Loss of I/O VCMI in TMR System - If the VCMI in an interface module in a TMR system fails, the outputs timeout to their configured default output state. The inputs are set to their configured default state so that resultant outputs, such as UDH, may be set correctly. Inputs and output healthy bits are reset. A failure of the VCMI in Rack 0 is viewed as equivalent to a failure of the control module itself.

Loss of I/O VCMI in Simplex System - If the VCMI in an interface module in a simplex system fails, the outputs and inputs are handled the same as a TMR system.

Loss of I/O Board in Simplex System – If an I/O board in a simplex system fails, hardware on the outputs from the I/O boards set the outputs to a low power default value given typical applications. Input boards have their input values set to the preconfigured default value in the Master VCMI board.

Loss of Simplex I/O Board in TMR System - If the failed simplex I/O board is in a TMR system, the inputs and outputs are handled as if they were in a simplex system.

Loss of TMR I/O Board in TMR System - If a TMR I/O board fails in a TMR system, inputs and outputs are handled as described previously. TMR SIFT and hardware output voting keep the process running.

Loss of IONet in Simplex System - If the IONet fails in a simplex system, the output boards in the I/O racks timeout and set the preconfigured default output values. The Master VCMI board defaults the inputs so that UDH outputs can be correctly set.

Loss of IONet in TMR System - If the IONet fails in a simplex system, outputs follow the same sequence as for a Loss of Control Module in simplex. Inputs follow the same sequence as for Loss of I/O VCMI in TMR.

Turbine Protection

Turbine overspeed protection is available in three levels, control, primary, and emergency. Control protection comes through closed loop speed control using the fuel/steam valves. Primary overspeed protection is provided by the controller. The TTUR terminal board and VTUR I/O board bring in a shaft speed signal to each controller where they are median selected. If the controller determines a trip condition, the controller sends the trip signal to the TRPG terminal board through the VTUR I/O board. The three VTUR outputs are 2/3 voted in three-relay voting circuits (one for each trip solenoid) and power is removed from the solenoids. Figure 2-22 shows the primary and emergency levels of protection.

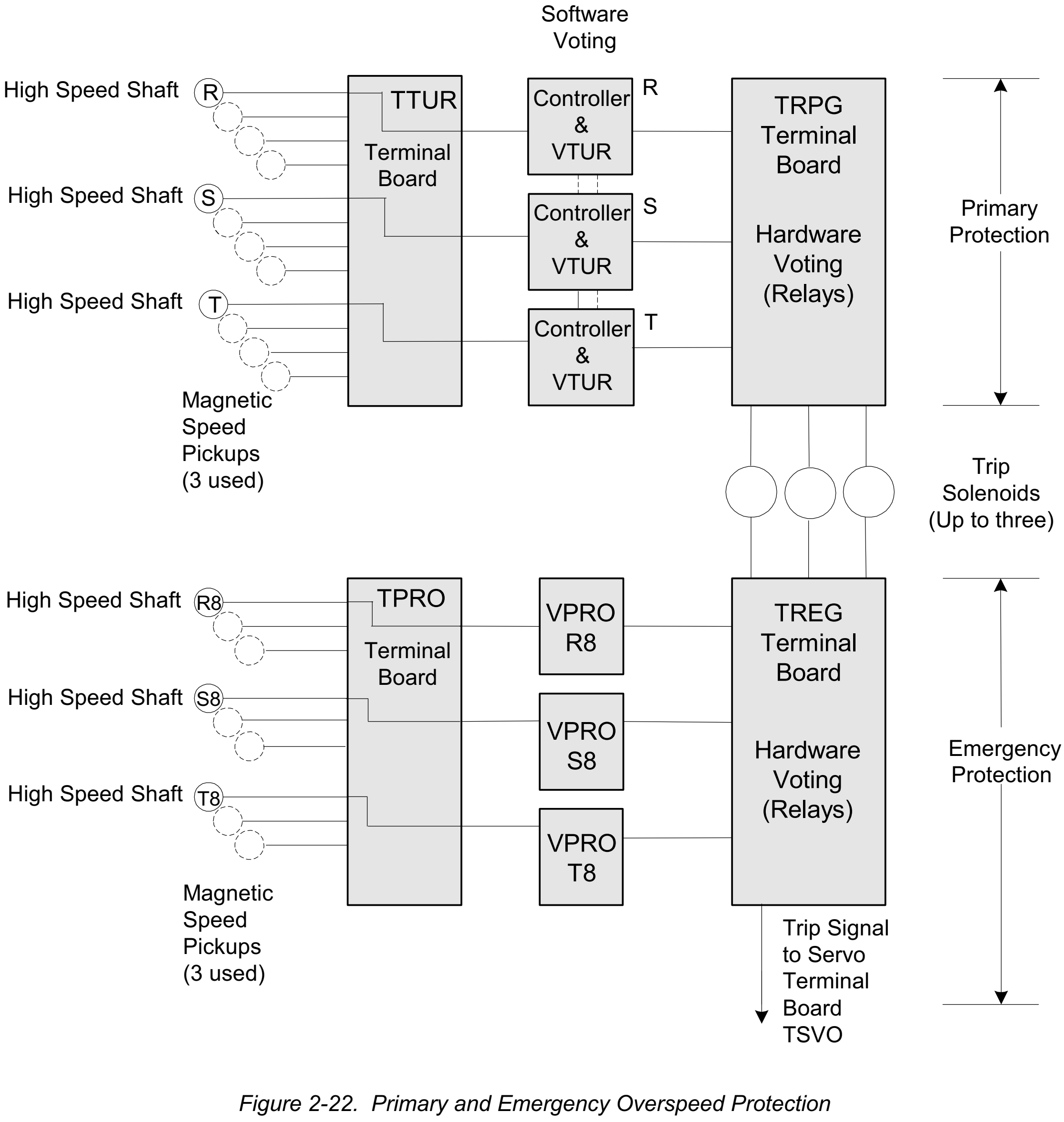

Figure 2-22. Primary and Emergency Overspeed Protection

Either the controllers or the protection system can independently trip the turbine.

Emergency overspeed protection is provided by the independent triple redundant VPRO protection system shown in Figure 2-22. This uses three shaft speed signals from magnetic pickups, one for each protection module. These are brought into TPRO, a terminal board dedicated to the protection system. Each VPRO independently determines when to trip, and the signals are passed to the TREG terminal board. TREG operates in a similar way to TRPG, voting the three trip signals in relay circuits and removing power from the trip solenoids. This system contains no software voting, making the three VPRO modules completely independent. The only link between VPRO and the other parts of the control system is the IONet cable, which transmits status information.

Additional protection for simplex systems is provided by the protection module through the Servo Terminal Board, TSVO. Plug J1 on TREG is wired to plug JD1 on TSVO, and if this is energized, relay K1 disconnects the servo output current and applies a bias to force the control valve closed.

Reliability and Availability

System reliability and availability can be calculated using the component failure rates. These numbers are important for deciding when to use simplex circuits versus TMR circuits. TMR systems have the advantage of online repair discussed in the section, *Online Repair for TMR Systems*.

Online Repair for TMR Systems

The high availability of the TMR system is a result of being able to do repair online. It is possible to shut down single modules for repair and leave the voting trio in full voting mode operation, which effectively masks the absence of the signals from the powered down module. However, there are some restrictions and special cases that require extra attention.

Many signals are reduced to a single customer wire at the terminal boards so removal of the terminal board requires that the wires be disconnected momentarily. Each type of terminal board must be evaluated for the application and the signal type involved. Voltages in excess of 50 V are present in some customer wiring. Terminal boards that have only signals from one controller channel may be replaced at any time if the faulty signals are being masked by the voter. For other terminal boards such as the relay outputs, the individual relays may be replaced without disconnecting the terminal board.

For those singular signals that are driven from only one I/O board, there is no redundancy or masking. These are typically used for non-critical functions such as pump drives, where loss of the control output simply causes the pump to run continuously. Application designers must avoid using such singular signals in critical circuits. The TMR system is designed such that any of the three controllers may send outputs to the singular signals, keeping the function operational even if the normal sending controller fails.

Note Power down only the module (rack) that has the fault. Failure to observe this rule may cause an unexpected shutdown of the process (each module has its own power disconnect or switch). The modules are labeled such that the diagnostic messages identify the faulty module.

Repair the faulty modules as soon as possible. Although the TMR system will survive certain multiple faults without a forced outage, a lurking fault problem may exist after the first unrepaired failure occurs. Multiple faults within the same module cause no concern for online repair since all faults will be masked by the other voters. However, once a second unrelated fault occurs in the same module set, then either of the faulty modules of the set that is powered down will introduce a dual fault in the same three signal set which may cause a process shutdown.

Reliability

Reliability is represented by the Mean Time Between Forced Outages (MTBFO). In a simplex system, failure of the controller or I/O communication may cause a forced outage. Failure of a critical I/O module will cause a forced outage, but there are non-critical I/O modules, which can fail and be changed out without a shutdown. The MTBFO is calculated using published failure rates for components.

Availability is the percentage of time the system is operating, taking into account the time to repair a failure. Availability is calculated as follows:

$$\frac{\text{MTBFO x 100\%}}{\text{MTBFO + MTTR}}$$

where:

MTTR is the Mean Time To Repair the system failure causing the forced outage, and MTBFO is the Mean Time Between Forced Outages

With a TMR system there can be failures without a forced outage because the system can be repaired while it continues to run. The MTBFO calculation is complex since essentially it is calculating the probability of a second (critical) failure in another channel during the time the first failure is being repaired. The time to repair is an important input to the calculation.

The availability of a well designed TMR system with timely online repair is effectively 100%. Possible forced outages may still occur if a second failure of a critical circuit comes before the repair can be completed. Other possible forced outages may occur if the repairman erroneously powers down the wrong module.

Note To avoid possible forced outages from powering down the wrong module, check the diagnostics for identification of the modules which contain the failure.

System reliability has been determined by calculating the Failures In Time (FIT) (failures per 10^9 hours) based on the Bellcore TR-332 Reliability Prediction Procedure for Electronic Equipment. The Mean Time Between Failures (MTBF) can be calculated from the FIT.

The Mean Time Between Forced Outage (MTBFO) of the control system is a function of which boards are being used to control and protect the turbine. The complete system MTBFO depends on the size of the system, number of simplex boards, and the amount of sensor triplication.

Third Party Connectivity

The Mark VI can be operated from the plant control room.

The Mark VI can be linked to the plant Distributed Control System (DCS) in three different ways as follows.

- Modbus link from the HMI Server RS-232C port to the DCS
- A high speed 10 Mbaud Ethernet link using the Modbus over TCP/IP protocol
- A high speed 10 Mbaud Ethernet link using the TCP/IP protocol with an application layer called GEDS Standard Messages (GSM)

GSM supports turbine control commands, Mark VI data and alarms, the alarm silence function, logical events, and contact input sequence of events records with 1 ms resolution. Figure 2-23 shows the three options. Modbus is widely used to link to DCSs, but Ethernet GSM has the advantage of speed, distance, and functionality.

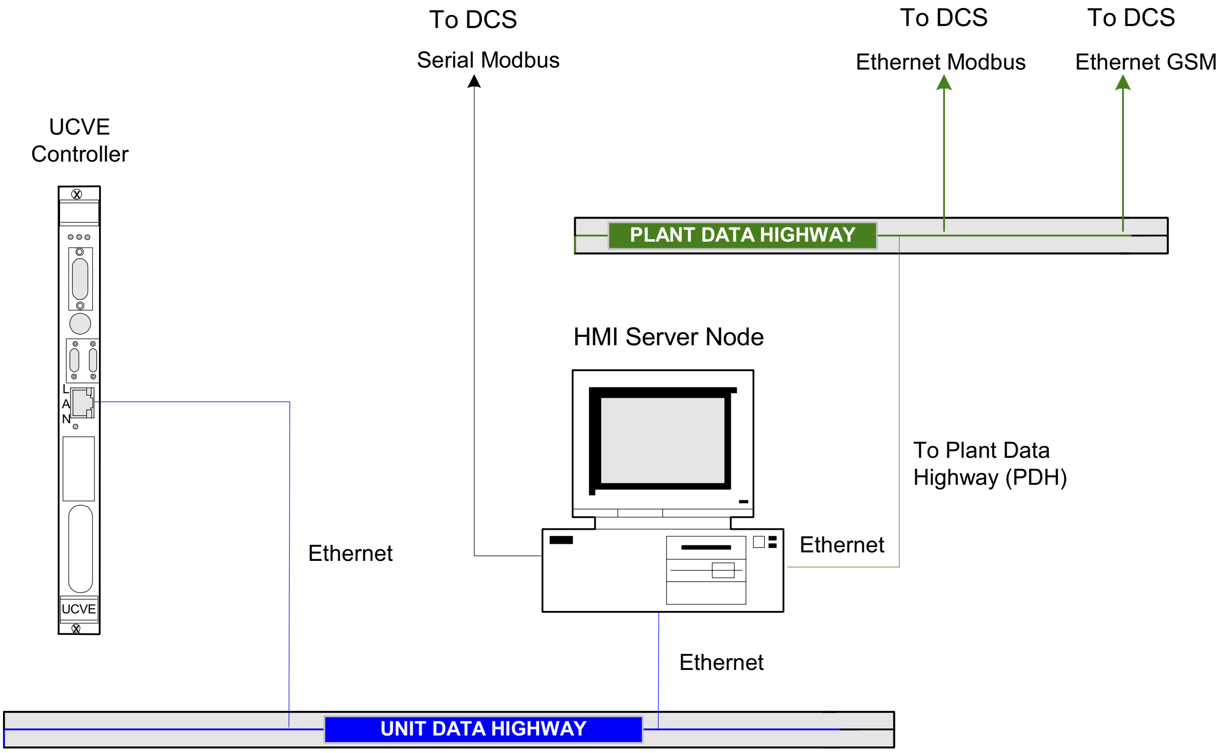

Figure 2-23. Optional Communication Links to Third Party Distributed Control System