Distributed Synchronization and Paralleling Control

ABSTRACT

A distributed paralleling and control architecture in a power generation system with multiple generators provides redundancy and fault tolerance for a more robust system for critical applications.

Larry Dover
Design Engineering Specialist
Controls Engineering
Electric Power, Caterpillar Inc.

LEXE23488-00

INTRODUCTION

In critical power applications, such as data centers or water treatment facilities, fault tolerance in the emergency power generation system is crucial for maintaining available power to critical loads, such as life-safety, cooling, servers, chemical feed systems, etc. For facilities with critical power requirements, multiple generators are paralleled to a common bus to provide sufficient capacity for the loads and redundancy, often designed in an N+1 fashion, meaning the number of generators required to support the load (N) is supplemented by one additional generator (+1). However, this redundancy is minimized when many traditional paralleling systems utilize a centralized control system that controls starting and paralleling all generators in the system.

With this in mind, Caterpillar has designed the Cat® Energy Control System (ECS) to integrate Cat Switchgear and Cat ECS 200 generator set controls to deliver a distributed control architecture for synchronizing, paralleling functions, and load sharing, alleviating the single-point-of-failure in the centralized control architecture.

DISTRIBUTED SYNCHRONZING/PARALLELING CONTROL

In many traditional paralleling systems, the site level sequence of operations, system level functions, and the generator set synchronizing and paralleling is facilitated by a central control system. A central control system allows the switchgear to control a variety of power sources along with complex sequences within a central code base. This process can simplify the code development process. However, in this type of control system, a failure of the central processor limits the functionality of the generator plant, as these critical synchronization and paralleling functions are no longer available. A failure of the central processor can be mitigated by the addition of a redundant, hot-standby processor, but adds exponential cost. In many cases, a need for the generator plant to run would require an operator to manually start a single genset and close its main breaker to the bus to power critical loads. In cases where the single genset capacity is insufficient to support facility loads, a second genset would need to be manually paralleled to the bus, if manual controls are designed into the system. This process is resource intensive, time consuming, and can be detrimental to customer safety or operations.

Cat ECS Enabled Controls are designed to integrate with Cat ECS 200 generator set controls to provide a distributed control architecture. In this design, each generator equipped with Cat ECS 200 controls contains its own synchronizing and paralleling functionality, eliminating the single point of failure embodied in the centralized controller. The failure of a single controller in a distributed control architecture may eliminate a single unit from participating in the system but maintains the operational integrity of the rest of the system. To initialize the crank cycle and subsequent synchronizing and paralleling functions, a Group Start signal is sent to either a single genset, which in turn broadcasts the start signal to all other gensets on the network, or to all gensets to eliminate the possibility of a single controller preventing the remaining generators being called to run.

In Cat ECS 200 low voltage (<=600VAC) applications, the generator main breaker is typically an electrically operated breaker mounted on the genset package. Whereas in a medium voltage (>600 – 15kVAC) application, the generator terminals are connected via cabling to a medium voltage breaker in a separate switchgear lineup. In either case, the onboard paralleling controls of each genset in the system actively synchronizes its output to the reference bus and closes its associated main breaker when all voltage, frequency and phase angle parameters are met. In a black start situation, with a de-energized bus, the gensets utilize a dead bus arbitration scheme to allow the first genset to reach rated speed and voltage to close to the dead bus, which prevents two gensets from closing to the dead bus simultaneously. At this point, the remaining gensets will synchronize and close their breakers, adding capacity to feed plant loads. Dead bus arbitration, synchronization, paralleling and subsequent load sharing is coordinated at the genset level and communicated to all gensets on the bus via the dedicated, ethernet based Advanced Paralleling Control Data Link (APCDL) communication network. In figure 1, the proprietary APCDL network is shown in the standard ring configuration, which further eliminates single points of failure. With a break in the APCDL network at any single point, communication between the paralleling controllers continues uninterrupted via the remaining, intact connections on the ring.
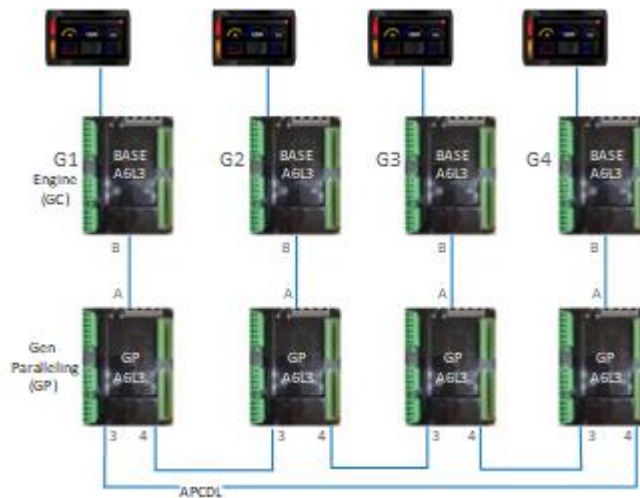
LEXE23488-00

Figure 1

In a normal operating state, dead bus arbitration (DBA) is accomplished using the APCDL network for communication between gensets. There is no master or group controller in DBA. A virtual token-based methodology is used to arbitrate between gensets and consist of the following:

- All units must agree that the bus is dead.
- All units are allowed to request the token if they are up to speed and voltage.
- Only one unit may capture (possess) the token.
- A unit that captures the token must receive permission from all other requesting units (dead bus grant) before it attempts to dead bus close.

ENTERING FAILSAFE OPERATION MODE

To enter Failsafe Operation Mode, any unit communicating over the network no longer sees one or more of the units it expects.

In the event of a communication failure of a single unit (Figure 2) or if no units detect other expected units on the network, a Failsafe DBA scheme is deployed. If a unit that previously detected that there were more units on the network, but only detects itself, then that unit will not participate in the normal automatic DBA. The other units on the network will execute the DBA, one unit will close its breaker to the dead bus and the remaining units will synchronize and parallel to the bus. The unit with the failed communication can then synchronize, parallel and load share with the other units in a Failsafe Load Sharing scheme.
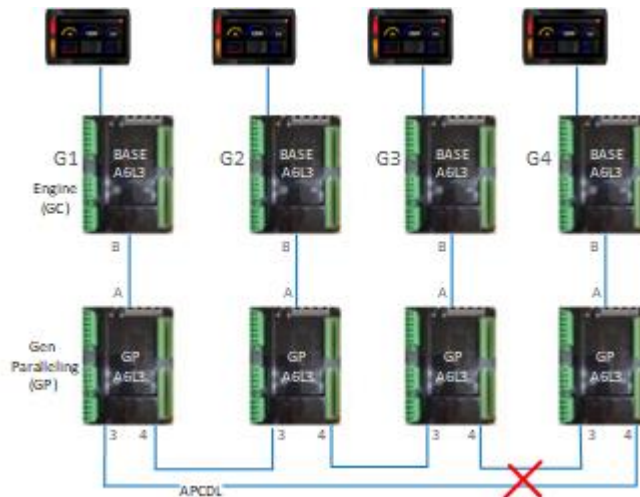

Figure 2

If there are multiple breaks in the communication network, resulting in multiple segments, units are separated into a Proceed as Normal (majority) group or a Proceed with Caution (minority) group defined in Table 1 below. The Proceed with Caution group is forced to be cautious when closing to a dead bus (only executes DBA function after a Proceed with Caution Delay has expired) since this group's communication is isolated from other units and other units' dead bus closure status is unknown. The Proceed with Caution delay allows the majority group to execute DBA prior to the minority group proceeding. The Proceed with Caution Delay is defined below:

Proceed with Caution Delay = [5 + (1.25 * Power System Control Unit Number)] seconds

The Proceed as Normal group executes the DBA functions as normal without delay. When the minority group sees an energized bus reference, the units can synchronize, parallel and load share with the majority group in the Failsafe Load Sharing scheme.

For more details on the failsafe operation of the ECS 200 see the white paper Failsafe Operation for Load Sharing Paralleled Generator Sets available on Power.Cat.Com.
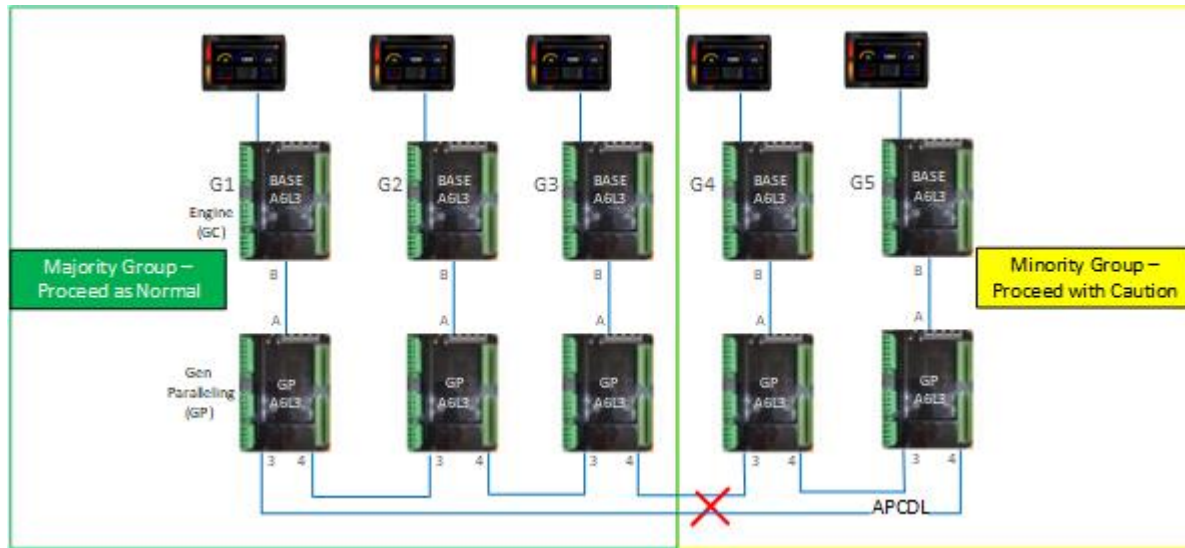

Figure 3

Scenario		Condition	DBA Mode
Majority Group	1A	Number of Units in My Group Communicating > 1/2 the number of Total Units Communicating Prior to Communications Loss	Proceed as Normal
	1B	Number of Units in My Group Communicating = 1/2 the number of Total Units Communicating Prior to Communications Loss AND Lowest Power System Control Unit Number Communicating is in My Group	
Minority Group	2A	Number of Units in My Group Communicating < 1/2 the number of Total Units Communicating Prior to Communications Loss	Proceed with Caution
	2B	Number of Units in My Group Communicating = 1/2 the number of Total Units Communicating Prior to Communications Loss AND Lowest Power System Control Unit Number Communicating is NOT in My Group	

EXITING FAILSAFE OPERATION MODE

To exit Failsafe Operation Mode, any of the following conditions are necessary:

- All units agree that the expected units before entering Failsafe Operation Mode are all now communicating on the network.
- Manual reset of the Expected Number of Units from the unit HMI.

Once all units see the expected number of units on the network, the units return to normal operation for DBA and Load Sharing.

SUMMARY

The distributed control architecture for synchronizing and paralleling gensets incorporated in the Cat ECS 200 design minimizes single points of failure inherent to centralized control systems, providing a more robust, fault tolerant system. The failure of a single controller allows continued operation of the remaining units, as each unit can receive the Group Start command, participate in DBA and/or synchronize independently. Failsafe DBA functionality accounts for communication failures through each unit knowing how many other units should be on the network and splitting into Majority and Minority Groups with predetermined rules governing failsafe operation in order to maximize operational capability of a compromised network. The Cat ECS system integrates scalable controls with advanced features to provide optimized solutions to meet our customers' needs.

Materials and specifications are subject to change without notice.

www.cat.com/electricpower