Protection Engineer Campfire Tales

A semi-random walk through the fields of protection engineering, sociology,
cultural anthropology, reliability engineering and etymology.

Presented to
Western Protective Relay Conference
Oct 2009
Spokane, Washington, USA

Prepared by
Ralph Barone, PEng
Senior Protection Planner
BC Hydro

Introduction:

In any culture, one will find folklore, legends and other stories which are passed on orally and informally from generation to generation. In addition to their entertainment value, these stories provide guidance to the members of the society as to how to act and behave (or not behave), in order to be accepted within the society. The tacit knowledge within the folklore is often presented in a manner which makes a stronger impact than a dry recitation of the embedded moral.

There also exists a body of folklore amongst protection engineers. However, being engineers and not sociologists, we do not always recognize it as folklore, preferring to call these "horror stories" or "disasters". These stories tend to get passed on from senior engineers to junior engineers at the coffee shop or pub, instead of around a campfire. It is the purpose of this paper to share some of the folklore I am familiar with, but more importantly, to dissect these stories and uncover the hidden lessons buried within the entertaining stories.

Protection engineering is as much an art as it is a science[1]. Protection folklore provides us with valuable clues as to how to approach the "art" portion of our jobs. In addition, within a particular company, the folklore of the group can often give valuable insight into the evolution of the protection practices of that group. In particular, any given company's history of major outages and failures (as well as the absence of such) will tend to uniquely affect their future protection practices. It may be argued that one of the benefits of conferences such as this one is that the sharing of "folklore" that spontaneously occurs during these conferences allows attendees to learn from other's experiences and promotes a homogeneity of protection practices in the long run.

In this paper, six stories are presented and then analyzed. After the analysis of the outage, lessons learned and possible "morals of the story" are presented. In most of the stories the derivation of the obvious moral is left as an exercise for the reader[1]. Instead, some of the more subtle lessons are examined. We shall examine some of the philosophical aspects of protection, focusing on first, second and n^{th} contingencies, the difference between non-credible and impossible, and the role of hidden failures in major outages.

It is my hope that this paper will cause the reader to think about not only the major protection problems that they have seen and the lessons that can be learned from them, but also to think about the role that these stories play in our education and our culture as protection engineers. If you enjoyed reading this paper, take a junior engineer out for coffee and share some of your stories with them.

Cascading Breaker Failures

Event Summary

As part of our Planning criteria, BC Hydro's Protection Planning department considers cascading breaker failures (ie: breaker failure protection operating on a breaker which was itself tripped by the breaker failure protection of another breaker) to be a non-credible scenario. Interestingly enough, in a 3 month period in 2003/2004, we had two disturbances where cascading breaker failure occurred.

In the first disturbance, a feeder fault resulted in the tripping of seven separate breakers, de-energizing two bus sections and a transformer. Of the seven breakers tripped, three breakers

---

[1] Don't you hate it when people do that?

initiated breaker failure tripping. Two of these breakers opened slowly and one breaker remained closed, albeit with a breaker failure flag.

In the second disturbance another feeder fault resulted in the tripping of eight breakers locally, plus another two which were tripped at a neighbouring station via DTT. One bus section, a transformer and a transmission line were deenergized. In this event, only two breaker failure protections operated, however, one breaker remained closed, with **no** associated breaker failure flag.

Analysis

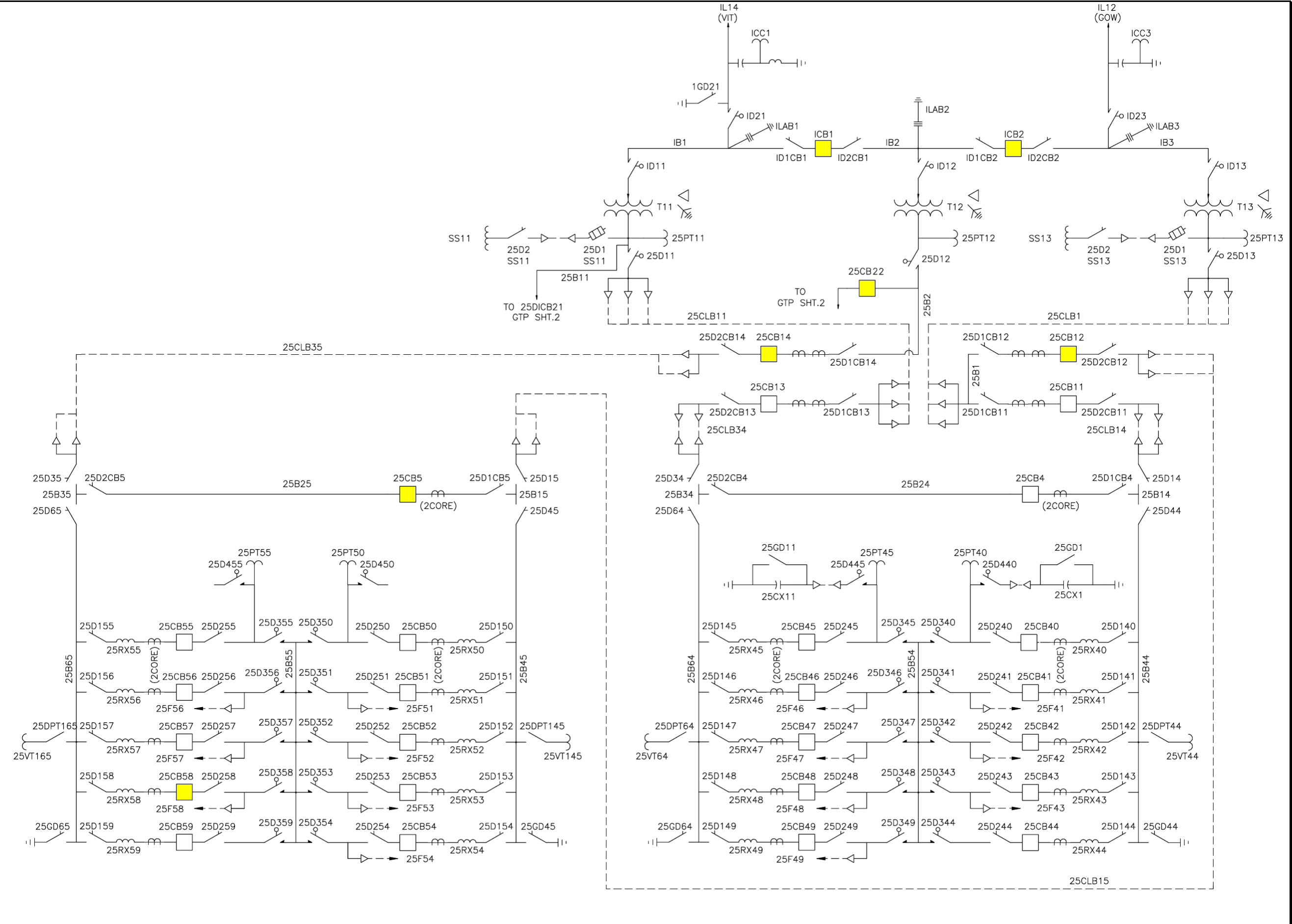

Figure 1 - GTP station one-line

At GTP substation (the first disturbance), a fault on feeder 25F58 was the initiating incident. Breaker 25CB58 failed to open before its breaker failure protection tripped into 25B65 protection[2], which sent trips to 25CB5 and 25CB14. Both 25CB5 and 25CB14 failed to open in time, and their respective breaker failure protections then operated. The 25CB5 breaker failure protection tripped into 25B45 protection, which tripped 25CB12. 25CB14 breaker failure protection tripped into T12 protection, which tripped 25CB22, 1CB1 and 1CB2. All breakers eventually opened, except for 25CB14.

---

[2] BC Hydro practice is for breaker failure to trip into adjacent protection zones, as opposed to directly tripping breakers. This practice reduces the number of trip outputs required on the breaker failure relay, reduces the number of changes required to be made to breaker failure protections as the system configuration evolves, and also simplifies testing. There is probably a very interesting group of stories behind this one design decision.

Timing tests performed on the breakers after these incidents showed very interesting behaviour. The first test trip operation of the breaker would be very slow (up to ½ second)[3]. However, subsequent trip commands would be processed faster, until by the second or third operation, the breaker would be operating at nameplate speed. Inspection of the breakers showed that improper maintenance procedures had been used, including the use of a non-recommended grease. This grease had thickened with age, causing sticking between two plates in the mechanism, which the low powered trip coil could not overcome.

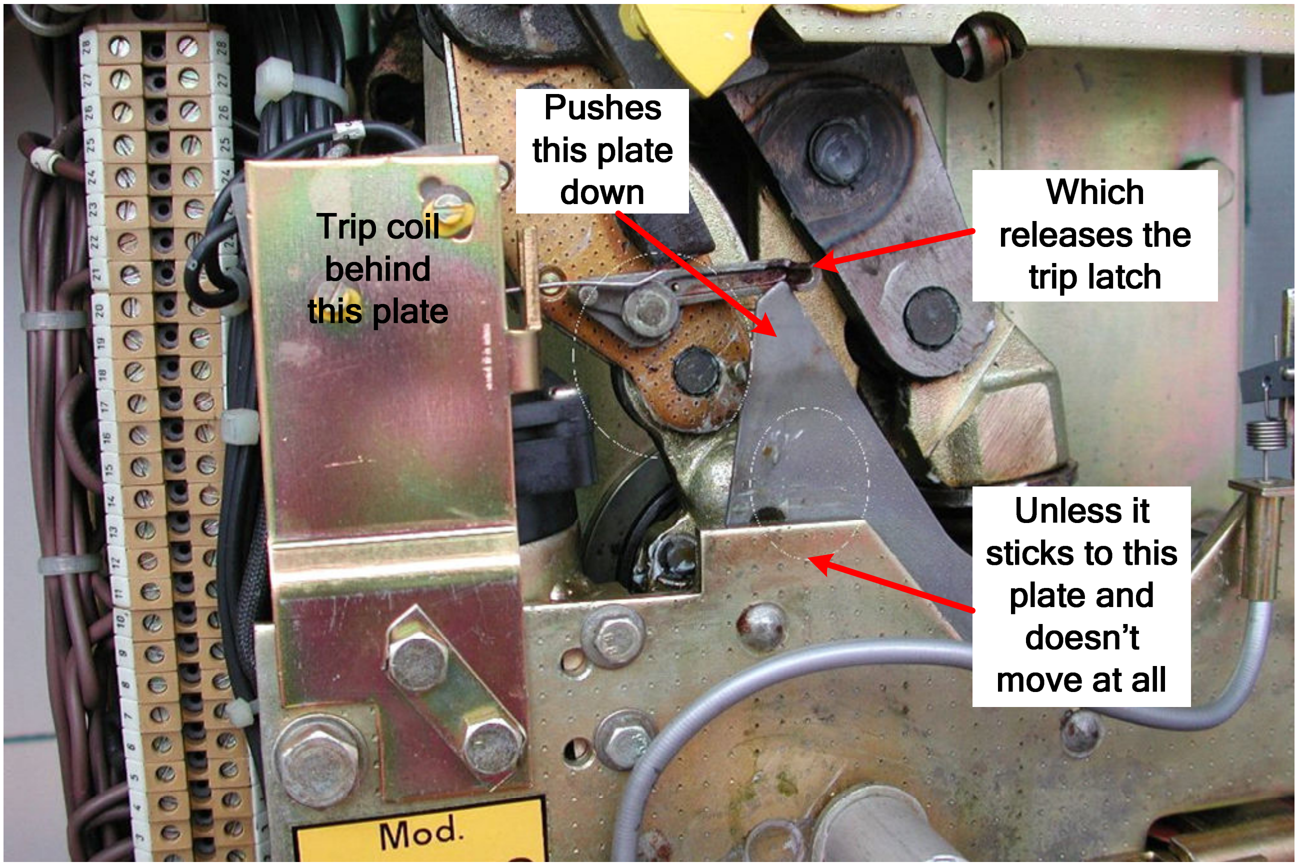

Figure 2 - Improper lubrication of 25 kV breaker

A second cascading breaker failure incident occurred at WHY substation less than 3 months after the incident at GTP. While the sequence of events and the root cause was a near duplicate of the first outage, there were two interesting differences. First, it involved a different make and model of breaker, with a different (although still low power) trip mechanism, maintained by a different maintenance crew. The second (and more immediately disturbing) difference, was that one breaker (25CB2) failed to open, with no breaker failure flag. The mystery of the missing breaker failure trip on 25CB2 was later shown to be a correct (if non-intuitive) operation. The breaker failure scheme on 25CB2 had been initiated by another breaker failure trip. However, this breaker failure trip also tripped enough surrounding breakers to clear the original feeder fault, which

---

[3] It should be noted that our breaker timing tests must be performed with the breaker isolated from the system, therefore, the first trip of the breaker must occur before the instrumentation is connected to the breaker. This was a perfect opportunity to not observe the true nature of the problem with these breakers.

reset the chain of breaker failure initiate signals before the 25CB2 breaker failure relay could time out.

Lessons Learned

Credible vs. impossible

In our planning criteria, we often speak of credible and non-credible scenarios. Credible is derived from the Latin word "credere", meaning to believe. We should constantly be reminding ourselves of the subtle difference between "non-credible" and "impossible". A non credible scenario is simply one that we do not believe will occur. Unfortunately, our beliefs tend to be shaped by our (limited) past experience, so we tend to discount how truly imaginative the universe can be. In these two incidents, we were saved by breaker failure protection that had been installed to guard against other more credible contingencies.

Non-credible events happen on a regular basis. It is the author's contention that if you wait long enough, pretty much any scenario you can imagine will eventually occur. If we accept this as fact, we should be able to hypothesize that larger utilities (which tend to have larger exposure to events and longer collective memories) should have more stringent criteria for what constitutes a non-credible event than a smaller utility would. What would be considered a "once in a lifetime" event for Ethel's Power and Light probably happens on a weekly basis somewhere in the Western Interconnection.

We also tend to assume that events in the universe are more independent than they really are. In the two events presented, our presumption of non-credibility was based on the absence of a common-mode failure (the improper maintenance practice). These hidden common-mode couplings tend to go unnoticed until they result in a non-credible outage (at which point we tend to say something ironic like "can you believe what just happened?!"). Some examples of these hidden common-mode couplings are:

- Relay digital input conditioning that appeared adequate until the station service AC was crossed onto the station DC supply. This resulted in every relay of that style in the station tripping simultaneously.
- The lightning storm, ice storm or forest fire that is wide enough to take out two lines that were presumed to be adequately spaced to be independent of each other. In 1972 we had an ice storm that took out two 500 kV lines spaced 170 km apart.
- Errors in relay setting practice or design philosophy which then get applied to multiple relays.
- Our newer line protections contain redundant breaker failure protection in which the initiation and tripping signals are connected primary to primary and standby to standby, with no cross-coupling. Taking the primary line protection relay out of service while the standby relay (either initiating or tripping) in an adjacent zone is also out of service will result in loss of breaker fail functionality between these two zones.

The importance of proper maintenance

On a less philosophical level, these outages spotlight the importance of proper (and properly documented) maintenance procedures. As companies downsize, experienced staff retires, or work is contracted out to third parties, some of these subtle but important maintenance procedures can be lost, either due to the disappearance of key staff, loss of critical documents, or contractual reasons (the company switches from prescriptive type maintenance standards to performance based standards).

1L212 Misoperation 2007/06/18

Event Summary

The North Thompson area in the BC Hydro system is a very long radial 138 kV system. In 2007, a new transmission connected customer load (REG) was added to the end of the system. To facilitate the load connection, a new 32 km long transmission line (1L212) was added to the end of the radial system at VLM.

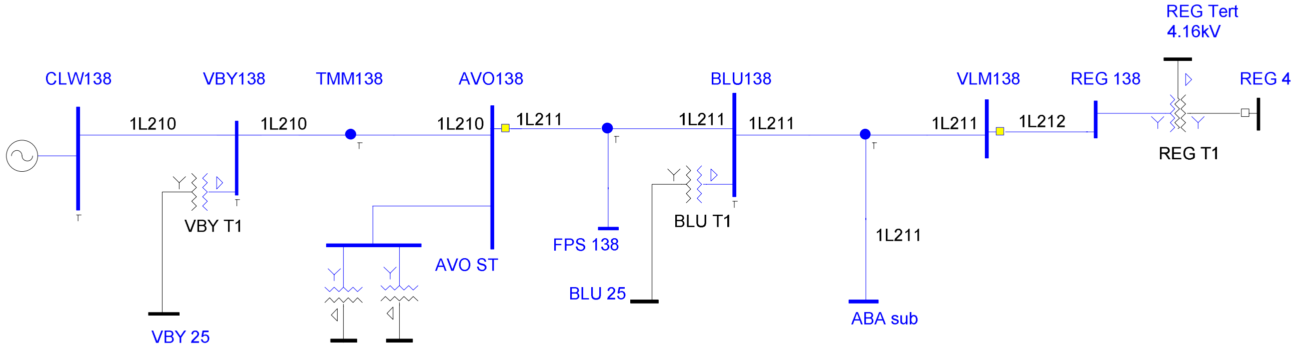

Figure 3 - North Thompson system

On 2007-06-18, existing AVO 1L211 line protection operated twice, isolating customer load at BLU and VLM, as well as the industrial load at FPS, ABA and REG. A line patrol failed to find any faults on 1L211. After sectionalizing at VLM, the line was successfully reenergized, however it tripped off again after 1L212 was reenergized. A line patrol of 1L212 found a broken cross-arm, one conductor hanging a foot above the sandy soil, and two dead bears near the conductor.

Figure 4 - Broken crossarm on 1L212[4]

---

[4] Photo credits - Matthew Barnes, BC Hydro Transmission Dept.

Figure 5 – High impedance ground fault on 1L212

Analysis

Post-analysis of the event records and settings from the AVO 1L211 and VLM 1L212 relays showed a subtle miscoordination between the ground elements on the two line protections. Both inverse time ground overcurrent elements were properly coordinated, but the effective pickup of the directional element torque controlling the 1L212 51N was set above the pickup of the element it controlled. The effective curves of the two overcurrent elements are shown in Figure 6. Note that the area of possible miscoordination is fairly small, especially when compared to the minimum bolted SLG fault level at the end of the line.

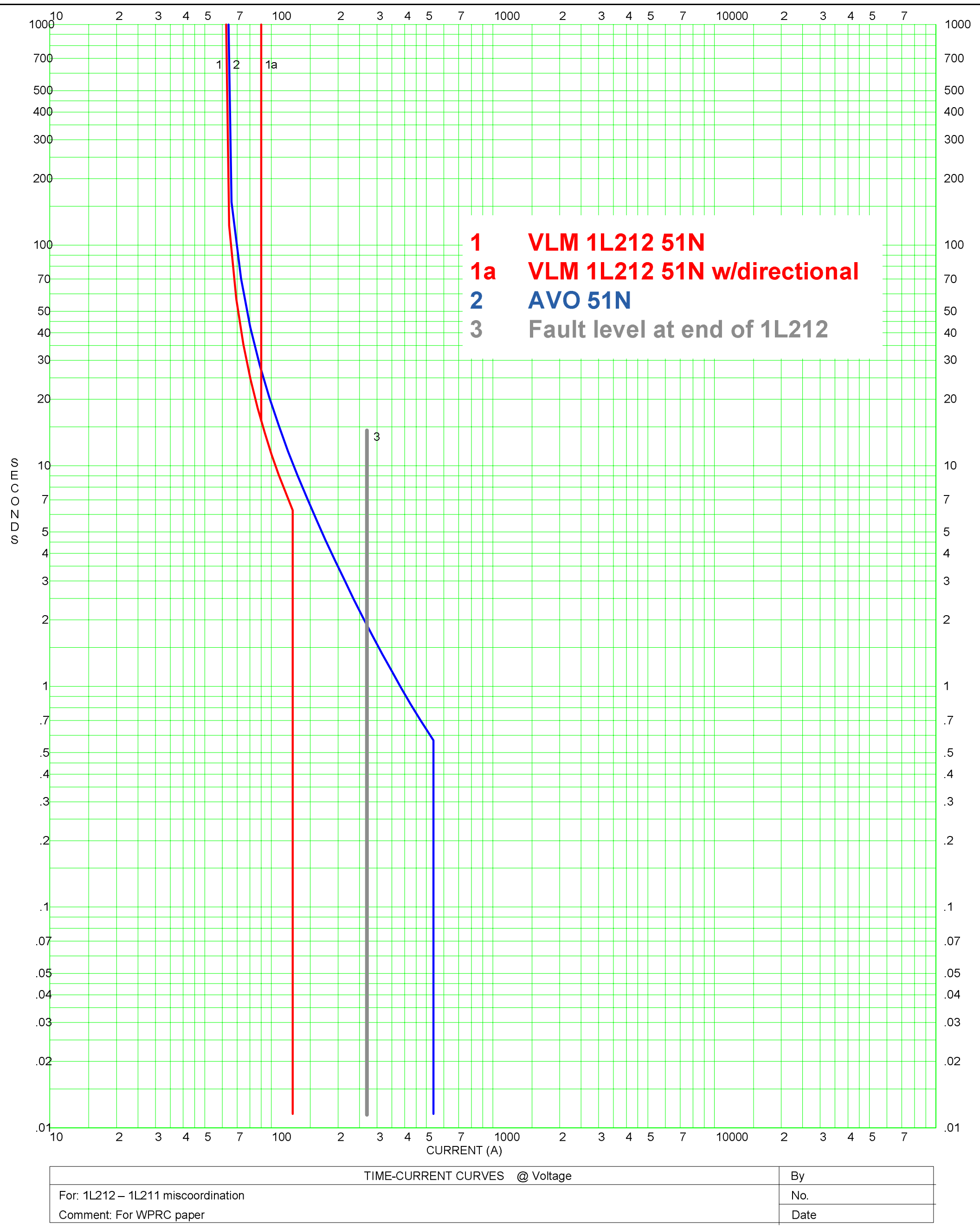

Figure 6 - Miscoordination caused by directional torque control

Lessons Learned

While the obvious lesson here is that directional elements have to be more sensitive than the element they directionalize, I would like to pick out a more subtle lesson here. In the coordination graph above, the area of possible miscoordination is fairly narrow and only reachable via a high-resistance ground fault, however the event that precipitated the misoperation occurred within six months of the line being put into service. If you wait long enough, any contingency you can think of (and a few you can't possibly imagine) **will** happen. Also, according to Murphy, as soon as you depend on something not happening, it will happen[5]. Regardless of what your planning criteria are, never say "well, that can't possibly happen."

South VI Outage 2008/10/12

Event Summary

The Southern Vancouver Island (SVI) power system was originally built as a radial 138 kV network which was later reinforced by overlaying it with a 230 kV network. The 230 kV network is not loaded as heavily as the 138 kV network, and there are only two places in the system where the 138 and 230 kV networks are interconnected. A condensed one line is shown in Figure 7.

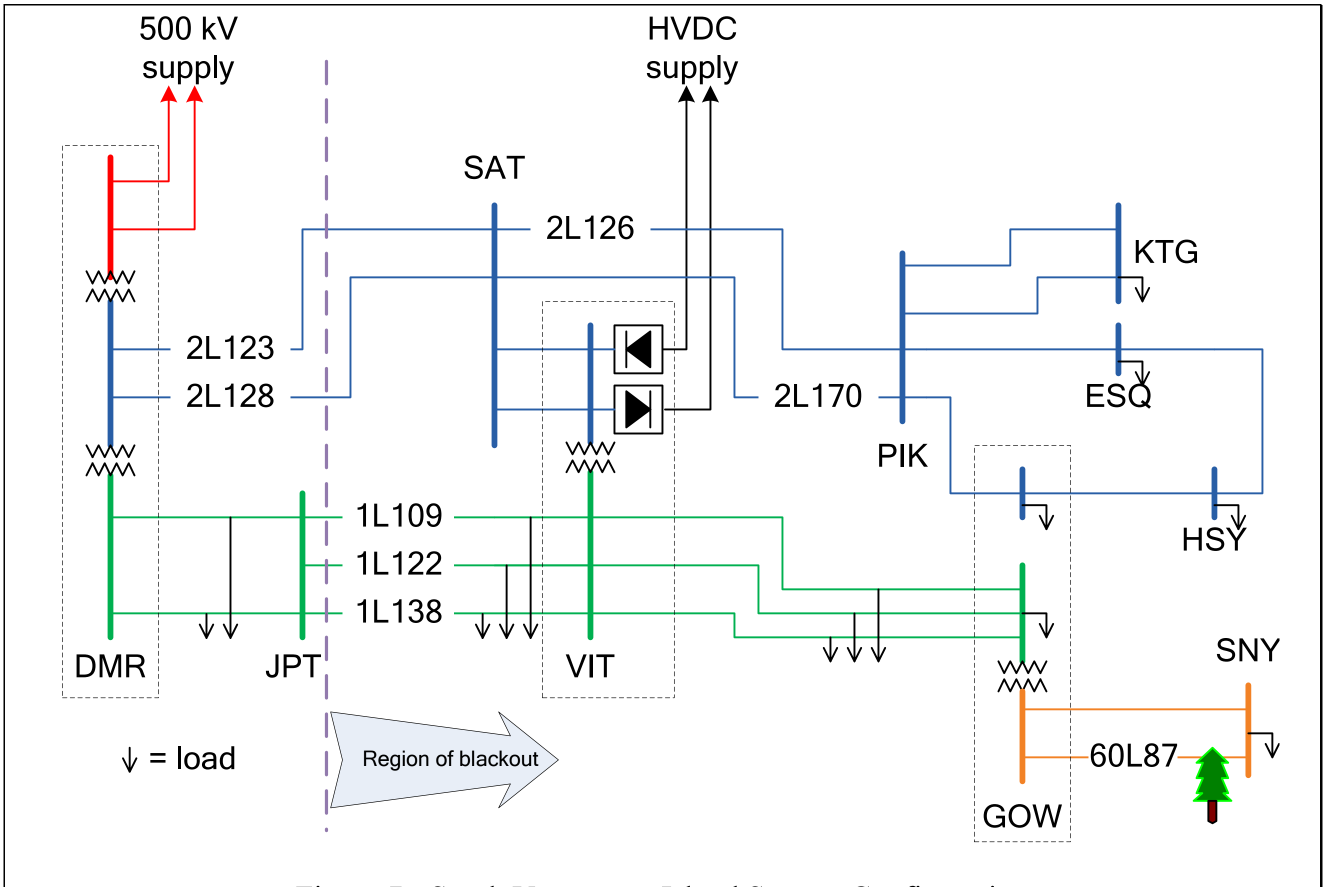

Figure 7 - South Vancouver Island System Configuration

On Oct 12, 2008, all load to the right of the dashed purple line (approx 700 MW) was lost as a result of cascading transmission outages caused by two protection misoperations in the 230 kV system triggered by a tree branch falling on circuit 60L87 [2].

The root cause for the escalation of this disturbance into a wide area outage was the unexpected misoperation of two critical protection systems on the two transmission lines (2L123 and 2L128) that form the backbone 230 kV supply to the SVI area. These two permissive overreaching transfer

---

[5] This particular outage is perhaps not a terribly good example of the variant of Murphy's law stated above. A better example was the station where both 230 kV lines feeding it false tripped due to excessively sensitive negative sequence directional elements coupled with system imbalance in the region. Setting revisions were proposed on a Friday afternoon, but not implemented in order that the calculations could be reviewed on the Monday. The protections misoperated on the Sunday, again dropping all customers fed from that station.

trip protection systems misoperated sequentially for different reasons. The loss of 2L128 by one problem triggered the subsequent loss of 2L123 by a different problem.

2L128 tripped first. This was caused by a setting error which resulted in incomplete coordination between the forward looking elements at DMR with the reverse looking elements at SAT.

When 2L128 tripped off line, 2L123 became more heavily loaded than it had ever been before (though still within rated capacity). Even though the protection on 2L123 was correctly set in accordance with our guidelines at the time, the unbalance in circuit 2L123 (caused by lack of transpositions combined with heavy load) resulted in an negative sequence voltages and currents that were sufficient to cause the sensitive forward looking directional elements at both terminals of the line to declare an internal fault and trip.

After both 230 kV lines tripped, the 138 kV circuits between JPT and VIT tripped on the ensuing power swing. The result was the complete loss of supply to South Vancouver Island.

Time (seconds)	Event	Cause
16:41:42.274	60L87 C-A fault inception	Fallen tree branch
+ 0.100	2L128 trip	DMR 2L128 SYPN misoperation for 60L87 fault
+ 0.133	60L87 fault isolated	Correct operation of 60L87 line protections
+0.377	2L123 trip	SAT and DMR 2L123 PN misoperation on internal unbalance caused by non-transposition
+0.852	1L109, 1L122, 1L138 trip	Line impedance PN operated on power swing (start of blackout)
+1.697	2L170 trip	SAT 2L170 SYPN misoperation during low frequency following separation
+90 minutes	All customer load restored	

Analysis

Post-disturbance analysis of the fault determined the initiating incident to be a phase to phase fault on line 60L87. The numerical stepped distance protection on the line at GOW substation detected the fault and tripped in 1.25 cycles. The breaker cleared the fault 6.75 cycles after that for a total of 8 cycles total fault clearing time. The event record for 60L87 is shown in Figure 8.

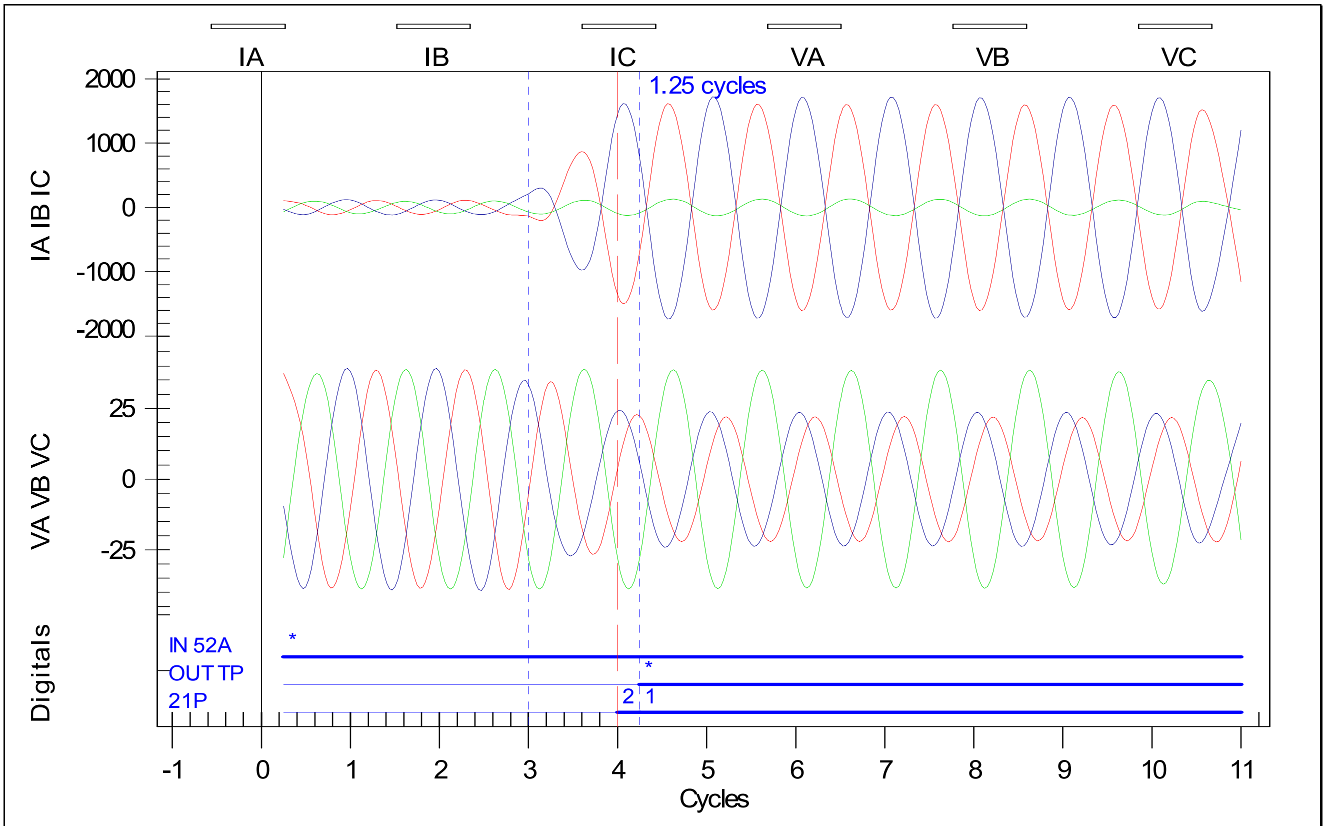

Figure 8 – 60L87 correct relay operation

However, the fault quantities were also seen by the 2L128 protections at both SAT and DMR terminals. The permissive overreaching transfer trip scheme used for 2L123 and 2L128 uses forward and reverse looking phase mho elements for multi-phase faults, together with negative sequence directionalized negative sequence overcurrent elements for unbalanced faults. A setting error at DMR terminal (DMR terminal had a different CT ratio, but negative sequence overcurrent elements at both terminals had the same setting in secondary amps) resulted in the DMR terminal seeing the fault in the forward direction, while SAT was not able to see it in the reverse direction. As a result of this, DMR keyed permissive trip, SAT reverse blocking elements failed to block the echo, and DMR tripped upon receipt of it's echoed permissive trip. In Figure 9, the 60L87 fault inception can be seen at approx 3 cycles. 67Q2 (the forward looking negative sequence overcurrent element) picks up at 3.75 cycles, resulting in the keying of permissive trip to the SAT terminal. At 6.25 cycles, the echoed permissive trip is received from SAT and the DMR terminal trips and keys DTT to SAT.

The event record from the SAT terminal is shown in Figure 10. Note that the reverse looking 67Q3 element does not pick up until the 2L128 breakers start to open. The absence of 67Q3 pickup allows the incoming permissive trip to be echoed after a 1.5 cycle delay. One cycle later, a DTT is received from DMR, indicating that DMR has tripped.

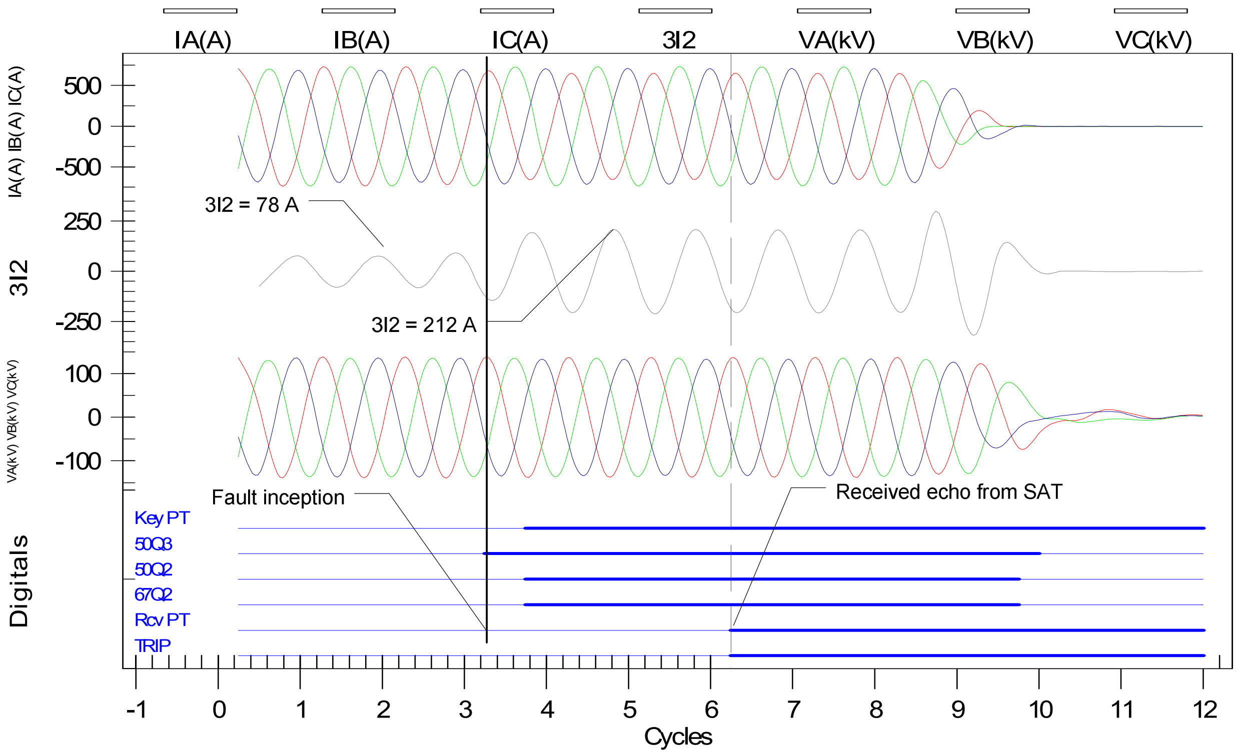

Figure 9 – DMR 2L128 Misoperation

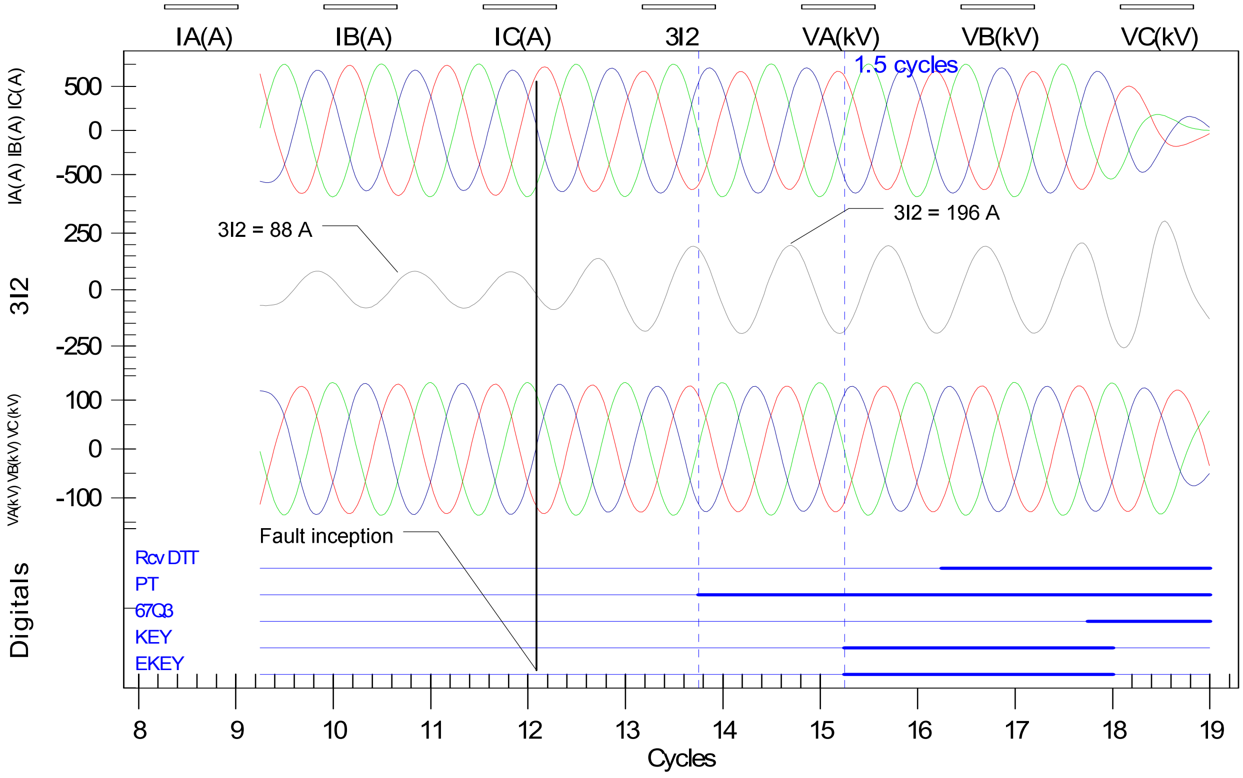

Figure 10 - SAT 2L128 failure to block

At DMR, because of the setting error, 50Q2 and 50Q3 (the level detectors in the negative sequence portion of the permissive scheme) were set at 200 and 132 pri A respectively. At SAT, 50Q2 and 50Q3 were set at 300 and 200 pri A respectively. In the event records above, the level of 3I2 after fault inception (approx 2.75 cycles into the fault record) is approx 212 A at DMR, while the SAT event record indicates 196 A of 3I2. The difference in measured I2 is reasonable, considering CT error, relay error and distributed negative sequence line charging current. However, this difference in measured I2, coupled with the setting error, caused the permissive scheme to fail to coordinate and the DMR terminal tripped after received echoed permissive from SAT.

After 2L128 tripped, the load on 2L123 essentially doubled. While the load current was still within the thermal rating of the line, it was higher than it had previously been. The extreme load current, coupled with the untransposed construction of the line, resulted in negative sequence voltage being induced across the line. This induced voltage then created a negative sequence current in the line. Akin to V0 reversals caused by zero sequence mutual coupling, the negative sequence voltages and currents in the line caused negative sequence directional elements at both ends of the line to indicate a fault in the forward direction. Once both ends had keyed permissive, the line tripped.

After 2L123 tripped, all SVI load previously fed via the 230-138 transformers at VIT was now solely connected to the DMR 138 kV bus (the HVDC supply at VIT was out of service). The load exceeded the transfer capability of the 138 kV lines and the three 138 kV lines between JPT and VIT tripped on their zone 1 distance elements as the power swing travelled through the lines, dropping all remaining load on the SVI system.

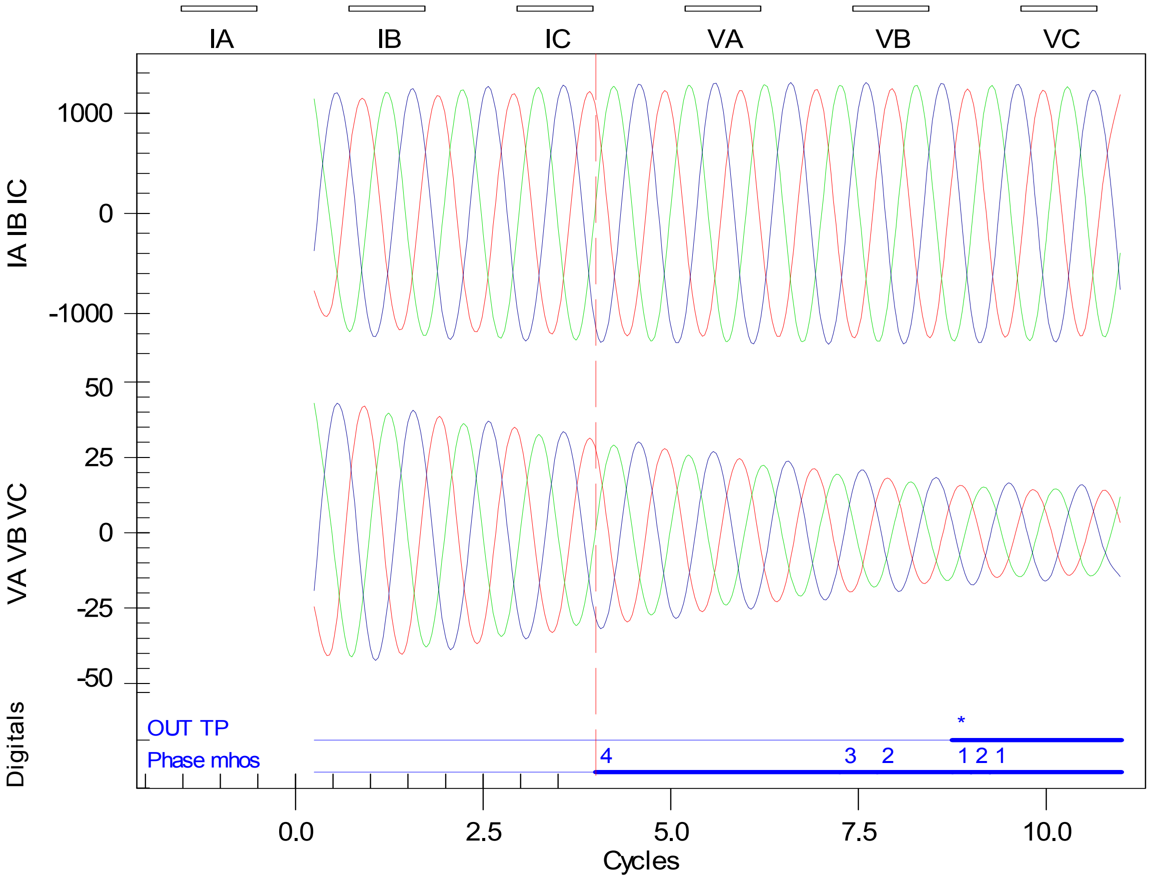

Figure 11 – JPT 1L109 Trip on Power Swing

All in all, 227,000 customers were without power for up to 90 minutes.

Lessons Learned

There are many lessons which can be learned from this outage, the first of which is "nobody appreciates it when you black out a quarter of a million customers who all have partially cooked turkeys in their ovens" (the outage occurred on the Canadian Thanksgiving holiday, just before 5 PM).

The value of consistency

The first misoperation was caused by a setting error in the negative sequence overcurrent elements in the DMR 2L128 relays. This was eventually traced back to an inconsistency between CT ratios in the two line terminals at DMR. 2L123, which had new protection installed first, had the protection connected to the CTs at a 3000-5 ratio. 2L128, which had new protection installed six months later, was connected to the CTs at a 2000-5 ratio. When generating the relay settings for DMR 2L128, the engineer started with the DMR 2L123 settings and accounted for the changed CT ratio in the distance and the phase and ground overcurrent elements, but missed revising the negative sequence overcurrent settings. While better review processes would also have helped to avoid this error, there is much to be said for leaving as little room as possible for error.

Continuous review of settings

The setting error in the 2L128 negative sequence directional settings was in service for 3 ½ years before the 60L87 fault provided the right conditions to make it misoperate. During this time period, two minor revisions were made to these settings by the author, who unfortunately, did not perform an in-depth review of all the existing settings before making his changes. If relay settings are kept in a database, automated tools exist which allow audits of various settings across the entire database with minimal human effort. After this outage, it was a simple matter to query the database and produce a report which showed that this was the only line which contained an error of this type. Every excuse should be taken to run these reports as a matter of course and investigate any discrepancies.

There's no such thing as a free lunch

Along with this outage, BC Hydro has been having a higher than normal number of problems with sensitive relay elements in numerical relays misoperating on load, system imbalance or out of zone faults. In most of these cases, the new numerical protection was set more sensitively than the electro-mechanical (EM) relaying that it replaced. There is a tendency to believe that modern numerical relays are vastly superior to older static or electro-mechanical relays and that the increased sensitivity and speed are a "free lunch", there to be consumed with impunity. What we are gradually learning is that:

1. In virtually all cases, older EM relays were sensitive enough. As part of the evolution of EM relays, the desire for increased sensitivity was balanced by the extra costs involved in making the relay more sensitive. This resulted in the relay designs eventually hitting a "sweet spot" where they were sensitive enough for most applications, but still robust, secure and as inexpensive as possible. Since extra sensitivity is essentially free in numerical relays, the onus now shifts to the protection engineer to ensure that this sensitivity can be used safely.
2. Those old guys knew what they were doing. We are occasionally recreating problems which were identified and solved 20 – 30 years ago by our predecessors. When replacing an older EM or static relay system with numerical relays, we occasionally see opportunities for "improvement" in the system. We are learning to go back and carefully read the previous

relay application and setting calculations to ensure that we are not inadvertently recreating traps that were carefully and thoughtfully removed in the past. This further emphasizes the importance of good documentation, especially that of documenting what you chose **not** to do, and why.

3. Positive and negative sequence elements are inherently transiently unstable. While the calculation of zero sequence quantities maps neatly to a corresponding process on data samples, the calculation of positive and negative sequence quantities requires that samples be converted to phasors before the calculation can be performed. Since phasors correspond to fixed phase, fixed frequency sine waves, the reliability of these calculations drops during transient events on the power system (like fault initiation). Allowing these quantities to stabilize before using them is highly recommended.

Inadequate modeling of the system

Protection engineers live and die by their system models. Any discrepancy between the response of the system and the response of the model will result in the in-service relays not responding the way the engineer intended. In this disturbance, the internal negative sequence quantities generated by the load current through 2L123 were not accounted for when the settings were calculated, with catastrophic results.

Unless transmission lines are properly transposed, positive sequence load or fault current through the line will result in zero and negative sequence quantities being generated within the line. The mathematical process for deriving the coupling coefficients are given in the EPRI red book[3], as well as the paper "Introduction to Symmetrical Components", by Zocholl and Schweitzer[4]. Due to the non-zero off-diagonal elements in the sequence impedance matrix, imperfectly transposed (or untransposed) lines will have negative and zero sequence voltages induced along them due to positive sequence current flowing through them. These voltages will then drive negative and zero sequence current flows through the line. The important thing to note is that because the voltage source is **inside** the line, directional elements at both ends of the line will tend to see these quantities as a forward fault.

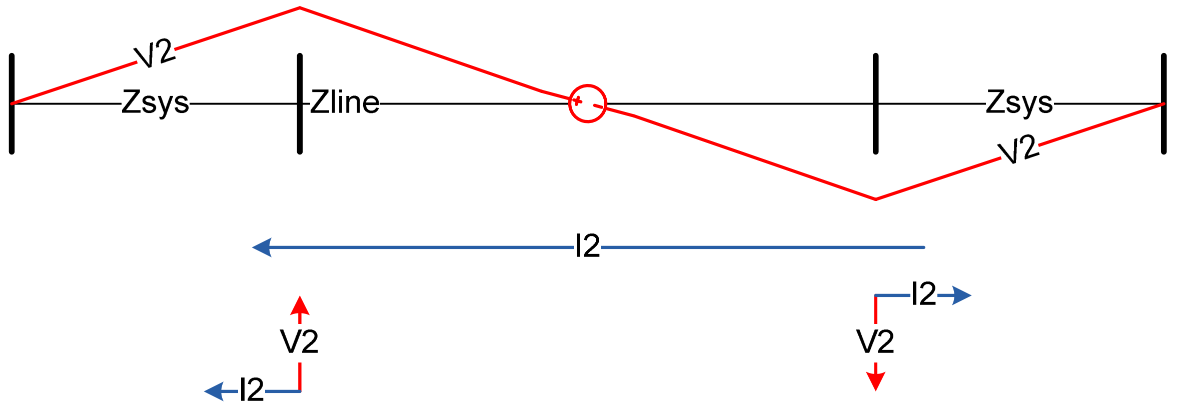

Figure 12 - Negative sequence directional elements operate for internal unbalance

In order to prevent directional elements from misoperating on internal imbalance caused by lack of line transposition, one can either block the elements when the negative (or zero) sequence current is below the maximum induced imbalance current[6], or block the directional element when the ratio of I2 (or I0) to I1 is less than a particular value. Use of the second method allows better sensitivity at lower load current levels.

As a result of this outage, we were forced to calculate the expected ratio of I2/I1 for all our line protections. A MathCAD spreadsheet was built to calculate Z_{22}/Z_{11} directly from line geometry data. It was determined that Z_{22}/Z_{11} is typically < 10% for non-bundled lines and that Z_{22}/Z_{11} < 12% for bundled conductor lines.

Downtown Vancouver Outage 2001/01/26

Event Summary

On Jan 16, 2001, the core of downtown Vancouver was blacked out after a sequence of improbable events, protection misoperations, miscoordinations and bad karma resulted in source outages to the three major distribution substations that supply the downtown area. Approximately 100,000 customers were out of power for between 1 and 3 hours[5].

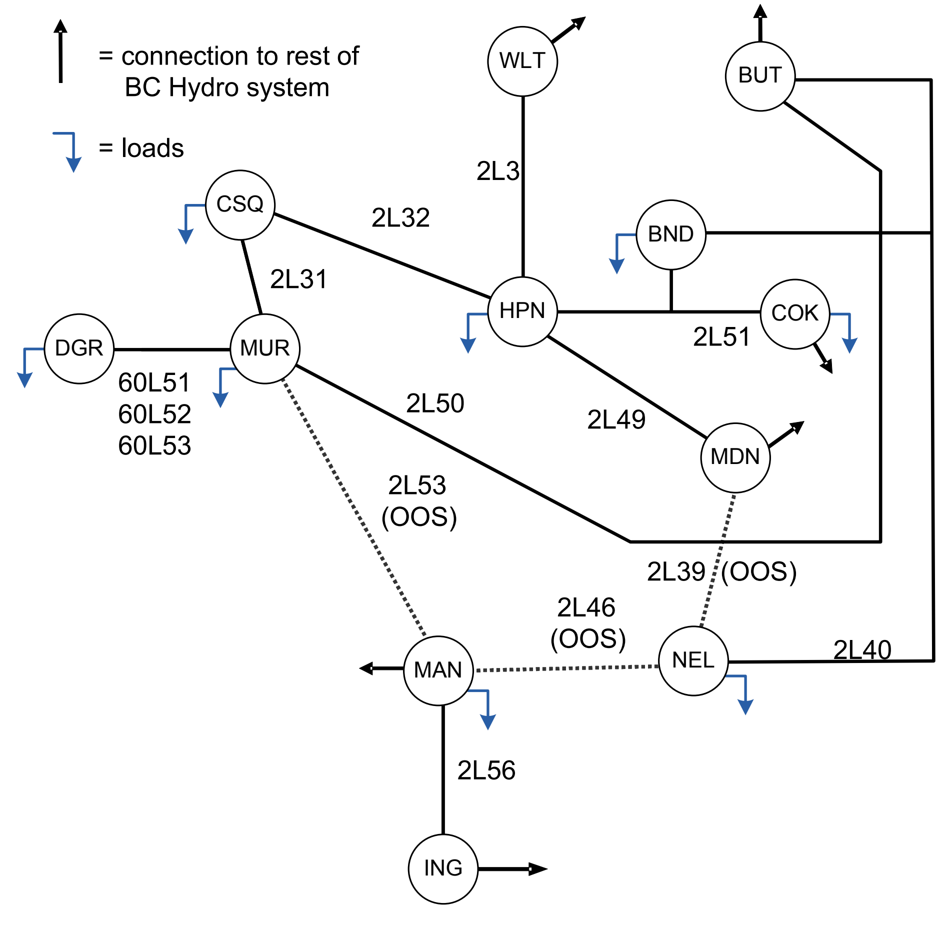

Figure 13 - Vancouver System Configuration Jan, 2001

---

[6] This is for load conditions only. It is assumed that during fault conditions, that the fault quantities will swamp any imbalance due to load.

Analysis

On Jan 16, 2001, switching was in progress to return line 2L51 to service after repairs. At the time of the switching, lines 2L53 and 2L46 were out of service, and line 2L39 had been recently decommissioned.

As part of the switching sequence, 2L51 was energized from the COK side, then line disconnect 2D24 at HPN substation was closed remotely. When the disconnect was closed, B phase of the disconnect broke at the hinge end and dropped into the grounded support structure. This did not cause an immediate fault, as the circuit was open on the energized side, and not yet energized on the faulted side. When the first circuit breaker at HPN was closed to put the line in service, it resulted in a bolted B phase to ground fault.

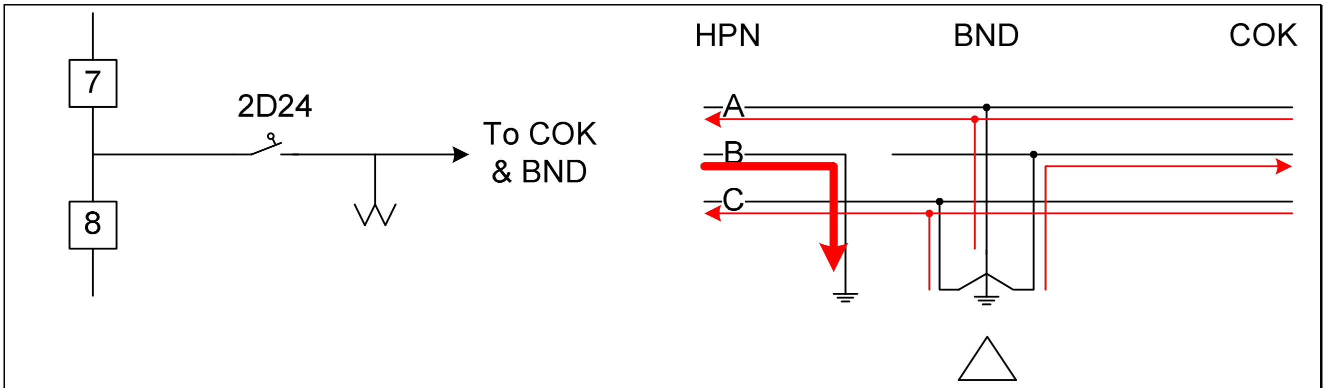

Figure 14 - HPN 2L51 configuration and fault current flows

The initial fault record from HPN is shown in Figure 15. The nature of this fault (combination of open phase plus short circuit on a line with tapped load which was energized from the remote end) acted to allow this fault to go undetected by many of the standard schemes that protection engineers apply. A high set ground instantaneous overcurrent trip was not applied at HPN due to coordination difficulties (being a fairly short cable circuit, the fault levels do not change much over the length of the line) and ground mho elements were not applied since that vintage of relay did not have those elements. Since the fault was undetected by local protection schemes, it would have been expected that the permissive scheme would quickly clear the fault. However, due to the open circuit on B phase at HPN and infeed via a tapped station on 2L51 (BND), the negative seqeunce directional element on the COK end of the line saw the fault in the reverse direction (ref Figure 17) and blocked operation of the permissive scheme.

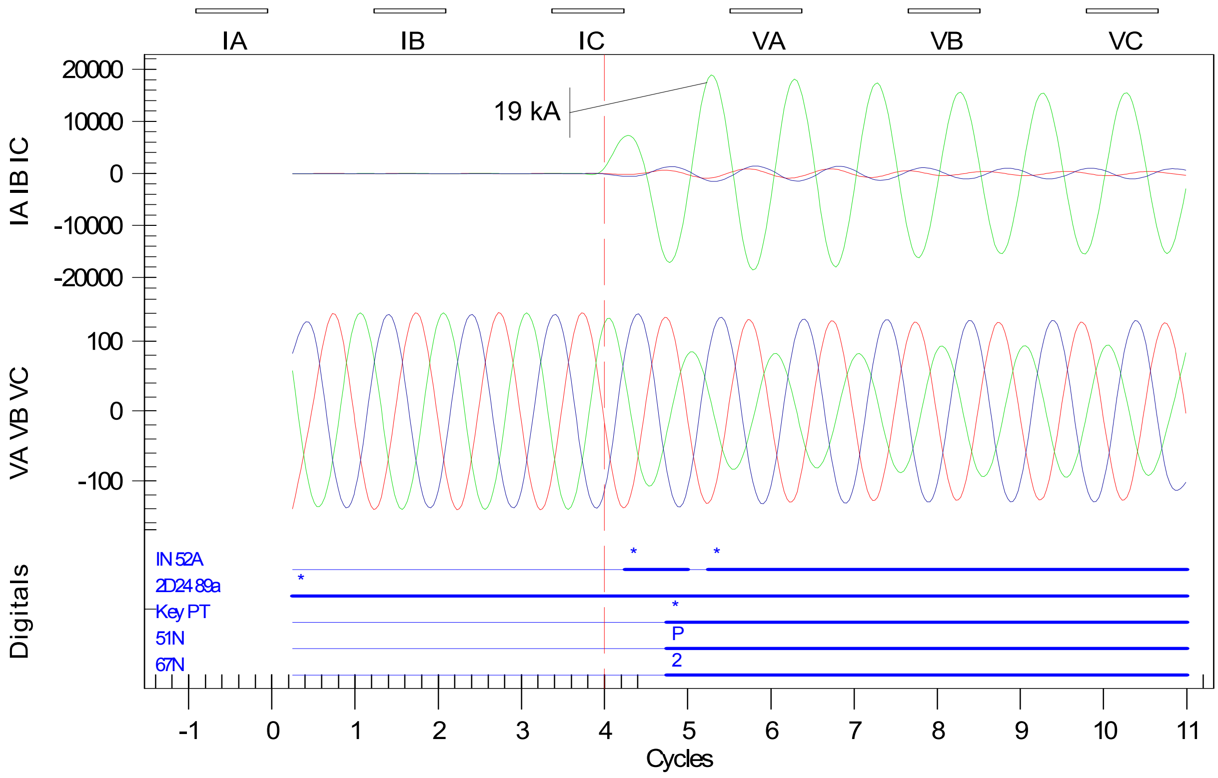

Figure 15 - HPN 2L51 Event Record (fault initiation)

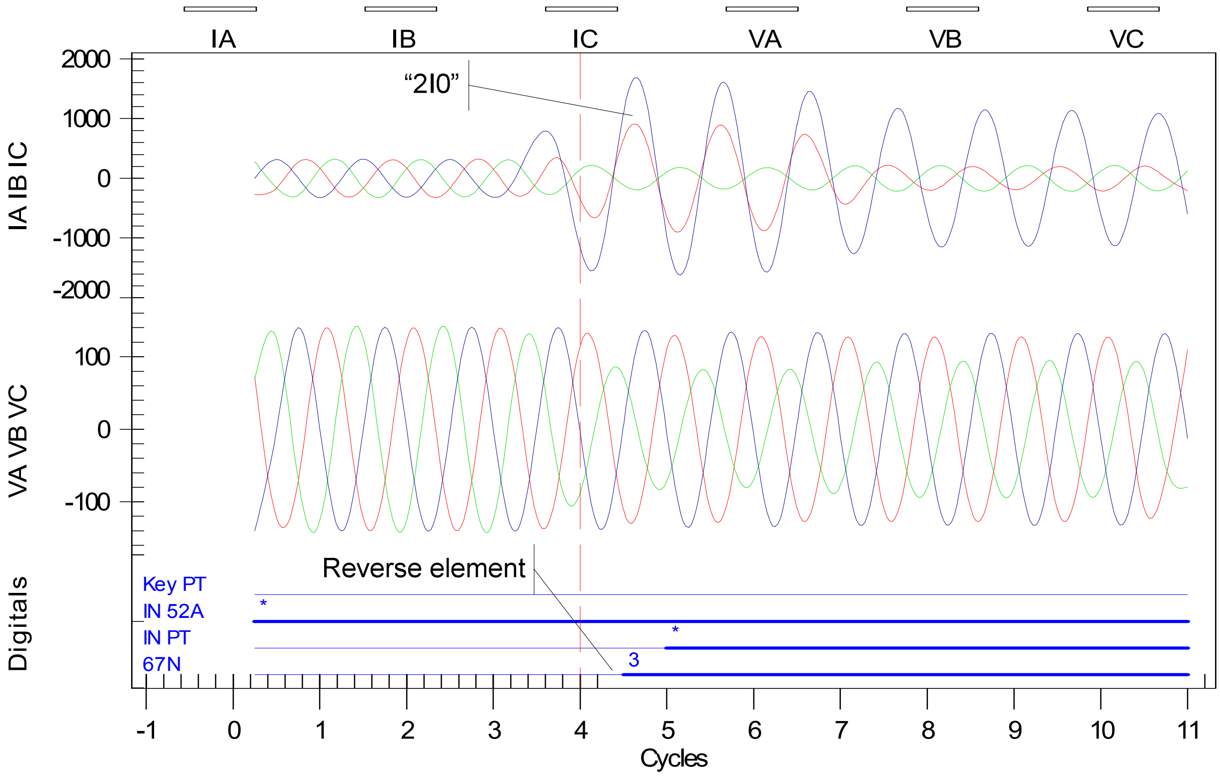

Figure 16 – COK 2L51 Event Record

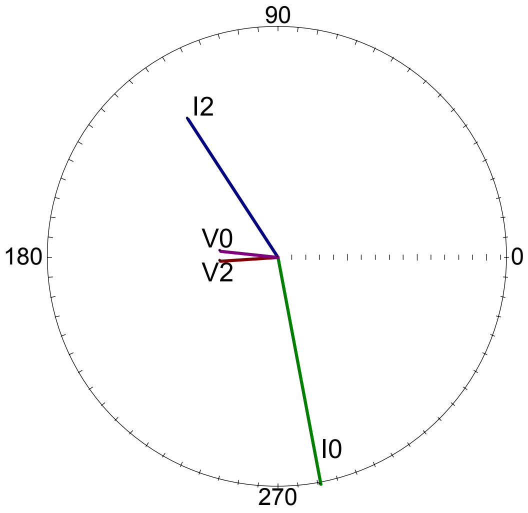

Figure 17 - Sequence phasors at COK terminal of 2L51

At this point, fault clearing was left to the inverse time ground overcurrent element at HPN. However, while this element was timing out, a number of other protections misoperated. The first misoperation was at the MDN terminal of 2L49, where a failed permissive trip tone receiver had resulted in the MDN 2L49 standby protection receiving a constant permissive trip. This terminal was able to see the HPN fault in the forward direction, so as soon as the forward elements picked up, the relay tripped.

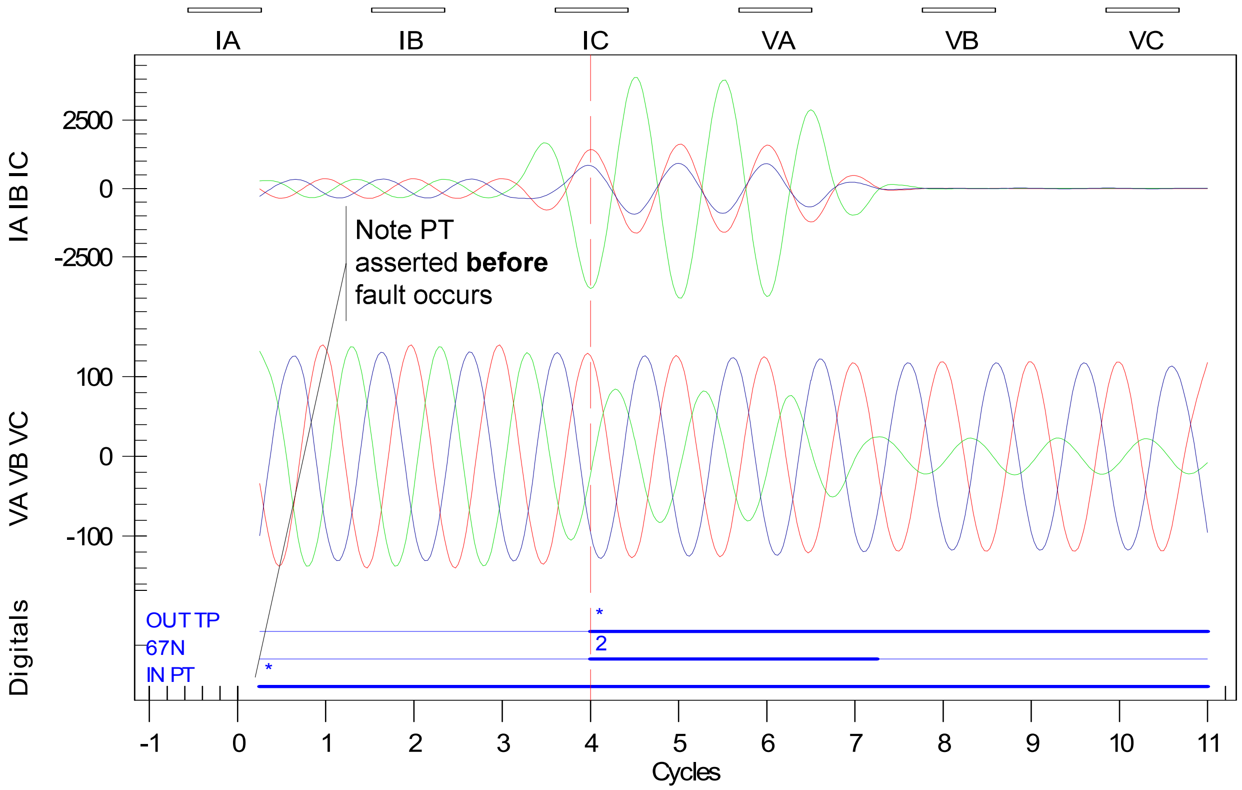

Figure 18 - MDN 2L49 Failed Permissive Trip Receiver

Due to poor coordination in the region, three surrounding inverse time ground overcurrent elements miscoordinated with the HPN 2L51 inverse timed ground overcurrent element. These three relays were at WLT 2L3, MUR 2L31 and CSQ 2L32 terminals. Due to these miscoordinations, all supply was lost to CSQ substation. Within one cycle of 2L32 tripping, the phase comparison protection on 2L50 also misoperated for an unknown reason, causing a source outage to MUR and DGR substations. Finally, 521 ms after fault inception, the inverse time ground overcurrent element at HPN operated to finally clear the fault.

Restoration was delayed due to an operating trap at CSQ substation (upon loss of CSQ supply, the station service had switched over to the backup supply which was fed from MUR. However, MUR was also deenergized, and there was no automatic return to the CSQ supply, so that when CSQ was reenergized, all transformer protections tripped and locked out due to lack of cooling). In addition, a cable circuit was damaged during the fault (an oil supply line was installed too closely to the pipe enclosing the cable and arcing between the two during the extended fault caused an oil leak).

Lessons learned

The value of monitoring

The 2L49 outage (failed permissive trip tone receiver) highlighted the value of monitoring equipment. One of the outcomes of this outage was the creation of a “Standing incoming permissive trip” (incoming permissive trip asserted for more than 1 minute) alarm in numerical relays which were capable of performing this logic. Over the years, more and more items have been added, with the result that now we monitor standing permissive trip (on permissive schemes which still use tonegear), high levels of voltage or current imbalance, breaker or line current which disagrees with breaker or line disconnect status, as well as individual open poles in breakers (excessive 3I0 in the breaker with balanced currents in the line).

Preparing for the n^{th} contingency

We typically consider first or second contingency situations when planning our power systems. In this case, note that it was the **eighth** contingency (2L39, 2L46 and 2L53 out of service, the failed disconnect at HPN, the permissive trip tone receiver at MDN, bad ground coordination at CSQ and MUR and the misoperation on 2L50) which caused the majority of the load loss. These kind of scenarios are beyond our ability to predict, model or plan for. Knowing this, how should this knowledge affect our actions? In the case of the ground relay miscoordination, it was recognized that the area was poorly coordinated, and studies had been performed, but the revised inverse time ground settings had not been issued because “it’s a second contingency, so we will reissue the relay settings as we make other changes in the area.” The cost savings most of the time are easily forgotten, but the embarrassment of contributing to a major blackout isn’t.

Hidden failures

This outage provides a beautiful example of how hidden failures contribute to major outages. Since we design our power system to withstand all first (and many second) contingencies, it can be assumed that whenever an outage of this magnitude occurs, it will be due to a 3rd or higher contingency. The problem is that whenever an outage of this magnitude occurs, many of the contingencies will have been unknown at the time of the event. A very good summary is provided in the document How Complex Systems Fail, by Richard I Cook[6]. This document, and the accompanying A Brief Look At The New Look in Complex System Failure, Error, Safety and

Resilience[7], while aimed primarily at the medical field, are quite salient to power system engineers. The first five points in "How Complex Systems Fail" are so directly applicable to protection engineers that I have quoted them below:

a) Complex systems are intrinsically hazardous systems. If the consequence of failures of the power system were trivial, we wouldn't have invested so much engineering effort and redundancy to make it robust.

b) Complex systems are heavily and successfully defended against failure. We apply multiple layers of protection (physical, and operational) in order to maintain reliable service. A good visual analogy would be to consider each layer of protection as a shield which may have a number of holes in it. Each layer of protection by itself does not provide perfect protection, but the combination of multiple layers of protection provides very robust protection.

c) Catastrophe requires multiple failures – single point failures are not enough. Because we do not want the power system to fail, we provide protection. Acknowledging the imperfect nature of our defenses, (and because NERC says we must) we apply multiple layers of protection. Since we design to withstand single failures, it obviously will take more than one failure to take us down.

d) Complex systems contain changing mixtures of failures latent within them. Murphy is alive and well. Nature fights to increase entropy and we fight to undo the damage that Nature does. To continue with the shield analogy, not only are holes constantly appearing in our shields and being patched, but as we operate the system differently, different holes are exposed to external threats.

e) Complex systems run in degraded mode. Since the power system is large and has high levels of redundancy, it can almost be guaranteed that there are failures and deficiencies within the power system that we are not aware of.

Figure 19 illustrates the interplay between Nature, which is constantly throwing contingencies (event triggers) at us from all angles, and our constantly changing, constantly failing defenses.

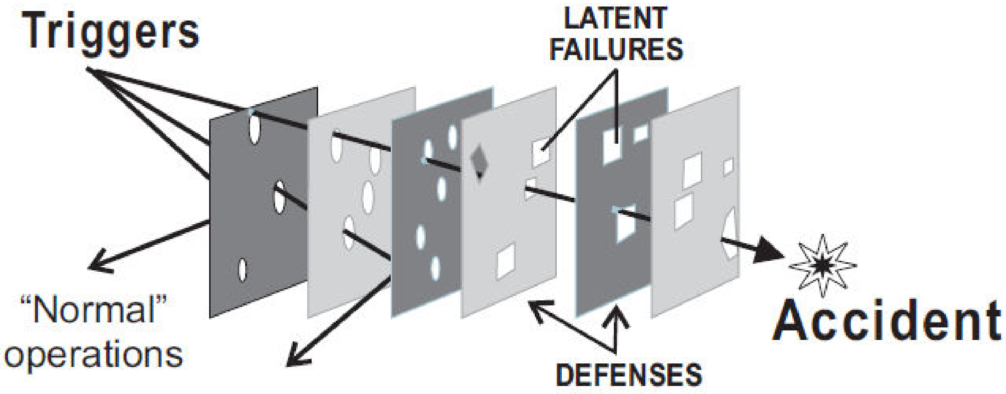

Figure 19 - The role of hidden failures

Vancouver Island Separations and UFLS

Event Summary

Vancouver Island has historically been generation deficient. System reinforcement from the mainland has come in 1956 (2 x 140 MVA 138 kV cables), 1967 (312 MW HVDC), 1977 (476 MW HVDC), 1983 (2 x 1200 MVA 500 kV cables) and most recently in 2008 (1 x 650 MVA 230 kV cable). A new combined cycle generating plant (ICG – 290 MVA) was also added on the Island in 2000. Between the years of 1996 and 2002, there were 5 double circuit 500 kV outages which resulted in islanding of Vancouver Island and associated underfrequency load shedding. In this section we will explore the frequency response of the Vancouver Island system during four of these incidents.

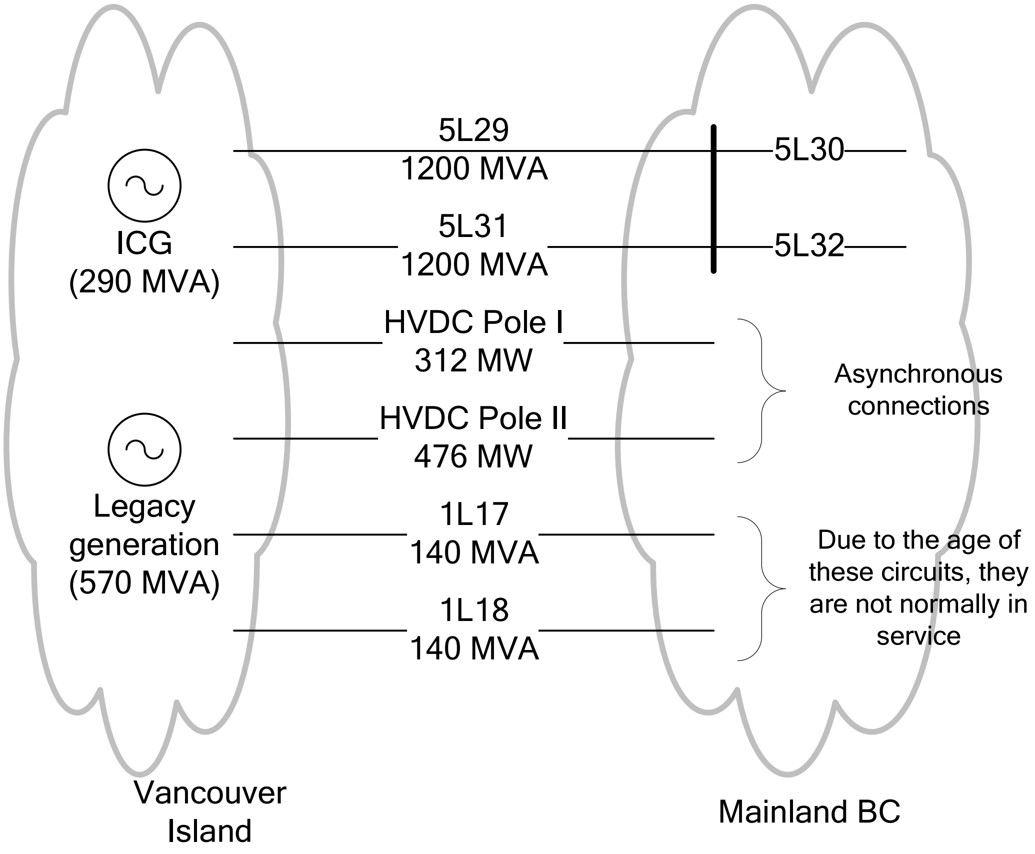

Figure 20 - Vancouver Island Generation and Supply

Analysis

1999/08/03

The 1999 Vancouver Island separation was initiated by a lightning storm which passed through the southern portion of mainland British Columbia. In the eight hours previous to the outage both 5L30 and 5L32 had tripped out and reclosed at different times due to lightning strikes. At 8:02 AM on Aug 3, 1999, 5L32 suffered a 3LG fault. As the last phase of 5L32 cleared, an A-G fault developed on 5L30. Both events were most likely due to a lightning strike to a tower in an area with high ground resistance, which allowed the ground potential to rise high enough to backflash to the line itself. Since both parallel circuits had tripped 3-pole[7] simultaneously, the two systems (Vancouver Island and the mainland) were out of synchronism and a reclose was impossible (loss of 248 MW). Due to the extreme voltage dip caused by the initial fault on 5L32, both HVDC converters blocked for 300 ms before restarting (loss of an additional 542 MW).

With the loss of the tie to the mainland and the HVDC temporarily out of service, we were left with 1068 MW of load connected to 278 MW of hydro generation. The frequency on the island began to drop at approx 4.9 Hz/sec and dropped to 57.7 Hz 6 cycles after the HVDC restarted. By this point, underfrequency load shedding had shed more than 248 MW (the generation deficit from 5L30/32), so at this point, the frequency began rising. Once the frequency hit 65 Hz, half of the HVDC and two synchronous condensors at VIT were tripped on overfrequency. The reduction of import power, resulted in the frequency stabilizing near 61 Hz. At 8:06, a fault on the AC system in the lower mainland near the HVDC rectifier terminal resulted in the temporary blocking of the other half of the HVDC and more underfrequency load shedding. When the HVDC restarted, the frequency rose up above 66 Hz and another synchronous condenser was tripped on overfrequency. The operators were restoring load to bring the island frequency down, but as they approached 61 Hz, another AC fault occurred near the HVDC rectifier terminal, resulting in another temporary block of the HVDC, and another round of underfrequency load shedding. Finally, the operators were able to restore frequency to near nominal and resynchronize Vancouver Island to the mainland.

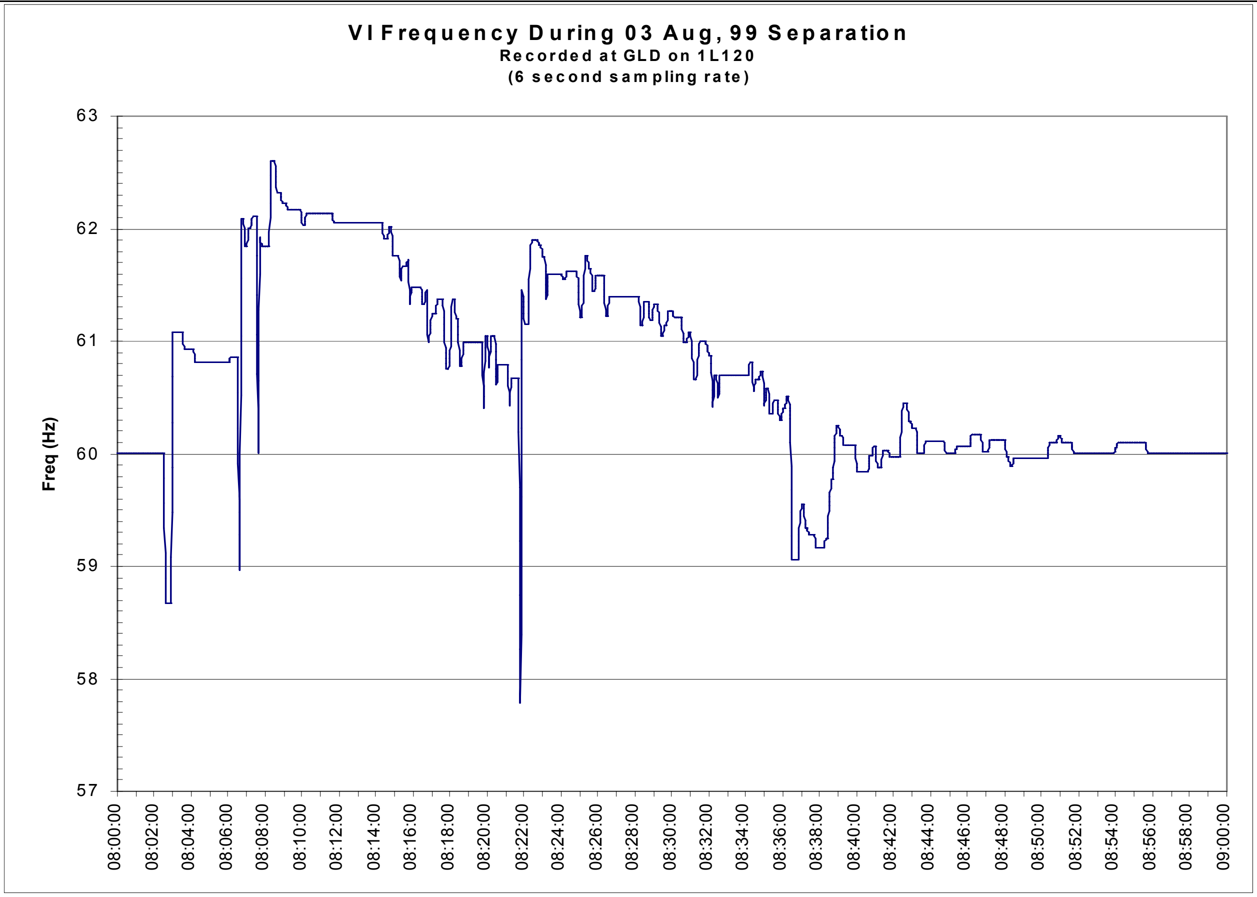

Figure 21 - Frequency trace for 1999 VI separation

---

[7] One interesting side effect of these 500 kV double circuit outages was the acceleration of the approval of the business case for adding of single pole tripping and reclosing to these circuits.

2001/12/15

On Dec 15, 2001, another storm system rolled across the southern part of the mainland of British Columbia. At 1:06 AM, insulator flashovers on one of the HVDC circuits resulted in that part of the HVDC being taken out of service. At 3:43 AM, one of the 500 kV circuits tripped out due to icing on the insulators and was returned to service 18 minutes later. Three minutes later, the line tripped out again, and remained out of service for the next 8 ½ hours. Eighty minutes later, the second 500 kV line tripped out (again due to insulator icing), severing the synchronous tie between Vancouver Island and the mainland. Because of the higher fault impedance of the insulator icing, the remaining HVDC link did not block, and the frequency declined at approx 1.4 Hz/sec. Underfrequency load shedding operated, but again overshed, and the frequency rose to 62.5 Hz, at which point the thermal generating plant on the island tripped on overfrequency, which triggered another round of underfrequency load shedding. After this, the frequency was reasonably well behaved until the operators could resynchronize with the mainland.

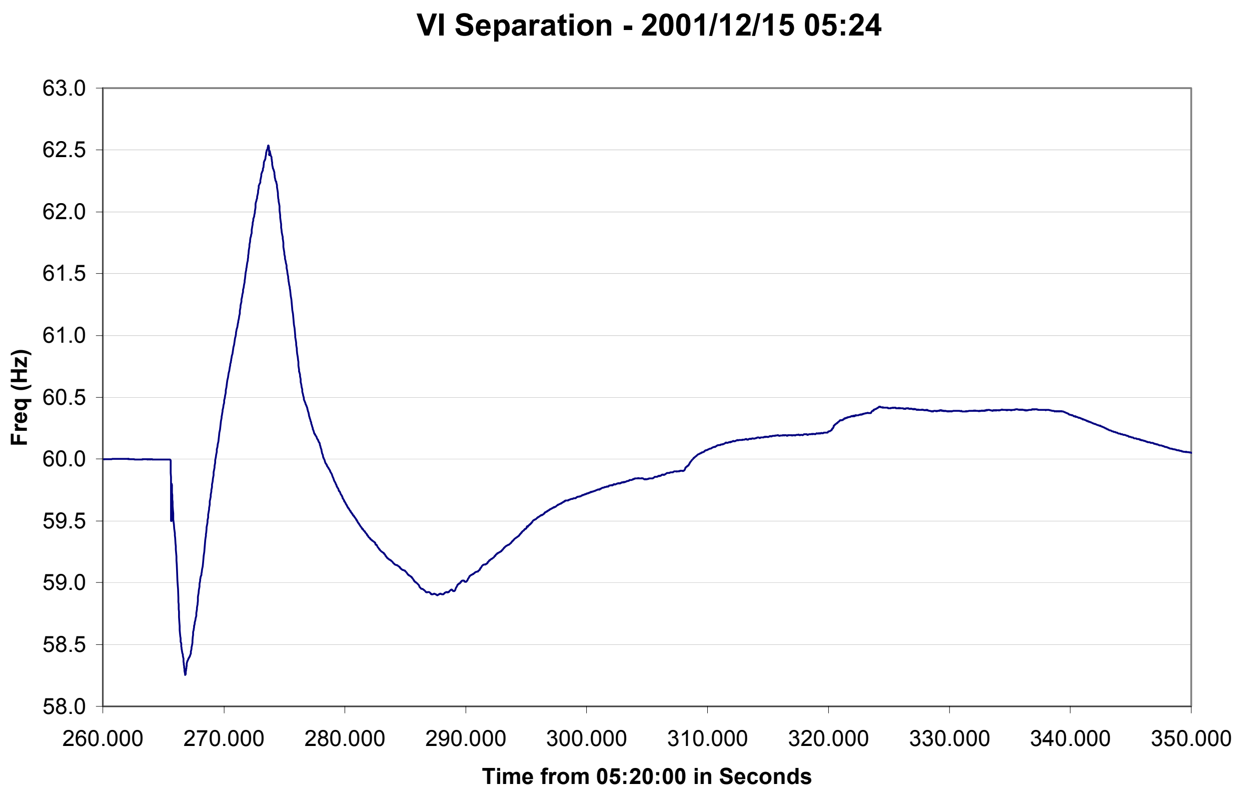

Figure 22 - Frequency trace for 2001 VI separation

2002/12/26

The Dec 26, 2002 Vancouver Island separation was perhaps the most spectacular in terms of frequency deviations. At the time of the event, 5L32 was out of service, due to a mudslide which had damaged six towers two weeks before the event. At 12:02 PST, circuit 5L30 tripped as a result of a flashover to a tree. The lack of clearance was caused by an extreme increase of conductor sag between towers due to an unequal ice loading on the conductors in adjacent spans. At the time 5L30 tripped out, the island load was 1567 MW, of which 372 MW was being fed via 5L30. The loss of import power resulted in the frequency dropping to 58.5 Hz before UFLS could drop enough load to arrest the frequency decline. By this point, 457 MW of load had been shed, so the frequency rose to 62.1 Hz, at which point ICG tripped on overfrequency. ICG output at this time was 220 MW. The frequency then dropped to 58.2 Hz before 277 MW of load was tripped via UFLS. With the largest source of rotational inertia on the island now offline, the frequency rose quickly to 64.5 Hz, at which point half of the HVDC was tripped on overfrequency. This resulted in the loss of 220 MW of import. One more round of UFLS (82 MW) ensued before the island frequency could stabilize at a point above any unoperated UFLS and below any unoperated overfrequency tripping.

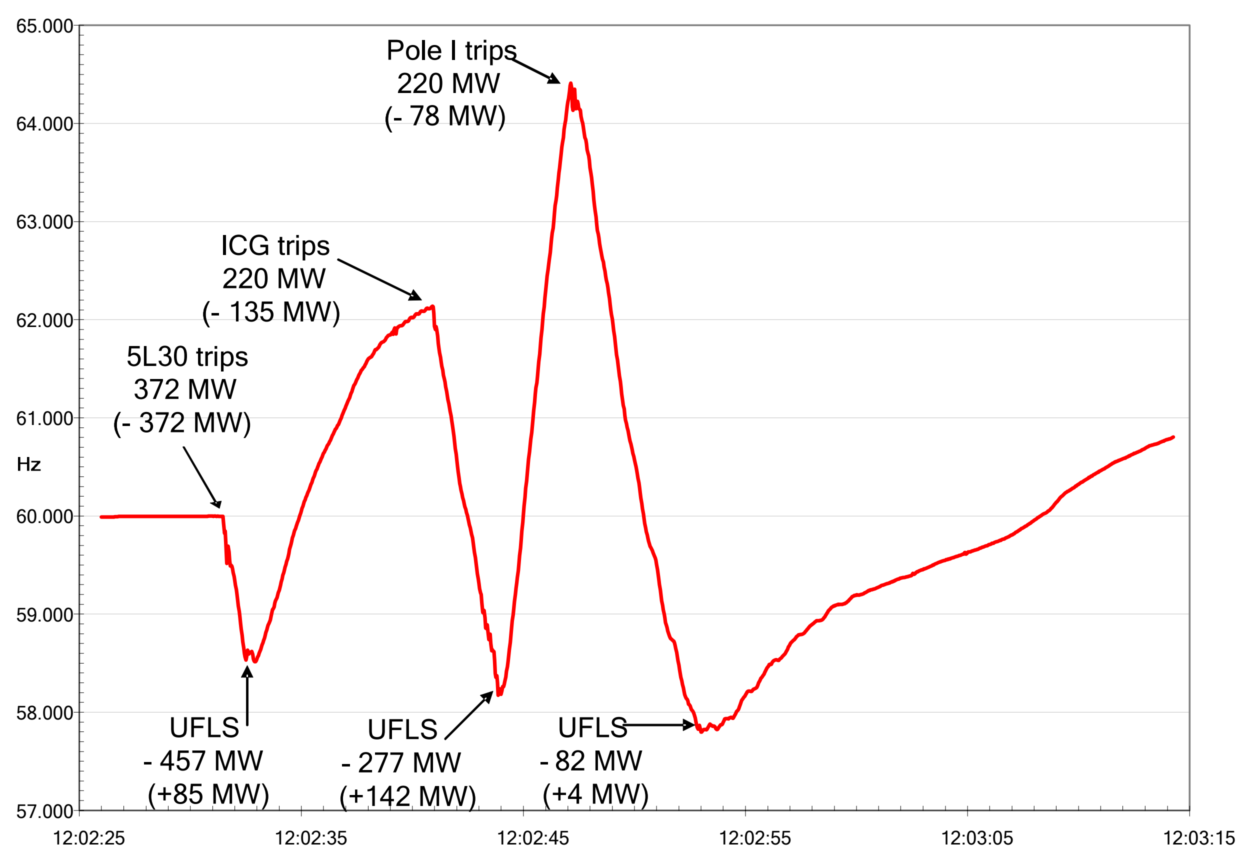

Figure 23 – Dec 2002 Separation (do not attempt this at home…)

2003/03/22

By the time of the most recent Vancouver Island separation, numerous improvements had been made to the Vancouver Island system. The underfrequency load shedding settings on the island had been re-coordinated, overfrequency restoration had been added to some of the feeders tripped by UFLS, a frequency control mode had been added to the HVDC, many line insulators were replaced, overfrequency tripping of the HVDC was staged to reduce the amount tripped off at a given frequency, and overfrequency tripping of the thermal plant was moved to a higher frequency.

On March 22, 2003 at 06:50:44.916 PST, simultaneous high-impedance A phase to ground faults appeared on 5L30 and 5L32. These faults were cleared by the line protection in 7.5 cycles.

When 5L30 and 5L32 tripped, the frequency on VI began dropping at an average rate of 5 Hz/sec. Underfrequency load shedding operated to arrest the frequency decline. The frequency had started to recover at approx 57.2 Hz, but just after the frequency started rising, one radially connected hydro generator (JOR G1) was lost due to its associated line protection tripping on a power swing. Two more stages of underfrequency load shedding then operated before the frequency decline was finally arrested at 56.6 Hz. The HVDC frequency control then dropped 80 MW of import power to relieve the overfrequency

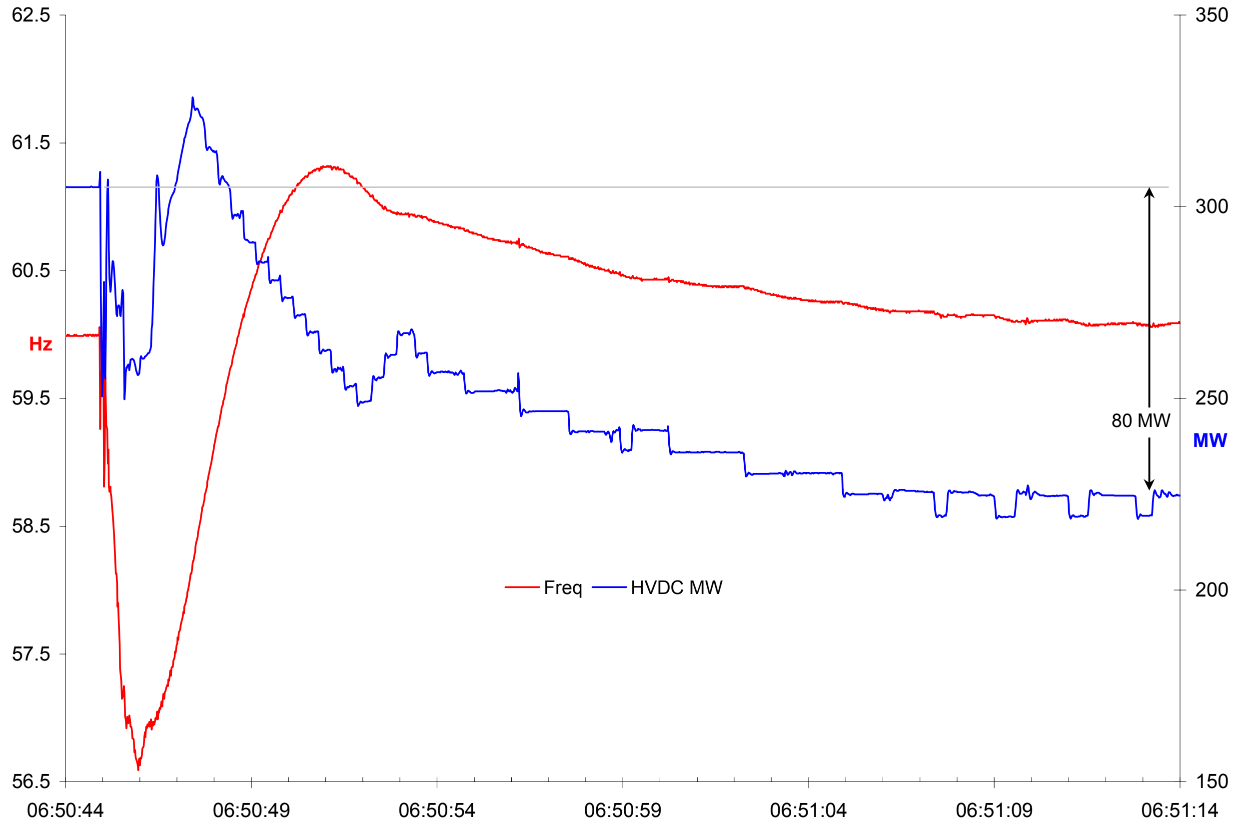

Figure 24 - Effect of HVDC Frequency Control

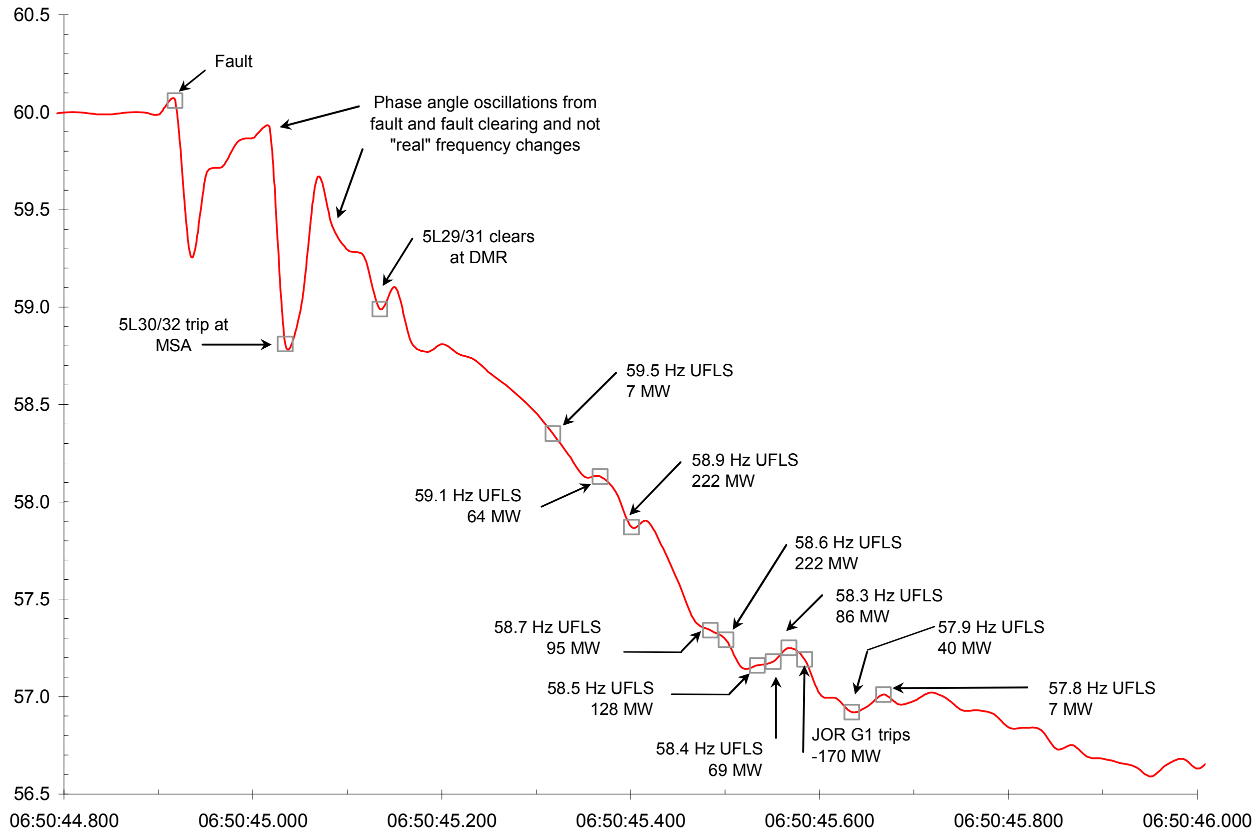

Figure 25 - Frequency trace for 2003/03/22 VI separation with UFLS and other protection operations

Lessons Learned

Underfrequency load shedding setup

WECC (and other regional reliability organizations, or RROs) provides criteria for the setup of underfrequency load shedding (UFLS) which all utilities must conform to. These criteria are designed to keep the interconnection as a whole from exhibiting a frequency collapse after a sudden loss of generation in the area. The RRO does not mandate how this underfrequency load shedding is to be distributed within a utility, nor does compliance with these criteria ensure that islanded areas **within** the utility will not suffer from a frequency collapse. When there are credible "islands" that can form within a utility, it is the responsibility of the utility to study these islands and allocate UFLS accordingly within the island. The allocation of UFLS in the Vancouver Island region is made more complicated by the following factors:

1. Very high ratio of import power to load. In the 1999 incident, approximately 75% of the Vancouver Island supply was lost simultaneously. This results in fairly high dF/dt. Normal time delays which are applied to UFLS in order to make them more secure then result in the UFLS effectively operating at a lower frequency (in the 2003 event, UFLS stages were tripping up to 1.2 Hz below the setpoint at which the relays themselves operated).
2. Hidden coupling between the 500 kV and HVDC systems. Bolted faults on the 500 kV system tend to reduce voltage levels at the HVDC converter terminals below that required

for proper commutation. The HVDC controls respond by blocking the converters temporarily until the voltage recovers. This behaviour has worsened the situation a number of times by reducing power import during the initial load shedding, then restoring that import after UFLS has operated, exacerbating the mandated underfrequency overtripping.

3. Overfrequency tripping. Tripping of HVDC or generators while overfrequency makes sense from a general point of view, but once UFLS has overshed, the remaining system tends to be fairly small, and overly sensitive to loss of import power. Therefore, one should tend to take a gentle hand with overfrequency tripping, while still protecting rotating machines from excessive overspeed.
4. Low system inertia. The HVDC makes no contribution to system H. The machine on the island with the highest H is a thermal plant which does not have extensive overspeed withstand capability, and therefore has to have overfrequency tripping. As generators and synchronous condensors are lost, the system becomes more and more sensitive to load/generation imbalances and will react faster and faster to these imbalances.

Once things start going bad in a situation like this, they tend to get worse. Every round of underfrequency loadshedding that operates results in the frequency needing to drop lower before the remaining UFLS can take any action. Overfrequency tripping of generators reduces system inertia and makes the frequency slew faster for a given imbalance. It may be very difficult to achieve desired behaviour via the typical "open loop" distributed control system that we create out of UFLS and overfrequency tripping.

Value of good monitoring for post analysis

In order to tune the behaviour of the UFLS in a given island, it is important to model the system correctly. However, one only knows that their model is good if the behaviour of the model can be compared to reality. In the 1996 outage (not discussed in this paper), frequency was measured by measuring the distance between zero crossings on paper oscillographs. In 1999, COMTRADE data from DFRs was post-processed in Excel to again measure time between zero crossings, supplementing low speed data archived from the SCADA system. By 2001, both high-speed digital meters and phasor measurement units were in service, providing data that could be used to validate system models.

Modeling Errors

Description

As mentioned before, protection engineers live and die by their data. The following story can be considered a "near miss".

The case of the mobile substation

HNY substation was put into service in Dec 2006. The substation was built under an EPC (Engineer, Procure and Construct) contract with an external engineering company. As the substation was to be looped into two existing 60 kV transmission lines, BC Hydro provided the line protection setting revisions at the two remote stations, as well as basic line protection settings for the four new terminals of line protection at HNY. The impedances of the four line sections were calculated based on the known impedance of the two lines, plus the reported location of the new substation.

Figure 26 - HNY Substation

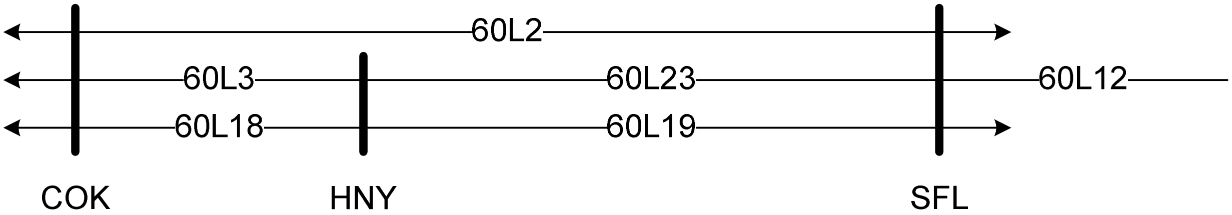

Figure 27 - Simplified One-line of HNY area

About a year later, the extension of a transmission line that terminated at one of the remote substations (60L12) necessitated the recalculation of 60L19 zone 3 distance elements at HNY (used as backup for remote breaker failures). During these calculations, it was noticed that the official "as-built" impedances of 60L19 did not match the numbers used in the original line protection calculations. This triggered a review of all line impedances in the area, with surprising results.

Line	Error in positive sequence impedance (Z1)
60L2	0 %
60L3	-15 %
60L23	+19 %
60L18	-12 %
60L19	+17 %

New line protection settings were hastily calculated for all eight line terminals.

Other common modeling problems

1) Zig-zag transformer windings modeled as delta. This can often be a "good enough" approximation, however, the zig-zag transformer is a weak zero sequence source, which

may need to be accounted for in systems where sensitive ground fault protections are applied.

2) Ungrounded Y connected transformer windings modeled as grounded Y. With the majority of Y connected transformer windings being grounded, this can be an easy error to miss. Similarly, impedance grounded transformer can be modeled with the wrong impedance (remember that 3 x Z_g goes into the zero sequence network) or no impedance at all.
3) Unaccounted fault current sources (motor loads) in area.
4) Unaccounted zero and negative sequence currents created by interaction of unbalanced fault voltage and loads.
5) Incorrect generator impedance used for time scale required.
6) Zero sequence mutuals are a rich ground for modeling errors.
   a) Polarity of coupling wrong.
   b) Coupling is modeled as being from 0 – 100% of line, but the lines are not parallel for their full length. Alternatively, the coupling may exist for 100% of one line, but not 100% of the second line.
   c) The location of mutually coupled sections is not taken into account during fault studies. In other words, the line coupling is modeled correctly, but the protection engineer running the fault study does not put faults into the right locations to get the required best or worst case fault currents from the model.
   d) Unaccounted underbuilds or parallel lines.

Lessons Learned

There is often an inherent contradiction involved in generating protective relay settings for system additions. We would like to base our settings on studies containing "as-built" line, generator and transformer data, but the most reliable data in these cases is often only available after the relay settings are required to be in service. In the case of HNY, accelerated project schedules resulted in the need to design based on assumptions or early calculations. It is important early on in the project to ensure that other groups are aware of the data that must be provided to protection engineers. There is also a need to have processes in place to review the "as-built" data to ensure that any errors or late changes in the data get integrated back into the system models.

Bibliography

1) “The Art and Science of Protective Relaying”, CR Mason, John Wiley & Sons, 1967
2) “South Vancouver Island Disturbance, 12 Oct 2008 Event Report”, CF Henville and DJ Sydor, Internal BC Hydro report, 2008
3) "Transmission Line Reference Book - 345 kV and Above", Electric Power Research Institute, 1975
4) “Introduction to Symmetrical Components”, SE Zocholl and EO Schweitzer, presented at WPRC 2007, http://www.selinc.com/WorkArea/DownloadAsset.aspx?id=2470
5) DA England, RP Barone, “Report on Vancouver Outage Jan 16, 2001”, (Internal BC Hydro report)
6) “How Complex Systems Fail”, Richard I Cook, http://www.ctlab.org/documents/How%20Complex%20Systems%20Fail.pdf
7) “A Brief Look At The New Look in Complex System Failure, Error, Safety and Resilience”, Richard I Cook, http://www.ctlab.org/documents/BriefLookAtTheNewLookVerAA.doc.pdf

I would like to thank all the protection engineers and technologists who took time to share their campfire tales with me over the last 21 years. Special thanks are due to Geoff Neily, Ed Mazzuca, Gary Young, Vladimir Kahle, Don Hurd, Larry Nettleton, Brian Burk, Charlie Henville, Don McNamara, Terry Treasure, Shane Kronebusch and Jatinder Parmar for allowing me to learn vicariously through their bad experiences. Extra special thanks go to Tyler Scott, Brian Burk and Mukesh Nagpal for their assistance in editing this paper.