plant vintage.

F. Awkward title (p. 6): "II Document Supporting to Development of SRP Appendix 8A-3"

G. Cost/benefit of option 4 (p. 8)

Statements like, "The cost benefit results for Option 4 do not look favorable" are too simplistic. Presumably this is meant to imply (but doesn't say) that backfitting four batteries into a two battery plant isn't cost effective. This may or may not be true depending upon accident sequence vulnerabilities. However, there are many design variants including 4-battery plants that have so many designed-in common vulnerabilities that they are effectively two-battery plants with respect to reliability or risk considerations. Greater care should be taken to be thorough and accurate. The reader might well conclude that it is a waste of money to design a new plant with 4 distinct essential batteries, which is not at all true.

III. Enclosure 2

A. Awkward subheadings 2.B and 2.C

B. Supporting info should include an LER analysis, and related material such as NUREG-0667, IE Bulletin 79-27, etc.

C. 2.C.2 should mention A-17 as well as the other relevant USI's or GI's

D. Equipment (p. 5)

The text suggests that any required new hardware will be "standard industrial equipment". This is hardly appropriate for Class IE, safety-grade devices.

E. Risk reduction assessment (p. 6)

There is a significant discrepancy between the NUREG-0933 estimate and the quoted estimate from Enclosure 5. Why? Is it because the NUREG-0666 base case is a bounding-analysis for an atypical design? Generally prioritization valuations of the kind developed in NUREG-0933 should not be used to justify ratchets; they are generally too conservative and imprecise. Here, however, it appears that the NUREG-0666 basis may be even more conservative. It casts doubt on its validity.

F. Industry costs (p. 7)

We are suspicious of so much precision in light of the great variability in plant designs and the vagueness of the SRP amendment.

G. Risk reduction for Option 1 (p. 8)

The gigantic risk reduction of Option 1 looks to us to be a bogus artifact of the hypothetical base case. What do the IREP or RSS PRA's suggest Option 1 is worth? What about Big Rock Point or the SEP plants? The reader doesn't get any idea of either the costs or the benefits for real plants differing substantially from the NUREG-0666 base case design.

IV. Enclosure 3 "Summary of Cost Benefit Analysis & Staff Recommendations for Implementation of SRP Appendix 8A-3"

A. Cost/Benefit of Option 2

No treatment is given of the costs/benefits of Option 2. We believe this harbors the one truly important element to public health and safety, as noted in the main memo. [Perhaps reference the follow-up project].

B. Again, the benefits may be an artifact of the NUREG-0666 base case conservatism, rather than realistic estimates. See note III.G above.

C. (pages 7-8, Option 2) The logic presented for dropping Option 2 presumes the applicability of the NUREG-0666 base case results to all plants. Without the comparisons with other PRA's suggested in III.G this is not clear. Then, too, if there remain plants like Robinson was in 1972, or Rancho Seco was in 1978, for which an I&C bus fault plus a single failure (or equipment outage for test &

maintenance) could lead to a TMLB'-like severe accident, mere likelihood reduction for the bus fault does not leave us with the feeling that public health and safety is adequately protected. [Perhaps cross reference the follow-up project].

V. Enclosure 4 SRP Amendment (Appendix 8A-3)

A. The proposed SRP Appendix 8A-3 revision incorporates guidelines to make the DC power system more reliable; however, SRP section 8.3.2 which deals with DC power System does not identify the appendix as containing acceptable guidance. Also the appendix does not contain a clear and concise implementation section. Therefore, in order to assure that the proposal revisions to SRP sections will remain congruent with the requirements of NRC regulations, current regulatory guides and approved staff requirements and guidelines, we recommend the following changes:

- a. The guidelines should be incorporated into NUREG-0800 as Appendix A to SRP Section 8.3.2, DC Power System (onsite).
- b. SRP Section 8.3.2 should be revised to incorporate the reliability of DC power system review in accordance with the appendix attached to the SRP section (this includes area of review, acceptance criteria, review procedures, and evaluation finding subsections).
- c. SRP Section 8.3.2 or Appendix A to 8.3.2 should contain an implementation procedure. The procedures should identify what guidelines are being implemented on ORs, OLs, and CPs and any special implementation provision which may be applicable to near-term OLs and standard designs.

B. Operating experience (Section 2)

Section 2 lists only the Zion event of 1976. Other serious precursors ought to be discussed, or supplied in an appendix or reference. In addition, there are a large number of relevant LER's of statistical interest. These should be studied for patterns. It is my impression that the great majority of I&C power supply failures can be traced to faulty maintenance. There may be clues here to better guidance to reviewers and/or better guidance for the preparation of procedures and administrative controls. Perhaps DRA and/or DHFS should be called in to help work on this.

C. New designs

That new plants are coming in with more-than-minimal DC power systems suggests that the industry may know something we don't know, either about our regulations or about risk. We should probably look into this before we plunge into an SRP revision.

D. Guideline 1

What leads you to believe that administrative control and manual actuation (of cross ties) is more reliable than a properly designed automatic system? It seems to us that administrative controls are not among the industry's strongest points.

E. Guideline 3

Provision of "bypassed" or "inoperable" indication is clearly desirable in principle, but raises problems in practice. What power supplies should be employed for indicating a dead I&C bus? If the power supply for the annunciation could be subject to common cause failure, might it not mislead operators into failing to diagnose the fault? More thought may be needed on this one. Perhaps we need small, dedicated batteries like those for building fire lights (Coconut Grove lights) to assuredly annunciate dead I&C power supplies. Perhaps the mere absence of illumination of a pilot light would do to flag dead I&C buses. DHFS may have some good advice on this.

F. Guideline 4. Procedures and Administrative Controls

In light of the importance of maintenance error in I&C bus faults historically, a more demanding approach than these motherhood admonitions may be called for. We suggest that a thorough FMEA and common cause failure analysis be required of all licensees for hypothetical errors in the conduct of surveillance, maintenance, and administrative controls.

G. Guideline 5. LCO's for surveillance and preventative maintenance

See note II.B above.

H. Guideline 6A [Applicable to follow-up project]

This guideline is the closest approach to be found in the package to a treatment of the common-cause failure potential in I&C bus faults. We certainly think it necessary that all plants be able to survive every I&C bus fault together with a single failure, i.e., that each I&C bus failure be treated along the lines of a DBA. However, it may not be enough. We may want more stringent

requirements to apply to vulnerabilities sharing more of the following attributes than we do for vulnerabilities which are addressed in 6A.

Given an I&C bus failure, together with a reasonably probable single fault (which may be a plausibly coincident initiating event, active failure, outage for test or maintenance, or human error), together with the probable consequences of fault propagation and operator action/inactions in response to the bus fault and other failure:

1. Does an initiating event occur that poses a critical challenge to standby engineered safety features?
2. Do the ESF's available to cool the core fail to start automatically?
3. Do the ESF's designed to cool the core fail outright (neither autostart nor manual start)?
4. Are the operators blinded or are they plausibly misled by the instrumentation faults so they either fail to take appropriate action or take counterproductive actions?
5. Does containment isolation work?
6. Does containment heat and/or radioactivity removal systems work?

Guideline 6A might not catch some of the more serious possibilities, i.e., a vulnerability that causes an initiating event and misleads operators and defeats containment heat removal, but does not directly (except through the operators) threaten core cooling. Also Guideline 6A doesn't discriminate between vulnerabilities that are expected to yield well-contained core damage from vulnerabilities that could plausibly cause very severe releases.

A further potential problem with 6A is that it doesn't extend to common-cause failures of two or more I&C buses, which may not have negligible probability despite guidelines 1-5. A thorough common cause failure analysis to explore for such vulnerabilities should be called for, perhaps in Guideline 4. Thus Guideline 6A (if used) should have criteria for inclusion of common-cause multiple I&C bus faults within the scope of 6A if they are of appreciable likelihood.

Yet another problem with 6A is associated with satisfying ourselves that all the probable effects of the I&C bus fault are considered. Qualitative treatments such as FMEA methods depend upon engineering judgment. Subtle fault propagation paths, like the one that resulted in the latched open PORV in the Crystal River event of 1980, are easy to miss. We need standards by which to judge that all the significant fault effects have been identified. The problem is complicated by the wide variety of plant configurations (value alignments, switch settings, modes of operation) that might be present at the time of the bus fault. Also relay races and switching sequences in response to the I&C power transient are hard to explore thoroughly, but might well harbor the unpleasant surprises we want to discover. Clearly we will need a good systems interaction analysis (related to A-17) to accompany the analysis of hypothetical I&C bus faults. Some care must be taken to keep this in mind when we review what was learned from IE Bulletin 79-27.

#### I. Guideline 6B

Clause 6.B a) appears to contradict the SRP which now calls for fully safety grade equipment for the transition from power generation to cold shutdown. Both safety grade and non-safety grade DC power supplies could make more trouble than its worth.

Clause 6.B b) doesn't address the heart of the issue: you want to be sure that no loss of safety grade I&C power supplies will prevent the powering of the non-essential switchgear buses, and a minimum complement of essential switchgear buses with offsite power. You may also want redundant power supplies for aligning the startup transformer and/or alternate transformer to bring power into the non-essential switchgear buses from the switchyard. 6.B b) could be literally satisfied without achieving either of these functional objectives.

We really need, we think, much more functionally and/or risk oriented criteria for taking exception to the DBA/SF guideline of 6A.

J. Guideline 8

If we are to require more than two essential I&C power supplies of new plants, and we think we should, then specifying more than the mere number is necessary to achieve anything significant to risk. What separation criteria?

How may the four I&C power supplies be mated with one another in logic modules and with AC power divisions in controlled or actuated ESF's? What kind of dependency or systems interaction or common-cause failure analysis is necessary? See also comment V.C above. Some care to establish review guidelines, if not ratchets, for the four-division designs we are receiving for CP review these days appears to be warranted.

VI. Enclosure 5 Cost-Benefit Analysis

A. Redundancy

There appears to be unnecessarily many cost/benefit analyses in the CRGR package. Why repeat it so many times? This one - Enclosure 5 - appears to be the best one technically, although some elements of the regulatory analysis are given elsewhere.

B. Dependence in NUREG-0666 design assumptions

Note prior comments on the biases this introduces. See, e.g., comment II.C, III.G, etc.