15D Probability Analysis of Pressure Regulator Downscale Failure

15D.1 Introduction

A reliability analysis has been performed on the ABWR pressure regulator fault tolerant controller architecture. The purpose is to determine the frequency at which simultaneous closure of all four turbine control valves (TCVs) might be expected to occur, initiated by the control system due to failure of the pressure regulator.

Fail closure of all four turbine control valves initiated by failure of the pressure control system is defined as "Pressure Regulator Downscale Failure (PRDF)".

15D.2 System Description

The elements of the control system are depicted in Figure 15D-1. The pressure sensor signals are subject to range limit checks to identify a fully failed sensor/signal. A selection logic is used to validate when all the three inputs are available and good. Upon failure detection of one signal, the validation logic automatically reverts to a high value gate (HVG) of the two remaining active signals.

The control system consists of three identical processing channels with necessary hardware and firmware. Means are provided to transfer data between processing channels. To avoid processing channel output divergence, the processing channels compare and vote on calculated integrator state variables. The signal voting and interprocessor communication is implemented to assure that no more than one sample period delay occurs between sampling the inputs and using them in the processor calculations.

Diagnostics are conducted by comparison of internal digital turbine control valve (TCV) position demand signals to determine the failure of any output signals to TCVs. The TCV demand output signal failure from the controller is considered as a channel failure. If two failures are detected, a turbine trip is initiated to avoid a PRDF.

15D.3 Analysis

15D.3.1 Analytical Conditions

(1) The assumption for this analysis is that TCV demand output signal failures from two channels having occured, one or more of these failures not detected by the detection diagnostics will result in closure of all four TCVs.

(2) It was assumed that the failure rates represent failures that result in loss of output.

(3) Mean-time-to-repair is 10 hours.

(4) Failure rates for electronic modules are estimated, based on anticipated complexity of the circuit functions. (processor failure rate = 10^{-5}/h).

15D.3.2 Approach

Using the system block diagram of Figure 15D-1, event trees were constructed to show the failure paths which could result in pressure regulator downscale failure. Basically, there are two ways that all four turbine control valves can be closed "simultaneously": (1) failure of combinations of all four valves, or (2) failure of any two of the three channels, with the two possible combinations of at least one of the two failures not detected. Logic equations were written from the event trees and after simplification were evaluated for the frequencies identified in the introduction.

15D.4 Results

The frequency of inadvertent closure of all 4 TCVs initiated by failure of the pressure regulator is found to be extremely low so that the event can be treated as a limiting fault (See Subsections 15.2.1.1.1 and 15.2.1.1.2.2).

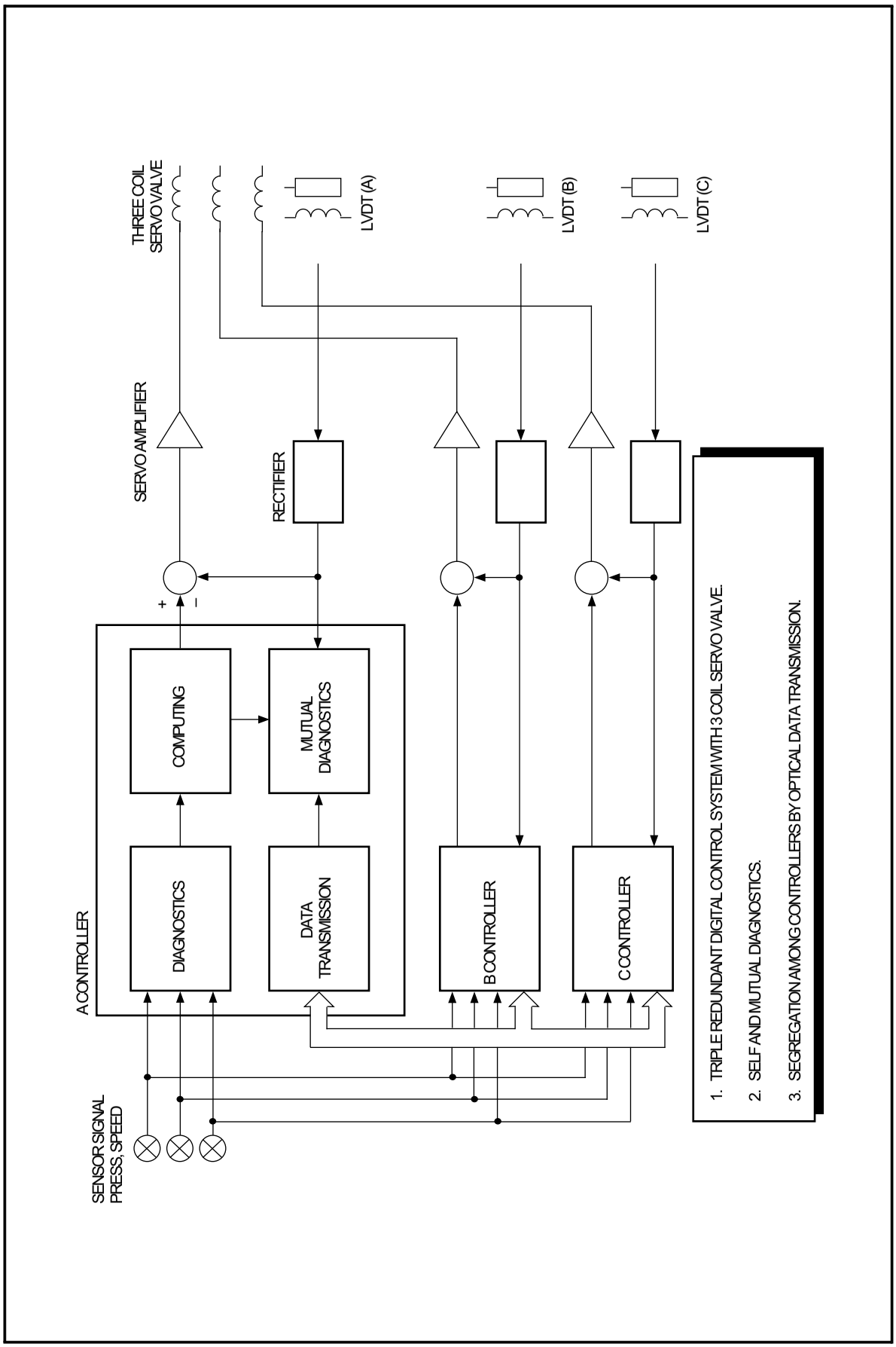

Figure 15D-1 Triple Redundant Control System

Figures 15D-2 through 15D-5 are Not Used