7 Conclusions

Results show the RSS improves security of the existing protection system by preventing incorrect operations due to hidden failures. Test cases illustrate the model operation under a variety of fault conditions, all of them producing expected results. This is true for all three operating modes: Normal, Emergency, and Out of Service. The RSS does add some complexity to the protection system. It requires more contacts and wiring, which can lead to hidden failures. Also, the RSS itself can fail. However, the RSS is providing redundancy in the system. It is extremely unlikely that two hidden failures, one of the existing relay scheme, and one of the RSS, will occur simultaneously. Since it is microprocessor based, the RSS should be more reliable than existing relays. Ideally, the RSS will have built in self-test capabilities, and will remove itself from service in the event of failure. Since the RSS is passive and waits for a trip signal, the worst case in any failure is the same security as a protection system without a RSS. Dependability of the protection system is the same with or without the RSS in service.

The actual operating time of RSS calculations is not considered in this model. During Emergency mode, the vote applied is just a logical combination of signals, with a negligible operating time. In Normal mode, the actual calculation time of the relay algorithms will slow down the protection system. At a relatively slow sampling rate of 12 times per cycle, it is reasonable to assume that the total calculation time for an individual protection scheme will be less than one sample. Of concern is the combination of multiple relay calculations made for a line with multiple protections operating. The device requires 3 consecutive successful trip calculations for a reliable trip result, and adds another contact that must operate for breakers to open. This slows the overall protection system by ¾ cycle, ¼ cycle for the device to return 3 trips, and ½ cycle for the contact to operate.

Microprocessor-based relays in the substation may reduce the need for this device. Microprocessor-based relays are more reliable, and have self-test capabilities. However, hidden failures include physical interconnections, such as contacts, so hidden failures still exist and need to be protected against. Also, there are operating situations where increasing the security of the system is desirable, making the "vote" mode very attractive. Microprocessor-based relays that are an "all-in-one" line protection scheme could be modified by the manufacturer to include a vote scheme very similar to the one in the RSS. However, this would only apply to newly manufactured relays, and would require a command from the system operator to every relay so equipped in the substation to switch to vote mode. With a RSS installed, only the RSS requires a command from the system operator to change to the vote scheme.

Since it is unlikely for the near future that substations may have completely digital protection, the RSS may be an affordable interim step to improve system security. The RSS should be straightforward to actually develop. All the relay calculations use well established algorithms. Developing the RSS is more a matter of physical design and combining some existing software functions than any actual new theoretical development. Also, the device can include and use any algorithm to model any relay or relaying scheme, making the potential applications for the device widespread.