218
0-31-81
(circled scribble)

(1)
B6841

LA. 2979

ALO-140

Printed: August 1981

MASTER

UCLA-ENG-8056

**ON THE APPLICATION OF DISTURBANCE ANALYSIS
METHODOLOGY TO SAFETY RELATED TRANSIENTS
IN THE ELECTRICAL SYSTEMS OF A NUCLEAR
POWER PLANT**

**S. GUARRO
D. OKRENT**

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

CHEMICAL, NUCLEAR AND THERMAL ENGINEERING DEPARTMENT

UCLA • SCHOOL OF ENGINEERING AND APPLIED SCIENCE

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use or the results of such use of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Printed in the United States of America

Available from
National Technical Information Service
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

Price: Printed Copy \$7.25; Microfiche \$3.00

DISCLAIMER

This book was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Distribution Category
UC-78

ALO-140
UCLA-ENG-8056

ON THE APPLICATION OF DISTURBANCE ANALYSIS METHODOLOGY
TO SAFETY RELATED TRANSIENTS IN THE
ELECTRICAL SYSTEMS OF A NUCLEAR POWER PLANT^Q

S. Guarro
D. Okrent

Prepared by

Chemical, Nuclear, and Thermal Engineering Department
School of Engineering and Applied Science
University of California, Los Angeles
Los Angeles, California 90024

Prepared for

U. S. Department of Energy
Light Water Reactor Safety Technology Management Center
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sponsored by

U. S. Department of Energy
Division of Nuclear Power Development
Washington, D. C. 20545

Work performed under Sandia Contract No. 61-1231

Submitted: September 1980
Printed: August 1981

TABLE OF CONTENTS

	Page
CHAPTER 1: DISTURBANCE ANALYSIS SYSTEM METHODOLOGY IN SAFETY ORIENTED APPLICATIONS	1
1.1 Main Functional Characteristics of a Disturbance Analysis System	1
1.2 Problems Associated with the Application of the DAS Methodology to Safety Related Transients	7
1.3 Description of the Significant Event Analysis (SEA) Applied to the Derivation of the DAS Logic Structures	15
CHAPTER 2: AN APPLICATION OF THE SIGNIFICANT EVENT ANALYSIS TO THE ELECTRIC POWER SYSTEMS OF THE SAN ONOFRE NUCLEAR POWER STATION, UNIT ONE	31
2.1 General Considerations	31
2.2 San Onofre 1 Electric Power Systems Configura- tion and Protective Logic: Identification of an SE to be Analyzed	34
2.3 Event Tree for the SE "Insufficient Power on Both Emergency Buses (1C and 2C)"	39
2.4 Fault Tree Structure for the Event "Insuffi- cient Power on Bus 1C"	44
2.5 Discussion of the Information that can be Pro- duced by a DAS Utilizing the Fault Tree Structure for the Event "Insufficient Power on Bus 1C"	49
2.6 A Few Additional Considerations on Some of the Branch Points in the Event Tree for the SE "Insufficient Power on Both Emergency Buses"	58
CHAPTER 3: A CRITICAL LOOK AT THE APPLICABILITY OF THE DAS AND SEA METHODOLOGIES TO TRANSIENTS THAT HAVE OCCURRED IN THE ELECTRICAL SYSTEMS OF NUCLEAR POWER PLANTS	97
3.1 General Purpose of a Qualitative Evaluation of the DAS Performance with Regard to some Reported Electrical Transients	97
3.2 Electrical Transients Initiated by Testing and Maintenance Operations	99
3.3 Electrical Transients Occurred During Plant Normal Modes of Operation	109

	Page
CHAPTER 4: CONCLUSIONS	137
4.1 Remarks on the General Features of the DAS and SEA Methodologies	137
4.2 Some Observations on the Particular Nature of the Transients of Importance in Electrical Systems, and the Consequences on the Associ- ated DAS Logic Structures	141
4.3 Some Practical Recommendations for Effective Ways of Implementing a Disturbance Analysis on the Electrical Systems of a Power Plant . . .	143
REFERENCES	147

LIST OF TABLES

	Page
2.I Legend for Figs. 2.8 through 2.20 and Table 2.II	62
2.II Partial List of "Basic Cut Sets" for the Event "Insufficient Power on Bus 1C"	63
2.III Classification of "Basic Cut Sets" According to Common Observable Conditions	70

LIST OF FIGURES

		Page
1.1	Examples of fault-tree and cause-consequence structures	25
1.2	Illustration of DAS/Process possible levels of interface	26
1.3	Illustration of logic structure pruning procedure . . .	27
1.4	Example of subdivision of a simplified plant parameter space into safety related domains	28
1.5	Illustration of a hypothetical plant state vector trajectory in the simplified plant parameter space	29
1.6	Example of event-tree structures originated by application of the SEA methodology	30
2.1	San Onofre 1: main one line diagram	75
2.2	San Onofre 1: simplified one line diagram of electrical system between 220/138 KV switchyards and 4.16 KV buses	77
2.3	San Onofre 1: 220/138 KV substation one line diagram .	78
2.4	San Onofre 1: 4.16 KV system one line diagram (buses 1A and 1C)	79
2.5	San Onofre 1: 4.16 KV system one line diagram (buses 1B and 2C)	80
2.6	Simplified event tree for the event "insufficient power on both emergency buses"	81
2.7	Event tree for the electrical systems potentially associated with the event "insufficient power on both emergency buses"	82
2.8	Fault tree for the event "insufficient power on Bus 1C".	83
2.9	" " " " (continued) " " " " .	84
2.10	" " " " (continued) " " " " .	85
2.11	" " " " (continued) " " " " .	86

	Page
2.12 Fault tree for the event "insufficient power on Bus 1C".	87
2.13 " " " " " (continued) " " " " "	88
2.14 " " " " " (continued) " " " " "	89
2.15 " " " " " (continued) " " " " "	90
2.16 " " " " " (continued) " " " " "	91
2.17 " " " " " (continued) " " " " "	92
2.18 " " " " " (continued) " " " " "	93
2.19 " " " " " (continued) " " " " "	94
2.20 " " " " " (continued) " " " " "	95
3.1 Duane Arnold: 125 VDC control power distribution system	130
3.2 Beaver Valley: 345/138 KV system interconnections . . .	131
3.3 Beaver Valley: 345/138-4.16 KV distribution system . .	132
3.4 Beaver Valley: main transformer fault	133
3.5 Beaver Valley: main generator out of step relays . . .	134
3.6 Oyster Creek: 230/34.5 KV-4.16 KV distribution system .	135
3.7 ANO 1 & 2: simplified block diagram of electrical distribution system	136

ABSTRACT

The present study tries to address the question of whether or not the computerized on-line procedures known under the name of "DAS" (Disturbance Analysis System) can be usefully and successfully applied to provide timely diagnostics and operational "suggestions" during the occurrence of a major electrical transient in the auxiliary systems of a nuclear power plant. The perspective of the study is from the plant-safety point of view.

For the reader not familiar with the DAS methodology we will provide in the first section of Chapter 1 a short definition of its relevant features and capabilities. Chapter 1 also includes a discussion of some of the problems of a general nature that are encountered in DAS safety-oriented applications. It then presents a method of analysis that will be used in the rest of this work, one which is based on a particular combination of the well known methodologies of event-tree analysis and fault-tree analysis.

Chapter 2 will deal specifically with the event "insufficient power on both emergency buses," with reference to a particular plant design (San Onofre 1). The analysis performed there has mainly the purpose of showing the extent to which DAS methodology can be applied to an existing configuration of the vital electric systems of a nuclear power plant and the kind of information it can accordingly provide.

Chapter 3 examines some transients that have recently occurred in the power supply systems of operating plants and considers whether

or not a DAS could have successfully dealt with such occurrences , and whether or not the information provided would have been effective in reducing the severity of the transient.

The final Chapter 4 contains a discussion of the relevant points that emerged from the analysis performed in the first three chapters. In short, these points can be summarized as follows:

- the DAS methodology can be considered adequate to deal with electric transients, if the main objective is to detect and diagnose substantial system faults and misalignments. Continuous time modeling features don't seem to be particularly useful, given the special nature of such transients.
- quantitative criteria to evaluate the usefulness of a DAS in absolute (i.e.: DAS vs. no DAS) or relative terms (i.e.: DAS capable of handling certain disturbances vs. certain other disturbances) are not available. Nevertheless, the indications gathered here seem to be at least favorable to the development of further studies in the area of disturbance analysis applied to electrical systems;
- the application of the DAS methodology at "high level" (that is, leaving out most of the failure mode analysis regarding components rather than systems) doesn't seem to be adequate, at least for the type of events considered in this study;
- any serious, application-oriented effort to develop a DAS should be only attempted in full awareness of the necessity for a good coordination and integration of the knowledge associated with several areas of nuclear plant design and analysis, such as plant control

and protection logic, component failure mode analysis, and fault tree analysis. The development of a DAS requires a great deal of detailed information which is available to the designer.

ACKNOWLEDGMENTS

This material is based in part upon research supported by the Department of Energy under Contract DOE ET-78-S-04-Mod 1, entitled, "Studies on Improvements of Light Water Reactor Safety" and ERDA EY 76-S-03 0034 P.A. 252 entitled, "Low Probability Events and Reactor Risk Assessment."

Any opinions, findings and conclusions in this publication are those of the authors and do not necessarily reflect the views of the Department of Energy.

The authors wish to thank Messrs. Fred Tajaddodi and Sigmund Stone of Bechtel Co., Los Angeles, for their many useful suggestions.

CHAPTER 1

1. Disturbance Analysis System Methodology in Safety Oriented Applications

1.1 Main Functional Characteristics of a Disturbance Analysis System

Even though at the present time only two DA systems have been developed^(1,2) and both are in a prototype-evaluation stage, it seems very unlikely that future applications would differ substantially from these two as far as the basic methodology is concerned. So it can be stated in general that a typical DAS consists at the functional level of the following parts:^(3,4)

a) Process Model:

This must be developed and included in the DAS software for all the plant systems and subsystems for which disturbance analysis capability is desired. The main requirement for this model is that it must include the cause-effect relations linking the system component conditions, normally described in a discretized manner (e.g.: "failed"/"working" etc.), and the values assumed by the relevant process parameters, also usually discretized as "normal"/"low"/"high" etc.

It is generally agreed that, at the present time, the most convenient way of providing the process model is in the fault tree or in the cause-consequence form. The "fault tree" expresses, essentially by means of the logic gates "OR" and "AND", the logic relations that must exist among sets of system primary conditions in order that a certain identified event (called the

"top") exist, with no special provisions made to describe any necessary sequential order to be observed by the single primary conditions or by particular subsets of these. In fact the structure of such a tree is not intended to describe the time evolution of the cause-effect relations existing between particular sets of conditions contained in the tree. In the most common applications, the primary conditions that form the base of the tree are usually statistically independent of one another. This condition is not respected in DAS applications, as we will see in the next chapter, due to the fact that a DAS fault tree has to describe, as contemporary sets of conditions, logic combinations of events that are actually linked through sequential relations of cause and effect. The "cause-consequence tree" (or diagram, as it is often called) is not substantially different from a fault tree of the DAS modified type (as was just defined above*), but the description of the cause consequence relations existing among system conditions (or sets of conditions), within the time frame in which such cause-consequence relations take effect, will be explicitly provided in it.

A clarifying example is given in figure 1.1. The fault tree a) and the cause-consequence diagram b) describe exactly the same essential logic, i.e., that the "top event", condition A, is verified if both the primary conditions B and C are verified. This is actually all the information that it is possible to

* This point would be better explained in Chapter 2, with specifically applicable examples.

derive from the fault tree a). On the contrary the cause consequence diagram b) tells us also that, if the event represented by condition B occurs at time $t=t_B$, and the one represented by condition C occurs at time $t=t_C$ with $t_C+\tau_2 > t_B+\tau_1$ ($t_C+\tau_2 < t_B+\tau_1$), the intermediate condition D will be verified (that is, event D will occur) at $t=t_C+\tau_2$ ($t=t_B+\tau_1$) and the top event will follow at $t=t_C+\tau_2+\tau_3$ ($t=t_B+\tau_1+\tau_2$).

It is thus seen that the cause-consequence diagram can give a more complete description of the real process, which makes it at the same time a more powerful tool for analysis and a much more difficult one to use in practical applications. In a real process in fact, the determination of such quantities as the time delays between the relevant diagram "nodes" is a painstaking and delicate task requiring a very detailed knowledge of the process (especially considering that these quantities are not fixed once and for all, but vary as functions of other process parameters such as temperatures, flowrates, etc., and of the plant's different modes of operation). It would seem therefore that unless it can be clearly proven that the cause-consequence diagram technique is needed to achieve the results desired for a specific application, the simpler fault tree technique should be preferred for derivation of the process model, at least at the first level of approach. This seems to be very reasonable considering the fact, apparent from what we said above and from the example of figure 1.1, that a cause-consequence structure can be obtained at any time, using as a starting point the fault tree structure

derived previously for the same portion of the process being considered.

Once the logic structures representing the process model have been derived, in whatever form is considered convenient by the DAS designer, they are translated in a form suited for permanent storage in the DAS computer unit, and become one of the data bases. Superimposed on the structure of the process model we can picture another structure, made up of the messages to be displayed to the operator when a condition is found verified. In principle, there could be a message (diagnostic and/or suggestive of specific actions to be taken to stop or mitigate the propagation of a disturbance) attached to every identified condition. In practice there would be a choice made beforehand, at the time of derivation of the process model logic structures, to display only the messages corresponding to some of the identified process model conditions. This choice could be made on the basis of several considerations, including the need to display only "meaningful" information and the desire not to present the DAS-elaborated information as an absolute truth to the human operator.

b) Process Interface:

This is the part of the disturbance analysis system that takes care of the continuous input of data from the process to be analyzed. Technically, the ways in which this module performs its task can vary, but in essence its function will be to monitor a number of

process variables and detect when any of those go beyond or below certain preset limits. At regular time intervals a "process image", made up of the discretized values of all the variables monitored (for instance -1 for values below a lower limit, 0 for normal values, and +1 for values beyond the upper limit), will be compiled by this module and passed on to the "analysis module".

c) Analysis Module:

This is the DAS computer procedure that is assigned the task of recognizing which branches of the logic structure representing the process model are activated. This is done by using the "process image" provided by the process interface, to determine which of the conditions appearing in the fault-tree (or cause-consequence) structures are actually verified.

In the present demonstrative DAS's some differences exist in the way this module operates and interacts with the process model, but the essential features and functions remain the same.

The analysis module also interacts with the last as yet unmentioned component of a typical DAS; the "operator interface", to which it passes the diagnostic and suggestion messages that it finds activated during its evaluation of the process image against the logic structures of the process model.

d) Operator Interface:

This consists essentially of the devices belonging to the DAS system that are specifically designed to provide the plant operator with the information elaborated by the DAS itself. In the most restricted applications it would basically perform the

function of receiving the messages selected by the analysis module and displaying them in a suitable form (typically on a color CRT) to the human operator. In DAS's designed for operator's interactive interventions, it would also provide (by means of a keyboard or similar device) the channel for "questions" or on-line inputs to the DAS from the operator. It is not the purpose of this short description to go into the details of such special provisions. It can, however, be said that an interactive capability can be foreseen in large complex DAS's where, for instance, after receiving a message the operator could request the DAS to display the active branches of its logic structures that have produced that message. In such a way he would obtain the information necessary to check if the DAS "conclusions" were undoubtedly appropriate or not.

The description presented above, although limited to the essential functional features, should be sufficient for a basic understanding of the principles upon which a DAS operates and of the objectives that it can potentially meet. It should be noted that early investigations of the subject of the best possible applications of a DAS were focused on the main objectives of increasing plant availability, with little attention given to the potential results obtainable in the area of plant safety. The next section tries to give an introduction to some of the problems that are encountered when dealing with this second type of application.

1.2 Problems Associated with the Application of the DAS Methodology to Safety Related Transients

From the short description of the DAS basic methodology given in Section 1.1, it clearly appears that the most crucial stage in its implementation will be at the time of deriving the logic structures that make it possible for the system to perform its diagnostic and operational* functions. It should, in fact, be kept in mind that a DAS is only capable of recognizing the occurrence of faults (or, more generally, transients) that are somehow modelled in its logic structures, and that therefore have been recognized as possible by the DAS designer. If a fault or transient occurs that has not been recognized as possible, and therefore has not been modelled, but which contains one or more DAS-modelled faults or transients as subsets, then only a partial diagnosis would be provided by the system, corresponding to these particular subsets. In other words, this would correspond to the case of a disturbance "D" that can be described in full by the "activation" of n_D logic conditions, of which only $n_x < n_D$ are actually anywhere included in the DAS "process model", with n_I of them possibly representing a disturbance "I", contained in the large unmodelled one, n_J another ("J"), etc. The partial diagnosis provided by the DAS would then be represented by the messages associated with the recognition by the system that the

*in the form of "suggestion" messages to the operator for appropriate corrective actions.

disturbances I, J, etc., are occurring*.

On the other hand, the objective of developing an all-comprehensive safety oriented DAS (that is, a system capable of detecting all the possible malfunctions in plant components with a potential impact, immediate or delayed, on the safe operation of the plant) does not appear to be realistically achievable. It is in fact possible to realize at first sight why the complexity of such a system would be overwhelming. It can be, nevertheless, worthwhile for the sake of a better understanding, to take a closer look at some of the problems that should be solved by anybody aiming at an objective of that complexity.

We will concentrate our attention on the problems that would arise at the "process model" and "process interface" level, ignoring other problems of a less conceptual and more technical nature, like, for instance, the need to keep the DAS total computer memory occupation and the computer execution time of the analysis module within reasonable limits (Remember that the DAS analysis must in general be executed on line in order to be of any use.)

In order to derive an all-comprehensive process model for the plant, the following would be needed.

- a) An unequivocal definition of all the plant components, and of all the functions they perform in the various plant operation modes.

*This possibility should be kept in mind when preselecting the diagnostic messages to be displayed by the DAS; that is, the message giving the diagnosis for a disturbance "I" should be worded in such a way as to suggest that the possibility does exist that disturbance I be only the "visible" part of a larger disturbance D which is not completely modeled in the "process model".

- b) a complete definition of the failure modes and operational upsets that can prevent the above mentioned components from performing their intended functions.
- c) a complete definition of those process parameters the observation of which could allow the identification of the operating states of all the plant components with respect to their possible functional failures and/or operational upsets.

The above three tasks are very strictly interrelated. For instance if one were to define a component in such a way that a reasonably low number of "state parameters" could describe its operational conditions satisfactorily, one would be naturally led into breaking down the plant and the plant systems in a large number of functional components. This way of proceeding could facilitate the identification of the potential component failure modes, but the task of correlating the failures and/or operational upsets of different components in a cause-effect scheme, would not be simplified by such a procedure. The question of completeness in the definition of the failure modes, and of particular types of interrelations existing between them, such as mutual induction of apparently unrelated failures or common cause mechanisms etc., would in any case remain open.

Another specific problem area is the one mentioned in point c), especially if one considers the practical limitations that will be imposed on the DAS at the "process interface" level. Even if we assume in fact that we had discovered a way of identifying unequivocally the operating states of all plant components by an appropriate choice of a number of state parameters (that is, we had defined a large set of physical variables whose values could be discretized and grouped in proper combinations to define the operational conditions of any one of such components), this would remain a merely theoretical exercise, since the number of process parameters that are actually accessible in a real plant is relatively limited and cannot be increased indiscriminately.

As we mentioned before, the purpose of the above discussion is not so much to convince ourselves that the objective of deriving a DAS capable of covering with its diagnostics all the potential malfunctions of a nuclear power plant is too ambitious. To arrive at this conclusion doesn't actually require much questioning. The important point to consider here is that the specific problem areas that were mentioned above are typical, with varying degrees of complication, of any DAS application that can be conceived. The first question that we have then to address is naturally the following: what kind of safety applications can indeed be attempted with reasonable hopes of success? In other words: what criteria can be used to reduce the "impossible" objective of an all comprehensive, safety oriented DAS to something within the reach of our present DAS methodology and yet still

meaningful and useful for the improvement of the overall plant safety? With regard to this question there seem to be at least two different approaches that could be followed.

If the designer considers from the beginning the currently existing practical system limitations (computer memory occupation, maximum possible number of plant parameters that can be covered by the "process interface" etc), but still wants to cover with a DAS monitoring the largest possible number of plant areas that are relevant to safety, he will have no other choice than to compromise with respect to the level at which the DAS monitoring and diagnostics will be provided. If we follow the conceptual sketch of figure 1.2 to visualize a hypothetical plant system-component hierarchy, this means that, in order to reduce the size and complication of the logic structures needed in the DAS "process model" and in order to be consistent with the "process interface" size allowed by the existing plant instrumentation, the level of DAS implementation would be limited for instance only down to subsystems. No further information relevant to the particular situation occurring and affecting the overall plant safety would be sought at the component and subcomponent level. The problem here would be clearly in that there might exist two different plant malfunctions that could be recognized as being different if analyzed at the component or subcomponent level but that will not if analyzed at the subsystem level. This could cause trouble if the recovery actions needed to bring the two disturbances under control were to differ substantially. A general class of disturbances that could originate problems of this nature is for example the one associated with instrumentation failures, in which a DAS, without the capability of double checking

(via the use of "diversified" or "indirect" readings) the value(s) of the parameter(s) measured by the faulty instrument(s), could be fooled into diagnosing a non-existing disturbance or one in fact very different from the one actually occurring. It should be kept in mind however that problems of this sort are not uniquely associated with instrumentation failures. In fact, for instance, the potential for indistinguishability of different disturbances will increase whenever the DAS implementation level is kept high (systems or subsystems rather than components etc.). Therefore the designer should be very cautious during the derivation of the logic structures for a DAS to be implemented at "high level".

The other possible approach is conceptually quite different and proceeds from the definition of a number of possible disturbances that can be considered particularly relevant in affecting the safety of plant operation. When we say "disturbance" in this context, what we really mean is some well defined event that is clearly potentially dangerous to the safe operation of the plant. Starting from the definition of such an event, the DAS design would then proceed with a two-fold analysis as outlined below:

- using the fault tree approach, with the above mentioned event as the "top event", derive the process logic structures from this level down to the "primary cause level", beyond which the disturbance analysis would not seek further detailed information. This "primary cause level" corresponds to what we have called before, the DAS "level of implementation".

- using the event tree approach, with the above event as the

starting point, proceed to verify which specific plant systems or subsystems would be in particular affected by its occurrence and how their operating status would in turn influence the path of disturbance propagation. The main advantage of this approach is in the fact that it makes the designer very aware of the modeling capabilities and limitations of the logic structures that he can derive in such a fashion. Also, the process model can be extended step by step by adding one model, corresponding to a specific set of disturbances, at every step. If any overlapping branches exist in the logic structures derived for different disturbances, it should be possible to identify them by inspection. This would help to prevent problems at the diagnostic level and ambiguities at the operator interface level (i.e., improper choice of the DAS messages, etc.).

If a general process model is derived in this fashion, the envelope of disturbances that will be "contained" in it (that is the ones which the associated DAS will have the capability to deal with) will be known to the designer. The DAS "level of implementation" will be determined according to the choice of the disturbances to be modeled, and more precisely according to the nature of the logic structures that will be derived for them. So, for example, after deriving the logic structure for a disturbance "X" in a manner as complete as possible in order to understand all the possible variations of that disturbance, the designer can decide to simplify it for use by the DAS, by "pruning" some of the lower branches of the tree structure. This is graphically illustrated in figure 1.3, where it can be seen that in a case of this kind the pruned branches are obviously substituted by

suitably defined "primary causes", or "primary events" (in figure 1.3, part a) represents a logic structure derived at the time of analyzing the disturbance X as hypothesized by the designer, and part b) represents a corresponding "pruned" structure to be utilized by the DAS in its on-line analysis).

Of the two approaches discussed above, the latter will be more or less closely followed in the present work. We choose for this approach the name of SEA (Significant Event Analysis) for obvious reasons that will be made even clearer in the next section. There we shall give a more complete discussion of its characteristics, and of some of the rationales for its use in the proposed form.

1.3 Description of the Significant Event Analysis (SEA) Applied to the Derivation of the DAS Logic Structures

In the previous section we have already given a partial discussion of the inconvenience of deriving the DAS logic structures by starting to model individual component faults and then trying to correlate these faults to find out how they can combine to produce disturbances. The very high number of the possible faults would make it in fact very easy to overlook some of their logic combinations as potential disturbances, to say nothing of the very difficult task of deriving a thorough initial "list" of such individual faults.

Equally unfeasible, because of its overwhelming complexity, would be the mere application of a fault tree procedure from top to bottom, if the top event were chosen to be too generic (as for example the event "core damage is occurring").

The most reasonable approach would therefore consist in starting by considering a number of events beyond the stage of single component faults, which have already developed into occurrences of clear significance to the overall plant safety, and yet are still simple enough in their manifestations that a clear definition of them would not be too difficult. A selection of such events can be initially based, for instance, on the results of some of the recent probabilistic safety studies that have attempted to identify the major contributions to the total risk of a nuclear power plant. But clearly the criteria for such initial choice could vary according to the objectives of the study to be made (feasibility, demonstration, real design, or else). In any case, the result of this selection should be a list of events that are

of importance from the point of view of plant safety and that are easily definable (which justifies the use of the conventional name of "significant event analysis" for this type of approach). From there the analysis will proceed by looking at each of these events individually and in a two-fold manner, that is, using both the fault-tree and the event-tree methodologies as outlined in section 1.2.

Before proceeding in our discussion of the steps involved in the derivation of the DAS logic structures, it is convenient to consider briefly what typically would be the nature and "mechanism" of a nuclear-power-plant safety-related transient. This will help us in identifying the basic criteria that can be employed in the definition of the "significant events" from which such derivation can be started, and of the type of approach that can be followed in the rest of the derivation itself.

All nuclear power plants are designed to be provided with a multiple line of defense against every possible type of operational upset or accident that is included in their design bases. This multiple line of defense consists of a number of safety systems, operable under automatic controls according to specific protection logics and, in most cases, also upon manual command by the plant operator. Therefore, once a transient* has started on a certain initial path, as determined by its primary causes (failures internal to the plant and/or upsetting external influences), the rest of its course would be very likely determined by the behaviour of such safety systems and their

*By transient we intend here a dynamic sequence of events that cannot be simply accomodated for by the action of the regular plant control loops.

ability to respond when called upon in order to modify the "natural" initial path. If we look at the problem in a more precise way, and we investigate more closely the way in which the plant safety systems operate (limiting our attention for the moment at their automatic actuation logic) we can see that their intervention is determined by the values of a number of important plant parameters (temperatures, pressures, flowrates, etc.), which may exceed certain pre-fixed set-points. In the n -dimensional space of the state vector having these plant parameters as components, the fixed set-points for intervention of the safety systems will determine what we can call a "safe domain" (SD). If the state vector is inside this domain, any transient occurring in the plant will be in its "natural" stage (that is determined only by its primary causes and by the regular control loops of the plant). If the state vector goes outside the domain, one or more safety systems should start operating, trying to modify the "natural", and under these circumstances, undesired course of the transient; unless some malfunction inhibits their operation to a substantial extent.

If we develop this concept a little more, we can conclude that actually the whole n -dimensional space of the state vector can be divided in a number of well identified domains: the "safe domain" (or SD, as defined above), plus all the domains characterized by the intervention (as hypothesized by the plant designer) of one particular combination of plant safety systems. This is illustrated for a simplified PWR situation in which only a couple of the significant plant parameters, with the related plant safety systems, are taken

into account, in figure 1.4. The space outside the "safe domain" can, according to this scheme, be divided into K separate "safety system intervention domains" (SSID's) where K will be the number of possible combinations of plant safety systems, operating alone or together.

The above considerations are very general in their nature and therefore will surely require a good amount of flexibility when applied to real situations; however, they give us a basis to understand what kind of useful functions a DAS can provide in a plant-safety type of application. If in fact we refer now to the purely illustrative picture in figure 1.5, we can see that the dashed line represents a particular trajectory of the state vector representing a process (that for simplicity we imagine here as fully described by only two components, p and ΔT). Such a trajectory represents what we would normally call a "transient", and a number of questions can be raised in relation to it, the most important of which we try to summarize below:

- a) whether or not the state vector trajectory, which is normally well inside the safe domain, is approaching the borders between this and any one of the safety systems intervention domains (SSID's)
- b) if the answer to a) is yes, why this would be occurring
- c) if the answer to a) is yes, which one of the K safety system intervention domains the state vector would enter
- d) if the state vector enters the k -th SSID, how the corresponding safety systems would respond and modify the state vector "natural trajectory."

- e) repetition of function d) for every other SSID that the state vector may possibly enter before stopping in a final stable position.

A DAS designed to answer the above questions will then have to perform the following functions:

- activate itself when the state vector passes point B of the trajectory
- while the state vector is covering the section BC of its trajectory, try to identify the primary causes of the transient and the possible remedies to avoid the crossing of the safe domain border line.
- if such crossing occurs and the SSID #1 is entered (section CD as hypothesized in figure 1.5), monitor the performance of the associated safety systems, making sure that they can perform their intended functions.
- similar monitoring for the SSID #3 (section DE of trajectory) and similarly for any other SSID's possibly entered in a more general situation, in the subsequent stages of the transient.

A rather important deduction that we can draw from the general concept illustrated above concerns an apparently natural criterion that can be used to classify the disturbances that may develop in the process considered. If in fact we consider all the "natural" trajectories of the process state vector that are bound to cross one specific borderline between the safe domain and the k-th safety system intervention domain, we can tentatively group them in the same class of disturbances. If we have been able to identify K SSID's bordering

with the SD, we will therefore end up with an initial classification of disturbances into K classes. It might be worthwhile in this regard to clarify that we are here talking about safety systems in a rather extended context, which could include in practice some of the simplest protection systems (such as the circuit breakers of the electrical power systems) and even, if judged to be convenient, some of the control systems whose operation might appear to be safety related to some non-irrelevant extent (such as the pressurizer relief valve or the secondary loop steam dump system, etc.). As we pointed out before, in order to make a beneficial use of the above theoretical framework some degree of flexibility in its application will be necessary.

Another important point to be made here, one which is closely related to the above classification of disturbances, regards the very definitions of the "significant events" that were mentioned before. If in fact we were looking at some plant system and we had already identified the relevant related SSID's according to the method previously outlined, we would be facing the problem of identifying at least a few significant events from which to start the derivation of the DAS logic structures. We have discussed above how the identification of the various SSID's leads, practically at the same time, to a more or less theoretical definition of the distinguishing characters of a number of classes of disturbances. Therefore a significant event can be envisioned as any realistically possible disturbance having all the distinguishing characteristics of a certain class. Typically such a disturbance can be labeled as a "significant event" when still in its "natural" stage and right before crossing the border line between the

SD and the SSID considered. In fact at that particular stage, being still unchecked, it will carry the greatest hazard potential for the plant, and thus, in this particular context, the greatest significance. Therefore it can be envisioned more easily by the process analyst. To clarify the above we can present the following example:

- suppose we had identified an SSID relevant to the primary circuit of a PWR, as characterized by values of the primary coolant loop pressure below 1600 psia but above 400 psia for a substantial duration of time, and by the corresponding sole intervention of the HPIS (we assume for simplicity that we need not be concerned with plant parameters other than the primary coolant pressure).
- we can then accordingly define a class "X" of disturbances (purely theoretical for the moment) as comprising all those transients in which the primary coolant pressure would start decaying at some time, from the normal range of values, towards lower values (say below 2000 psia), but at a rather slow depressurization rate. We can in fact reasonably envision that for disturbances of this class the state vector will cross the border of the aforementioned SSID and remain in it for a non-negligible amount of time.
- the above characterization leads us then in the next step to visualize a small LOCA; since this event might still be judged a little too general, we can try to be more specific by considering some better defined events included in this same general classification (such as small pipe break, coolant pump seal leak,

pressurizer relief valve leak, etc.) but keeping the basic requirement that, if such an event is hypothesized as occurring, the next event to follow would be the intervention of the previously identified safety system (if this is not in a failed condition).

As was pointed out at a previous stage of this discussion, the practical selection of the significant event to be modeled and analyzed for a real DAS application should be obtained by use of appropriate specific information, regarding, for instance, the probabilities of occurrence, the importance of the possible consequences, etc. On the other hand, when the analysis is more explorative and demonstrative than applicative in nature, and such information on the relative importance of significant events is scarce and not easily accessible, the choice will necessarily reflect a certain degree of arbitrariness.

Once the significant events to be used as starting points of the analysis are selected, the combined fault-tree/event-tree methodology outlined in section 1.2 can be applied. In particular, the fault-tree analysis shall proceed using the significant event under consideration as the top event and constructing the tree branches that can lead to it. But the advantage of using the SEA technique can be seen especially in the event-tree part of the analysis. Having in fact identified the significant event to be analyzed as the set of conditions characterizing a restricted section of the process state vector trajectory, inside the SD (safe domain) but just before crossing into the next identified SSID (safety system intervention domain), we can make an important assumption which considerably simplifies our job in the derivation of the

desired logic structures and leads to a rather unequivocal procedure to perform it. In short this assumption consists in taking the process state vector trajectory (that is the course of the transient) as essentially determined by the successful or unsuccessful operation of the applicable safety systems, once it has crossed the borders of the safe domain.

The above concept is illustrated, although in a somewhat simplified manner, in fig. 1.6, and has a number of implications that require some consideration. For instance, if the significant event X pushes the state vector trajectory into the kth SSID, characterized by the intervention of N safety systems, there will be N^2 possible outcomes (assuming that every safety system can be described by a binary variable: yes for operating, no for non-operating). Then N^2 outcomes must be analyzed to determine which ones will lead the state vector into the lth SSID, which ones into the nth, etc., so that the procedure can be repeated for all the SSID's that are found to be potentially involved. The overall resulting scheme will not be quite as complicated as it would seem at first glance by considering the theoretical number of possible combinations of outcomes in each SSID, for two main reasons:

- the total number of safety systems and SSID's associated with a particular plant system is not that large.
- even more important, the analysis work that derives from the application of this procedure is additive in nature, that is, the analysis done for one particular SSID potentially involved with a significant event is independent (with the exception of the specific area of common mode and common cause failures)

of the analysis to be done for another; this means that a large part of the job can be performed stepwise, with the various derived pieces to be added together at the end (at this final stage an additional analysis will be necessary if common cause and common mode failures of components belonging to totally different safety systems are considered important contributors).

In the above we have not specified, even though it is almost self evident, that as a necessary complement of the event tree procedures aimed at the identification of the safety systems interrelationships, a number of additional fault tree analyses would be needed, in order to identify the path taken by the process state vector in correspondence of the various "ramification points" shown in figure 1.6 and describing the successful or unsuccessful operation of the safety systems.

Our procedural framework is at this point completed. It will be used and tested in the following chapter when we will try to perform the analyses mentioned in the introduction. These will be applied to real systems and will resemble the derivations for a real DAS application in their essence, if not in extension. Again, we underscore that the methodology outlined in this chapter should not be regarded as a rigid, perfectly self-contained construction, but rather as a flexible thinking aid, to be suitably adjusted, should the particular nature of the problems to be examined suggest that.

A number of minor observations that could have been made with regard to the DAS methodology in general and to the proposed SEA procedure in particular, have been omitted in this chapter, since it will be easier to bring them up in a more practical context in the next chapters.

a) Example of Fault Tree

b) Example of Cause Consequence Diagram

Fig. 1.1: Examples of fault-tree and cause-consequences structures

Fig. 1.2: Illustration of DAS/Process possible levels of interface

a) Original structure

b) "Pruned" structure utilized by the DAS process model

Fig. 1.3: Illustration of logic structure pruning procedure

Fig. 1.4: Example of subdivision of a simplified plant parameter space into safety related domains

Fig. 1.5: Example of a hypothetical plant state vector trajectory in a simplified plant parameter space

Fig. 1.6: Example of event-tree structures originated by application of the SEA methodology

CHAPTER 2

2. An Application of the Significant Event Analysis to the Electric Power Systems of the San Onofre Nuclear Power Station, Unit One

2.1 General Considerations

The main purpose of this chapter is to show how the Significant Event Analysis (SEA) can be implemented in a real problem, and what type of information it would make available to us.

From the discussions of Chapter 1 we can derive the following conclusions about the application of the SEA method:

- a) a "significant event" is constituted by any set of plant (or system) conditions that is sufficient to determine the intervention of one or more safety systems (what systems can be considered as "safety systems" is a subject left to the analyst's judgment rather than to a rigid classification).
- b) a natural criterion for a first level classification of SEs is according to what specific safety systems would be called into operation (singularly or in combination) by the occurrence of such SEs.
- c) in the analysis of each SE, an event tree must be developed to determine the most relevant transient paths that may develop from it. Such potentially possible paths can be identified by hypothesizing the proper or improper performance of the safety systems that are activated during the progression of the SE into its subsequent stages. In the event tree so derived, there will exist as many fundamental ramification points as the number of safety systems potentially involved with the considered SE.

- d) for each of the above ramification points a fault tree analysis must be performed. This is in order to develop a logic structure that can be utilized by a DAS to determine whether or not the safety system associated with that ramification point is operating properly, and to provide diagnostics in the case it is not, together with suggestions for recovery actions whenever it will be possible.

In this chapter the above concepts are applied to analyze a portion of the electrical power systems of the San Onofre Power Station - Unit 1, and to make an evaluation of the type of information that can be obtained by applying the DAS methodology to deal with those transients that can be associated with similar systems. It should be realized that this will be a rather particular area of investigation, in that such types of transients are pretty different in their time frames and general manifestations from the thermal-hydraulic transients that characterize the majority of the systems of a power plant. We will return to this point later in this chapter.

Due to its explorative character, our analysis will not attempt to be exhaustive. The non-electrical* systems that may play an important role in the Significant Event considered in this chapter ("insufficient power on both emergency buses"), will not be modeled or analyzed by other means, this being beyond the purpose of our study. We will thus remain focused on the electrical systems that are relevant to the particular SE considered. Our analysis will have these

* By non-electrical we mean here non-related to the function of bringing electrical power to other systems.

systems as objects and will be carried out with the purpose of bringing to the reader's attention those points, related to the characteristics of the systems themselves and to the application to them of the SEA methodology, that appear to have some value for consideration. A totally systematic derivation of the logic structures will not therefore be attempted here. However, their essential event tree "skeleton" will be defined and a detailed derivation will also be presented of the fault tree structure associated with the chosen significant event itself. As we will see later, practically all of the remaining branch points that, in the above mentioned event tree, model the operation of electrical emergency systems would not require, with the important exception of the diesel generators, a detailed fault tree analysis.

2.2 San Onofre 1 Electric Power Systems Configuration and Protective Logic: Identification of a SE to be Analyzed

The main one line diagram for the auxiliary power system of San Onofre is given in fig. 2.1. Fig. 2.2 gives the simplified one line representation of the portion of this system comprised between the 138 and 220 kv switchyards on one side, and the 4.16 kv - 1A, 1B, 1C and 2C buses on the other. In fig. 2.2 the essential instrumentation devices available on the system are also shown. Those readings that are duplicated somehow are represented as single ones, since we will not consider here situations of continuous instrumentation* failures and therefore there is no reason to include in the system logic models a description of instrument redundancy. Also, certain instruments, whose readings are not independent of other instruments' readings, are not shown there, and the information they provide will not be used since it represents in practice a duplicated output. So, for instance, watt-meters are not shown, since they do nothing more than combine the outputs of a volt and an amp-meter already available in the system. The complete representation of the same portions of the system shown in fig. 2.2 is given in fig. 2.3, 2.4 and 2.5, where all the associated instrumentation is schematically indicated, together with all the protective relays and circuit breakers that, as we will see in the following, are the principal elements that are modeled in the logic structures to be devised for the system.

If we concentrate our attention on the part of the system comprised between the 138 kv switchyard and the two emergency buses 1C

* we use here the term continuous instrumentation to distinguish such devices as amp-meters or volt-meters from tripping relays that are in a way themselves, pieces of instrumentation.

and 2C (fig. 2.3, 2.4 and 2.5) we can see that the associated protection logic is basically the following:⁽⁵⁾

- a) A fault in one of the loads of bus 1C (or 2C) is supposed to be detected by the overcurrent relay placed on the feeder to that load, which, in turn, would cause the load circuit breaker to trip and isolate the fault.
- b) A fault on bus 1C (or 2C), i.e., downstream of the low side tap(s) of the transformer C's differential relay, is supposed to be detected by the overcurrent relay(s) placed immediately upstream of CB 11C02 (and 12C02). This relay(s) will operate CB 11C02 (12C02) to isolate the fault.
- c) A fault anywhere upstream of the transformer C's low side differential relay taps is supposed to be detected by one* of the following relays
 - transformer C's current differential relay
 - transformer C's sudden pressure relay
 - transformer C's high side overcurrent relay

The trip of any of these relays activates the following actions, which are conventionally grouped under the name "Function A":

- trip CB 4E
- trip CB 4W
- trip CB 11C02
- trip CB 12C02

* For certain types of faults it is not clear which one of two or three different relays would trip first; therefore, in the logic structures we will keep open the possibility of any of these relays acting to clear the fault.

It is therefore evident that, when the associated protection works as intended, a fault of type c) causes a total loss of voltage on both the emergency buses 1C and 2C; while a single fault of type a) normally causes just the loss of the affected load, and a single fault of type b) normally causes the loss of one emergency bus, leaving the other unaffected.

In addition to the protection discussed above, undervoltage relays exist on buses 1C and 2C that, whenever the voltage drops on both buses below 70% of the rated 4.16 kv value for more than 20 seconds, initiate the following sequence of actions,⁽⁵⁾ that we indicate conventionally by the name of "Function B":*

1. The turbine is tripped
2. Cbs 11A04, 11B04, 412, 612 (and the exciter field breakers, not shown in fig. 2.2 given here, since unessential to our purposes) are tripped (open)
3. The two diesel generators are started and brought to speed and voltage
4. All the 4.16 kv motor circuit breakers (except the Safety Injection Pumps) are tripped
5. The generator disconnect switch starts to open (30 seconds after generator voltage has decayed to 40%; another 30 seconds are required to complete the opening maneuver)
6. CBs 11A04 and 11B04 are reclosed
7. CBs 11C01 and 12C01 are closed

* The numbers in the Function B list of actions indicate the sequential order of execution of such actions.

If the sequence is successfully completed, the auxiliary transformer C and the generator will be both isolated, and power would be restored to the emergency buses from the 220 kv network, if available, via the 220 kv switchyard, main transformer, auxiliary transformers A and B, and bus ties 1A-1C and 1B-2C. This can be done by closing manually CBs 412 and 612.

In case power from the 220 kv SWYD is not available, CBs 11C01 and 12C01 must be reopened manually and the diesel generators 1 and 2 must be connected to the buses 1C and 2C by closing CBs 11C14 and 11C15.

From all of the above discussion it is apparent that a loss of power on both emergency buses can be taken as a "significant event" for the system considered, as its occurrence is certain to cause the state vector of the plant to drift away from its "safe domain" of normal operation. In fact, among others, the following essential plant components would be inoperable:

- all feedwater pumps
- all condensate pumps

Also, the following systems essential to maintain the plant safety systems in a ready stand-by would be lost:

- all charging pumps
- all safety injection pumps

The safety system interventions that are prompted by the occurrence of such an event are obviously those listed under the denomination of "Function B". It might be worthwhile to notice that the loss of power on just one of the two emergency buses itself constitutes a significant event, since two of the condensate pumps and one of the

feedwater pumps would be lost in such an occurrence (to say nothing of the other major components that would be rendered inoperable). Such an event would produce, in effect, a turbine trip triggered by the loss of one of the two feedwater trains.⁽⁵⁾ In any case the event "insufficient power on any one emergency bus" is a subset of the event "insufficient power on both emergency buses", and we will therefore analyze explicitly the conditions that cause it to occur as an essential part of the analysis for the other event. Actually, this is the part of the analysis that will be explicitly carried out in fault-tree form, since the analysis structure for a double bus loss of power can be derived immediately from it.

2.3 Event Tree for the SE "Insufficient Power on Both Emergency Buses (1C and 2C)"

In the previous section we have seen how, if the condition exists for more than 20 seconds, the significant event "insufficient power on both emergency buses" will call on the actuation of Function B (also explained in section 2.2). The sequence initiated therein will comprise two basic types of interventions:

- A) Thermal-hydraulic system interventions
- B) Electrical system interventions

The thermal-hydraulic system interventions stem from the turbine trip signal produced by Function B. The turbine trip would also produce a reactor trip via the protective hardwired logic. Also confining our attention at first on the secondary loop side, the ensuing transient will call into operation the steam dump system, while the loss of main feedwater caused by the loss of power will call into operation the auxiliary feedwater system. On the primary loop side, the pressurizer relief valve (and maybe, in case of failure of this to operate, the pressurizer safety valve) might be called into action. The mode of operation of these systems will strongly depend on the behavior of the other systems that will have been called upon immediately before. For instance, the operation of the steam dump system and of the auxiliary feedwater system would strongly affect the operation of the pressurizer relief valve. To achieve a detailed understanding of the cause-consequence relations existing in the event tree that should be constructed to model the behavior of these systems, and to carry out the significant event analysis as outlined in Chapter 1,

a systematic thermal hydraulic simulation study should be performed.

An analysis of the electrical system interventions triggered by the SE that we have selected can fortunately be attempted in a simpler manner, since the performance of such devices as circuit breakers, etc., can be characterized by "on"/"off" binary variables and therefore is much easier to model in the form of logic structures. The electrical system actuations included in the automatic sequence of Function B were listed in Section 2.2.

In fig. 2.6, a simplified event tree is presented for the SE that we are considering. As explained in Chapter 1, we have relied, in the derivation of such a tree, on the assumption that the course of a transient triggered by the occurrence of a SE is most likely determined by the behavior of the "safety systems" that are successively called upon after the transient starts. It was also mentioned that the term "safety system" has in this context a rather extended meaning, since it includes all the corrective interventions that are needed to bring the transient under control. Some of these interventions can even be manual, and in fact in the event tree of fig. 2.6, certain actions are indeed actions required of the operator(s).

The tree of fig. 2.6 includes a rather sketchy picture of the thermal-hydraulic system interventions that are positively or potentially involved in the SE considered (according to what was outlined above). These are presented in the upper portion of the figure, whereas the lower portion contains the part of major interest to us, which represents the electrical system interventions. The convention fol-

lowed in the tree representation of fig. 2.6 is that the spatial location of events in the tree, proceeding from left to right, indicates the existing sequential order, or anyway a relation of dependence of the events on the right on those on the left. For instance, the operation of the auxiliary feedwater system is indicated by a branching placed to the right of all the branches corresponding to the electrical system interventions. This is because, if the electrical systems fail to restore power to the emergency buses, only the steam driven auxiliary feedwater pump will remain available. In other words, the operation of the auxiliary feedwater system is substantially affected by the operation of the plant electrical systems. We have in fig. 2.6 also used the convention of representing certain system interventions with dashed lines, wherever such interventions are requested only for certain specific courses of the transient considered and not in all cases. The interventions requested in all cases are indicated by the use of solid lines. Thus we can see from fig. 2.6 that, once the SE has started on its course (i.e., the condition of insufficient power on both emergency buses is verified) the plant protection logic will necessarily require a turbine trip, reactor trip, steam dump system operation, fault isolation, diesel generator start-up, etc., while for instance the operations of alignment to the diesels and diesel loading will be necessary only if the operation of the alignment to the alternate off-site source is not successful.

In fig. 2.7 the "electrical portion" of the event tree of fig. 2.6 is expanded in further detail, with the main purpose of showing what specific operations were grouped in fig. 2.6 under the labels

of "preparation of alignment to alternate sources", "alignment of off-site alternate source" and "alignment to on-site alternate source" respectively. In short, it can be seen that the first of these comprises the whole automatic sequence of Function B (see Section 2.2) except the turbine trip operation, the second indicates the manual operation of closing BCs 412 and 612 to restore power to buses 1C and 2C from the 220 kv switchyard (if available) and reconnecting all loads to the buses, and the third indicates manual operations of closing CBs 11C14, 11C15 and the load CBs to connect the buses 1C and 2C to the diesel generators and the various loads to the two buses. The connection of loads to the buses can be somehow different when the diesel generators are involved and therefore is considered here a different operation than the connection of loads to the buses when power is restored from the 220 kv SWYD.

In the framework of the SEA methodology, and limiting our attention to the electrical side of the shown event tree only, we should proceed by deriving for each of the branch points of the tree a suitable fault tree type of structure, in order to have a tool capable of telling us which branch the transient will follow and, if the wrong direction is taken, why it has been taken and how it can be reverted into the right direction (if this is possible).

Of all the branching points shown in the event tree of fig. 2.7, only the one corresponding to the initiating SE (which is not really shown as a branch point, since we are considering the verified, i.e., faulted, condition as the trigger for all of the following), and the two numbered 3 and 12 respectively, need to be analyzed with a more or

less complicated fault-tree type of derivation in order to be fully understood. The information regarding branch point #2 will be in fact implicit in the structure derived for #1 (as we will see in Section 2.5). Branch points #4 through 11 imply on the other hand very simple logic structures, essentially limited to a verification of a few circuit breaker positions. The suggestions for recovery actions when any one of the CBs is found in the wrong position would not require any special effort to be devised either. We would however return for a global look at these branch points in Section 2.6.

Of the three branch points requiring a more detailed investigation we have chosen to analyze #1 only (the initiating SE), in order not to make our analysis exceedingly complicated and to stay within the main purpose of this study, which is to look at electrical systems without drifting into detailed investigations of components of such systems that are not strictly electrical in spite of their strong interface connections with the purely electrical components themselves. A fault tree analysis of the performance of the diesel generators, under start-up and loading conditions, would indeed require a very specialized insight into the characteristics of a number of mechanical and fluid systems, like the internal combustion engines, their fuel and lube oil supply systems, their speed regulators, their cooling systems, etc., that could well require a full study by itself.

2.4 Fault Tree Structure for the Event "Insufficient Power on Bus 1C"

We anticipated in Section 2.2 that the event "insufficient power on any one emergency bus" is an essential subset of the event "insufficient power on both emergency buses". As a matter of fact, if we recall what was said in Section 2.2 about the logic of the protections applied to the electrical circuits between the 138 kv switchyard and the buses 1C and 2C, it is apparent that all these faults that call on the actuation of Function A provide in practice a common cause mechanism for loss of power on both buses contemporarily. Since such faults turn out to be the ones that require most of the analytical work to be identified and understood, one can look at the event of loss of power on just one bus in order to find the cut sets for the event of loss of power on both emergency buses: these will be simply all the common cause cut sets mentioned just above, plus the cut sets for independent failure of bus 1C when occurring simultaneously with any one of the analogous independent cut sets for bus 2C. In the fault tree structure that we are going to present for bus 1C it will be easy to see which ones are the independent cut sets; therefore, it is perfectly convenient to proceed in the stated manner.

The fault tree for the event "insufficient power on bus 1C" is shown in the series of figures numbered 2.8 through 2.20. The tree is broken down in a convenient number of portions and each of the sections shown is more or less self-explanatory. In any case, before trying to decipher the information contained in these logic structures, it is worthwhile to make a couple of additional remarks regarding their nature and peculiarities:

A) The fault trees needed for a DAS application are not coherent, that is, one can find among their primary conditions both certain events and their complements. This is due to the fact that it can be important here to bring into evidence all of the detectable conditions that make a situation different from another. Another peculiar characteristic is that certain conditions are normally linked by specific cause-consequence relations.* These can on the other hand fail under particular circumstances and it would be then important to detect such failures as they occur. In fig. 2.10 through 2.20 these cause-consequence relations are conventionally shown by means of dashed arrow lines (this is done also when the relation is defeated by a malfunction with the addition of a slanted transversal line to point out the abnormal situation). For example, in set 1a (fig. 2.10) the "AND" gate to the right of the tree structure shows the normal condition for tripping circuit breaker 11C02, that is a transformer C's low side overcurrent relay trip causing the trip of CB 11C02. Looking from outside after the trip has occurred, which is what the DAS will have to do, one would simply see that the LSOR and the CB 11C02 are tripped. As another example we can see, again in set 1a, that the "AND" gate in the lower portion shows the failure of a cause-consequence relation that normally links the occurrence of an internal fault in CB 11C02 to the tripping of the transformer C's differential relay. In general, in the course of a transient of the type considered here, the success

* Therefore, they are not independent events.

or the failure of these tripping-logic relations will make a substantial difference and therefore it must be modeled in the DAS logic structures.

- B) Certain non-minimal cut sets that are usually not represented in a normal fault tree are included in the DAS fault trees. For instance, if we look at the cut sets represented in the structure obtained by following through branches 1, 1d, any one of 1d1, 1d2 or 1d3, "and" 1d4 (fig. 2.9 and 2.11 through 2.14), we can clearly see that the top condition is verified, for the part modeled in structure 1d4 (fig. 2.14), whenever CB 4E (or 4W) fails to trip and CB 11C02 trips alone. However, we modeled also the condition in which CB12C02 trips too, since, even though it is not necessary in order to get the top condition verified, it represents a different situation from the one in which CB 11C02 trips alone.
- C) In the logic structures derived here the activation of any specific branches will be mainly shown by relay and/or circuit breaker positions. Therefore the sets of observable conditions that will be associated with any particular cut sets are directly derived from the logic structures themselves. In certain cases, certain additional instrument readings might give some additional clues to the situation. These cases are not frequent though, as the time frame for transients originated by electrical faults is normally too short for any continuous reading instrument to provide information to the DAS.

In the upper structure of the derived fault tree, we have shown in fig. 7.8 five main contributing branches. Of these, the "external black-out" and the "Bus 1C open Failure" conditions were not further investigated since they were judged to be beyond any possibility of control, by a DAS as far as possible recovery actions are concerned. The Bus 1C overload situation was also not analyzed, mainly because insufficient data were available to attempt such an analysis in detail. At the simplest level of approach it can be said however that an overload condition originating in any of the loads attached to Bus 1C can be easily detected, as it will originate a larger-than-normal current in the feeder(s) to such load(s) together with a lowering of the voltage on the Bus itself.* The situation can be obviously corrected before it causes a trip of the Bus 1C undervoltage relay (which has a 20 sec time-delay) by tripping the circuit breaker(s) on the feeder(s) to the affected load.

Other conditions beyond the possibility of control by a DAS appear in fig. 2.9 ("open failure upstream", i.e., an open conductor upstream of Bus 1C) and 2.17 ("external power feed maintained", i.e., failure of the relay protections of the electrical network upstream of the plant switchyards to react to an unprotected fault inside the plant).

Finally we notice that the condition of an "unprotected fault in the power circuits associated with Bus 1C" (logic structure 2, fig.

* This would be one specific exception to what we said above about the limited usefulness of the "continuous instrumentation".

2.8)^{*} was analyzed even though it is all but likely that a situation of that kind can exist without irreparable damage to some of the major components of the system, and for long enough to allow a diagnosis to be completed and a recovery action to be undertaken. We have arbitrarily assumed that it can.

^{*}This situation represents another exception to the statement made about the "continuous instrumentation".

2.5 Discussion of the Information That Can be Produced by a DAS Utilizing the Fault Tree Structure for the Event "Insufficient Power on Bus 1C"

The fault tree shown in fig. 2.8 through 2.20 has, between branch 1 and 2, 220 "basic" cut sets* (143 for branch 1 and 77 for branch 2 respectively).

In Table 2.II we have listed the first 26 of these basic cut sets (2 for branch 1a, 2 for 1b, 2 for 1C and 20 for 1d1 $\cap$ 1d4) with the purpose of showing explicitly what information the protective relays and circuit breakers on one side (second column of the table), and the electrical instrumentation on the other (third column of the table), are able to provide correspondingly. Using the list of Table 2.II we were then able to classify the 26 considered basic cut sets into 15 groups in Table 2.III, each group containing basic cut sets that are not distinguishable from one another in that they produce the same set of observable conditions. Every group is however distinguishable from any other group.

By looking mainly at the contents of Tables 2.II and 2.III some useful observations can be made; these are summarized in the following:

- A) The correspondences of cut sets and observable conditions shown in Table 2.II justify the assertion previously made that the continuous electrical instrumentation does not provide much additional information over that provided by the protective relays, and by the circuit breaker positions. The reason for this is that in most cases the actuation of the

* We don't call them "minimal" because they include non-minimal cut sets of the type mentioned in point B of Section 2.3.

protective CBs "erases" the peculiar pattern of instrument readings that was associated with a particular abnormal situation. The normal DAS scanning time in present systems is of the order of 1 sec; therefore, unless a method is devised to detect and record the available instrument readings from the field on a continuous basis (or at extremely small scanning intervals), the information contained in these readings will be lost. An obvious exception to this situation would exist whenever an abnormal situation (i.e., a fault) developed unprotected in the system. This is the situation modeled in branch 2 of our fault tree, but, as we mentioned already at the end of Section 2.3, the assumption that a situation of this type would last for a non-negligible duration of time (that is: with respect to the DAS scanning time) is probably non-realistic.

- B) In branch 1c of our fault tree (see fig. 2.10) we show the two fundamental modes for a circuit breaker spurious actuation, that is: a) the circuit breaker itself trips without any incoming signal requesting the trip, and b) the relay (or one of the relays) that is (are) coupled to the circuit breaker sends a spurious tripping signal, causing the CB to open. The corresponding situations for the circuit breaker CB 11C02 are represented also in Tables 2.II and 2.III under the identifiers 1c/01 and 1c/02.

If one assumes that the only valid diagnostic inputs for the DAS are those provided by the protective relay and circuit break-

er positions* listed in column 2 of Table 2.II and column 1 of Table 2.III, it follows that the situation a) above can be easily identified as a spurious trip since in this case the DAS will not see the protective low side overcurrent relay in the tripped position (in which it would be, had a real fault-produced trip occurred). Situation b) however would be totally indistinguishable from a real trip, as in this case the protective relay would also be tripped together with the associated circuit breaker CB 11C02. What we have just discussed is reflected clearly in Table 2.III, where the cut set 1c/02 is classified in the same group A** that comprises cut sets 1a/01, 1a/02 and 1b/01, while cut set 1c/01 is classified by itself in group C.

It should be noted that this type of situation is quite general. In fact, for instance, if one goes back to the fault tree structure of fig. 2.9 and follows through the branches 1e and 1f, one can see that, among some other cut sets for the simultaneous actuation of CBs 4E and 4W with which we are not concerned here, two modes of spurious trips are identified: a simultaneous independent spurious trip of CBs 4E and 4W (branch 1f itself, fig. 2.15) and a spurious Function A condition produced by one of the related protective relays (branches 1d3 and 1e1, fig. 2.15, 2.14 and 2.16). This is just the mirror image,

* A discussion related to this particular assumption is given in point C below.

** For the distinction of group A into subgroups A' and A'', see point C below.

for a slightly more complex configuration, of what we have illustrated above for one circuit breaker.

- C) In Tables 2.II and 2.III we indicate that a distinguishing observable condition between the two cut set subgroups A' and A'' (including cut sets 1a/01, 1a/02, 1b/01 and cut set 1c/02 respectively) might exist, given by the position of the Bus 1C's GDR (ground detection relay). In a three-phase, three-conductor electric network (as the 4.16 kv San Onofre 1 auxiliary power system is) a GDR has the capability of detecting any condition of imbalance that moves the center of the three-phase voltage vectorial diagram away from the origin ($\vec{V} = 0$ position). Therefore, such a device should be capable of detecting both one-phase and two-phase faults, and also all those three-phase faults that are not symmetrical with regard to the three different phases. Such a device is only used to give a warning wherever it is activated by a fault.

On the other hand, the protective relays that are used to actuate circuit breakers are engineered to react, in a three conductor system, only to two-phase or three-phase faults, as a one-phase fault would not affect the phase-to-phase $\Delta\vec{V}$.

It follows that, if the calibration of the Bus 1C's GDR were such to make it much faster than any of the protective relays associated with the system considered, a two or three-phase fault would cause both the pertinent protective relay and the GDR to trip (except in the very unlikely case of a perfectly balanced three-phase fault). This could be very useful in order to

discern between a spurious trip of the protective relay and a real trip caused by a two or three-phase fault, since in the first case the GDR would "contemporarily" trip, while in the second it would not (except in the very unlikely case of a contemporary spurious trip on its part). The cut set 1c/02 could then be distinguished by the DAS from the cut sets 1a/01, 1a/02 or 1b/01 in a real situation. Power to Bus 1C could accordingly be restored safely by simply reclosing CB 11C02, as it would be recognized that no real fault had occurred.

Unfortunately the information available on GDRs and the type of operational behavior to be expected of them as parts of a complex electrical power distribution network seems to suggest that their ability to trip, when "in competition" with a protective differential or overcurrent relay, cannot be really relied upon. We can only underscore here that it would be pretty useful to achieve such ability for the reasons given above, and that, as the possibility of real implementations of DASs becomes more concrete, the protective circuit designer may have to decide about the opportunity of obtaining a GDR's behavior of that type.

The point discussed here is somehow reflected formally in the classification of Table 2.III. There, the cut sets 1a/01, 1a/02, 1b/01 and 1c/02 are placed together in the same group A, to acknowledge the fact that they are totally indistinguishable when only the information provided by the protective switchgear

is utilized; however, the first three are classified together in a subgroup A' and the fourth in another subgroup A'' to indicate the potential possibility of distinguishing between the two subgroups by use of the GDR indication.

- D) In branch 1b of our fault tree (see again fig. 2.10) we present the two fundamental modes for the failure of a CB to trip in the presence of a faulted condition. These modes represent in a way a "mirror" situation with respect to the spurious trip modes discussed in B).

The part of the addressed branch that is of interest is the one under the lower "OR" gate. Given a fault in load k of Bus 1C, the load k CB can fail to trip in one of the two following ways:

- a) the load k overcurrent relay (kLOR) fails to generate the required tripping signal
- b) the kLOR trips as required but the load k CB fails to trip upon receiving the tripping signal

Under both situations the fault may be in general cleared by some upstream protection, and indeed branch 1b considers the case in which the fault is detected by the LSOR and cleared by CB 11C02. The important point to note, however, is that situation a) cannot be distinguished from a trip caused by a fault upstream of the load kCB, whereas situation b) can, as the kLOR tripped position would give us the leading clue to what happened.

The above discussed observations are reflected in Table 2.III, cut set 1b/01's classification in group A (subgroup A'),

Fig. 2.1: S. Onofre 1
Main one line diagram

and cut set lb/02's classification in group B. It is needless to say that the detection of a situation like the one of cut set lb/02 can lead to a ready recovery action consisting of:

- manual trip of load kCB
- manual reset (to closed position) of CB 11C02

For the sake of completeness we have to mention two additional situations that are theoretically possible and that would have to be classified in group B of Table 2.III, even though we did not include them there, nor in the fault tree of fig. 2.8-2.20, since they appear to be very unlikely and not of great relevance. These are:

- c) a kLOR spurious trip with load k CB failure to trip, and a simultaneous LSOR spurious trip with CB 11C02 trip
- d) a kLOR spurious trip with load k CB failure to trip, and a simultaneous fault upstream causing a LSOR trip with CB 11C02 trip

It can be noticed that situation c) could constitute a distinguishable event if the GDR indication could be utilized according to what was said in point C). Besides this fact, the recovery action proposed before in response to a group B condition would be even too conservative for this particular event, in which all the trips would be spurious and therefore there would be no need to even isolate load k. A problem could indeed exist, as far as the proposed recovery action is concerned, if condition d) were verified; but even in this situation the re-

setting of CB 11C02 should cause only a new trip of the LSOR and of CB 11C02 itself.

Again what we have just discussed can be similarly repeated for more general situations: for instance, by looking at the sub-branches 1d1 and 1d2 of branch 1e (fig. 2.15, 2.12 and 2.13), it can be seen that a condition of fault downstream of CB 11C02 with LSOR trip, CB 11C02 failure to trip and consequent Function A actuation can be distinguished from a Function A actuation due to a fault in transf. C (or equivalent). In this case the ability to recognize the first type of situation could be especially important, since then the Function A could be reset, before tripping the actuation of Function B as a result of having produced a total loss of power on Buses 1C and 2C. The only trip required would be that of CB 11C02 resulting in loss of power on Bus 1C only. A similar, but even more extreme, case of this type is also represented in fig. 2.13 and contemplates a fault in Bus 1C's load k with a kLOR trip but with both load k CB and CB 11C02 failing to trip, so that the fault would result again in a Function A actuation. The ability to diagnose the true situation makes here the difference between a simple isolation of load k and a total loss of power on the two emergency buses. Again, with the instrumentation available in the system considered, such ability exists only if the load k CB's failure is a failure to respond to the detector relay's signal (in this case kLOR's) and not a failure of the detector relay itself to produce the tripping signal.

E) As we already mentioned in Section 2.3, the fault tree analysis of the initiating SE would also explicitly provide the information needed for the branch point #2 of the event tree in fig. 2.7. In fact, as the circuit breaker positions are systematically used throughout the SE fault tree to identify the activated branches, the same structure can be accordingly used to gather and make evident all the available information concerning the success or failure of the fault isolation procedures.

The situations that are non-trivial with respect to the problem of fault isolation are of course the ones in which there has been at least one failure of a circuit breaker to trip. Therefore the DAS's ability in this regard goes totally in parallel with its ability to diagnose a situation of that kind, and therefore it is subject to the same considerations that we made above, in point D).

As a final remark, we can point out that even though the considerations of points A) through E) were initially derived by looking at the partial list of basic cut sets given in Tables 2.II and 2.III, they reflect in a fairly complete way the essential patterns that we were able to identify throughout the entire fault tree structure of fig. 2.8 - 2.20, and therefore give a good indication of what sort of information a DAS can retrieve from a system like the one that we have analyzed.

2.6 A Few Additional Considerations on Some of the Branch Points in the Event Tree for the SE "Insufficient Power on Both Emergency Buses"

We stated in Section 2.3 that the branch points numbered 4 through 11 in fig. 2.7 require only simple logic structures in order to be analyzed. This is due essentially to the following two orders of reasons:

- every one of these branch points is associated with one or more "on/off" switching operations for which it is very easy to verify the success or failure.
- the recovery actions for the failure of any of the above operations do not depend in practice on the cause(s) of the failure itself. This is due to the fact that all such operations that are automatic can also be performed manually (some of the required operations can indeed be done only manually, like the ones associated with branch points #9 and #11). It follows that, if for instance a failure of the automatic logic sequence of branch points #4 through 8 occurs and is detected by a verification of circuit breaker positions, the obvious recovery action would be to attempt the same operation manually (for the operations that are only manual, a direct local action might be attempted whenever possible instead of the normal remote actuation). A precise diagnosis of the causes of such failure would not be in fact likely to lead to a faster restoration of the desired conditions. One might think, for instance, of a failure in the hardwired logic unit that sequences the operations of branch points #4 through 8: a complicated analysis might succeed in determining which component(s) of this hardwired unit failed, but

this would be hardly any help in completing the required sequence of operations.

Having in the above provided a simple basis for the type of analysis that could be sufficient in association with the mentioned branch points, we have also to point out the limits of this simple approach. The principal of these limits is that, if we choose to only worry about what we can call "the proper alignment and circuit breaker positions" necessary to connect the two emergency buses with either the 220 kv switchyard or with the two diesel generators, we practically choose not to include in our concerns what could happen to our system after it has been properly connected to either one of these sources. To understand how this could theoretically be an unnecessary limitation it is better to consider the following example:

- a) suppose that a fault occurs in Bus 1C's load k, but that the associated load k's over current relay fails to trip and so does the transf. C's low side overcurrent relay.
- b) suppose also that the fault is cleared then by the transf. C's high side overcurrent relay, which causes the actuation of Function A and as a consequence a complete loss of power on both buses and the actuation of Function B.

Applying the sort of considerations made in point D) of Section 2.5, we can see that this situation cannot be distinguished from one in which a fault in transf. C causes the HSOR to trip with consequent Functions A and B actuation. If we assume that in the present situation the operations associated with Function B are completed and that also the connection of buses 1C and 2C to the 220 kv SWYD is success-

fully completed we would then be "facing" branch point #10 of fig.

2.7. Considering specifically the loading of Bus 1C we can now assume that load k was successfully disconnected from Bus 1C at the time of executing the operations associated with branch point #5 and that now must be reconnected. If we assume that the failure of the kLOR was not an occasional one but a persistent one, the closing of load kCB will cause the trip of CB 11C01 and a new loss of power on Bus 1C, somehow unexpected since in a normal frame of mind the operator would think that the original fault initiating the transient had been isolated with the actuation of Function A.

A DAS capable of handling the above described situation could be devised by deriving logic structures for the system also when aligned to the alternate sources and by combining the information obtainable from these with the information derived from the logic structures of the initiating SE. For the case discussed, the initial Function A actuation, and then the trip of CB 11C01 upon closing the load k CB, would be in fact a pretty strong piece of evidence that a DAS could use to diagnose the situation. This could allow an almost complete recovery to a normal situation by opening the load k CB and returning power to the system via the normal 138 kv source.

The objection that can be raised against attempting to develop a DAS with such a refined capability should be whether or not the potential benefit obtainable is really worth the pretty conspicuous complication of the system needed to perform a diagnosis of the type described. Questions of this kind can be asked today about almost any of the potential applications of DA systems and they are also rather hard

to answer without some direct experience gained from more or less experimental applications.

Table 2.I

LEGEND for Fig. 2.8 through 2.20 and Table 2.II

kLOR	=	load k's overcurrent relay
LSOR	=	transformer C's low side overcurrent relay
DR	=	transformer C's differential relay
SPR	=	transformer C's sudden pressure relay
HSOR	=	transformer C's high side overcurrent relay
GDR	=	Bus 1C's ground detection relay
CB ⁽⁺⁾	=	circuit breaker
AI	=	current indicator
VI	=	voltage indicator
TRANSF	=	transformer
SWYD	=	switchyard
kv	=	kilovolt
- - ->	=	cause consequence relation among conditions or sets of conditions (also shown when the relation is defeated by a failure)

(+) followed by specific identifier

Table 2.II: Partial list of "basic" cut sets for the event "insufficient power on Bus 1C"

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1a/01</u>		
- Bus 1C fault	- LSOR tripped	- GDR tripped (uncertain)
- LSOR trip	- CB 11C02 tripped	- no voltage indication on Bus 1C
- CB 11C02 trip		- no current indication on Bus 1C feeder AI
		- no current indications on Bus 1C load feeder AIs

<u>1a/02</u>		
- CB 11C02 internal fault		
- DR fails to trip		
- LSOR trip	- same as 1a/01	- same as 1a/01
- CB 11C02 trip		

<u>1b/01</u>		
- Bus 1C load k fault		
- kLOR fails to trip	- same as 1a/01	- same as 1a/01
- LSOR trip		
- CB 11C02 trip		

Table 2.II (continued)

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1b/02</u>		
- Bus 1C load k fault	- KLCR tripped	
- KLOR trip	- LSOR tripped	- same as 1a/01
- load k CB fails to trip	- CB 11C02 tripped	
- LSOR trip		
- CB 11C02 trip		

<u>1c/01</u>		
- CB 11C02 spurious trip	- CB 11C02 tripped	- same as 1a/01 except: GDR will not be tripped (unless a single phase ground exists concurrently on the secondary side of transf. C)

<u>1c/02</u>		
- LSOR spurious trip	- same as 1a/01	- same as 1c/01
- CB 11C02 trip		

<u>1d/01</u>		
- fault in between CBs 4E, 4W and Transf. C	- HSOR tripped	- no voltage indication on Bus 1C VI
	- CB 11C02 tripped	- no voltage indication on Bus 2C VI
- HSOR trip	- CB 12C02 tripped	- no current indication on Bus 1C feeder A1

Table 2.II (Continued)

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1d/01 (continued)</u>		
- CB 4E fails to trip	- CB 4W tripped	- no current indication on Bus 2C feeder AI
- CB 11C02 trip		- no current indications on Bus 1C load feeder AIs
- CB 12C02 trip		- no current indications on Bus 2C load feeder AIs

<u>1d/02</u>		
- same as 1d/01 except: CB 4W (instead of 4E) fails to trip	- same as 1d/01 except: CB 4E (instead of 4W) tripped	- same as 1d/01

<u>1d/03</u>		
- same as 1d/01 except: CB 12C02 fails to trip	- same as 1d/01 except: CB 12C02 will not be tripped	- same as 1d/01 except: voltage and current indications associated with Bus 2C might not be positively "zero"

<u>1d/04</u>		
- same as 1d/03 except: CB 4W (instead of 4E) fails to trip	- same as 1d/03 except: CB 4E (instead of 4W) tripped	- same as 1d/03

Table 2.II (Continued)

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1d/05</u>		
- same as 1d/01 except: Transf. C fault (instead of "fault in between..")	- same as 1d/01	- same as 1d/01

<u>1d/06</u>		
- same as 1d/05 except: CB 4W (instead of 4E) fails to trip	- same as 1d/02	- same as 1d/01

<u>1d/07</u>		
- same as 1d/05 except: CB 12C02 fails to trip	- same as 1d/03	- same as 1d/03

<u>1d/08</u>		
- same as 1d/07 except: CB 4W (instead of 4E) fails to trip	- same as 1d/04 except: CB 4E (instead of 4W) tripped	- same as 1d/03

<u>1d/09</u>		
- same as 1d/05 except: SPR (instead of HSOF) trip	- same as 1d/01 except: SPR (instead of HSOR) tripped	- same as 1d/01

Table 2.II (Continued)

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1d/10</u>		
- same as 1d/09 except: CB 4W (instead of 4E) fails to trip	- same as 1d/09 except: CB 4E (instead of 4W) tripped	- same as 1d/01
<u>1d/11</u>		
- same as 1d/09 except: CB 12C02 fails to trip	- same as 1d/09 except: CB 12C02 will not be tripped	- same as 1d/03
<u>1d/12</u>		
- same as 1d/11 except: CB 4W (instead of 4E) fails to trip	- same as 1d/11 except: CB 4E (instead of 4W) tripped	- same as 1d/03
<u>1d/13</u>		
- same as 1d/05 except: DR (instead of HSOR) trip	- same as 1d/01 except: DR (instead of HSOR) tripped	- same as 1d/01
<u>1d/14</u>		
- same as 1d/13 except: CB 4W (instead of 4E) fails to trip	- same as 1d/13 except: CB 4E (instead of 4W) tripped	- same as 1d/01

Table 2.II (Continued)

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1d/15</u>		
- same as 1d/13 except: CB 12C02 fails to trip	- same as 1d/13 except: CB 12C02 will not be tripped	- same as 1d/03

<u>1d/16</u>		
- same as 1d/15 except: CB 4W (instead of 4E) fails to trip	- same as 1d/15 except: CB 4E (instead of 4W) tripped	- same as 1d/03

<u>1d/17</u>		
- same as 1d/13 except: Fault in between Transf. C and CBs 11C02, 12C02 (instead of "Transf. C internal fault")	- same as 1d/13	- same as 1d/01

<u>1d/18</u>		
- same as 1d/17 except: CB 4W (instead of 4E) fails to trip	- same as 1d/14	- same as 1d/01

<u>1d/19</u>		
- same as 1d/17 except: CB 12C02 fails to trip	- same as 1d/15	- same as 1d/03

Table 2.II (Continued)

Cut set identifier and determining conditions	Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation
<u>1d/20</u>		
- same as 1d/19 except: CB 4W (instead of 4E) fails to trip	- same as 1d/16	- same as 1d/03

Table 2.III: Classification of "basic" cut sets according to common observable conditions.

Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation	Identifiers	
		Cut sets	Cut set groups
- LSOR tripped	- GDR tripped (uncertain)	- 1a/01	
- CB 11C02 tripped	- no voltage indication on Bus 1C VI	- 1a/02	A'
	- no current indication on Bus 1C feeder AI	- 1b/01	
	- no current indications on Bus 1C load feeder AIs		A

	- no voltage indication on Bus 1C VI		
	- no voltage indication on Bus 1C feeder AI		
	- no current indications on Bus 1C load feeder AIs	- 1c/02	A''
	(- GDR could be tripped only if a single fault exists concurrently on the secondary side of Transf. C)		

- KLOR tripped			
- LSOR tripped	- same as for cut set group A'	- 1b/02	B
- CB 11C02 tripped			

- CB 11C02 tripped	- same as for cut set group A''	- 1c/01	C

Table 2.III (Continued)

Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation	Identifiers	
		Cut sets	Cut set groups
- HSOR tripped	- no voltage indication on Bus 1C VI		
- CB 11C02 tripped	- no voltage indication on Bus 2C VI	- 1d/01	
- CB 12C02 tripped	- no current indication on Bus 1C feeder AI	- 1d/05	D
	- no current indication on Bus 2C feeder AI		
- CB 4W tripped	- no current indication on Bus 1C load feeders AIs		
	- no current indications on Bus 2C load feeder AIs		

- HSOR tripped		- 1d/02	
- CB 11C02 tripped	- same as for cut set group D	- 1d/06	E
- CB 12C02 tripped			
- CB 4E tripped			

- HSOR tripped	- no voltage indication on Bus 1C VI		
- CB 11C02 tripped	- very low or no voltage indication on Bus 2C VI	- 1d/03	F
- CB 4W tripped	- no current indication on Bus 1C feeder AI	- 1d/07	
	(continues on next page)		

Table 2.III (Continued).

Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation	Identifiers	
		Cut sets	Cut set groups
	- very low or no current indication on Bus 2C feeder AI		
	- no current indications on Bus 1C load feeder AIs		
	- very low or no current indications on Bus 2C load feeder AIs		
<hr/>			
- HSOR tripped			
- CB 11C02 tripped	- same as for cut set group F	- 1d/04	G
- CB 4E tripped		- 1d/08	
<hr/>			
- SPR tripped			
- CB 11C02 tripped			
- CB 12C02 tripped	- same as for cut set group D	- 1d/09	H
- CB 4W tripped			
<hr/>			
- SPR tripped			
- CB 11C02 tripped			
- CB 12C02 tripped	- same as for cut set group D	- 1d/10	I
- CB 4E tripped			
<hr/>			

Table 2.III (Continued)

Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation	Identifiers	
		Cut sets	Cut set groups
- SPR tripped			
- CB 11C02 tripped	- same as for cut set group F	- 1d/11	J
- CB 4W tripped			
- SPR tripped			
- CB 11C02 tripped	- same as for cut set group F	- 1d/12	K
- CB 4E tripped			
- DR tripped		- 1d/13	
- CB 11C02 tripped	- same as for cut set group D	- 1d/17	L
- CB 12C02 tripped			
- CB 4W tripped			
- DR tripped		- 1d/14	
- CB 11C02 tripped	- same as for cut set group D	- 1d/18	M
- CB 12C02 tripped			
- CB 4E tripped			
- DR tripped		- 1d/15	
- CB 11C02 tripped	- same as for cut set group F	- 1d/19	N
- CB 4W tripped			

Table 2.III (Continued)

Cut set observable conditions associated with protective relays and circuit breakers	Cut set observable conditions associated with other electrical instrumentation	Identifiers	
		Cut sets	Cut set groups
- DR tripped			
- CB 11C02 tripped	- same as for cut set group F	- 1d/16	0
- CB 4E tripped		- 1d/20

Fig. 2.2: San Onofre 1: simplified one line diagram of electrical system between 220/138 KV switchyards and 4.16 KV buses

Fig. 2.3: San Onofre 1 - 220/138 substation one line diagram

Fig. 2.5: S. Onofre 1 4.16 kV system one line diagram (buses 1B and 2C)

Fig. 2.6: Simplified event tree for the event "insufficient power on both emergency buses"

Fig. 2.7: Event tree for the electrical systems potentially associated with the event "insufficient power on both emergency buses"

Fig. 2.8: Fault tree for the event "insufficient power on Bus 1C"

Fig. 2.9: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.10: Fault tree for the event "insufficient power on Bus 1C" (continued)

(*) The situation described here can be of three different types:

- a fault develops downstream of CB 11C02 with failure of the directly associated protections: in this case the trip of CB 11C02 would succeed in isolating it, but bus 1C will remain inoperable
- a fault develops upstream of CB 11C02, or downstream of CB 12C02 with failure of the directly associated protections: then the trip of CB 11C02 makes bus 1C operable with an alternate power source available, but the fault will remain unprotected and will likely evolve into a damage-induced open circuit
- the actuation of CB 11C02 is due to a spurious Function A condition.

Fig. 2.11: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.12: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.13: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.14: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.15: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.16: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.17: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.18: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.19: Fault tree for the event "insufficient power on Bus 1C" (continued)

Fig. 2.20: Fault tree for the event "insufficient power on Bus 1C" (continued)

CHAPTER 3

3. A Critical Look at the Applicability of the DAS and SEA Methodologies to Transients that have Occurred in the Electrical Systems of Nuclear Power Plants

3.1 General purpose of a Qualitative Evaluation of the DAS performance with Regard to Some Reported Electrical Transients

In the present chapter we are going to consider some significant transients that have occurred in U.S. nuclear power plants, and that were originated in the electrical power systems. Our intention in doing this is to verify, from a general point of view, the applicability of the DAS and SEA methodologies to the analysis of real occurrences. In association with the above, we have chosen (with one exception as we will see later) a group of events that were able to cause the loss of at least one of the sources of power to one or more of the essential 4.16 kv plant buses (some of the events were actually so severe as to cause the loss of all offsite power). The investigation of these events will essentially aim at giving a qualitative answer to the following questions: a) Would the primary conditions "responsible" for the transient be identifiable by a disturbance analysis system of reasonable complexity? b) Would the identification of such primary conditions be of any help in restoring the plant to a normal situation? By trying to answer the questions listed above, we clearly do not expect to give a "yes or no" answer to the general problem of DAS feasibility and usefulness, but we hope to give some indications, in addition to those provided by the elaborations presented in Chapter 2,

of what can be done with such a system in relation to electrical transients, and upon which a judgement can be made of the opportunity or not of proceeding to some more comprehensive research work in this area.

In the following sections we will briefly examine, from the specific point of view that we have described above, seven reportable occurrences involving events dated in between years 1978 and 1980. No special criteria were used in the selection of these events, except the one mentioned before of being somehow subsets of a loss of offsite power event, in association, of course, with the condition of availability of sufficient information attached to each associated Licensee Event Report (LER) as to allow an interpretation of the events themselves and an elaboration of the related matters that appear to be relevant to our purposes (this need for detailed information explains why we have restricted our attention to relatively recent occurrences only).

3.2 Electrical Transients Initiated by Testing and Maintenance Operations

A good percentage of the electrical transients that do occur in power plants is due to personnel errors during the performance of routine testing and maintenance procedures. We are presenting in this section some examples of such occurrences that had varying degrees of relevance to the safety of plant operation. The rationale for looking at events of this type is more to verify whether the use of disturbance analysis could somehow help the plant operator(s) in establishing a better "communication" with the field during maintenance and testing operations, than to try to monitor directly the human interventions on the system during such operations, which cannot be considered a realistic objective for a disturbance analysis system today. What we mean in practice by "better communication" shall be made clearer within the discussions offered in association with the forthcoming examples.

a) Edwin Hatch 1 occurrence on May 6, 1978 (6)

This event cannot be considered as a true transient, and its occurrence was not related to a significant malfunction of the electrical power supply systems either. Nonetheless, as it is explained below, we think that there is justification to include it here.

During a surveillance test in the Georgia Power Co. Edwin Hatch (Unit 1) plant on May 6, 1978, the Core Spray (CS) pump 1A failed to start. This failure did not have a direct effect on the plant

operability and it was later discovered that the lockout overcurrent relay associated with the pump was tripped and the control switch for the activation of the pump start-up had malfunctioned due to a broken positive stop. The LER pertinent to the event does not specify if the overcurrent relay trip was somehow related to the switch malfunction or independent of it. In any case, the reason for bringing this event to the attention of the reader is in the fact that no lockout relay trip annunciation for the CS Pump 1A was available in the control room at the time of the occurrence, and a successive investigation performed on other systems of the plant showed that the same was true for a number of these systems also. A design change was initiated by the Georgia Power Co. to provide such annunciation of tripped lockout relays in the control room, but it is clear that a very simple DAS provision would be the most efficient way to deal with a situation of this type since the same diagnostic information provided by the annunciators can be offered in a more synthetic and meaningful way on a DAS CRT display. This event confirms that in general a means of monitoring tripping relay positions is a useful tool for quick diagnostic of certain types of malfunctions.

b) Duane Arnold occurrence on April 2, 1980⁽⁷⁾

The event described here is rather interesting since a mistake made while performing a rather simple maintenance operation caused temporary loss of one of the essential 4.16 kv buses. We quote

from a letter accompanying the license event report (refer to fig. 3.1 to interpret the text):

"While preparing to change out a cell in 125 VDC batter 1D2, a station electrician opened the breaker between 1D2 and 125 VDC bus 1D20. He then noticed that charger 1D22, which was then powering 1D20, was carrying a load and incorrectly assumed this meant 1D22 was still charging battery 1D2. He then opened the breaker between charger 1D22 and bus 1D20. This resulted in a loss of control power to essential bus 1A4 as well as all other loads being supplied by 1D20 which includes control power to standby diesel generator 1G-21. He then reclosed the breaker between charger 1D22 and bus 1D20. This restored control power to 1A4 which was immediately tripped by undervoltage relays which had been installed as part of an emergency power modification. Essential bus 1A4 supplies power to charger 1D22 so 125 VDC bus 1D20 was again dead. This meant no control power was available so standby diesel generator 1G-21 did not start to supply power to 1A4. The electrician then reclosed the breaker between battery 1D2 and bus 1D20 which restored control power to 1G-21 and the diesel generator auto started and began supplying power to 1A4. Normal system line up was subsequently restored."

In analysing the applicability of a DAS diagnostic to an occurrence of this kind we have to recognize that a human action would not under normal conditions be included among the primary

causes of a DAS logic structure. However, the DAS would be obviously able in a situation like the one depicted above to keep the plant operators informed of the situation occurring, indicating the abnormal breaker position(s) (such as CB 72-202's) as responsible for the various power distribution failures.* In the reported occurrence this may not seem strictly necessary, since the electrician responsible for the malfunction seemed able to undertake the necessary recovery actions by himself, but the situation could have evolved in a different way and it might have been very useful for the operator(s) to be readily made aware of the evolution of the transient. We are therefore tempted to speculate from this example, that a DAS monitoring could represent an aid to ready interaction between field personnel, performing tests and maintenance, and the control room in anomalous circumstances of similar nature. In fact it should be capable of focusing the attention of the plant operators in the direction of the systems affected by the maintenance errors. The problem should, however, be studied in more detail to see if one should go as far as including, for example, a "testing mode" provision in the DAS which would suitably modify the logic structures for a specific system when said system is undergoing testing, or if a simpler solution would be sufficient, contemplating the

(*) We incidentally note that the undervoltage trip of Bus 1A4 is rather poorly explained in the LER and its relation to the manual reclosure of CB 72-202 appears quite inexplicable.

the activation of a special warning in the logic structures to include a testing or maintenance error (generically indicated as such by the DAS) as a possible cause for any malfunction occurring in a system upon which some kind of external human intervention is underway. Both these solutions would imply an interactive DAS provision since the DAS should be "informed" of which system(s) would be undergoing the test and maintenance activity. For the specific event presented here it would seem that the "regular" logic structures would be by themselves a sufficient aid to the plant operators, without any special provision included at all for "maintenance conditions." It is to be seen case by case if for other situations involving difficult systems and circumstances the same would be true or if, viceversa, the information provided by the "regular" logic structures would be misleading.

c) Edwin Hatch 2 occurrence on April 4, 1980⁽⁸⁾

Again we give the description of the event by quoting the narrative report which accompanied the pertinent LER: "During cold shutdown and while performing 18-month surveillance procedure HNP-2-3832, a LOSP was simulated on diesel generator 2C and bus 2G within 5 minutes after a 24-hour full load run on the diesel generator. The diesel generator started but did not tie to the bus to carry the load. During the interval between the 24-hour run and the LOSP while the diesel generator was shutdown the sync speed alarm annunciated, and personnel adjusted the setting to clear the alarm. This was an error. The setting should not have been changed at that time. After the

sync speed setting was changed, it was too low to allow the diesel generator to come up to the necessary speed. Therefore, after the diesel generator started, the auto closing mechanism would not let the diesel generator output breaker close. After the LOSP was initiated and the output breaker did not close, it was noticed that the D/G speed was too low. Personnel readjusted the sync speed setting, and the output breaker closed, tying the diesel generator to the bus as it should. After the error was corrected, the surveillance procedure was reinitiated and completed successfully."

The occurrence reported above seems to confirm the conclusion that we tentatively drew in association with the event described immediately before. A DAS analysis of the transient could in fact have detected the diesel low speed condition immediately and therefore would have called the attention of the operator(s) into the area that was affected by a previous human mistake. In this particular case it is not unreasonable to assume that a low sync speed setting would be normally included by the DAS designer as one of the suggested causes of a diesel generator low speed, in which case the DAS indication resulting from the given situation would have been even closer to pinpoint the event primary cause to the full possible extent. Even without giving the DAS this much credit, we can however agree that for this event no special provision would be needed in it, in order to give some useful and quick information (note that the LER specifies that at first the low diesel speed went unnoticed).

d) SAN ONOFRE 1 occurrence on April 22, 1980⁽⁹⁾

The narrative report accompanying the LER for this event gives the following description (refer to Fig. 2.1, 2.2, 2.4, 2.5, to the contents of Section 2.2, and to the footnote attached to this page for better interpretation):

"On April 22, 1980 with the unit in cold shutdown for refueling, AC power was supplied to the site through one 220 KV switchyard PCB to auxiliary transformers A & B. Auxiliary transformer C and the No. 1 Diesel Generator were out of service for maintenance. Both Safeguard Load Sequencing Systems (SLSS) were also out of service for maintenance. This combination of power sources and equipment outages is permitted by the Technical Specifications.

At 1107, a test technician performing routine auxiliary transformer C relay testing failed to block open a set of relay contacts which subsequently tripped the 220KV PCB supplying power to auxiliary transformers A & B resulting in a loss of power to all 4KV and 480V buses.* The inservice Diesel Generator (No. 2) was manually started by the control room operator; however, the diesel generator was not loaded to the bus as the control room restored offsite power at 1111. The 220 KV supply PCB to auxiliary transformers A & B was reclosed after verifying that the loss of power was not due to equipment malfunction."

(*) According to the protection logic that we have assumed in Section 2.2, based on the plant FSAR information available for us, this sequence would not be possible since a trip of one of the relays associated with Transf. C would cause the 138KV (and not the 220KV) PCBs direct trip. This discrepancy might be due to the fact that the source of our information is not the most up-to-date, or to the fact that some information is missing from the LER. Whatever the case, the substance of our consideration would not change significantly.

To discuss the above occurrence in the proper context it is convenient to refer, with regard to the actuation and failure modes of tripping relays and circuit breakers, to the observations made in Chapter 2. In particular we recall the basic idea that was used in the derivation of the logic structures presented in that chapter, which was to use essentially the relay and circuit breaker positions to diagnose the conditions of the system being analysed, with the additional aid of continuous instrumentation indications whenever available and meaningful.

If we assume that a typical DAS would be capable of monitoring the positions of the relay "flags" rather than those of the relay contact themselves*, we can observe the following:

- for the occurrence considered, the information available to the DAS would be: relay tripped, 220 KV PCBs (Power Circuit Breakers) tripped, zero voltage and current indications downstream of the 220 KV PCBs. This information would practically be the same available had a real trip occurred. Therefore, the DAS would not be able to single out the testing error as the primary cause for the event, but it would call the operator's attention to the right direction (by indicating the relay responsible for the trip). If the operator were aware of the testing procedure underway in that particular area of the electrical systems, the DAS indication would be still useful

(*) The "flag" is an indicator of the relay having tripped, which nevertheless is independent of the relay contact positions; therefore it is quite possible that the flag be "tripped" without the relay contacts having closed (this would happen if they are blocked open for testing or if a failure prevents their closing).

to him to understand what had happened. We must notice in any case that in reality it took only four minutes (as reported in the LER) to detect the problem and take care of it. It is doubtful that a DAS assisted operator could have reacted much faster than that.

- if we assume that the test had been performed without error, the information available to the DAS would have been: relay tripped, circuit breakers not tripped, regular voltage and current indications throughout the system. It is important to notice that such observable conditions are different from the ones the DAS would detect in case of a fault induced relay trip accompanied by a failure of the breakers to trip. The difference, for such a faulted situation, would be in the information coming from the continuous instrumentation, which would show low voltage conditions throughout the system and overcurrent conditions upstream of the fault.

For this particular transient a DAS analysis might not, in conclusion, have been particularly relevant; but, based on the above discussion, it doesn't seem either that its elaborations would go off track by having to deal with the specific testing procedure considered. However, it can be seen from this example why a careful consideration of the impact of testing and maintenance procedures on the input information used by a DAS for its diagnosis is certainly necessary.

After our brief look at these few examples of events initiated by human interventions on the plant, we can conclude tentatively

that in circumstances of this kind a disturbance analysis system could prove in general to be useful, even though we believe that a certain amount of careful evaluation would be necessary, case by case, to make sure that the information generated by means of its logic models would not, in some other situations determined by such human interventions, be misleading rather than useful or "neutral."

One additional conclusion can on the other hand be drawn with a good degree of confidence, regarding these events that we have considered: the DAS would generate no information at all, relevant to these occurrences, unless its logic structures be developed to a considerable level of detail. For instance: in case b) above, the logic tree should go as far as modeling the operating conditions of breakers CB 72-201 and CB 72-202 (see fig. 3.1) in order to detect the existing misalignment.

The above consideration could therefore confirm that, given the apparent necessity of developing rather detailed logic structures in order to generate any information at all, and given the practical impossibility of modeling a whole plant to such level of detail, the SEA methodology proposed in Chapter 1 represents a quite reasonable approach, in that it allows a pragmatic step by step procedure rather than an overambitious all-encompassing analysis. We will return to this point with some additional comments in the next concluding chapter.

3.3 Electrical Transients Occurred During Plant Normal Modes of Operation

In this section we present events that affected the electrical power systems of nuclear plants and that were initiated by equipment faults. We also include in this section events that were the consequence of some engineering or design error. The main rationale for including these here, rather than with those resulting from testing and maintenance errors (which would be logical if an classification were made according to a more or less traditional "human error" vs. "equipment malfunction" scheme) is that, while a plant operator, and theoretically even a DAS, can be advised that a certain plant system, or component is undergoing testing and/or maintenance, which would be somehow a clue to any kind of disturbance originating there, an engineering or design error would arise with no other clues to it than the conditions that it produces in the plant. Thus, in this particular aspect relevant to the diagnostics that we would like to perform, it is indeed similar to a component fault or malfunction.

a) Beaver Valley occurrence on July 28, 1978⁽¹⁰⁾

This event was rather severe and almost resulted in a total (offsite and onsite) power blackout, since, with the offsite sources totally unavailable after a reactor and turbine trip, only one of the two diesel generators was initially able to start and accept load.

The detailed sequence of the occurrence is given below in the initial part of the description originally attached to the event LER (refer for interpretation to fig. 3.2, 3.3 and 3.4):

"On July 28, 1978 at 1536 hours, system operations time, a fault occurred on the Main Transformer resulting in the following: Generator trip, Turbine trip, Reactor trip, Safety Injection, and the loss of all offsite power (station blackout). Both the primary and the secondary plant were placed in a hot shutdown condition in a controlled manner on emergency diesel generator power only. As anticipated in the BVPS FSAR, throughout the whole duration of the event, the Reactor Coolant System was not overpressurized. Pressurizer safety valves did not lift nor were required to relieve. No adverse conditions occurred in the reactor core and the health and safety of the general public were not jeopardized.

By 1557 hours, all offsite power was restored to the station and, at 1614 hours, it was decided to cool the plant down to Operational Mode 5 conditions until the Main Transformer could be returned to service. The specific details relating to the event are as follows:

At 1536 hours, a short circuit between the 345KV high voltage winding and the 21.5KV low voltage winding of the main transformer occurred. The high voltage impressed on the low voltage side of the transformer resulted in a ground from insulation failure of the A phase low voltage termination within the main transformer and a simultaneous failure of the B phase surge arrester within the Main

Generator Potential Transformer Compartment. The simultaneous occurrence of these two grounds applied a single phase short circuit across the main transformer A phase low voltage winding and the main generator A to B phase leads. The main transformer and its immediate area caught on fire due to ignition of the oil spray from the main transformer sudden pressure relief valve. All three Reactor Coolant Pumps tripped on underfrequency. Both the reactor coolant pump underfrequency and the turbine trip provided the Reactor Protection System with the necessary signals to cause a reactor trip to occur.

The following relays were caused to trip: 87-101xx1 (Main Generator Differential), 87-103x1 (Main Generator Differential Auxiliary), 87-102B (Main Transformer Differential), 87-102x1 (Main Transformer Differential Auxiliary), 59-101G (Main Generator Ground Backup Overcurrent), 51-101Gx1 (Main Generator Ground Backup Overcurrent Auxiliary). The station service buses successfully transferred to the offsite sources (The No. 1 and No. 2 bus sections in the 138KV Shippingport Power Station switchboard). Fifteen seconds later as the Beaver Valley Turbine Generator coasted down, while still supplying fault current to the short circuit, the Main Generator Out of Step relays operated. This faulty out of step relay operation* caused an isolation of the Beaver Valley 345KV Switchyard by tripping all 345KV line breakers

(*) The OOS relay operation was not faulty in itself but rather it was the consequence of a design error (see considerations in this regard at the end of the event description and in the subsequent quote from the transcript of the 221st ACRS meeting.

and the tie to the 138KV Shippingport Switchyard tripped. This action isolated the Shippingport Power Station as the only power source on the 138KV bus supplying power to the two remaining 138KV loads and the Beaver Valley Power Station System Transformers. This total load was in excess of the Shippingport Power Station ability to supply the load and the frequency declined to approximately 58 Hertz.

The Turbine trip armed the Steam Dump System's Turbine Trip Controller and, sensing a Tavg (auctioneered high) - Tref mismatch, the steam dump valves opened to reduce Tavg to its no-load value. The actuation of steam dump resulted in a steam flow that was just above the no-load Hi-Steam-Flow Safety Injection setpoint. Since the Reactor Coolant Pumps were tripped, the RTD manifolds in two of the Reactor Coolant loops cooled down much faster than the third loop and, since steam dump operates on auctioneered high Tavg, low-low Tavg was reached on the two loops prior to the steam dump isolating. The Low-Low Tavg interlock on the steam dump system secured the dump valves; however, since the Steam Flow for steam dump was just above the Safety Injection flow setpoint for no load, the Low-Low Tavg completed the logic and Safety Injection was actuated within approximately one minute into the transient.

At this time, all safety systems functioned as designed. The operators in the control room were utilizing the BVPS emergency procedures and the Fire Brigade was proceeding to the Main Transformer where they found the fire at the Main Transformer

extinguished by the fire protection system with minor spot oil fires in the immediate area still burning.

After attempting to reduce the output of the Shippingport Power Station for over three minutes, the Shippingport unit was tripped from the line at 1540 hours. This removed the only source of power from both 138KV bus sections and resulted in a loss of offsite power at Beaver Valley.*

Immediately, the No. 1 Emergency Diesel Generator at BVPS sequentially loaded the 4KV AE emergency bus to provide power to one of the redundant trains of safety related equipment. However, the No. 2 Emergency Diesel Generator failed to flash field and, although running at nominal speed, it did not provide power to the redundant DF emergency bus. Station maintenance was immediately called to trouble shoot the failure of the No. 2 Emergency Diesel Generator.

Meanwhile, the control room operators were stabilizing the plant at a no-load hot standby condition by following the station emergency procedures. Auxiliary feedwater flow was throttled down to 150 gpm to each Steam Generator to provide a slow rise in water level until normal level was achieved and, since the turbine-driven Auxiliary Feedwater Pump is capable of providing the adequate flow, the 1A

(*) This sentence is all but clear since it was previously stated that the Shippingport station was overloaded by the demand of auxiliary power for the Beaver Valley Station, while here the reader is induced to think that Shippingport was troubled by an overproduction of power.

Motor Driven Auxiliary Feedwater Pump was shut down. The 1B Motor Driven Auxiliary Feedwater Pump was not running due to the loss of power on the DF emergency bus. After approximately 8 minutes into the event, since pressurizer level was adequate, the running charging pump was shut down to terminate Hi Head Safety Injection until the normal charging path could be realigned. Within the first 10 minutes of the blackout, a diesel air compressor was started to assure adequate air pressure for the operation of all air operated valves. At approximately 15 minutes into the blackout, with the help of station maintenance, the field was flashed on the No. 2 Emergency Diesel Generator and power was restored to the DF emergency bus. The problem was that the field flash contact failed to close and had to be manually closed. During this time, the Fire Brigade extinguished the remaining spot fires at the Main Transformer and the decision was made to vent the hydrogen out of the Main Generator and purge it with CO₂.

At 1557 hours, all offsite power was restored to the station and, at 1608 hours, the 1A Reactor Coolant Pump was started, returning forced flow to the Reactor Coolant System.

At 1613 hours, cooldown to Mode 5 (cold shutdown) was commenced by means of dumping steam to the atmosphere. At 1630 and 1634 hours, the power supplies to the DF and AE emergency buses, respectively, were transferred from the emergency diesel generators to offsite power...

....No damage to safety related equipment occurred as a result

of this incident. The Main Transformer has been returned to the vendor's shop for rewinding.

The Main Generator out of step relay operation was incorrect during the incident. This bus shedding scheme was a backup protection scheme and has been removed. Other protection trips will still provide primary protection for the main generator and transformer.

The diesel generator field flash failures have been attributed to an intermittently sticking field flash cutout relay. The relay occasionally stuck in the picked-up position, which inhibits application of the generator battery banks to the generator field. This prevents flashing of the diesel generator field.

A suitable replacement for the cutout relays is being investigated. Until a replacement can be provided, a test circuit has been installed in the diesel start control circuitry to allow monitoring of the cutout relay contact status to ensure the relay is not left in the picked-up position after a diesel run.

A remote generator field flash control has been installed in the control room to manually flash the diesel generator field. This control bypasses the field cutout relay to insure field flashing in an emergency."

From the above, it can be seen that the transient described was very complex since it even involved interaction between two different power plants (e.g.: Beaver Valley itself and Shippingport). Without concerning ourselves with all the mechanistic details of the transient we can nevertheless identify two points that were crucial in it and

that were also strictly related to the types of occurrences with which we have been dealing in this and in the previous chapter, namely the trip of the generator out of step relays and the failure of the #2 diesel generator field flash relay.

A good explanation of why the OSS relays operated and why this operation can be considered a design error was given in the 221st ACRS meeting in response to a specific ACRS question. We report here the transcript of the pertaining question and explanation⁽¹¹⁾ (refer to fig. 3.5 for a graphic illustration also):

"QUESTION:

Why did the out-of-step relay trip and why did operation of the out-of-step relay leave a situation where the Shippingport plant was overloaded?

RESPONSE:

The out-of-step (OOS) relay is designed to sense a loss of synchronization between the Beaver Valley (BV) generator and the remainder of the Duquesne Light Co. (DLC) distribution system. This is accomplished by monitoring the BV main generator output voltage and current, from which the ratio of voltage to current is derived, and may be expressed as an impedance. An increase in system impedance, as indicated by shifts in phase angle and magnitude of the main generator output, would be indicative of a major system disturbance (i.e., grid blackout). Should a disturbance occur that caused an impedance swing to within the actuating range of the OOS relay, the relay would initiate a bus shedding scheme to isolate

the 345 KV and 138 KV switchyards by opening a number of breakers. This protection removes the 345/138 KV switchyards from the DLC system, leaving only two small block loads off the 138 KV switchyard. The original intent and design of this protection scheme was to isolate the BV and Shippingport switchyards with a small "island of load" during a major system upset (e.g., a Northeast blackout situation), to maintain generation within the island of load and allow for a rapid recovery of the system once the initiating fault was cleared. Inherent to the acceptability of this bus shedding scheme was the assumption that the BV would maintain generation capability to supply its own house loads and the island loads. During the sequence of events following fault inception in the main transformer, several main generator and transformer protection trips acted immediately to trip the generator and open the generator tie breakers to the 345 KV switchyard. The momentum of the main generator and decaying field voltage produced generator neutral currents for approximately six minutes to feed the fault. Oscillograph recordings of voltages and currents show a fault involving A phase to B phase to Ground with substantial arcing as indicated by changes in both magnitude and phase angle of voltages and currents. It is postulated that the generator essentially became a high resistance grounded to an arcing fault. It was during these conditions, 15 seconds after fault inception and after the BV unit had been separated from the system, that the OOS relay was "fooled" into sensing that a legitimate trip condition existed,

when, in fact, the relay was subjected to a pseudo swing trip condition due to the nature of the fault. The OSS relay protection operated correctly to provide the isolation described above. However, this left the Shippingport Power Station as the only supply to carry its own station service, the BV station service and the small block loads all of which are above the Shippingport load capabilities. The licensee has concluded that the bus shedding protection provided by the OOS relays was improper in the situation where the BV generation capability is also lost. The bus shedding scheme from the OOS relays was a backup protection scheme and has been removed. Other protection trips will still provide primary protection for the main generator and transformer. The OOS relays will still be used to provide backup generator protection, by providing trips to the main generator output breakers, the exciter field breaker and the unit station service transformer 4160V bus supply breakers."

If one examines carefully the situation that occurred in the plant after the initial double fault, one would have to notice the following:

- The operation of the OOS relays was crucial in degrading the availability of auxiliary power to the Beaver Valley station;
- The design error in the installation of such relays was two-fold. Not only the possibility of the Shippingport station alone having to supply the auxiliary loads of Beaver Valley was not foreseen, but neither was the case (which indeed occurred) of the OOS relays operating because of a short circuit after the fault had been isolated by other protections.

To analyze the transient from the point of view of a DAS it is convenient to refer to the event tree of fig. 2.6. Without paying attention to certain differences that exist between the SAN ONOFRE 1 and the BEAVER VALLEY electrical power systems and protections, we focus our attention on two "ramification points", namely the "fault isolation" and the "alignment to alternate offsite source" (which for SAN ONOFRE was the 220 kv SWYD and for BEAVER VALLEY is instead the 138 kv SWYD). If we refer to the BV electric system design as it was before the transient, the DAS logic structures would certainly have to model a main transformer fault, and accordingly recognize, by monitoring the positions of the relative circuit breakers, the successful or unsuccessful isolation of the fault, which also means the isolation of the main generator from the rest of the plant and of the grid. They would be also able to detect a failure to maintain an alignment with the offsite alternate source, by detecting the trip of the 138 kv circuit breakers, provided the logic itself had been derived with the objective of recording partial failures as well as total ones (in fact the BV station was still aligned to the alternate offsite power represented by the Shippingport station and the 138 kv CBs trip was only a partial failure in the alignment to any of the alternate offsite sources. And naturally there would be no reason for the tree structures not to contain the OOS relay actuations as a definitely possible cause for the isolation of the 138 kv switchyard, which would also include the possibility of a spurious actuation of such relays. The success or not of a DAS analysis for the part of the transient that we are considering,

would however depend essentially on whether or not a provision would be made in the DAS logic to recognize that a trip of the OOS relay with the main generator already isolated should indeed be considered spurious. Once again we see here a situation showing that the DAS methodology has a chance to be successful only if applied at a considerable level of system and component detail. It is almost needless to say that if the OOS relay trips had been recognized as spurious there would have been no reason to keep the two power stations isolated from the 138 KV grid and a recovery action in this sense could have been undertaken.

As to the other electrical failure that we have mentioned before, that is the #2 diesel generator failure to start, we can certainly conclude that a DAS could have taken care of the problem much faster than it was actually possible. In fact the attachment to the LER that we have transcribed here does say that a monitoring system for the field flash cut-out relays was installed in the plant, together with a manual bypass of such relays operable from the control room.

b) Oyster Creek occurrence on August 24, 1978

The description of this event as given by the utility is reported below ⁽¹²⁾ (the pertinent diagram is given in fig. 3.6):

"During a routine plant shutdown on August 24, 1978, the power sources for the auxiliary electrical power system did not meet the requirements for reactor power operation as specified in paragraph 3.7 A of the Technical Specifications. When the turbine was manually

tripped at approximately 10:21 p.m., all 230 KV circuit breakers opened simultaneously and isolated the two 230 KV transmission lines from the ring bus in the plant switchyard. Normally, only the two 230 KV circuit breakers which isolate the generator from the bus would have opened. The first of the tripped breakers necessary to restore the 230 KV power supply was reclosed within one minute of the trip...

...At the time of the event, the plant auxiliary load was being supplied through the two startup transformers which is normal for a routine shutdown. The isolation of the 230 KV power supply removed one of the two sources for offsite auxiliary power. During the brief period of time the 230 KV supply was isolated, the plant auxiliary power was supplied from the 34.5 KV system."

This occurrence was, unlike the one described in the previous point a) of this same section, rather simple, since it involved only the spurious actuation of some of the 230 KV circuit breakers. Very little can be said here about the benefit obtainable from the use of a DAS, since the description of the event doesn't go so far as to specify what type of spurious trip caused the 230 KV CBs to open (we have discussed in Section 2.5 of which spurious actuations can be considered DAS-detectable and which cannot). The descriptive LER also specifies that the recovery time for realignment of the plant to the 230 KV switchyard was only one minute, which leaves little room for improvement.

c) Arkansas Nuclear One - Units 1 & 2 occurrence on September 16, 1978

The event of interest here involved the interaction of two

units, which was somehow the case for event a) of this section also. The description given below is taken from an NRC information notice ⁽¹³⁾ (and so is the related simplified electric diagram presented in fig. 3.7):

"Initially Unit 1 was operating at 100 percent power; Unit 2 was in hot standby performing hot functional testing in preparation for initial criticality and power operation. Unit 1 auxiliary electrical loads were being supplied from the Unit 1 main generator via the unit auxiliary transformer. Unit 2 auxiliary electrical loads were being fed from the offsite grid through Startup Transformer No. 3. The normal operating status was interrupted by the failure of the Unit 1 Loop "A" Main Steam Line Isolation Valve (MSIV) air operator solenoid causing the MSIV to close as designed. The Unit 1 Reactor Protection System sensed conditions requiring reactor shutdown and tripped the reactor. The Unit 1 turbine-generator tripped concurrently. Because the Unit 1 generator could no longer supply power for the Unit 1 auxiliary loads, these loads were automatically transferred to Startup Transformer No. 1 to supply this power from offsite. The sequence of events should have ended at this point.

The power to Startup Transformer No. 3, which was feeding Unit 2, and to Startup Transformer No. 1, now feeding Unit 1, normally passes through a single piece of equipment, the Bus Tie Auto-Transformer. The Auto-Transformer has the capacity to provide power for both units, but due to an error, the protective relays were still

adjusted for the operation of Unit 1 only. As a result, when both units concurrently drew power from the Auto-Transformer these protection relays tripped and cut off power to Startup Transformer Nos. 1 and 3.

Startup Transformer No. 2...thus became the only source of off-site power for both Units 1 and 2. The onsite switching equipment automatically transferred the full auxiliary loads for both units to this transformer. However, this transformer is not designed to carry full auxiliary loads for both units. For this reason, Startup Transformer No. 2 became overloaded and the voltage dropped on the station distribution system for offsite power. At this time and during most of the incident operating personnel at both units were unaware of the degraded voltage condition due to the overloaded Startup Transformer No. 2.

At Unit 2, eight seconds after the switch to Startup Transformer No. 2, the relays* which operate to protect Engineered Safety Feature (ESF) equipment from low (degraded) voltage disconnected and therefore deenergized both Unit 2 ESF buses as designed. At the same time, the Unit 2 Core Protection Calculator (CPC) instrumentation registered trips which indicated a loss of AC power to

(*) These relays are the second level of undervoltage protection required as a result of the NRC staff review of the 1976 Millstone 2 degraded voltage event. Corrective design changes (i.e., undervoltage relays and load sequencing to offsite power) had been implemented on Unit 2 for degraded voltage protection. These design changes had not been implemented on Unit 1 at the time of the event.

the circuits that supply at least two instrument channels...

...Each one of the four CPC instrumentation circuits receives power from a vital AC bus which in turn receives power from a battery through an inverter that converts DC power to AC power. Each inverter normally provides power through a circuit with access to both an ESF bus and the station batteries. Each inverter also has an automatic switch that can cut off this normal supply circuit and shift the loads to an alternate supply circuit, which includes just the ESF bus.* With both Unit 2 ESF buses momentarily deenergized the only source of instrument power was from the station batteries through the normal switch position. However, although the exact cause is unknown, all four inverter automatic switches were found in the alternate position. Three of four inverters had improper settings on time delay relays and one inverter had the undervoltage trip setting too high, which may have in part been the cause...IE Circular No. 7902, Failure of 120 Volt Vital AC Power Supplies, dated January 16, 1979, provided details of the inverter problems and recommended items to be reviewed to avoid similar problems...

...The loss of power on two 120 volt vital AC instrument buses caused, as designed, an actuation of all Unit 2 Engineered Safety Features. Thus, when the two Unit 2 emergency diesel generators started and provided power to the previously deenergized ESF buses, the Engineered Safety Features equipment began to operate. However,

(*) See insert on Fig. 3.7.

due to inverter failures, premature actuation of the Recirculation Actuation System (RAS) occurred. This actuation momentarily opened a flow path directly between the Refueling Water Tank (RWT) and the containment sump. ESF operation and premature RAS operation combined to transfer approximately 60,000 gallons of borated refueling water to the containment sump in about 90 seconds.

The normal design sequence calls for the RAS to automatically change the valve lineup when signals from the level instruments on the Refueling Water Tank (RWT) indicate that the tank is nearly empty, which is expected to occur approximately 30 minutes after the LOCA. During this incident, the RAS acted immediately in response to the failure of the inverters and made the change in lineup while the RWT was nearly full. The loss of power from the inverters caused a false low water level indication in the RWT. This false indication provided the signals for the actuation of the RAS.

Had the Emergency Core Cooling System and/or the Containment Spray System been needed in the event of a design basis loss of coolant accident, it would not have performed as designed because of the premature RAS valve actuation. ESF degradation on Unit 2 did not involve a threat to the health and safety of the public because Unit 2 was preoperational and had no radioactive fission product inventory in the core. However, there was no assurance that the inverter deficiencies which caused the premature operation

of the RAS valves would have been corrected prior to Unit 2 power operation.

In the event of a LOCA with a fission product inventory, if the RAS were to initiate at the beginning of the accident, as it did in this incident, the low pressure and high pressure coolant injection subsystems (LPCI and HPCI) of the Emergency Core Cooling (ECC) and the Containment Spray System might not function properly. Actuation of RAS causes isolation of the water in the RWT, which is the source of short term cooling water for Emergency Core Cooling and Containment Spray. The premature actuation of RAS also causes these pump suction lines to be connected to the containment sump when there may not be sufficient water available.

Initially, the sequence of events on September 16 did not indicate any problem with the electrical distribution system of Unit 1. However, subsequent analysis indicated that in the event of a LOCA at Unit 1 during which Startup Transformer No. 1 received both the auxiliary electrical loads and starting loads of the Engineered Safety Features a voltage reduction would result. The safety loads might not initially transfer to the Unit 1 diesel generators but could remain on the startup transformer with reduced (degraded) voltage. Although there is margin in the sizing of emergency equipment and the conditions of operation of such equipment, this situation could cause fuses to blow in Engineered Feature circuits which could result in disabling the safety equipment..."

It's not hard to realize that the above illustrated event was rather complicated. If we try to take a "piecewise" look at it we can nevertheless identify these rather crucial turning points in its course, namely:

- The operation of the Bus Tie Auto-Transformer protective relays, due to their set-point error.
- The overloading of Startup Transformer No. 2, due to the design error in the sizing of the same.
- The ESF actuation, due to the misalignment of the low voltage DC/AC power inverters.

Of these three occurrences listed above the first doesn't seem to be DAS-diagnosable, unless we envisioned an unreasonably complex system, capable of registering continuous instrumentation readings for currents and voltages and containing also in itself all the information regarding the values of trip set-points in the various modes of plant operation. The last two appear instead suited to being rather easily analysed, since both the degraded voltage condition in Transf. No. 2 and the inverter misalignments can be detected by an on-line analysis.* In both cases, once the diagnosis were available, a recovery could be easily performed, even though it is unlikely that it could be performed in the short time available (order of ten seconds) to prevent the ESF actuation.

(*) Note that the first of these two conditions represents a case in which the key information for a DAS diagnosis could be supplied by a piece of continuous instrumentation (voltmeter) and not only by a relay (4.16 KV undervoltage).

The ESF actuation could have had a better chance of being avoided only if a continuous switch alignment monitoring with automatic action capability were somehow associated with the DAS (but this again envisions a system of probably unrealistic complexity).

Having completed the illustration of our examples, we can summarize some of the points that were presented in this section and add a comment or two that appear necessary in the context of this chapter.

The "detectability" of faults that were the result of electrical component failures appears to be good for a relatively simple DAS (utilizing for instance logic structures essentially similar to those derived in Chapter 2): we underscored already that situations like the main transformer fault and the failure of the field flash contacts in the Beaver Valley occurrence, or the misalignment of the low voltage DC/AC inverters in the Arkansas Nuclear One (ANO) occurrence can be apparently coped with without particular problems by use of such a DAS.

For situations involving spurious trips and actuations the ability of diagnosing the event properly depends on the type of spurious actuation involved. The discussion of point B), Section 2.5, applies to these circumstances.

Finally, for situations involving design or operation errors, the applicability of a DAS can vary, but it is encouraging to notice that at least some of these situations can be properly detected, like the transformer overload condition at ANO, and possibly the unwarranted OOS relay actuation of Beaver Valley.

An important thing to notice is that sometimes the design of the plant systems is such that it makes the recovery action after the discovery of a fault almost impossible. So, for instance at ANO the time delay for actuation of the 4.16 KV undervoltage protection relays on the essential buses is reported by the source of our event-description to be only eight seconds, which would not have given much of a chance for an emergency unessential-load-shedding action, even if the Startup Transformer No. 2 overload condition could have been pinpointed by a DAS diagnostic scan while it occurred. Without making judgements that could be unwarranted, as we do not have all the information necessary to express specific ones, we surmise that, if and when disturbance analysis systems will be accepted as part of the typical facilities available to improve the safety and protection of nuclear power plants, there might be cases in which their presence would be accounted for in the design of certain protection systems. This would be clearly convenient whenever it could facilitate the DAS's performance without compromising the effectiveness of the protection system involved.

Fig. 3.1: Duane Arnold: 125V DC control power distribution system

Fig. 3.2: Beaver Valley: 345/138 KV system interconnections

Fig. 3.3: Beaver Valley: 345/138 - 4.16 kV distribution system

Fig. 3.4: Beaver Valley: main transformer fault

Fig. 3.5: Beaver Valley: main generator out of step relays

Fig. 3.6: Oyster Creek: 230/34.5 - 4.16 KV distribution system

Fig. 3.7: ANO 1 & 2: simplified block diagram of electrical distribution system

CHAPTER 4

4. Conclusions

4.1 Remarks on the General Features of the DAS and SEA Methodologies

In Chapter 1 we have described the main characteristics of the disturbance analysis methodology, and we have also proposed a particular way of implementing it, that we have called for convenience "Significant Event Analysis". In Chapter 2 we have also proceeded to apply these methodologies, although in an incomplete way, to a real system. Such an exercise illustrated some of the benefits and problems that can arise in the application of the proposed type of logic.

Before looking in the next two sections at the particular problems that are posed by the nature of the systems that we chose to be the subjects of our investigation (that is, the electrical power systems of a plant), it is here convenient to summarize some of the conclusions that can be drawn on certain general questions regarding the procedures that we have tried to apply.

The indications that we have collected in Chapter 2, and somehow in Chapter 3 also, do not give us any reason to believe that the SEA approach, as outlined in Section 1.3, would not be suitable for practical applications of the DAS methodology to vital plant systems. And on the other hand we have already pointed out (see Section 1.3) the advantages of starting off the derivation of the DAS logic structures by modeling selected disturbances (which is one of the basic ideas underlying such approach) rather than trying to model the entire system of interest with all its possible failure modes. Even if the

convenience and flexibility of the SEA approach are in its favor, at least one major problem associated with its application warrants further discussion and investigation. This concerns whether or not any criteria could be used for the identification of priorities in the selection of the "significant events" themselves.

The natural tools to be employed to establish such criteria could be developed by applying the methods of probabilistic risk-benefit analysis; however, presently there seems to be not enough agreement on the fundamental definitions of the elements needed in such sort of analysis (the definition of risk itself as applicable to nuclear power plants is the subject of investigation and discussion); and in any case not enough results are available to allow the use of such an approach to make real DAS design choices. It is, however, worthwhile mentioning that fortunately there exist a number of rather well identified "significant events" whose relevance to the safety of a plant is generally recognized and accepted, and that certainly provide the DAS engineer with enough material to start his analytical work (the condition considered in Chapter 2 was an obvious example of this widely acknowledged class of SEs).

Another problem of general nature that requires some further attention concerns the possibility of different SEs simultaneously induced by common cause mechanisms. This problem, although general indeed, does not seem amenable to an easy solution by applying a universal "recipe" to it. The only way that we can envision to deal with it at this stage, would be, after deriving the DAS structures for different SEs, to verify the realistic possibilities of common

mode activation of such SEs, and whether special features should and could be added to the logic structures in order to cope with those circumstances.

A final point of very general nature that it is very important to make here, concerns the very question of whether or not it can be worthwhile to undertake and carry out the complex task of performing the analyses necessary for the development of a working DAS. In Chapter 2 we saw that the application of a DAS would allow the detection of certain types of spurious component activations and certain types of component failures that would otherwise be pretty hard to detect. This is certainly useful and is probably applicable to many malfunctions that can occur in any electrical or thermal-hydraulic system of a nuclear plant. But the real point here is actually whether or not a designer can today afford to trust the protection systems of a plant, engineered as they are to cope with an envelope of hypothesized situations, and its human operators, trained as they are to cope with a similar envelope of situations, to do their intended job, without attempting himself to do the costly and painstaking analytical work necessary to find out the kind of circumstances in which the plant defenses would be in serious danger of being defeated. If the answer to this question is that analysis of this kind is certainly warranted, then a disturbance analysis system should be only regarded as a natural appendix of such work, or actually as a convenient way to store, and retrieve when necessary, the information that was in the above sense derived about the plant.

The better knowledge and understanding of the plant that is achievable by the study of its failure and malfunction modes is the real benefit that we can derive from an analysis of this kind. The DAS in itself might be a reliable way to pass this better knowledge down, from the system analyst to the system operator.

4.2 Some Observations on the Particular Nature of the Transients of Importance in Electrical Systems, and the Consequences on the Associated DAS Logic Structures

The main characteristics of the transients that characterize the electrical power systems of a plant are the usually very short time frame in which the transient develops before some kind of protection is activated, and the consequent very quick suppression by the protective systems of the "natural" conditions originated by it.

In the analysis performed in the previous chapters we have assumed that the instrumentation usable as the input source of information to the DAS, and the DAS itself, would not have sufficient "resolution power" to track in such a short time frame the instantaneous variations of current and voltages at different points of the systems considered. As a result, it was only natural to discard the time-delay modeling feature of the cause-consequence diagrams normally used in the experimental DASs developed so far in favor of the simpler fault-tree-like structures employed in this study. Also, we saw how in most cases the continuous instrumentation available on the electrical systems appeared to be of scarce use for our diagnostic purposes (with a few exceptions the most notable of which was seen in one of the examples given in Section 3.3), as opposed to the extensive use that we made of the "yes/no" type of information associated with such variables as relay and circuit breaker positions. We expect these conclusions concerning the use of the cause-consequence diagrams and of the continuous instrumentation readings, as applied to the analysis of electrical transients, to remain valid at the

present state of the art. In fact, even if the problem of reducing sufficiently the DAS scanning times, etc., were solvable today, a lot of analytical work, probably involving simulation studies and the development of rather complex logic models, would have to be performed in order to classify the information that would be contained in the instantaneous recordings of electrical parameter variations with time, for all the different transients that could take place in a system. In the cursory examination made of the examples presented in Chapter 3, we were able to see that the diagnostic capability of the DAS analysis was in most cases dependent on the availability of logic structures modeling the observed disturbances to a relatively high degree of detail. The monitoring and modeling of all the continuous parameters that would have to be considered in correspondence with such a detailed implementation would be extremely difficult to handle. It seems therefore that an approach based mostly on the use of the binary variables with which we have been dealing in the course of this study, would be at the moment the most viable one for real applications also.

4.3 Some Practical Recommendations for Effective Ways of Implementing a Disturbance Analysis on the Electrical Systems of a Power Plant

It is our intention to conclude our study with some recommendations of a rather practical nature, in that they condense the impressions that we have collected in the course of this work regarding the question of how the task of developing a working DAS for the electrical systems of nuclear power plant should be oriented and organized.

A first observation is that the analytical work necessary to develop a DAS should be performed at an interdisciplinary level. As we see it, at least three different areas of expertise should be adequately covered and well integrated together.

- a) Plant control and protection logic: the various modes of plant operation and protection must be in fact known inside out to derive and link properly the logic structures that constitute the DAS's essential skeleton.
- b) Electrical component failure modes and protective device characteristics: this information would be essential to determine which symptoms and indications can be used to detect and diagnose faults and malfunctions. This type of knowledge should be clearly associated with a solid background of information on the characteristics of the whole plant auxiliary power system itself.
- c) Fault tree analysis: needless to say, the derivation of the logic tree structures is at the very core of the derivation of

a DAS and must be performed as thoroughly and efficiently as possible.

The necessity of the best possible coordination between the three above areas is in our view a very important point. Indeed the task of collecting adequate information on the systems we were trying to analyze was perhaps the one that took the biggest portion of the time devoted to this study.

Special care should be paid in the derivation of a real, on-line DAS, to make sure that the system logic can account for the different alignments of plant systems and components required during different modes of operations, since failing to do so will most certainly result in a total failure of the DAS logic to match the real conditions occurring in the plant during such different modes of operation.

The interaction of protection logics and DASs might be interpreted in the future not as a mere one-way dependence, but according to some sort of coordination in the respective design philosophies; that is, among all possible relaying logics, an effort could be made to implement the ones that would make the DAS's task easier to accomplish. We expect a similar problem to arise in the future, regarding the choice of the type and number of instruments to be placed in the plant systems.

A further recommendation that we want to make, concerns a point that we have touched a few times before, but that we feel is important enough to be explicitly recalled here. Concerning the level of detail at which the logic structures for a certain distur-

bance should be sought, we believe that is probably better to proceed to a full derivation for only a few disturbances rather than to develop only "high level" structures for a great many of them. This opinion is based on the findings of our analyses of Chapters 2 and 3, which seemed to show that diagnoses and recovery actions are often impossible without the processing of what we can call "fine information". If the DAS designer decides that certain branches of the structures that were derived are not so essential, such branches can be "pruned" (as we mentioned in Section 1.2), but in this case the simplification will be rationally justified and not based on pre-judgment.

Finally, we must notice that a practical DAS should certainly have features allowing a relatively easy modification of its structures. If one wants to convince oneself of the opportunity of this, one has only to take a look at the documentation associated with nuclear power plant reportable occurrences, describing the continuous process of adjusting set points, modifying protective relay logics and so forth. A DAS without a provision for easy adaptation of the logic structures to new plant configurations would be out of service far too often.

REFERENCES

1. F. Frogner, C. H. Meijer: "On-Line Power Plant Alarm and Disturbance Analysis System", EPRI NP-1379, 1980.
2. L. Felkel, R. Grumbach, A. Zapp: "Analytical Methods and Performance Evaluation of the STAR Application in the Grafenrheinfeld Nuclear Power Plant", IAEA Specialists' Meeting on NPPCI, Dec. 1979, Munich, Germany.
3. B. Frogner, C. H. Meijer: "On-Line Power Plant Alarm and Disturbance Analysis System", EPRI NP-613, 1978.
4. F. Owre, L. Felkel: "Functional Description of the Disturbance Analysis System for the Grafenrheinfeld Nuclear Power Plant", Enlarged Halden Programme Group Meeting, Loen, Norway, June 1977.
5. Southern California Edison Company, San Onofre Nuclear Generating Station - Unit 1, Final Safety Analysis Report, Docket No. 50-206.
6. Georgia Power Company, Edwin I. Hatch Nuclear Plant - Unit 1, Docket No. 50-321, LER 78-31, June 6, 1978.
7. Iowa Electric Light & Power Company, Duane Arnold Energy Center, Docket No. 50-331, LER 80-014, April 10, 1980.
8. Georgia Power Company, Edwin I. Hatch Nuclear Plant - Unit 2, Docket No. 50-366, LER 80-046/036-0, April 28, 1980.
9. Southern California Edison Company, San Onofre Nuclear Generating Station - Unit 1, Docket No. 50-206, LER 80-015/01T-0, May 5, 1980.
10. Duquesne Light Company, Beaver Valley Power Station, Docket No. 50-334, LER 78-43/01T-1, December 29, 1978.
11. 221st ACRS Meeting, September 1978 (Transcript p. 13).
12. Jersey Central Power & Light Company, Oyster Creek Nuclear Generating Station, Docket No. 50-219, LER 78-14/3L-0, September 22, 1978.
13. Nuclear Regulatory Commission, IE-Information Notice No. 79-04, February 16, 1979.

DISTRIBUTION:

TID-4500 - UC-78 (197 copies)

J. H. Carlson, NE-540 (5)
Office of Nuclear Power Systems
U. S. Department of Energy
Mail Stop B-107
Washington, DC 20545

A. C. Millunzi, Team Leader
Safety Research and Development Team, NE-540
Office of Nuclear Power Systems
U. S. Department of Energy
Mail Station B-107
Washington, DC 20545

Leo Beltracchi
U. S. Nuclear Regulatory Commission
Division of Systems Safety P-350
Office of Nuclear Reactor Regulations
Washington, DC 20555

Raymond DiSalvo, Branch Chief
Operations Safety Research
U. S. Nuclear Regulatory Commission
Mail Stop 1130SS
Washington, DC 20555

W. Lipinski
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

O. Meyer
Idaho National Engineering Laboratory
EG&G Idaho, Inc.
P. O. Box 1625
Idaho Falls, ID 83415

Oak Ridge National Laboratory (2)
P. O. Box X
Oak Ridge, TN 37830
Attn: R. Kisner
J. L. Anderson

J. Gallager
Westinghouse Electric Corp.
P. O. Box 355
Pittsburgh, PA 15230

Distribution (cont'd):

Len Rucker
Boston Edison Company
800 Boylston St.
Boston, MA 02119

Joseph Turnage
Nuclear Energy & Development Dept.
Yankee Atomic Electric Co.
25 Research Drive
Westborough, MA 01581

Georgia Institute of Technology (2)
Engineering Experimental Station
Computer Science & Technology Laboratory
Atlanta, GA
Attn: J. L. Russell
J. A. Mahaffey

University of California (2)
Chemical, Nuclear, and Thermal Engineering
5532 Boelter Hall
Los Angeles, CA 90024
Attn: S. Guarro
D. Okrent

A. Long
Electric Power Research Institute
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, CA 94303

Babcock & Wilcox Co. (2)
P. O. Box 1260
3340 Old Forest Road
Lynchburg, VA 24505
Attn: E. J. Bateman
E. Dowling

Combustion Engineering Inc. (2)
Nuclear Power Systems Division
1000 Prospect Hill Road
Windsor, CT 06095
Attn: W. R. Corcoran
C. H. Meijer

R. L. Clark
U. S. Department of Energy
Albuquerque Operations Office
Albuquerque, NM 87185

Distribution (cont'd):

4400 A. W. Snyder
4440 G. R. Otey
4443 D. A. Dahlgren
4443 P. Shea (20)
4443 P. Yarrington
8214 M. A. Pound
3141 L. J. Erickson (5)
3151 W. L. Garner (3)
DOE/TIC (Unlimited Release)