Subject: Transmission Relaying – Digital Logic

(What's the Logic?)

Primary Interest Groups
Transmission Owners
Generation Owners
Distribution Providers

Overview
An analysis of information over the last three years indicates that a large number of misoperations are due to incorrect relay logic used within the Protection System. These issues comprise a variety of problems that involve relay settings. The following sections construct scenarios that could potentially result from incorrect relay logic used within the Protection System.

Details
Modern digital relays often provide great flexibility in how the protective elements initiate actions such as tripping and closing breakers and sending pilot relay signals. Two potential mistakes are the selection of incorrect protective elements to initiate actions and the inappropriate application of internal relay logic.

In the first example, an entity inadvertently enters the wrong protective element in the trip logic. The instantaneous element and delayed element are nearly identical in variable name except for one extra character in the delayed function. The entity uses the non-delayed element resulting in an undesired trip as the operating element has insufficient delay for an external line fault.

In the second example, incorrect switch-on-to-fault logic setting fields are selected. The result is undesired trips on unfaulted circuits after another circuit experiences an automatic reclosure into a fault.

In the third example, the breaker status is not programmed correctly into a relay applied as transformer lead protection. This relay also has switch-on-to-fault logic enabled. While the relay incorrectly senses the breaker was opened, it issues an unnecessary trip for an external fault based on the open breaker logic.

In the fourth example, a relay used in a directional comparison blocking scheme receives the blocking signal from the remote end for an external fault but the relay still trips. The pilot logic in the relay did not match the intended settings, causing it not to recognize the reception of the blocking signal.
In the fifth example, setting errors are made in the fuse failure logic. The setting errors then prevent the relay from blocking distance elements from tripping when two potential fuses fail.

In the sixth example, stub bus logic is initiated by the position of a line disconnect switch. The “a” finger of the switch is used to indicate its status. When DC is removed from the relay, the relay goes into stub bus mode prior to powering down as the relay detects a low status input for the line disconnect. This incident results in a false line trip.

**Corrective Actions**

In each of the examples, the immediate action to be taken is to correct the relay setting errors. The following additional corrective actions were dependent on the circumstances of the applicable example.

- In the second example, the entity would review and revise, as necessary, the switch-on-to-fault settings of all the relays on its system of the specific relay types that had misoperated.

- In the third example, the entity would reprogram the input to properly follow the breaker status. It would also determine whether the switch-on-to-fault logic was needed in the application and thereafter would remove the unnecessary logic.

- In the fourth example, the entity would determine that the logic settings as well as other settings had been disturbed when ancillary settings in the relay were changed after commissioning. The entity would review all installations of this relay type on its system to determine if logic errors had also been introduced inadvertently.

- In the sixth example, the entity would change future designs to only use “b” contacts to indicate line disconnect status. In applications that had used “a” contacts, a time delay would be added to allow the relay enough time to power down (after loss of the DC supply) before it could enter the stub bus mode.

**Lessons Learned**

The relay logic settings are some of the uncalculated settings that determine the relay’s functional interface. As seen in the previous examples, small errors in the logic can be very unforgiving. It is important to review trip logic and be aware that some protective elements sound the same but do not operate the same. Thorough testing can help validate the relay logic; however, adequate guidance is needed to develop procedures that truly test the relay’s elements and logic.

In reviewing the application, the protection engineer should determine if special logic is justifiable. The logic may be designed to cover certain situations that do not apply to the specific instance at hand. The merits gained by the logic must be weighed against the security or dependability lost.
Making minor setting changes can inadvertently and drastically modify the way a relay functions. At a minimum, the entire active settings in the relay should be compared to the settings of record after a change is implemented.

Accordingly, it is possible that relay settings may be modified to address the salient issues. At times, the appropriate solution may include design changes external to the relay.

RFC staff contact for more information: Art Buanno, art.buanno@rfirst.org, (330) 247-3442

October 21, 2010

The sole purpose of this document is to provide guidance through illustrative examples. It is not intended to, nor does it, create, modify, or in any way alter any Reliability Standard or obligation of a Registered Entity or ReliabilityFirst. ReliabilityFirst will continue to assess compliance based on the facts and circumstances of a given situation as applied to the relevant Reliability Standards. Implementation of any suggestions or recommendations in this document does not, in and of itself, guarantee compliance to any Reliability Standard. Rather, each Registered Entity is responsible for assessing and taking all necessary actions to establish compliance with all of the requirements of all applicable Reliability Standards.