# The Power of Modern Relays Enables Fundamental Changes in Protection and Control System Design

(Build a Substation That Continuously Tests Itself)

Michael Thompson, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Modern microprocessor relays are fundamentally different from protective relay technologies used in the past. Many paradigms that drove designs in the past are no longer valid. This paper describes many design concepts that can be used to improve the performance, reliability, robustness, and fault tolerance of protection and control systems. The design concepts that are presented in this paper are based upon experience gained in designing and commissioning many fully integrated protection and control systems currently in the field.**

**If the design is approached from the beginning with consideration for integrating protection, metering, and control upon a foundation of modern multifunction programmable relays, we can create a system that has built-in continuous self-test features. We can extend the concept of continuous self-test that we have enjoyed in the relays themselves to the entire system. The design concepts discussed in this paper can make problems and failures that would be hidden in a traditional design, readily apparent so that they can be corrected before undesired operation can occur. These features generally do not require increased cost but are obtained by making use of the capabilities available in the powerful relays already being used.**

## I. Introduction

A power system can be operated without automation, metering, and remote control. It cannot be operated without protection. Modern protective relays include many ancillary functions that can provide most of the nonprotection requirements of an electrical substation protection, monitoring, and control (PCM) system when coupled with integration technology. Thus, when using these powerful programmable multifunction protective relays, there are fundamental differences in the way the PCM system should be built compared with the way it was done in the past.

The protective relays form the logical basis for any integrated PCM system. To build an integrated system, we need to have a foundation to build upon. That foundation is the protection system.

Modern protective relays allow us to improve the reliability of the PCM system. Design concepts that eliminate single points of failure for critical protection and control functions reduce the urgency and consequences of failures. A properly designed integration system can leverage the capabilities of the protective relays. We want to build in continuous self-test features that will allow the system to detect failures and alarm so that corrective action can take place before undesired operation occurs.

This paper covers concepts that will enable you to design fault-tolerant, robust, integrated PCM systems. The concepts cover a number of diverse but related topics. To build a robust and fault-tolerant system, we need to use architecture that will eliminate single points of failure for critical functions. To reduce maintenance and testing and improve reliability, we need to design continuous self-test features into the integrated PCM system.

To further improve reliability, we need to use dc control-circuit design concepts that take advantage of the characteristics of numerical relays. These are subtle suggestions that can enhance the reliability of the design. Finally, it is important that the design documentation package be up to the challenges presented by this new technology.

### *A. Integrated System Advantages*

Integration of powerful multifunction devices allows us to save initial cost by eliminating unnecessary devices that only duplicate functionality that is currently available in necessary devices (the protective relays). Alternatively, it allows us to have advanced functionality on systems where we could not have previously justified the cost of that functionality. Such functionality includes: advanced metering, telemetry, and load data recording; remote control, automatic controls, and interlocking; and system monitoring, equipment monitoring, and maintenance data recording.

Integration allows us to save ongoing maintenance and operating costs by: reducing device counts, automating many inspection and test activities, automating many data gathering and archiving activities, and continuously monitoring systems.

Using advanced protection and control features available in modern programmable relays can improve power quality and continuity of service by improving fault clearing times, improving selectivity, and providing better information for faster service restoration.

## II. Eliminate Single Points of Failure

Systems must be designed that have no single point of failure for critical functionality. Failure of a system or component should create a condition that is perhaps undesirable or inconvenient but is not intolerable. That is, we never want to be in a position where a failure of a component requires shut down of the electric supply facility and its loads until it can be repaired.

### A. Basic Protection Concepts

Before we get into the details of electrical substation PCM design, a review of some basic protection concepts is warranted. Protection systems consist of devices that detect faults on the power system (protective relays), and devices that interrupt fault current (circuit breakers and circuit switchers). In some cases, both functions are combined. Fuses and self-contained circuit reclosers are examples of this.

The way we design our protection system to deal with failure of either of these two functions can generally be categorized in one of two ways:

- Overlapping relays tripping different devices.
- Dual redundant systems.

With overlapping relays tripping different devices, we use relays that are capable of "seeing" faults in adjacent or downstream zones of the power system. Thus, if the primary relay or circuit breaker fails, the adjacent or upstream relay will time out and trip to clear the fault. This scheme has typically been used at distribution levels and industrial facilities where the loads are fed radially and the consequences of delayed tripping for a failure are less severe. This architecture treats failure to detect faults and failure to interrupt faults as the same failure.

With dual redundant systems, we apply two independent relays to eliminate a single point of failure for fault detection. These two systems can be equal, or the backup system can be a lower cost, lower performance system. To cover the function of fault interruption, we apply a single circuit breaker. To eliminate the single point of failure of the circuit breaker, instead of dual circuit breakers, we apply a breaker failure protection scheme. In this paper, when we are talking about dual redundant systems, we will refer to the two systems as System A and System B.

Dual redundant schemes have typically been used at transmission levels where the system is networked and the ability of relays to see all faults in adjacent zones is less assured. It is also typically used where the consequence of delayed tripping for a failure is more severe.

The scheme chosen will affect what approaches we take to eliminate single points of failure in our control system.

### B. Basic Manual Control Concepts

Let's first define some terms:

- Local Manual Control is any command that originates inside the substation. An HMI computer or breaker control switches mounted on the panel or inside the breaker cabinet are all possible sources of local control.
- Remote Control is any command that originates outside the substation. A typical example is a remote HMI link or, more traditionally, a supervisory control and data acquisition (SCADA) system.

Manual control is often not considered as critical as protection, so full backup of this function is not always a design requirement. In substations equipped with remote SCADA control, often, the local and remote control systems inherently provided redundancy for this critical function. If remote SCADA is out of service, local control can be used and vice-versa. In traditional architecture, the local panel control handle is relatively independent of the remote SCADA control that operates through interposing relays in the remote terminal unit (RTU) cabinet.

In an integrated PCM system, local control often uses a local HMI computer system with a communications link to the protective relay for manual control functions. Alternatively, control features built into the front-panel HMI on the protective relays might be used to provide local panel control. In some cases, both systems may be used for redundant local control. For remote SCADA control, in an integrated PCM system, the RTU interposing relays (and often, the RTU itself) are eliminated such that remote control also uses a communications link to a PCM device.

If the same protective relay is providing both local and remote control functions, it could represent a single point of failure. The shared communications links (communications processors, managed Ethernet switches, communications cables, etc.) can also represent single points of failure. Proper integrated system design should eliminate these single points of failure problems for this critical function. The way we eliminate single points of failure for the control function depends upon whether or not we are using single or dual protection systems.

When the PCM system uses dual protection systems, a single point of failure for manual control can be eliminated by routing local control through the System A relay and remote control through the System B relay. The communications paths, which are routing control signals from the local HMI and the remote SCADA system to these separate control relays, should also be separated so that they do not share any common communications processors, computers, Ethernet switches, or communications cables.

When single protection systems are being used, one approach to eliminate the single point of failure for the critical functions of circuit breaker open and close is to specify optional independent control pushbuttons on the PCM device. These optional independent controls can be used to manually open the circuit breaker—even when the relay is out of service. Alternatively, if the single relay is used for local control, remote SCADA control can be routed through other devices to eliminate this single point of failure.

Table 1 provides three scenarios to help determine if relays with only logic-controlled pushbuttons should be specified or if relays with independent pushbuttons should be specified. The three scenarios include systems without remote SCADA control, systems with a traditional SCADA RTU, and systems with an integrated PCM system.

TABLE 1
INDEPENDENT CONTROL BUTTONS

| Scenario | Control | | Protection | | Independent Control Buttons Required |
|---|---|---|---|---|---|
| | Primary | BU | Primary | BU | |
| **Substation w/o SCADA** | | | | | |
| Dual Relays | Controls on Sys. A Relay | None | System A Relay | System B Relay | Yes |
| Single Relays | Controls on Single Relay | None | Single Relay | Adjacent Coordinated Relays | Yes |
| **Substation w/SCADA RTU** | | | | | |
| Dual Relays | RTU | Controls on Sys. A Relay | System A Relay | System B Relay | No |
| Single Relays | RTU | Controls on Sys. A Relay | Single Relay | Adjacent Coordinated Relays | No |
| **Substation w/Integrated Control** | | | | | |
| Dual Relays | HMI/ SCADA via Sys. B Relay | Controls on Sys. A Relay | System A Relay | System B Relay | No |
| Single Relays | HMI/ SCADA via Single Relay | Controls on Single Relay | Single Relay | Adjacent Coordinated Relays | Yes |

The following assumptions were used in compiling this table.

- In the case of dual relay systems, the System A relay includes large operator controls on its front panel. A relay so equipped often has the option of the control interface operating through the relay's internal logic or being independent of the relay's internal logic.
- In the "With SCADA RTU" scenario, it is assumed that the RTU contains its own interposing relays for direct operation of the breaker open and close coils.
- The "Independent Control" column indicates if the control feature has to be independent of the relay's logic—independent control buttons on its front panel or, if not available, an independent manual control switch.

Examination of this table shows us that if a single relay is used and both local HMI and remote SCADA control are completely integrated with the relay, then failure of the one relay would constitute a single point of failure for control. Use of independent control switches or buttons is recommended. Otherwise, integrated control through the relay is generally suitable.

### *C. Fault-Tolerant Integrated Control Systems*

As mentioned in the previous discussion, redundancy for manual control systems can be obtained by ensuring that local and remote control functions share no common relays, communications processors, etc. Fig. 1 shows an example that includes a local HMI computer.

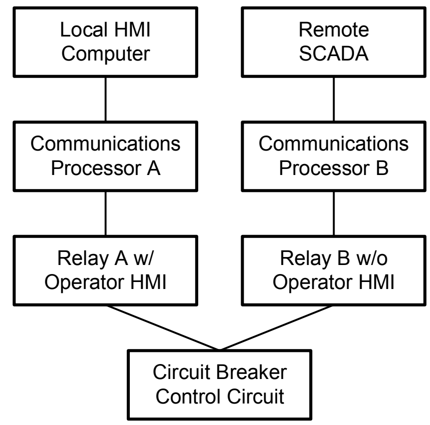



Fig. 1. Integrated Control System Design With Separated Local and Remote Control Systems

A local HMI computer, while not a necessary component of an integrated PCM system, is often included due to the great deal of functionality that it can provide. This integration system is often connected to relays with large operator control interfaces (front-panel HMI) that provide direct control functions at the panel. Thus, the local control system often includes an additional level of redundancy:

- Primary: HMI computer
- Backup: Panel control via relay front-panel HMI

Because the least reliable component in most integrated PCM systems is the computer, it is recommended to use relays with front-panel HMI control features to provide backup for local control via the relays at the panel. Thus, if the HMI computer is down, many features will not be as conveniently accessible, but it will still be possible to locally operate the system.

To eliminate multiple sources of local control being active, a "heartbeat" system can be implemented in the HMI computer. This system consists of a script running in the HMI computer that periodically pulses a timer in the relay. Failure to hear the "heartbeat" indicates that the HMI computer or the communications path has failed. If the timer is not refreshed, it times out and enables the local panel controls.

Fig. 2 shows an example where the integrated control system has not been designed with the recommended redundancy. The remote SCADA control and the local HMI control (if included) share communications paths to the single relay. In this example, a relay with front-panel HMI is necessary to provide redundancy. For this design, the relay must also include independent control buttons to open the breaker if the single relay itself has failed. This is an acceptable design because there is no single point of failure.

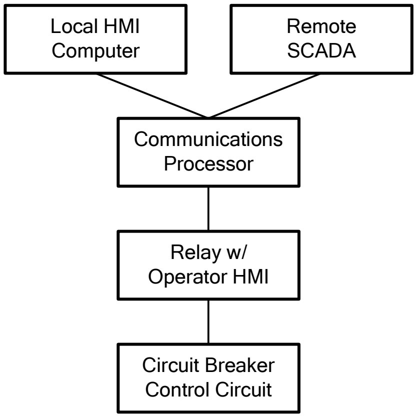



Fig. 2. Integrated Control System Design With Single Relay With Independent Control Pushbuttons

## III. Include Continuous Self-Test Features

To build robust, fault-tolerant systems that require little maintenance, system self-checking logic should be built into the integrated PCM system. The more the system continuously monitors itself, the less it has to be periodically inspected and/or tested. If problems are detected immediately, they can be corrected before improper operation can occur. Reliability is directly affected by the time to detect and correct failures. Therefore, immediate detection via self-test dramatically improves system and service reliability.

The most obvious item is the relay's continuous self-check capabilities. Well-designed integrated PCM systems monitor and detect relay continuous self-check, which is indicated via the "Relay Fail" output contact. With this, we no longer need to disable and manually test the relay. However, there are limits to what the relay's continuous self-check can identify. The relay cannot directly verify that the binary and analog inputs that it is reading actually represent the state of the power system that it is monitoring. Or, that when it commands a breaker to operate via an output contact, it will actually close the circuit and energize the trip or close coil of the circuit breaker. For this reason, simply monitoring the relay fail contact does not eliminate the need to periodically verify its interaction to the outside world. More specifically, the following items need to be independently verified beyond the relay's continuous self-test.

- Are the current- and voltage-sensing circuits correctly measuring? Is a measurement of 5 amps really 5 amps, or is it something different?
- Are the contact sensing input circuits correctly reporting the state of the contact? Is a breaker open, or has a component or wire failed in the circuit?
- Will the output contacts operate their circuit? When the relay asserts its contact, does it really close? Does it really operate the circuit?

In an integrated PCM system, we can extend the continuous self-test concept to the entire system. We can build continuous self-test features into the HMI computer, communications processors, and programmable relays that can nearly eliminate the above holes in the continuous self-test capabilities of the individual relays. The following sections of this paper present ideas on how to build a system that continuously monitors itself and identifies problems so they can be corrected before undesired operation can occur.

### *A. DC Battery System*

The dc battery system is probably the single most critical system in the substation. Monitoring the system is important. There are different levels of sophistication and cost of battery monitor systems. If a dedicated battery monitor system is not installed, it is still relatively easy to monitor the following system components:

- Voltage levels
- Battery grounds
- Charger health

A smart battery charger integrated to the system can provide relatively inexpensive monitoring of the dc system. Otherwise, monitoring of the dc voltage levels should be provided by using the dc voltage metering and protective elements included in the relays. If dc systems are monitored in this way, it is advisable to read values from multiple relays on each dc system. Thus, if a relay that is taken out of service happens to be the source of the dc system monitoring and alarm logic, the integrated system computer will switch to a different relay to maintain continuity of this important function.

### *B. Monitor Every DC Circuit*

Every individual dc circuit should be monitored.

- Loss of a fuse in a circuit powering a multifunction relay will be detected by the Relay Fail contact as a result of the relay powering down.
- Relay trip circuit monitor (TCM) logic can monitor each breaker trip circuit. Notice that the "C" in TCM stands for "Circuit" and not just "Coil." Properly designed, the TCM logic will detect not only an open trip path or coil but loss of a fuse in the circuit as well; see Fig. 3 for an example. If access to the point in the circuit between the 52a contact and the trip coil is available, the alternate connection will also detect an open trip coil when the breaker is open.
- If the breaker close circuit is isolated from the trip circuit, monitoring logic should be included for that circuit as well.
- Each auxiliary tripping relay circuit, such as lockouts, should include TCM logic as well. Of course, in an integrated design including modern programmable relays, the use of problem prone auxiliary relays can be virtually eliminated. This will be discussed in more detail in section *V. DC Control Circuit Design Concepts*.

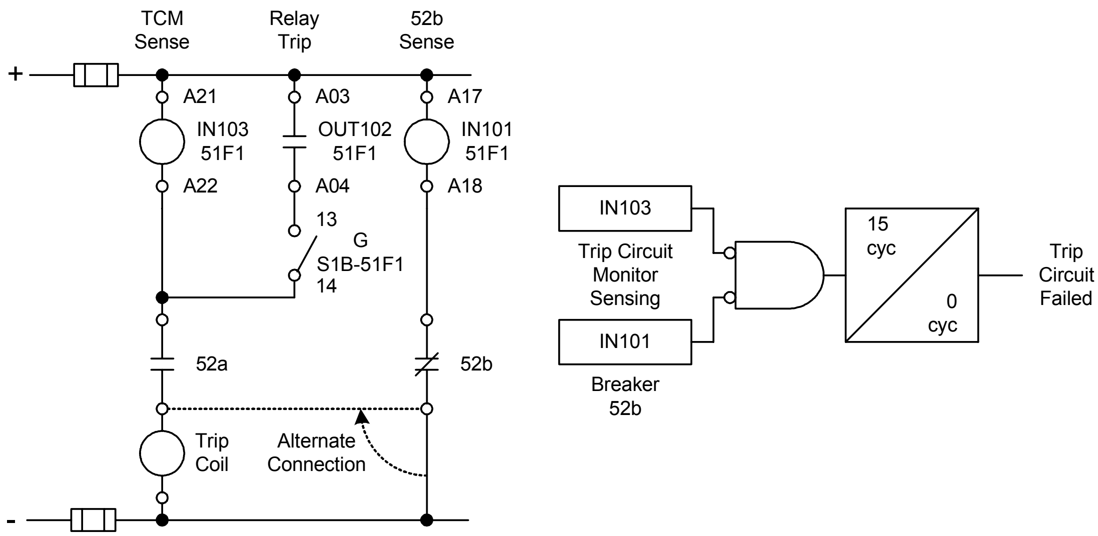



Fig. 3. Trip Circuit Monitor Logic

### *C. Validate Status Signals*

Switch and breaker status is often used in multiple circuits. In a traditional design, a separate contact is required for each control circuit. If a contact or connection fails or is otherwise in the incorrect state, some circuits may not operate properly while others are fine. This can cause hidden failures waiting to happen and difficulty in troubleshooting.

Building reality checks into the system can help eliminate these hidden failures. Such checks verify that values are reasonable, i.e., within expected limits, changing value at appropriate speeds or otherwise not contradicted by a redundant value. One simple example is to monitor both 52a and 52b, and set logic to alarm if their states are ever the same. A better approach is to use dual systems. This allows you to build logic into the integration system to monitor both systems and alarm if the state of each system is incongruent. With dual systems, it is important to use separate dc circuits for each. For example, the contact sensing inputs for System A might be wetted from the circuit for Trip Circuit 1, and the contact sensing inputs for System B might be wetted from the circuit for Trip Circuit 2.

Distribute the validated signal to all devices and logic schemes that require it via the integration system communications links. For example, use the same status point for the protection system as for indication. By doing so, you have the human operators monitoring the protection critical status point.

Another consideration that should be used in the design effort is to be consistent in using a single logic point to indicate a status point. For example, use a logic element such as 52A in all places where breaker status is required and use !52A (NOT 52A) if its inverse is required. If IN101 is wired to 52b and IN102 is wired to 52a, do not use IN101 in some places and IN102 in others.

A device such as a protection logic processor is useful for distributing status points to multiple devices. Protection-critical status points should not be distributed through the SCADA communications links.

### *D. Validate Output Circuits*

Combine all output signals for a circuit in logic before connecting them to an output. That way, the “connections” are within the relay’s continuous self-check monitoring. For example, by combining the manual trip functions with the protective trip functions on the same contact, every time you manually open the circuit breaker, the trip circuit is also verified. This has the desirable effect of the failure becoming known during a manual opening operation instead of when the power system is faulted.

In an integrated system, there are typically three sources of trip decisions that go through this single relay trip contact:

- Circuit protective trips
- External protective trips
- Manual trips

The relay should indicate a trip target only when it makes the trip decision for its protected zone. If the trip is from an external device (the protection logic processor for example) or the operator, the relay is only acting as an auxiliary tripping or interposing relay. Thus, you do not want the relay to target those trips. You might need to build in a separate trip seal-in logic equation for these other trips; see Fig. 4 for an example.

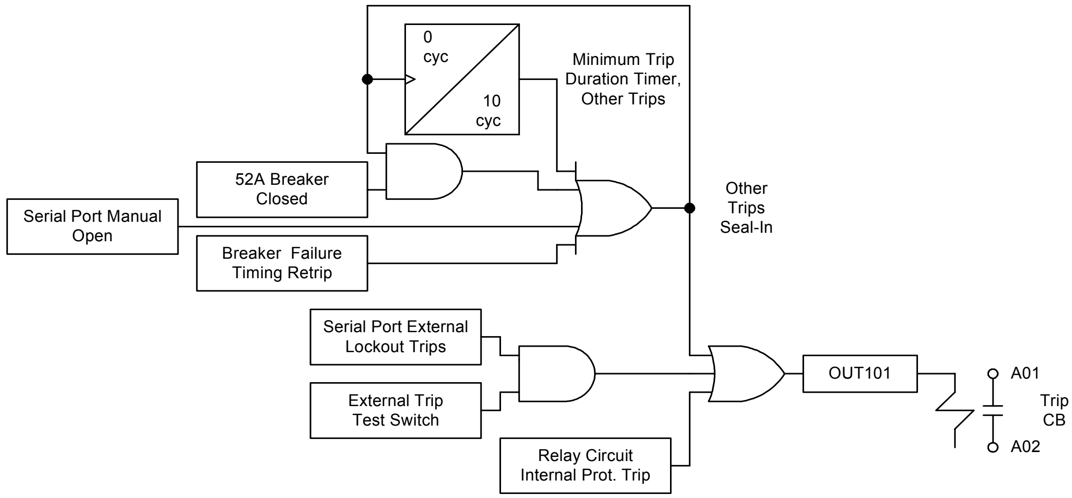



Fig. 4. Trip Logic

### *E. Validate Analog Signals*

The relay self-check can detect many problems in its A/D circuit, but there are some things that the self-check cannot detect. It is possible in an integrated PCM system to program it to validate the operating quantities measured by the relays. This can detect calibration problems, as well as problems in the external CT and VT wiring.

With smart systems, it is possible to validate signals by doing reality checks. The following are several examples:

- The loss-of-potential logic determines if voltage unbalance is accompanied by current unbalance. If not, it declares an alarm.
- Compare values from redundant devices on the same circuit. For example, alarm if the readings are more than 5% off.
- Sum readings. For example, watts and VARs around the bus must sum to zero, or in relays with a fourth independent current circuit that is connected residually to the three-phase currents, compare the calculated three-phase residual to the measured residual.

**Note**: When comparing readings, be careful that all of the devices use the same measuring principle. For example, do not compare a reading from a true RMS sensing metering device to a relay with fundamental filtered sensing.

Modern PCM devices also include the capability of synchronized phasor measurements when connected to an appropriate high-accuracy time source. With synchrophasor capability in nearly every relay, it is now possible to build into the integrated PCM system the ability to automatically compare magnitude and angle of critical power system measurements between devices on the same primary circuits. Logic can be included in the substation computing platform or in the communications processors to periodically compare the instantaneous measurements between the System A relay and the System B relay on a given primary circuit. Problems in the instrument transformer circuits and relay input and analog to digital converter circuits can be identified and corrected before undesired operation can occur. This will improve the reliability of the PCM system. It will also eliminate the need to do periodic calibration checks on the protective relays, which will further reduce ongoing maintenance and operating costs.

Perhaps one of the most powerful reality checks available is to use metering data out of the relays for local HMI and remote SCADA. This makes what the relay is reading visible to the ultimate reality check—system operators who are monitoring the system 24/7. This is an often-overlooked and extremely important benefit of integrating relay data for metering purposes. If critical current and voltage signals that are required by the relay to detect faults have a problem, it is much more likely that this is going to be detected immediately if the system operators use this same reading.

### *F. Monitor Communication Links*

Because, in a fully integrated system, control commands and status signals travel across communications links, monitoring and alarming for communications failures will improve reliability of the system. This is especially true of using communications links for status signals. A broken termination wire is difficult to detect. A broken communications link can be detected immediately.

One example is monitoring the critical control path via the "heartbeat" system described in the section on Basic Control Concepts. If the path is interrupted between the HMI computer and the relay, the front-panel backup control is enabled.

Another method is to use protocols with continuous self-check functionality over fiber links to carry field data into the control house in lieu of multiple pairs of copper termination wires. One recommended protocol that provides relay-to-relay logic status communications for eight status points at protection speeds provides continuous monitoring to indicate immediate loss of a single message. It also includes built-in monitoring for channel availability statistics.

IEC 61850 GOOSE messaging over Ethernet communications links does not inherently include similar monitoring of critical protection signal paths. If the PCM system uses this protocol for critical protection signals, it is recommended to build heartbeat logic into the system to alarm for failures in the communications links.

### *G. Additional Monitoring Concepts*

Use the advanced features provided by modern multifunction relays and additional monitoring IEDs to monitor equipment and reduce the need for periodic inspections. Automate many of the activities that are part of periodic inspections to make the process more efficient. Use advanced monitoring features to enable switching from periodic maintenance to condition-based maintenance. Examples of data providing power system apparatus condition information include:

- Breaker Internal Systems (contact wear, insulating gas, stored energy, motor run time, etc.)
- Transformer Internal Systems (oil level, loss-of-life, through-fault duty, cooling system efficiency, dissolved gas, etc.)
- Ambient Conditions (weather, HVAC system performance, smoke and heat detectors, etc.)

### *H. Alarm Handling Considerations*

With these continuous self-test features built into the system, there may be a larger number of alarms. It is important to remember in your design that alarm points can be handled differently locally vs. remotely. It is normal to group and/or summarize alarms for remote annunciation with detail kept locally in the HMI computer or relay display points.

You need to consider whether you want the alarm annunciation to follow the status of the alarm point, or seal in the alarm state after the point returns to normal but only until acknowledged by an operator. It is not unusual to need to handle this differently locally vs. remotely for any given alarm point. An integration system computer makes it possible to log alarm points in an alarm log, annunciate alarm points on the screen, or both.

## IV. Case for Using Equal Dual Systems

As we discussed earlier, there are two basic protection design foundations that we can build upon:

- Single coordinated relays tripping different fault interrupting apparatus.
- Dual redundant systems

When considering dual systems, what are the considerations in choosing a second relay? If we use a less featured alternative, we gain many of the advantages that we seek with a less expensive product. If we use a completely equal dual system, we can save a great deal in design, testing, and documentation. Therefore, implementing two fully featured dual redundant devices is often less expensive in the long run than using a different dual device. The scheme can be designed and tested once and simply duplicated, and future maintenance is simplified. The traditional desire to use more or less comparable systems but with different designs to minimize the possibility of common mode failure has become less important now that many relays support multiple protection principles within one device.

### *A. Why Use Dual Systems?*

First, let's discuss why dual systems should be used even at lower voltage levels. In the past dual systems were considered too expensive for use on lower voltage, radial systems. With the low cost of microprocessor relays, adding a second relay for dual protection and control is relatively inexpensive.

In most installations without dual systems, ensuring that an overlapping relay can see 100% of adjacent or downstream zones is not always possible; so, significant compromises must be made. Ensuring that there are no single points of failure for both critical protection and control becomes trivial when dual systems are employed. The task of setting and coordinating the relays to ensure that there are no contingencies for loss of a relay is also greatly simplified and this is probably the most significant benefit when dual systems are applied on networked systems.

With dual systems, any component failure is no longer an emergency situation because it has a dual device performing the same function. Nonemergency reaction to the failure saves operating and maintenance expense and improves flexibility.

For these reasons, the overall and lifecycle cost of using dual systems is easily shown to be much less than nondual redundant systems.

### *B. Why Use Equal Dual Systems?*

If you are considering the use of dual systems for all the advantages it provides, consider the design approach of the application of two identical and robust systems. Applying dual systems that are relatively equal makes the implementation of continuous self-checking logic very easy. An integrated PCM system with comprehensive continuous self-test features saves operating and maintenance expenses by eliminating most periodic inspection and testing. Also, the training and upkeep of a single software setting tool reduces the workload on the engineers and technicians.

By designing an integrated PCM system that uses relatively equal dual systems (same manufacturer, programmable logic systems, similar integration features, etc.), the design and documentation task is significantly reduced. Contingency analysis is reduced. The design of System B is pretty much a duplicate of System A. Plus, you have the benefit that the settings task for two identical relays is cut almost in half when compared with two dissimilar relays. These reasons can actually result in a lower overall installation cost. The alternative that is often considered is to use different but equal systems. If you do this, much of the economy of replicating the two very similar PCM system designs is eliminated.

There are several reasons for designers to consider applying different but equal systems. One concern is that there may be a common mode failure that will take out both relays under the same conditions. In modern protective relays, it is highly unlikely that a common mode failure of a component would occur simultaneously.

Another scenario is that a fault might occur that the relay's algorithms are blind to. If using different relays, they may not suffer the same problem. This concern can be mitigated by only using relays with a well-proven track record, relays with multiple algorithms in one device, and by fully testing and validating the relay and settings for the application.

We find that today, one of the most common causes of relay misoperation is mistakes made in setting these flexible relays for complex scenarios. This hazard is actually reduced by using two identical or very similar relays. By limiting the number of relays with which system designers, setting engineers, and maintenance and commissioning technicians must stay familiar with, skill levels become greater. When it becomes necessary to divide the available time for setting the relays between two very dissimilar devices, it is not possible to do as thorough a job with both as it would be to devote all the available effort towards one. Additionally, it will be much easier to maintain working knowledge, over time, of a smaller number of unique devices.

## V. DC Control Circuit Design Concepts

Modern multifunction relays have many attributes that can be exploited to improve the reliability of the PCM system. Some of these improvements are relatively subtle, but combined they can have a significant impact on the robustness of the system. One previously mentioned example is to use a single output contact in each circuit so that its operation is validated each time the circuit is operated. This section of the paper offers other examples and suggestions.

### *A. Use Programmable Logic*

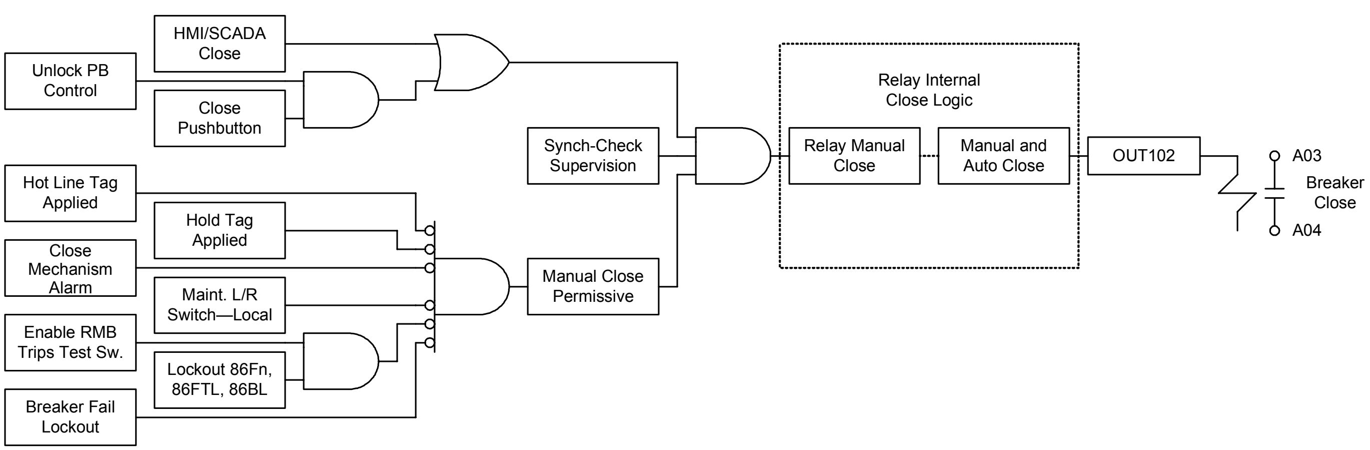
The protection and control logic should be done completely in programmable logic inside the relays. All external enable switches and interlocks, if they have not been entirely eliminated from the design, should be brought into the relay via contact sensing inputs or communications links and combined in logic. This has the following advantages:

- It is easy to adapt and change the design as situations change.
- It reduces the need for multiple, problem-prone auxiliary contacts for isolation. Only validated status signals are used by distributing them to all devices that need them via communications links.
- The status of all control inputs is available in the event reports to aid analysis.
- The dc circuitry becomes very simple, easy to commission, and easy to maintain.
- The maximum amount possible of the circuit remains inside the continuous self-test of the relays.

Fig. 5 shows an example of a close supervision circuit built entirely in programmable logic. This same logic requires a large number of contacts in series to physically duplicate the supervise function for the close circuit using contact logic.

In the past, designers were motivated to limit the complexity of the PCM scheme because each interlock represented an additional component in the system that could fail. With programmable relays, the complexity/functionality vs. reliability equation has changed.

With programmable logic, PCM system designers can build more complete and better control systems without compromising reliability. But, this must be balanced. Designers should not make the system any more complex than it needs to be to provide the desired functionality. The new motto to design by is, “As complex as it needs to be, but no more.” If unnecessary complexity is added, then the possibility exists for problems associated with this complexity to be introduced.




Abbreviations:

HMI/SCADA Close. Human-machine interface (local close control)/supervisory control and data acquisition (remote close control)
Maint. L/R Switch—Local. Maintenance local/remote switch in local position
Unlock PB Control. Unlock pushbutton control
Enable RMB Trips Test Sw. Enable received communications trips test switch
Lockout 86Fn, 86FTL, 86BL. Lockout trip from breaker fail lockout for Breaker Fn, Breaker TL, and bus fault lockout for Bus L

Fig. 5. Close Circuit Programmable Logic Example

## B. Additional Considerations for Using Programmable Logic

A digital relay processes tasks in serial order. This needs to be taken into consideration when designing your protection and control logic. There are two design situations to be aware of:

- Consider a logic equation that feeds into another logic equation. If they are in the wrong order, an undesired extra processing interval may be added into the execution time.
- If the logic relies on one element to block another element, and the blocking element is processed after the supervised element, the logic may assert momentarily because of the transposed order and cause an unintended output.

**Note**: The design engineer should always test the logic to ensure that it works as intended!

In a traditional design, a contact interlock can always be jumpered out to deal with an abnormal contingency. This is difficult in a design using programmable logic. Consider all possible contingencies.

With contact logic, test switches may be used in series with output contacts to build in testability. This is no less important in a fully integrated design where many of the status and trip "contacts" travel on communications links. With I/O coming into the relay on communications links, different approaches must be used. One approach is shown in Fig. 4. Notice that the logic point labeled "Serial Port External Lockout Trips" is "AND"ed with a logic point labeled "External Trip Test Switch."

Fig. 6 shows the dc schematic associated with this logic. The logic point labeled "External Trip Test Switch" in Fig. 4 is IN203 of the relay. In Boolean logic, the AND operator is equivalent to putting two contacts in series. Thus, the logic is equivalent to putting a test switch contact in series with a trip contact. The trip contact in this case is a tripping status bit coming in through a communications link. In the dc schematic, this received trip bit is labeled RMB. Similarly, IN202 is used in the relay logic to block transmitted trip bits (labeled TMB on the dc schematic shown in Fig. 6).

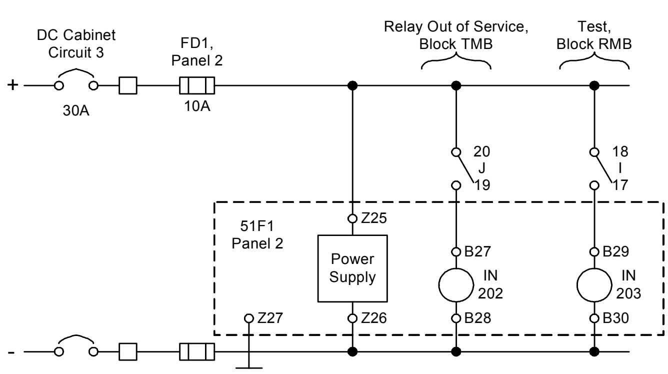



Fig. 6. Serial Port Trip Test Switches

## C. Indicate Critical Status

In a traditional design, displaying status involved adding annunciators and lights to the panels. An integrated design that uses microprocessor relays easily provides a great deal more indication of the system status to aid operators and maintenance personnel. Many microprocessor relays are equipped with programmable LCD displays on the relay that can indicate the following:

- Interlocks exist that are blocking certain functions
- An external trip is being held on the relay
- Various functions are in a disabled state

Trip targeting is another consideration. Today, relays are capable of many more protective features than there may be targets to indicate. To supplement the targets provided, latched display points and/or pushbutton LEDs are used as pseudo targets. In addition, many of the relays today have programmable target LEDs that can be programmed to function as designers wish in order to meet specific needs.

## D. Isolated Contact Sensing Inputs

Each contact sensing input circuit of the relay is typically isolated from the others. Thus, to sense the status of contacts in the yard, it is possible to connect the wetting voltage for that contact to the dc circuit that is already at that device. This allows the relay's dc circuit to remain relatively protected inside the control house.

This concept is taken one step further when all contact inputs and outputs between the yard and the control house are communicated on a fiber-optic link using remote I/O (RIO) modules (see Fig. 7(a–c)).

There are two typical topologies for connecting RIO modules that use point-to-point serial communications links as part of the substation PCM system. There are benefits and drawbacks to each topology. Fig. 7(a) shows a logic communications device used as a fiber-optic hub. Fig. 7(b) shows RIO modules as relay I/O.

The topology in Fig. 7(a) uses a single port on the relay and directly distributes status information to all devices in the station. However, in this topology, the protective trip and close to the breakers must be hard wired because it is not desirable to have the logic communications device become part of the primary trip path.

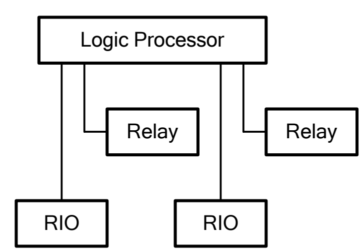



Fig. 7(a). Fiber-Optic Hub Topology

The topology in Fig. 7(b) requires two ports on the relay for logic I/O communications. This topology can reduce the complexity somewhat in that the communications links are more direct. With this topology, even though the relays have a direct connection to the RIO, it is still recommended to hard wire the trip circuit between the control building and the circuit breaker. This is because there are typically multiple relays for each of the zones of protection on each side of the circuit breaker that need to trip the circuit breaker. For example, in a straight bus application, System A and System B for the line protection and System A and System B for the bus protection. Running the trip bus to multiple relays in the control house is simpler and more reliable than running primary trip signals through multiple communications links.

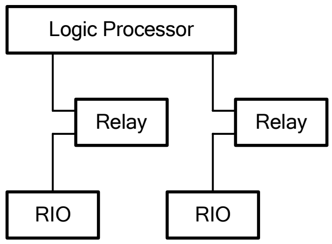



Fig. 7(b). Direct Relay I/O Topology

The topology in Fig. 7(c) uses Ethernet as the communications link. In this topology, the multiple relays (four in the previously described example) that need to trip the breaker can access the RIO directly (through a managed Ethernet switch). In this case, as long as the Ethernet network and RIO modules are adequately redundant, eliminating the hard-wired trip signal is permissible because the Ethernet switch does not introduce any latency.

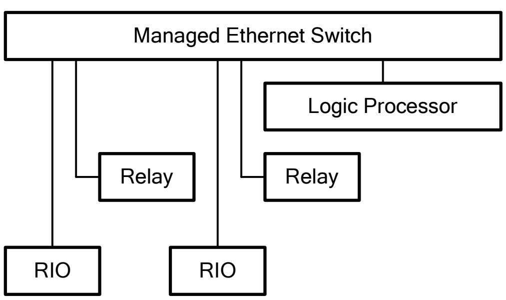



Fig. 7(c). Network RIO Topology

### *E. Tripping and Interlocking*

Each relay includes protective elements for its designated zone of protection. When these elements call for a trip, the relay will attempt to trip each breaker directly to clear the zone. This is quite straightforward for feeder trips.

For zones that require tripping a large number of breakers, (for example, transformer, bus, and breaker failure) a lockout relay was often used in traditional designs. The lockout relay served two purposes:

- Multiply the number of trip contacts.
- Interlock the closing of the breakers.

Because this lockout relay represents a single point of failure, redundant lockout relays for the zone are required. Modern relays include many programmable output contacts. So, the contact multiplication purpose of a lockout relay is no longer valid. Each relay should be programmed and wired to directly trip every breaker required to clear its zone of protection. This eliminates the expense of installing redundant lockout relays and improves performance by eliminating the delay associated with the operation of the lockout relay. The lockout relay, if it is installed at all, can also be tripped, which provides an alternate path for tripping and primary path for interlocking.

Fig. 8 illustrates an example of direct tripping from each relay. The transformer protection is often a dual system. System A might consist of a multifunction differential relay (labeled device 87T in Fig. 8) for sensitive, high-speed differential protection and transformer through-fault protection. System B might consist of a multifunction overcurrent relay (labeled device 51T in Fig. 8). The sudden pressure protection is routed through this relay to provide redundant, sensitive, high-speed protection in addition to the transformer overcurrent through-fault protection.

Each relay directly trips the appropriate breakers through its own programmable outputs. Each relay also sends the transformer trips to the lockout relay (labeled 86T in Fig. 8). The lockout relay (whether it is an actual lockout relay or a software latch tripping through communications links) then serves as the backup tripping path to trip the appropriate breakers.

In a fully integrated design, a device such as a logic processor easily handles the lockout tripping and interlocking functions. This greatly reduces wiring and improves reliability. This device, which has communications cable and alarm contact connections to each of the relays, distributes the status of each of the lockout latch states for breaker failure tripping, for bus fault tripping, and for transformer tripping to the various breaker and switch control relays for close supervision interlocking.

For the example illustrated in Fig. 8, a physical lockout relay was used. In this example, device 51T also provides manual control of the high-side circuit breaker. So, the status of the lockout relay asserts IN103 of device 51T to provide the interlocking function via hard-wired connection. When IN103 is asserted, manual close commands are blocked from operating the close circuit of the circuit breaker. In Fig. 5, the logic point labeled "Lockout 86. . ." would be IN103. It is important to understand that the close interlock system does not need to be redundant. The primary system for preventing undesired closes is proper switching procedures.

Another subtle nuance is that it is acceptable to have a single path for tripping because breaker failure is a backup function already. Redundant lockout relays are typically not included for this function; therefore, redundant communications link tripping paths are not required.

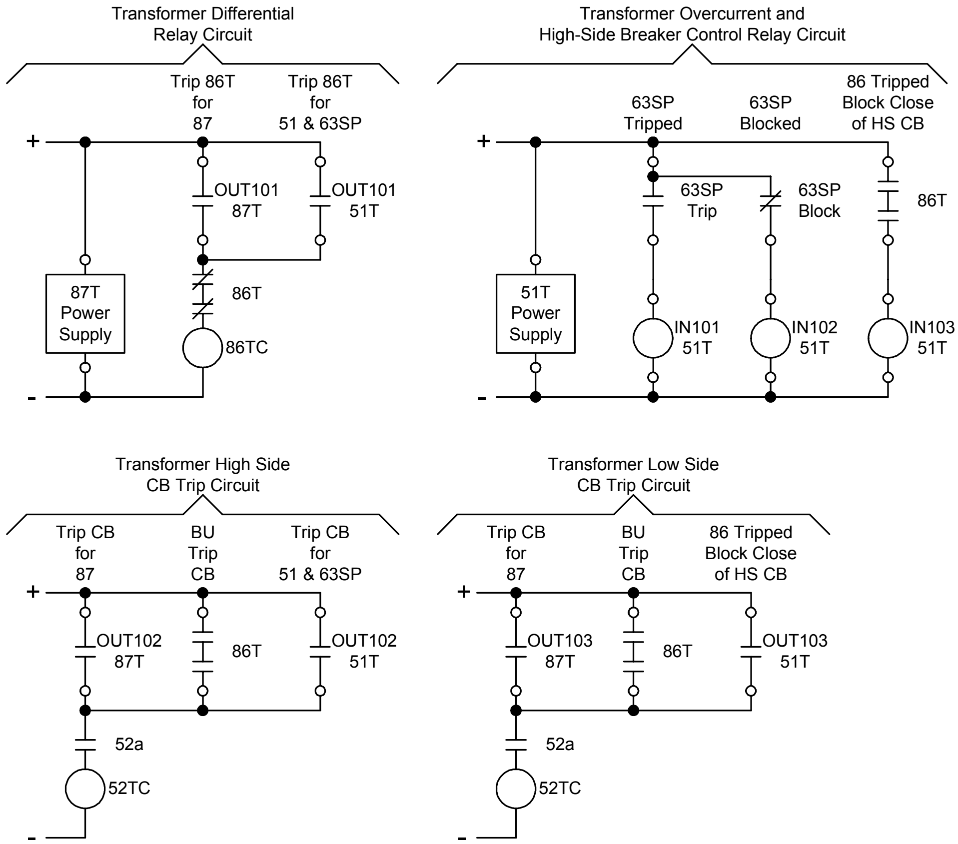



Fig. 8. DC Elementary Diagram

## VI. Design Documentation

A PCM system cannot be built, operated, and maintained without an adequate design documentation package. This section of the paper reviews what is included in a successful design documentation package. Also, the limitations of traditional drawings are recognized and suggestions made to create a complete design documentation package for a fully integrated PCM system.

A design documentation package for a typical substation includes electrical diagrams, such as schematic diagrams and wiring diagrams, and physical diagrams, such as panel details and control house details. The physical design drawings for a traditional substation design and a fully integrated design are similar so, we will not discuss those.

### *A. Electrical Design Package*

Schematic diagrams are designed to show the “scheme” of how the system works. They are arranged to best show the arrangement and logic of the circuits.

- Single-line diagrams provide a summarized “every-thing at a glance” view of the system. These include various levels of detail.
- AC and dc elementary diagrams show a detailed view of the circuits. In a traditional design, the dc elementary diagrams show how the protection and control logic works.
- Logic diagrams supplement the dc elementary diagram to show what is going on inside the “black boxes.” Logic diagrams are now a required part of a complete electrical design documentation package.

Additional documents are available that provide the user with an understanding of the way the circuit works.

- A design standard may be referenced that documents the internal logic programming of the relays used in a particular application.
- The relay instruction manual is useful in explaining how a particular protective element or built-in protection logic operates.

Wiring diagrams are designed to show how the circuits are physically laid out and are typically shown for each of the panels. Wiring diagrams are not designed to be used as a stand-alone means of troubleshooting the system. A cable table often shows the cabling that interconnects the various panels and control cabinets.

In a fully integrated design, many of the control circuits connect via communications cables. The routing of these communications links must be shown on a diagram. This can be on the same wiring diagrams and cable tables as the electrical circuits, but a separate communications diagram may be a better approach.

### *B. Schematic (Elementary) Diagrams*

A fully integrated design can be complex. Sometimes, it is no more complex than a traditional PCM scheme. In other cases, it is because there is no longer a reliability penalty that was previously associated with increased complexity. Functionality is added by simply enabling features, rather than adding discrete devices. In many cases, the appearance of complexity comes from unfamiliarity with the new architecture.

Another contributing factor to the appearance of complexity is when the design package has not been adapted to meet the challenges presented by the new technology. Here are a few issues that drive the need for better documentation.

- DC schematics alone are not adequate to tell how the system works because most of the functionality is in the relay programmable logic.
- Often, the relay logic settings are the culprit when the system does not work. The logic settings are intermixed with the coordination and protection settings. Sometimes, logic settings may accidentally get changed when coordination settings are entered, which affects the PCM system functionality.
- Relay inputs and outputs, which interconnect by communications links, never become contacts or inputs that appear on a traditional dc schematic. If they are not represented on the diagrams, a large part of the system schematic is hidden.

Suggestions to address these challenges are provided in the following sections.

*C. DC Elementary Diagrams*

It is recommended to cross reference information on the dc elementary diagram. Fig. 9 shows the dc elementary diagram for the relay circuit. Included is the device code, device type, panel location, and which logic diagrams apply to it.

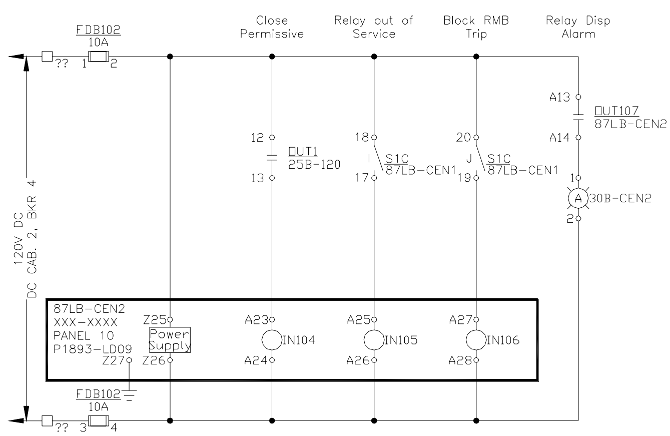



Fig. 9. DC Elementary Diagram

As you can see, the schematic is very simple. The status of switches and contacts are connected directly to inputs with no complex circuit connections. In fact, the designer has taken advantage of the isolated contact sensing inputs. Most of the inputs are connected to other circuits. In this diagram, only input circuits that are connected in the relay's circuit are shown in the schematic view, but all inputs and outputs are referenced in a table as shown in Fig. 10. Each input and output would be shown in each of their respective circuits as referenced in the table column labeled "DWG REF" and "CIRCUIT."

| 87LB-CEN2 XXX-XXXX | | | | |
|---|---|---|---|---|
| RELAY | TEST SWITCH S1C-87LB-CEN2 | DWG REF. | CIRCUIT | FUNCTION |
| OUT101 | A | P1893-DC42 | CB110 T2 | TRIP CB110 TC2 |
| OUT102 | B | P1893-DC42 | CB110 C&T1 | CLOSE CB110 |
| OUT103 | C | P1893-DC43 | CB120 T2 | TRIP CB120 TC2 |
| OUT104 | D | P1893-DC43 | CB120 C&T1 | CLOSE CB120 |
| OUT105 | E | P1893-DC40 | 21A-CEN2 | BFI/79RI LINE, 421A |
| OUT106 | F | | | WIRED OUT NOT USED |
| OUT107 | | P1893-DC40 | 87LB-CEN2 | ALARM DISPLAY LIGHT |
| ALARM | | P1893-DC03 | DCP-B2 | RELAY FAIL ALARM |
| OUT201 | G | P1893-DC42 | CB110 T2 | TRIP CB110 TC2 |
| OUT202 | H | P1893-DC43 | CB120 T2 | TRIP CB120 TC2 |
| OUT203 | | | | NOT USED |
| OUT204 | | | | NOT USED |
| OUT205 | | | | NOT USED |
| OUT206 | | | | NOT USED |
| IN101 | | P1893-DC42 | CB110 T2 | 52B CB110 |
| IN102 | | P1893-DC43 | CB120 T2 | 52B CB120 |
| IN103 | | P1893-DC42 | CB110 T2 | CB110 SYS A CONTROL VOLTAGE ALM |
| IN104 | | P1893-DC40 | 87LB-CEN2 | CLOSE PERMISSIVE, 25B-120 |
| IN105 | I | P1893-DC40 | 87LB-CEN2 | RELAY OUT OF SERVICE |
| IN106 | J | P1893-DC40 | 87LB-CEN2 | BLOCK RMB TRIP |

Fig. 10. I/O Cross-Reference Table

It is also difficult to convey where the many programmable outputs that are available in each device are used. Again, these are often in completely different circuits. In Fig. 10, the designer has used a table to show the input, output, and test switch information. The device code and device model option table is listed at the top of the table so that it is clear to which relay the table applies. All output contacts and test switch poles are listed whether they are used or not.

A table such as this is also an effective way of including information on relay I/O that is connected to other devices via communications links.

*D. Logic Diagrams*

It is necessary to create logic diagrams for any design that uses advanced programmable relays. This is especially true for a fully integrated system.

The programmable logic is an extension of the schematic design. The settings file containing the settings equations is inadequate for serving the purpose of a schematic diagram. It is similar to the wiring diagram. It tells you how the system is wired together, but it does not show you how it works. It is nearly impossible to see the functioning of the logic from the equations alone.

The circuit functionality is now mostly in programmable logic. Trying to understand and troubleshoot a system by looking at the relay settings equations is similar to trying to understand and troubleshoot a system by using only the wiring diagrams.

Another problem is that the relay's logic settings are intermixed with the coordination settings. If there is no design documentation that describes the PCM system settings, it is very difficult for the person creating the actual settings file for each relay to know how to make these settings. Often when things do not work, it is because a logic setting has been inadvertently changed or overwritten. A project drawing documenting the PCM system logic is less volatile than a relay settings file.

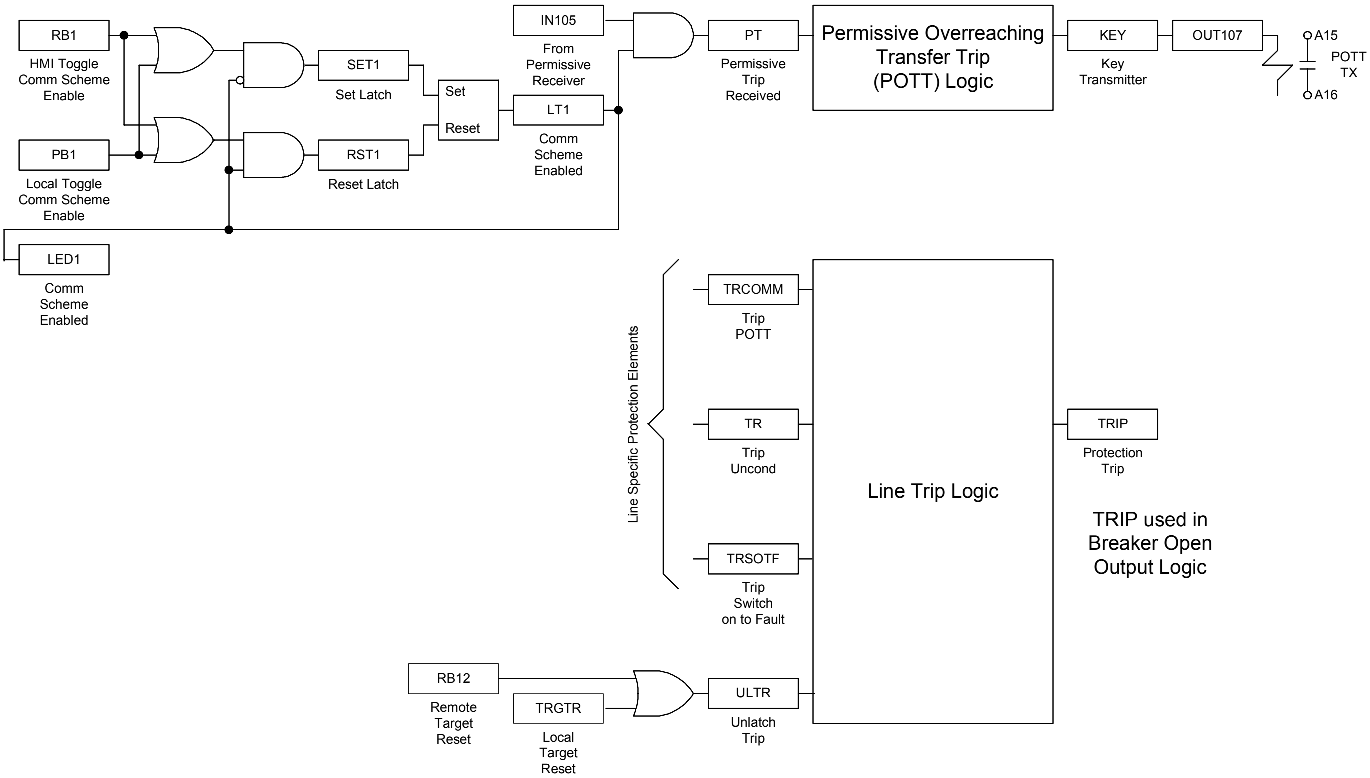



Fig. 11. Example Logic Diagram

When troubleshooting a system, the logic diagrams serve as ready reference of what the logic settings should be. They eliminate a great deal of confusion regarding what is correct and allow the system to be restored much more quickly.

There are several approaches to creating a logic diagram:

1. Create partial (summary) diagrams that contain only a partial representation of critical logic, such as an interlock. The user is left to examine the logic settings to see the detailed design.
2. Diagram logic that is part of the integrated system design but excludes the logic that will vary from circuit to circuit. In this case, you can have one logic diagram that applies to all of the feeder circuits, for example.
3. Diagram all logic settings in the relay. In this case, you may have to generate a logic diagram for each individual relay in the system.
4. Diagram all logic in the relay, i.e., expand out and reproduce all of the relay's hard-coded logic, in addition to all of the user-programmable logic.

Of these options, Option 2 is recommended because it is easiest to generate and maintain. It includes most of the information required to work with the system and keeps the amount of information that is not documented down to a manageable level.

Of these options, Option 4 is not recommended. There is risk that the information in the manual could be incorrectly transcribed or interpreted. If the manufacturer's information changes, the drawings can become out of date.

Fig. 11 shows an example of a partial logic diagram that follows Option 2. It includes all of the logic settings that are part of the integrated PCM system. The circuit-specific protection, reclosing initiate, and reclose and close supervision settings are not included in the diagram.

Where the logic drives an input to a fixed logic block inside the relay, it shows this as a black box with inputs and outputs. The user must refer to the documentation provided by the manufacturer to understand how the protective function processes the inputs and creates the outputs.

### *E. Standards*

It is desirable to create standards for application of programmable relays. This improves consistency of how the relays are applied and how they respond throughout the system. In many cases, these standards can serve the purpose of, or supplement project-specific, logic diagrams. In this case, the dc elementary diagram might reference a specific standard number. The user would go to the standard to understand how the relay is programmed.

If you do this, standards must be controlled. If a standard is changed or updated, the old standard must be retained because it serves as documentation for specific installations. It is not reasonable to require going back to all relays that were installed per the original standard and updating the programming to the new standard.

This is a case where a well thought out line between what is included in the standard and what is left up to the specific application can be helpful.

## VII. Summary

When the power of modern relays is used to eliminate ancillary nonprotection devices, it is often possible to inadvertently reduce redundancy for critical protection and control functions. To do the design properly, each critical protection and control function must be examined to eliminate single points of failure. When a project is properly designed, failure of a system or component should create a condition that is perhaps undesirable or inconvenient but not intolerable. This paper describes some typical examples of eliminating single points of failure. These concepts can be applied to review other cases in order to assess a new integrated design.

By using the power of programmable relays and smart integration platforms, it is possible to design a system that includes continuous self-test features. The system has reality checks built into it that validate the signals being used to protect and control the system. Implementing monitoring of all aspects of the system is easy to do. The continuous self-test features reduce operations and maintenance costs. The need to inspect and test the system is significantly reduced because the system immediately detects and notifies system operators of problems. By addressing these problems before undesirable operation occurs, reliability is improved. Using dual equal systems permits simple implementation of these features that also provide for component failure contingencies.

Design of dc control circuits is significantly different when integrated PCM systems are built using programmable relays. Using programmable logic inside the relays instead of contact logic increases functionality and improves reliability. Examples were included on how to build testability into the system. Examples were also shown of using isolated input circuits, programmable output contacts, and using communications links for tripping and interlocking to make improvements in the system.

Finally, the shortcomings of a traditional design documentation package were discussed and alternatives proposed. To have a complete understanding of the design, it is important to show not only contact I/O on the diagrams but also communications link I/O. Logic diagrams must be provided to supplement the control schematic diagrams because most of the protection and control logic is internal to the programmable devices.

## VIII. Biography

**Michael J. Thompson** received his BS, Magna Cum Laude from Bradley University in 1981 and an MBA from Eastern Illinois University in 1991. He has broad experience in the field of power system operations and protection. Upon graduating, he served nearly 15 years at Central Illinois Public Service (now AMEREN) where he worked in distribution and substation field engineering before taking over responsibility for system protection engineering. Prior to joining Schweitzer Engineering Laboratories, Inc. in 2001, he was involved in the development of a number of numerical protective relays. He is a Senior Member of the IEEE and a member of the main committee of the IEEE, PES, Power System Relaying Committee. Michael is a registered Professional Engineer in the State of Washington and holds a patent for integrated protection and control system architecture.


20070116
TP6238-01