SPaRC
Secure Pathways for Resilient Communications

Direct Underreaching Transfer Trip Testing - Summary

This document provides a high-level summary of the Direct Underreaching Transfer Trip (DUTT) Testing completed through the Secure Pathways for Resilient Communications (SPaRC[1]) program under the Office of Electricity.

[1] https://securecomms.ornl.gov/

Overview

This document summarizes the **D**irect **U**nderreaching **T**ransfer **T**rip (DUTT) testing completed through the SPaRC (**S**ecure **Pa**thways for **R**esilient **C**ommunications) program under the Office of Electricity (OE).

Background

DUTT is a teleprotection scheme used in power systems worldwide to transmit states between protective devices to improve reliability and protect the electrical grid. The foundational concept is to provide situational awareness between protective devices supported by low latency communications systems. The testing for DUTT under SPaRC had four contributing National Labs, Idaho National Labs (INL), Oak Ridge National Laboratory (ORNL), Pacific Northwest National Laboratory (PNNL), and Sandia National Laboratories (SNL) which examined different scenarios and conditions for the impairment and constraint of the communication pathway supporting the DUTT protocol and potential impact to protective devices and teleprotection schemes. The impairment and constraining testing of the communication channel was designed to test "to failure" of the communication channel and understand potential impacts on the relay protection.

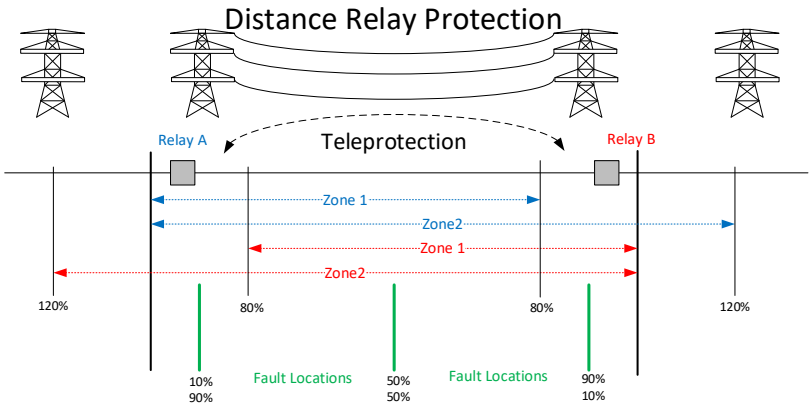

Figure 1. Teleprotection for relays

In the United States power grid, two favored teleprotection protocols by utilities are SEL Mirrored Bits® and IEC 61850 GOOSE. Both protocols were tested to failure in the protection scheme via different communication systems, such as wireless and wired systems where interference or quality of service could be implemented and results or the protection measured.

Testing Implementation

1. The power systems were simulated with various hardware-in-the-loop and simulation software packages (RTDS, OPAL-RT, Power World) and included protective relays as hard-in-loop with the simulated power system. Multiple communication systems supporting Mirrored Bits and GOOSE were tested. Constraining and/or impairing the communication channel was implemented via interference tools and software for wireless systems as well as network emulators for wired systems providing fine control over the communication path quality of service (QoS).

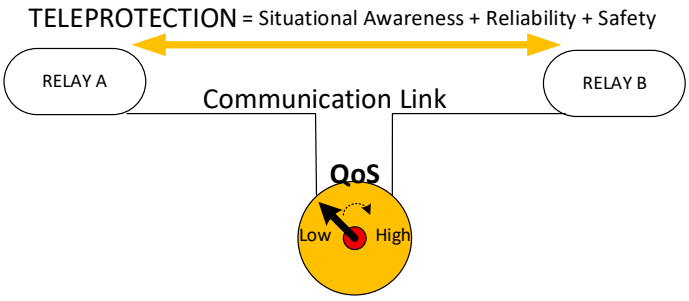

Figure 2. Teleprotection QoS

Communication systems tested included: serial connections, switched packet over wired and wireless (6 GHz), and serial over wireless (900 MHz). Each of the complete descriptions are described in detail in the SPaRC - Direct Underreaching Transfer Trip - Testing Technical Summary and the SPaRC - Direct Underreaching Transfer Trip Test Methodology and Results documents available on the SPaRC website.

Findings

- Investigation by each laboratory found that both GOOSE and SEL Mirrored Bits teleprotection schemes are robust and reliable. Mirrored Bits provides robust "guardrails" via the native serial protocol and SEL implemented security protocols which provided secure and repeatable boundaries for performance of the Mirrored Bits protocol in several different impaired communication conditions.

- All communication impairments of the Mirrored Bits protocol performed in a binary fashion, the communication channel was either good (i.e. up) or bad (i.e. down), and the relay acted accordingly. Even in conditions when the delay of the path was extended past the zone 2 timer (Z2T), the relay would trip on the timer and still received the remote bit afterwards, which is expected.

- Similar to Mirrored Bits, under a variety of delay conditions to the GOOSE protocol, the relay behaved as expected. Receipt of the communications trip signal prior to detection of a zone 2 fault resulted in the relay waiting for the fault to be detected and tripping. receipt after detection of the zone 2 fault and the starting of the zone 2 timer resulted in immediate tripping; and receipt of the communications trip signal after the zone 2 timer expired and the relay tripped resulted in no change.

- Under some packet corruption scenarios with the GOOSE protocol, the bravo relay would fail to respond to communications until both the SDN switch providing the connection, and the relay were rebooted. Observation of network traffic suggests that this was not an issue with the switch, traffic was still being passed, however the relay simply stopped responding. If this condition was triggered by the corruption, it persisted until reboot even if unaltered packets were sent.

- Teleprotection schemes have latency requirements, and the communication system is one component of latency. Communication and protection engineers need to coordinate on understanding overall latency needs and how each component of the entire system, relay to relay, affects latency: See Latency Implications for Grid Communications

- Many wireless Internet of Things (IoT) protocols can interfere with the 900 MHz SEL radio for Mirrored Bits if they are collocated with other 900 MHz devices or are in an area where the 900 MHz band is overcrowded. However, channel hopping and the security checks of Mirrored Bits ensure reliability of the teleprotection given the relays are set up with an adequate link budget between the transceivers. It is important to coordinate relay event recording and sequence of events between relay action and teleprotection to avoid unintentionally interfering with expected relay action.

- Noise on serial lines was also found to degrade and impede relay signals using serial connectors and cables. However, the amount of noise coupled into the cable itself is improbable unless extremely long serial cable lengths (i.e. > 100 m) are used.

- Impairing the communication path (reducing QoS) could be readily achieved with network emulators. The Mirrored Bits security checks and serial protocol error checks provide robust mitigation against the interference from wireless systems that can impact the relay's communication channel. Under Mirrored Bits between 1.0% and 0.75% of dropped or altered packets would result in the relay "bouncing" the communication path for the relay. In all testing the relay acted accordingly by either tripping on the receipt of the remote bit or expiration of the zone 2 timer.

- Mirrored Bits protocol is reliable and resilient and can be better understood with knowledge of the potential errors of asynchronous serial protocols, the SEL security checks and the impact to the Remote OK (ROK) bit.

- Protection schemes are a critical and important configuration of protective relays in the electric grid today and more attention needs to be brought to fusion of communications and power systems.

It is important to develop integrations steps for utilities to migrate to more modern communication systems that have performance parameters needed to support high-speed protective relaying.

Challenges and Next Steps

Discussion with utilities highlighted several challenges faced by utilities to transition from older widely deployed teleprotection schemes based upon serial protocols such as Mirrored Bits to modern packet-based protocols such as GOOSE messaging. Overall implementation of a new protection scheme often relies on changing multiple components not limited to the protective relay, the protection scheme, and the communications channel. Each of these have inherent risk to the overall protection scheme and often increase the risk and technical challenge to an unacceptable level for utilities to implement, resulting in limited options for a utility. As part of this research serial to internet protocol (IP) implementations were investigated and tested, resulting in robust implementation of Mirrored Bits over packet-switched networks. This technology can provide an intermediate step for utilities seeking to mitigate risk in upgrading teleprotection schemes. Implementing serial to IP conversion can allow a utility to upgrade communications from older private line, dedicated, or other time division multiplexing (TDM) systems to packet-based systems while maintaining existing serial-based teleprotection, ultimately providing a derisked transition for the utility's protection program.

Communication systems have become an essential and foundational component of electric grid operations. Often it is assumed that the current utility communications system is 100% available and capable for carrying critical grid services. It is crucial to understand the communication path performance requirements needed to support grid operations and ensure they align with the communication system capabilities. Stress-testing grid processes against communication failures can yield critical insights into operational resilience. This data is essential for validating recovery strategies and ensuring utility preparedness during extreme events.

Related Documents

1. SPaRC - Direct Underreach Transfer Trip - Testing Technical Summary
2. SPaRC - Direct Underreach Transfer Trip Test Methodology and Results
3. Understanding and Managing Quality of Service in Grid Communications
4. Latency Implication for Grid Communications
5. Other SPaRC documents

The US Department of Energy's SPaRC (Secure Pathways for Resilient Communications) program is leading grid communications research and development through a multi-National Lab testbed, established to design, test, evaluate, and benchmark next-generation secure communications architectures and technologies. A secure communications system protects the end-to-end physical pathway that transports data from origin to destination. Key SPaRC activities include the Grid Communications Test Bed, Next-Generation Communication Experiments, and Education & Technical assistance. For more information see: https://securecomms.ornl.gov/