Security Criterion for Distance Zone 1 Applications in High SIR Systems With CCVTs

Bogdan Kasztenny and Ritwik Chowdhury *Schweitzer Engineering Laboratories, Inc.*

Presented at the 50th Annual Western Protective Relay Conference Spokane, Washington October 10–12, 2023

Originally presented at the 76th Annual Georgia Tech Protective Relaying Conference, May 2023

Security Criterion for Distance Zone 1 Applications in High SIR Systems With CCVTs

Bogdan Kasztenny and Ritwik Chowdhury Schweitzer Engineering Laboratories, Inc.

Abstract—In this paper, we present a practical engineering procedure for verifying security of a directly tripping distance Zone 1 protection element in applications to lines with high source-to-line impedance ratios. We consider transient security errors caused by capacitively coupled voltage transformers, as well as steady-state errors caused by instrument transformer errors, line impedance errors, ground potential rise, and mutual coupling.

While factors that impact the Zone 1 security are generally known, there are no practical procedures for verifying the security of Zone 1 applications based on simple engineering calculations that use readily available data. This paper closes this gap by proposing how to quantify the impact of key interfering factors and showing how to verify the Zone 1 security.

The presented Zone 1 security criterion is intended to guide practitioners by either confirming the protection security of the preferred Zone 1 application or directing them to change application parameters, such as reducing the reach setting or adding a time delay.

I. INTRODUCTION

An underreaching directly tripping Zone 1 distance element is a valuable option for line protection. It operates without reliance on a protection channel. For lines without a protection channel, it provides primary protection. For lines with a protection channel – available to most lines today – it provides redundancy for communications-assisted protection schemes, such as directional comparison schemes and line current differential schemes. The directly tripping Zone 1 element may also reduce the protection operating time, especially if the protection channel is relatively slow while the line is relatively long and the local terminal is relatively strong.

For a Zone 1 element to trip without communications assistance, it must be secure. Directional supervision built into the Zone 1 elements ensures directional integrity for reverse faults. Therefore, from the application perspective, the Zone 1 security is only concerned with overreaching (tripping for forward out-of-zone faults). We classify the Zone 1 overreach as either a transient overreach or a persistent overreach. These two types have different causes and solutions [1].

A transient overreach is caused by transient components in the relay voltages and currents. Even though transients in any of the distance element voltages and currents play a role, the capacitively coupled voltage transformer (CCVT) transients are by far the most consequential. Protective relays provide effective filtering for both high-frequency oscillatory components in voltages and currents, as well as for the decaying direct current (dc) component in currents. These interfering signal components have a frequency spectrum that is far from the fundamental frequency, allowing the relay to effectively suppress them. The CCVT transients, in contrast, may have large magnitudes, and their frequency spectrum is relatively close to the fundamental frequency [2]. As a result, it is challenging to suppress the CCVT transients, especially if a fast Zone 1 operation is desired.

Persistent overreach is caused by steady-state errors in voltages and currents, including voltage transformer (VT) ratio errors, current transformer (CT) ratio errors, errors in the line impedance value (magnitude and angle, positive- and zero-sequence), infeed and mutual coupling effects, as well as ground potential rise (GPR) [1].

Filtering and other advanced security measures built into distance relays can address transient overreach. A user can further improve Zone 1 transient overreach by adding a time delay or by shortening the reach. Persistent errors may be addressed by shortening the Zone 1 reach. We define persistent errors as steady-state errors during fault conditions and use persistent and steady-state interchangeably.

High source-to-line impedance ratio (SIR) applications dramatically exacerbate the danger of Zone 1 overreach – both transient and persistent. When the SIR is high, the relay voltage for faults at the remote bus is low (so is the loop voltage of a distance element). The distance element operating signal (IZ - V) is even smaller [1]. When a protection operating signal is small, even small errors in voltages and currents may impact security.

The impact of the combination of the CCVT transients and a high SIR on the security of distance Zone 1 protection elements is well understood [1] [2]. However, because a combination of several factors affects the Zone 1 security, including the Zone 1 element design and the CCVT transient response, no accurate and practical criterion exists for verifying the security of the Zone 1 applications. The classification of transmission lines into short, medium, and long included in the IEEE Std C37.113-2015 (Line Protection Guide) [3] omits many of the practical dimensions of the impact of the SIR on Zone 1 applications, making it too simplistic to be a practical security criterion. Additionally, the Line Protection Guide [3] does not provide application recommendations that would depend on the SIR or the line length. Protective relay manufacturers routinely claim a 5 percent Zone 1 transient overreach for an SIR as high as 30 and any CCVT make and model. Sometimes these claims are vague and do not specify if the 5 percent overreach applies to CCVTs or magnetic VTs.

Also, these claims are known to be challenged by reports of occasional Zone 1 misoperations.

Consequently, a practitioner may be left with a void and uncertainty regarding the security of a Zone 1 application. Reference [1] provides an in-depth description and analysis of the relevant factors but does not include specific methods for engineering a particular application. This paper builds on [1] to provide simple and practical methods that quantify the relevant factors to verify the Zone 1 security in high SIR applications. Both the transient overreach and the persistent overreach criteria start with these input data:

- Worst-case SIR values for phase and ground faults obtained from a short-circuit program.
- Intended Zone 1 reach setting.

The Zone 1 security criterion we present in this paper for transient overreach due to CCVTs is based on the following data:

- The Zone 1 operating time published by the relay manufacturer.
- The Zone 1 intentional time delay, if any.
- The CCVT transient response envelope available from the CCVT manufacturer.

The transient overreach security criterion allows the practitioners to select a combination of the reach setting, CCVT type, and intentional time delay (preferably 0) that ensures a secure Zone 1 application.

The Zone 1 security criterion we present in this paper for persistent overreach is based on the following data:

- VT and relay voltage accuracy specification.
- General information related to GPR.
- Short-circuit current in parallel lines, if these lines are magnetically coupled to the protected line, and the parallel line current that is large relative to the protected line current.

The persistent overreach security criterion allows the practitioners to balance the reach setting against the VT and relay errors and the impact of GPR and mutual coupling.

This paper is organized as follows. Section II explains the Zone 1 operating signal and shows how to use it when analyzing the impact of errors on Zone 1 security. Section III derives the transient security criterion for Zone 1 applications in high SIR systems with CCVTs. Section IV presents a stepby-step procedure of evaluating Zone 1 security with the CCVT transients and illustrates it with examples. Section V proposes a new format that relay manufacturers can use to specify the Zone 1 security in relation to the CCVT transients. Section VI derives the Zone 1 security criterion in relation to steady-state errors that are independent of the measured voltage and current. Section VII summarizes the calculations for steady-state errors and provides a step-by-step procedure to follow. Section VIII explains how to combine the various errors when selecting the final Zone 1 reach setting, while Section IX discusses how our findings compare with the IEEE Std C37.113 Line Protection Guide and field experience.

II. ZONE 1 OPERATING SIGNAL AND SIR

A. Zone 1 Operating Signal

The distance element operating signal (IZ - V) is convenient when explaining and analyzing Zone 1 security issues [1]. In the IZ – V term, which is a voltage term, I is the loop current, V is the loop voltage, and Z is the impedance corresponding to the reach point of the Zone 1 element. The IZ – V operating signal applies universally to all distance element implementations. It also applies to both the mho and reactance operating characteristics. A Zone 1 element operates based on a phase comparison of the IZ – V operating signal and the selected polarizing signal.

The CCVT transients and other voltage errors do not impact the Zone 1 polarizing signal because the polarizing signal is derived by using memory (memory-polarized mho elements) or current (reactance elements). It is only the IZ - V operating signal that is impacted by both the transient and persistent errors in the loop voltage and current and the persistent errors in the reach impedance. This observation allows us to develop a common Zone 1 security criterion for both the mho and the quadrilateral distance elements.

A Zone 1 element in a distance relay measures the voltages and currents and effectively acts on the IZ - V operating signal. We can think of the measured IZ - V operating signal as comprising the true IZ - V operating signal and an error. Because the IZ - V operating signal is effectively a voltage, we can write:

$$(IZ - V)_{MEASURED} = (IZ - V)_{TRUE} + V_{ERROR}$$
(1)

 V_{ERROR} is the error in the loop voltage (V) or in the IZ term or both. The error in the IZ term results from the error in the loop current (I) or the reach impedance (Z).

Equation (1) provides a high-level concept. Different relays apply different low-pass or band-pass filtering before obtaining the IZ – V operating signal. When processing the IZ – V operating signal, some distance relays use phasors and phase comparators, while other relays use instantaneous values and coincidence timing. Some relays use the IZ – V term explicitly, while other relays perform equivalent calculations, such as the m calculation, the polarized apparent impedance calculations, or the torque calculations [4]. Conceptually, however, we can analyze all these relays by looking at the true IZ – V operating signal in relation to the error signal, V_{ERROR} .

The main point of (1) is that as long as the magnitude of the error (V_{ERROR}) is small compared to that of the true IZ – V operating signal, the measured IZ – V operating signal has the correct polarity or phase angle relationship relative to the polarizing signal, and the Zone 1 element operates correctly. Therefore, we can conceptualize the Zone 1 security criterion as follows:

$$|(IZ - V)_{TRUE}| > |V_{ERROR}|$$
⁽²⁾

where || stands for magnitude.

Condition (2) allows us to simplify the analysis by neglecting the relative polarities of the true IZ - V operating signal and the error signal. These two signals can effectively

add or subtract. When the error signal has the same polarity as the true operating signal, it increases the measured operating signal and the Zone 1 element will not overreach. When the error signal has the opposite polarity as the true operating signal, it decreases the measured operating signal; if the measured operating signal polarity is inverted, the Zone 1 element overreaches. By requiring that the error signal be smaller than the true operating signal, we ensure that the measured operating signal polarity will not be inverted and the element will not overreach.

The true IZ - V operating signal in per-unit values of the loop nominal voltage depends on the SIR and the Zone 1 perunit reach (m₁), as shown in (3) [1]:

$$|(IZ - V)_{TRUE}| = \frac{|m - m_1|}{SIR + m}$$
 (3)

where m is the per-unit fault location.

B. Source-to-Line Impedance Ratio

Recently, a common agreement emerged that the SIR is based on the per-unit relay voltage magnitude for a metallic remote bus fault instead of the line and system impedances [1] [5] [6]. This improved SIR definition is consistent with thinking of the SIR as a parameter in a voltage divider that represents the simplified faulted-loop circuit. In this concept, the SIR determines how high or low the relay voltage is for a fault at the end of the protected line. This recent understanding of the SIR makes (3) exact.

As a result of linking the SIR to the relay voltage for a remote bus fault, two SIR values must be considered: SIR_{LL} and SIR_{LG}, for phase and ground faults, respectively. SIR_{LL} is for evaluating the security of the Zone 1 phase element. SIR_{LG} is for evaluating the security of the Zone 1 ground element. SIR_{LG} is often lower than SIR_{LL} because of the grounding paths presented by network transformers. For simplicity, we use a single variable SIR in this paper and avoid differentiating between the phase and ground elements, unless necessary. In addition to experiencing different SIR values, the Zone 1 phase and ground elements may use different reach settings. As a result, the security of the Zone 1 phase and ground elements must be verified separately. For simplicity, we use a single variable for Zone 1 reach (m_1) and avoid differentiating between the phase and ground elements, unless necessary.

As expected, (3) shows us that the operating signal is zero when the fault is located at the reach point ($m = m_1$). When the fault moves away from the reach point, either inside Zone 1 ($m < m_1$, internal fault) or outside Zone 1 ($m > m_1$, external fault), the operating signal increases proportionally to the difference between m and m_1 .

We are concerned with the Zone 1 security (an overreach for a remote bus fault), and therefore, we consider the IZ - V value not for any fault location (m) but for the closest external fault in the Zone 1 direction, i.e., for a remote bus fault (m = 1). Inserting m = 1 in (3) gives us:

$$|(IZ - V)_{TRUE}| = \frac{1 - m_1}{SIR + 1}$$
 (4)

Because Zone 1 is set to underreach $(m_1 \le 1)$, we can remove the absolute sign in (4). Equation (4) allows us to account for the SIR: the weaker the system, the smaller the IZ – V operating signal and the greater the security problem. Equation (4) also allows us to account for the Zone 1 reach, m_1 : the longer the reach, the smaller the IZ – V operating signal and the greater the security problem.

We combine (4) and (2) and obtain a general Zone 1 security criterion as follows:

$$\frac{1 - m_1}{\text{SIR} + 1} > \left| V_{\text{ERROR}(\text{PU})} \right| \tag{5}$$

Condition (5) shows a Zone 1 margin of $1 - m_1$. To understand this margin better, we distinguish between two types of errors: *ratio errors* and *fixed errors*.

C. Ratio Errors and Fixed Errors

A ratio error, when considered within the specified measurement range, is a small error that is proportional to the quantity of interest (measured loop voltage, measured loop current, or the impedance used in the relay settings). Ratio errors are best accommodated by reducing the reach in proportion to the sum of the percentage errors, as explained in [1]. For example, assume that the voltage ratio error is 2 percent, the current ratio error is 5 percent, and the impedance error is 5 percent. To ensure Zone 1 security in the presence of these errors, the Zone 1 reach must be reduced from the theoretical limit of 1 pu by at least 2 + 5 + 5 = 12 percent (Zone 1 shall be set below 100 - 12 = 88 percent of the line impedance, in this example).

A fixed error is an error that is independent of the measured voltage and current. For example, a CCVT transient is proportional to the change between the pre-fault and fault voltages and is not proportional to just the measured fault voltage. On the contrary, the CCVT transient can be many times larger than the measured fault voltage. Or a voltage induced by mutual coupling and appearing as an error signal in the measured voltage for the protected line is proportional to the current in the parallel line and not to the measured current in the protected line. Fixed errors are best accommodated by using (5) to further reduce the Zone 1 reach after reducing it to account for the ratio errors.

III. TRANSIENT SECURITY CRITERION

Because distance relays filter high-frequency transients in voltages and currents, as well as decaying dc components in the current, we can focus on the CCVT transients only.

A. CCVT Transients

During fault conditions, a significant transient component is present in the CCVT secondary voltage. That transient is proportional to the change in voltage between the pre-fault and fault states. In high SIR applications, the voltage changes from the pre-fault nominal value to a very small value. Fig. 1 through Fig. 3 show the CCVT secondary voltage for sample CCVTs. Each figure shows a set of waveforms for bolted faults at the CCVT location that occur at different points on wave. Because the true ratio voltage during these faults is zero, the secondary voltage represents the highest possible CCVT transient. We can see that the magnitude, character, and duration of the CCVT transients depend on the CCVT type and point on wave. Reference [2] provides more information on the CCVT transients in relation to the impact of the CCVT parameters and burden, a transient damping device (if present), and the ferroresonance suppression circuit.



Fig. 1. CCVT transients: exponential decay response.



Fig. 2. CCVT transients: oscillatory response.

In theory, the voltage signal that appears after t = 0 in Fig. 1 through Fig. 3 is the V_{ERROR} component in (5). However, we would face several challenges if we were to apply (5) to this V_{ERROR}. Consider these points:

- The CCVT transient is not a number but a time series, and its waveform depends on the fault point on wave.
- Distance relays apply filtering and reduce the CCVT transients in the loop voltage.
- Different CCVTs output very different transients.
- The transient response cannot be easily determined from the CCVT nameplate data.

We solve these challenges in the following subsections.



Fig. 3. CCVT transients: a case of large and prolonged transients.

B. Quantifying CCVT Transients With Respect to Time

Fig. 4 shows a sample CCVT transient and a data window of a distance relay that operates in T_{OP} milliseconds following the fault inception. We assume a microprocessor-based relay and show its finite impulse response (FIR) filter window. The window length is W cycles (W = 1 cycle, for example).



Fig. 4. Sample CCVT transient and the relay data window at the time of Zone 1 operation.

It is justified to assume that if the Zone 1 element overreaches for a fault just beyond its reach point, the time of misoperation would be similar to the time of correct operation for a fault just short of the reach point. This key observation allows us to use the Zone 1 operating time as the estimate of effective internal delay that the Zone 1 element design applies for security. The longer the operating time for an internal fault close to the reach point, the more secure the Zone 1 element is. If that element misoperates for a fault beyond the reach point, it would do so after a similar time.

We introduce the following variable:

 T_{OP} is the Zone 1 operating time for the SIR of interest and the farthest fault location for which the manufacturer publishes the operating time. If the manufacturer publishes separate curves for magnetic VTs and CCVTs, use the latter to obtain T_{OP} .

When the Zone 1 element operates in T_{OP} milliseconds, the relay filters are filled with data that stretch between $T_{OP} - W$ and T_{OP} .

Assume further that the user can intentionally delay the Zone 1 element by using a pickup timer of T_D milliseconds. Of course, T_D could be zero.

Under the above rational assumptions, we observe that, at the time of a possible Zone 1 overreach for an external fault, the filters are filled with data that stretch between $T_{OP} + T_D$ and $T_{OP} + T_D - W$. This means that the CCVT transients between the fault inception (t = 0) and t = $T_{OP} + T_D - W$ have no or little impact on the Zone 1 security.

As a result, we replace the voltage error in (5) with the CCVT transient error (E_{CCVT}) starting from $t = T_{OP} + T_D - W$ onward:

$$\frac{1 - m_1}{\text{SIR} + 1} > \left| E_{\text{CCVT}(\text{PU})} \right|_{(t)} \quad \text{for } t > T_{\text{OP}} + T_{\text{D}} - W \tag{6}$$

Criterion (6) captures the expected relationship between Zone 1 security and the intentional time delay (adding delay subjects the Zone 1 element to a smaller CCVT error because that error decays with time). Criterion (6) also captures the expected relationship between the Zone 1 security and the inherent speed of the Zone 1 element (slower Zone 1 designs will typically have less problems with the CCVT transients).

Furthermore, (6) ensures coherence between the effective internal time delay (T_{OP}) and the additional time delay the user may apply (T_D). Criterion (6) uses the sum of the two delays ($T_{OP} + T_D$), making it irrelevant how the delay is achieved (a slower Zone 1 element design or an additional time delay applied by the user).

The window length (W) may be challenging to obtain. Some Zone 1 element designs use both full-cycle and half-cycle windows. Some designs use variable data windows. Yet other designs use finite response filters to prefilter the voltage, current, or both. Obtaining and using these design details from the relay manufacturer would not be practical.

We propose using W = 1 cycle as a reasonable estimate. This approximation is justified by the fact that if the Zone 1 element overreaches because of the CCVT transients, it does it relatively late (after 1 to 1.5 cycles). If the relay uses a variable data window, that window will have already grown in length to one cycle by that time. If the relay uses a half-cycle window, using W = 1 cycle is a conservative and secure approximation because the CCVT transients subside over time, and therefore a full cycle window would have higher transients inside of it than a half-cycle window.

Therefore, we substitute W = 1 cycle in (6) and write:

$$\frac{1 - m_1}{SIR + 1} > |E_{CCVT(PU)}|_{(t)}$$

for
$$t > T_{OP} - 1 \text{ cycle} + T_D$$
 (7)

Normally, a Zone 1 element would not operate faster than in 1.5 cycles for high SIR values and faults near the end of the zone (i.e., $T_{OP} > 1.5$ cycles). Therefore, $T_{OP} - 1$ cycle + T_D is always positive and typically greater than 0.5 cycle. During the first half cycle, the secondary voltage may still be ramping down from a pre-fault magnitude level. When the filtered secondary voltage is still high (ramping down), it is very unlikely that the Zone 1 element would overreach. Therefore, we limit the ($T_{OP} - 1$ cycle) time in (7) to 0.5 cycle, and write:

$$\frac{1 - m_1}{\text{SIR} + 1} > \left| E_{\text{CCVT}(\text{PU})} \right|_{(t)} \text{for} \tag{8}$$

$$t > max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$$

Condition (8) tells us that for Zone 1 to be secure, the CCVT transients from a certain time onward must be smaller than a certain threshold value. The time threshold depends on the Zone 1 operating time (T_{OP}) and an optional time delay (T_D). The level threshold depends on the SIR and the Zone 1 reach setting, m₁. Condition (8) must be satisfied for any fault point on wave.

C. Quantifying CCVT Types and the Impact of Fault Point on Wave

As illustrated in Fig. 1 through Fig. 4, the CCVT transients depend on the CCVT make and model, as well as on the fault point on wave. The CCVT standards, IEC 61869-5 [7] and IEEE C57.13.9 [8], provide a method to quantify the CCVT transients. The IEEE standard is in a draft stage at the time of this paper (Draft IEEE PC57.13.9). The two standards follow a very similar approach. In reference to Fig. 5, the standards confine the CCVT transient with a step-like envelope. The standards define transient response classes. We use the term transient error envelope to mean the way the CCVT manufacturer quantifies the transient error and avoids disclosing CCVT design details, especially about the ferroresonance suppression circuit. The envelope of a particular CCVT may or may not comply with a specific class. If the CCVT complies with a specific class, its transient error envelope can be found in the CCVT standard. If the CCVT does not comply with a specific class, its transient error envelope may be obtained from the CCVT manufacturer.

The selection of the time breakpoints for the transient envelope is arbitrary. The objective of the envelope, however, is to provide the upper limit of the CCVT transients from the specified time to any future time for a bolted fault at the CCVT primary terminals.

The IEC 61869-5 standard defines three transient accuracy classes by specifying three transient envelopes (see Fig. 6 for an example transient envelope). The Draft IEEE PC57.13.9 standard defines two transient accuracy classes. The IEC and IEEE classes are not the same. Our Zone 1 security criterion does not rely on a specific transient accuracy class. Instead, the transient envelope itself is the input to the calculations.

The CCVT standards acknowledge that the transient envelopes and classes are introduced to facilitate engineering protection applications that use voltage. The standards do not explain how the classes or envelopes are to be used and they do not make references to any other related documents. This paper may be one of the first (if not the first) use cases for the transient accuracy information contained in the CCVT standards.

Both the IEEE and IEC standards leave the first 0.5 cycle of the fault without any requirements for the transient error. This recognizes the reality that it takes several milliseconds for the secondary voltage to ramp down from the pre-fault level to the very low fault voltage level. This 0.5-cycle exclusion time is compatible with (8) in which we ignore the CCVT error earlier than 0.5 cycle into a fault.



Fig. 5. Transient envelope for all possible CCVT transients for a given CCVT make and model.





It is critically important to remember that the percentage error in the CCVT transient envelope (such as in Fig. 6) relates to the pre-fault peak voltage and not to the fault ratio voltage. For example, the 10 percent error in Fig. 6 is 10 percent of the nominal peak voltage. This value can be several times higher than the relay voltage during a fault in high SIR applications. As discussed in Subsection III.B, this is a fixed error and not a ratio error. Therefore, the 10 percent transient error cannot be accommodated by pulling back the Zone 1 reach by 10 percent of the line impedance.

CCVTs have a long lifespan. It is unlikely that your inservice CCVTs comply with the transient accuracy classes of the IEC 61869-5 or IEEE C57.13.9 standards or that you have a record of the transient envelope for those CCVTs. Refer to the two standards [7] [8] and request the transient envelope information from the CCVT manufacturer. The CCVT manufacturer can provide you with the envelope or with just the sample test results – the secondary voltage plot for a fault at the voltage zero-crossing and for a fault at the voltage peak. In the latter case, you can use the maximum of the two transients to obtain the worst-case transient and draw a transient envelope as illustrated in Fig. 7. The approach in Fig. 7 is justified because the CCVT transients fall between the two extreme transient cases (for the zero-crossing and peak points on wave).



Fig. 7. Obtaining the CCVT transient envelope based on the absolute value of the secondary voltage plots for the fault at voltage zero (red) and voltage peak (green).

We are now ready to use the CCVT transient envelope to advance our Zone 1 security criterion (8). Because the envelope is an upper limit for transients that occur at any fault point on wave, we can substitute E_{CCVT} with $E_{ENVELOPE}$. However, the envelope signal corresponds to the bolted fault at the CCVT location (the fault causes a change in voltage from 1 pu to 0 pu). We are concerned with faults at the remote bus. The change in voltage for a remote bus fault is:

$$\Delta V_{(PU)} = 1 - \frac{1}{SIR + 1} = \frac{SIR}{SIR + 1}$$
(9)

The CCVT transient is caused by the change in the energy stored in the CCVT stack capacitors and inductors, primarily the tuning reactor. Therefore, the CCVT transient is proportional to the change in primary voltage that the fault causes. The CCVT envelope corresponds to a specific transient that occurs for the greatest possible change from 1 pu to 0 pu under any point on wave. Therefore, we write:

$$\left| \mathbf{E}_{\text{CCVT}(\text{PU})} \right|_{(t)} = \frac{\text{SIR}}{\text{SIR} + 1} \cdot \frac{\left| \mathbf{E}_{\text{ENVELOPE}} \right|_{(t)}}{100\%} \tag{10}$$

We can substitute the transient error in (8) with the transient envelope as in (10) and obtain:

$$1 - m_1 > SIR \cdot \frac{|E_{ENVELOPE}|_{(T_0)}}{100\%}$$
where: (11)

$$T_0 = max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$$

Condition (11) uses a single point in time (T_0) on the transient envelope. This is possible because the transient envelope, by definition, decreases with time (unlike an individual transient at a particular point on wave that may temporarily increase with the passing of time). Condition (11) brings an expected relationship between the operating time and security. Because the transient envelope decreases with the passing of time, adding a time delay (T_D) or using a slower Zone 1 element (T_{OP}) improves security: the greater T_0 , the smaller the E_{ENVELOPE} value.

D. Accounting for Relay Filtering

Condition (11) can be used directly to evaluate Zone 1 security. It would, however, yield overly conservative results. Zone 1 elements apply filtering to their voltage signals. Filtering reduces the CCVT transients that propagate into the Zone 1 element logic. We introduce an attenuation factor (A) for the CCVT transient to recognize that the relay filtering reduces the CCVT transients A-fold:

$$1 - m_1 > \frac{1}{A} \cdot SIR \cdot |E_{ENVELOPE}|_{(T_0)}$$
where: (12)

$$T_0 = max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$$

We have obtained a conservative estimate for the value of A by performing transient simulations. We expect our estimate of A to be a universal value because of the following explanation.

CCVTs are designed and tuned based on well-established rules. For example, the series reactor is tuned to zero out the phase shift between the primary and secondary voltages at the system nominal frequency. As such, the inductor value is not an independent parameter but is tied to the total CCVT stack capacitance and the system nominal frequency. Furthermore, certain other parameters of a CCVT can be neglected (winding resistances, for example). As a result, the transient response of a CCVT is controlled by a small number of parameters and is relatively universal [2] [9].

We simulated several CCVT designs by using an electromagnetic transient program to obtain a range of CCVT transient waveforms by varying the point on wave for a bolted fault. The true secondary voltage for a bolted fault is zero; and therefore, the measured secondary voltage is equal to the CCVT transient. We processed these transients with a range of filters (full-cycle Fourier and cosine) and estimated the ratio between the highest magnitude of the filtered CCVT transient and the maximum CCVT transient value in the window of the filter.

First, we scanned through all point-on-wave values to obtain the maximum CCVT transient for any given point in time. This maximum transient is related to the CCVT transient envelope in IEC 61869-5 and Draft IEEE PC57.13.9. Next, we calculated the filtered magnitude, took its maximum value for all points on wave, and related it to the envelope of the maximum CCVT transient in the window.

Fig. 8 illustrates this process for one CCVT by plotting a range of CCVT transients (blue solid lines), the maximum absolute value within the 1-cycle data window (dashed blue

7

line), and the range of voltage magnitude values after filtering with a full-cycle filter (red solid lines). At any point in time, the attenuation is the ratio of the maximum absolute transient value (dashed blue line) to the upper limit of the magnitude plots (red solid lines). The attenuation tells us how much the filtering reduced the CCVT transient. For example, if the maximum absolute transient is 0.2 pu and the upper limit of the magnitude is 0.05 pu, the attenuation is 4-fold (A = 4).

We selected the minimum value of the attenuation for a time larger than 1.5 cycles. This time threshold is justified by our experience that if a Zone 1 element misoperates in high SIR applications with CCVTs, it does so after 1.5 cycles.

We repeated this activity for a range of CCVTs and for a range of filters and obtained the worst-case (lowest) attenuation:

$$A = 2.5$$

A = 2.5 means that the CCVT transient envelope is reduced more than 2-fold – to 40 percent or less of its original value – when it passes through a practical relay filter.



Fig. 8. Illustration of finding the attenuation value.

Having the attenuation estimated (A = 2.5), we write our final Zone 1 security criterion as follows:

$$1 - m_1 > 0.4 \cdot SIR \cdot \frac{|E_{ENVELOPE}|_{(T_0)}}{100\%}$$
where: (13)

 $T_0 = max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$

Condition (13) has a very simple form. The left-hand side in the inequality is the margin between the remote bus and the Zone 1 reach in per unit of the line impedance. The Zone 1 application is secure if that margin is greater than the right-hand side value in the inequality. The right-hand side is a product of the SIR, the CCVT envelope at the time of Zone 1 operation including the optional time delay, and the 0.4 factor associated with the relay filters. Condition (13) is easier to satisfy when:

- The Zone 1 reach is short.
- The SIR is low.

- The CCVT has a small transient envelope.
- The relay has a long operating time.
- The optional time delay is long.

The above is exactly what we intuitively expect in this application. We can use the variables in (13) to compensate for the impact of SIR in applications with high SIR values.

IV. STEP-BY-STEP PROCEDURE FOR ASSESSING TRANSIENT ZONE 1 SECURITY AND EXAMPLES

A. Step-by-Step Procedure for Verifying Zone 1 Security in High SIR Applications With CCVTs

Verify (13) separately for the Zone 1 phase and ground elements. If the security condition is satisfied, you can be confident that the Zone 1 application is secure. If the security condition fails, the Zone 1 application may still be secure, but you may need to contact the relay manufacturer or perform more studies or testing. Follow these steps to verify the security of the Zone 1 application.

- 1. By using a short-circuit program and considering all credible contingencies, obtain the highest SIR value for your application.
- 2. By using the Zone 1 operating time curves published by the relay manufacturer, obtain the operating time (T_{OP}) for the SIR value from Step 1 and the farthest fault location for which the operating time is published.
- 3. Decide on the per-unit Zone 1 reach (m_1) and intentional time delay (T_D) . Start with the m_1 value according to your standard practice, such as 0.75 or 0.80 pu, and $T_D = 0$.
- 4. Obtain the CCVT transient envelope from the CCVT documentation or manufacturer according to the IEC or IEEE standards. Obtain the per-unit envelope value for $T_0 = max(0.5 \text{ cycle}, T_{OP} 1 \text{ cycle}) + T_D$.
- 5. Verify the security criterion:

$$1 - m_1 > 0.4 \cdot SIR \cdot \frac{|E_{ENVELOPE}|_{(T_0)}}{100\%}$$

where:

$$T_0 = max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$$

- 6. If the security condition is satisfied, you can be confident that the Zone 1 application is secure and you do not need to perform other studies.
- 7. If the security condition is not satisfied, consider the following options:
- a) Consult the relay documentation to study the Zone 1 CCVT security claims; contact the relay manufacturer if necessary. Use the past field experience and any transient simulation studies for the same CCVT and relay makes and models.
- b) Use the security condition to determine if reducing the Zone 1 reach setting (m₁), and by how much, would satisfy the security condition.
- c) Use the security condition to determine if adding an intentional time delay to Zone 1 (T_D), and how much, would satisfy the security condition.

- d) You may also consider a combination of a shorter reach and a time delay. Typically, in high SIR applications, adding a time delay is more effective than reducing the reach.
- e) You may also consider using the security condition to obtain the required CCVT envelope and to help specify the CCVT for greenfield applications given the SIR value and the preferred relay.

B. Graphical Representation of the CCVT Security Criterion

Because the CCVT envelope is a graph, we can rearrange (13) to allow a graphical representation as follows:

$$|E_{ENVELOPE}|_{(T_0)} < 2.5 \cdot \frac{1 - m_1}{SIR} \cdot 100\%$$
where: (14)

$$T_0 = max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$$

We can use (14) graphically by plotting two lines on the CCVT transient envelope chart (Fig. 9):

a horizontal line at:

$$2.5 \cdot \frac{1-\mathrm{m_1}}{\mathrm{SIR}} \cdot 100\%$$

and a vertical line at:

$$max(0.5 \text{ cycle}, T_{OP} - 1 \text{ cycle}) + T_D$$

If the two lines cross above the CCVT envelope, then the application is secure. If the application is not confirmed to be secure, move the horizontal line up by reducing the Zone 1 reach, m_1 , and/or move the vertical line to the right by adding a time delay, T_D .



Fig. 9. Graphical illustration of the CCVT transient security condition.

C. Transient Security Example 1

Assume a CCVT with the transient envelope shown in Fig. 6 (Class 3PT2 per IEC 61869-5). Fig. 10 shows the Zone 1 operating time curves of the applied relay. The preferred Zone 1 reach setting is 80 percent of the line impedance. Assume that by using the short-circuit program, you obtained the worst-case voltage of 0.065 pu at the relay location for a bolted remote bus fault. Calculate the SIR and obtain 1/0.065 - 1 = 14.4.

Is this Zone 1 application secure, and if not, what can be done to ensure security of the application?



Fig. 10. Zone 1 operating time curves (Relay A).

We use the SIR value of 14.4 to determine the Zone 1 operating time for the farthest fault location in Fig. 10 and obtain $T_{OP} = 1.5$ cycles. We assume no intentional time delay $(T_D = 0)$ and the per-unit reach setting of $m_1 = 0.80$. We obtain the CCVT envelope value for t = max(0.5 cycle, 1.5 cycles - 1 cycle) + 0 cycles = 0.5 cycle. From Fig. 6, we see that the CCVT transient at 0.5 cycle is below 25 percent. We use the Zone 1 security criterion and calculate:

$$1 - 0.8 >^{?} 0.4 \cdot 14.4 \cdot \frac{25\%}{100\%}$$

The above condition computes to:

 $0.2 >^{?} 1.44$

The security criterion fails, and we cannot guarantee the phase Zone 1 security in this application without performing more studies or enabling CCVT security logic if it is available in this relay.

If we decide to use an intentional time delay, we will need to delay the operation until the CCVT envelope falls below:

$$2.5 \cdot \frac{1 - 0.8}{14.4} \cdot 100\% = 3.47\%$$

From Fig. 6, we see that the CCVT transient error envelope falls below 3.47 percent (to 2 percent) at 2 cycles; therefore, we calculate T_D from this equation, 1.5 cycles – 1 cycle + T_D = 2 cycles, and obtain T_D = 1.5 cycles. With a 1.5-cycle intentional time delay, we can guarantee security of this Zone 1 application without testing or obtaining any more details from the relay manufacturer.

If we decide to shorten the reach instead, we will calculate the reach as:

$$m_1 < 1 - 0.4 \cdot 14.4 \cdot \frac{25\%}{100\%}$$

Which computes to:

$$m_1 < -0.44 \text{ pu}$$

The maximum reach being negative means that Zone 1 security cannot be ensured by reducing the reach.

D. Transient Security Example 2

Assume the same CCVT as in Example 1 but consider that a different relay is used (Fig. 11).



Fig. 11. Zone 1 operating time curves (Relay B).

We use the SIR value of 14.4 to determine the Zone 1 operating time for the farthest fault location in Fig. 11 and obtain $T_{OP} = 3$ cycles. We assume no intentional time delay $(T_D = 0)$ and the per-unit reach setting of $m_1 = 0.80$. We obtain the CCVT envelope value for t = max(0.5 cycles - 1 cycle) + 0 cycles = 2 cycles. From Fig. 6, we see that the CCVT transient at 2 cycles is below 2 percent. We use the Zone 1 security criterion and calculate:

$$1 - 0.8 >^{?} 0.4 \cdot 14.4 \cdot \frac{2\%}{100\%}$$

The above condition computes to:

0.2 >? 0.115

The security criterion is satisfied, and we can guarantee the phase Zone 1 security in this application without performing further studies.

We can use the graphical method to illustrate the above two examples. Fig. 12 shows the CCVT envelope and the points representing Relays A and B with the reach set to 80 percent of the line impedance.



Fig. 12. Graphical illustration of CCVT Examples 1 and 2.

V. A NEW FORMAT FOR SPECIFYING ZONE 1 TRANSIENT OVERREACH

The CCVT classes create an opportunity for the relay manufacturers to provide a more comprehensive Zone 1 application recommendation for the CCVT classes specified in IEC 61869-5 and Draft IEEE PC57.13.9. A CCVT class constrains the CCVT transient error and allows the relay manufacturer to specify the Zone 1 transient overreach with that CCVT as a function of the Zone 1 reach, CCVT security setting (enabled/disabled), SIR, and intentional time delay.

We suggest using the format shown in Fig. 13. We label this specification as "Zone 1 security chart." A separate chart may be provided for each CCVT class. The two CCVT standards specify a total of five CCVT classes. The chart may be different for the Zone 1 phase and ground elements. The chart will be different based on any CCVT security logic being disabled or enabled if the relay includes a setting to control the additional security logic. The Zone 1 security chart would reflect all proprietary CCVT security logic in the relay and therefore would be more accurate than the generic Zone 1 security criterion that we presented in Section III. Such a chart may be considered for inclusion in future revisions of IEC 60255-121 [10] or IEEE C37.113 [3].

The users may also adopt and develop Zone 1 security charts as in Fig. 13 as a part of their line protection standards. These user charts can be based on information from the relay manufacturers, transient testing results, and field experience.



Fig. 13. Proposed Zone 1 security chart (specific to a given CCVT class and relay make and model).

VI. STEADY-STATE SECURITY CRITERION

Steady-state errors associated with the voltage and current measurements and the line impedance data impact the Zone 1 security and should be accommodated by shortening the Zone 1 reach or disabling the Zone 1 protection. The following steady-state errors may impact Zone 1 operation (see [1]):

- VT and CT errors.
- Relay voltage and current input errors.
- Line impedance errors.
- GPR.
- Mutual coupling.

Even in high SIR applications, the relay currents are well within the accurate measurement range of CTs and protective relays. Therefore, we can neglect the CT errors and the relay current input errors. These errors are small (at the level of 2 to 5 percent of the measured value). Moreover, they are ratio errors (i.e., they are proportional to the measured current) and, as such, are already included in the customary Zone 1 reach setting margin.

The lack of or imperfect line transposition adds to the line impedance errors. Only a perfectly transposed line is fully defined by the positive- and zero-sequence impedances, Z1 and Z₀, respectively, and has all six loop apparent impedances equal to the positive-sequence impedance. During remote bus faults at the end of an untransposed line, a distance relay measures slightly different loop apparent impedances depending on the fault type and faulted phases. Differences in the apparent impedance magnitude of 5 percent are not uncommon. Also, inaccuracy in the zero-sequence compensation factor (k₀) may affect the measured apparent impedance for ground faults. In this paper, we assume that the user has already accounted for the line impedance errors in the customary Zone 1 reach setting margin. For example, the phase distance Zone 1 reach is set based on the lowest apparent impedance of all three phase loops, and the ground distance Zone 1 reach is set based on the lowest apparent impedance of all three ground loops with additional margin for uncertainty in the k₀ factor [1].

This section addresses the remaining sources of steady-state errors. It is important to realize that all the remaining errors are voltage errors that are not necessarily proportional to the measured voltage. For example, when the primary voltage is just a few percent of the nominal value, the VT and relay errors are not specified as a percentage of the measured value. Similarly, the GPR that affects the voltage that the VT measures is not proportional to the relay voltage or current but is related to the total ground current flowing into the substation ground. Similarly, the voltage induced through mutual coupling is proportional to the current in the coupled line and has no relationship with the voltage or current measured in the protected line.

Because the steady-state voltage errors tend to be a fixed portion of the nominal voltage and not the measured voltage, reducing the Zone 1 reach by the percentage error is not a proper way to accommodate these errors. Any error that is moderate and proportional to the voltage and current measurement is accommodated in the reach setting [1]. Instead, we will use (5) to evaluate the Zone 1 security in relation to the steady-state errors because (5) applies to the case of a fixed voltage error rather than a percentage voltage error. We use (5) and write that the Zone 1 per-unit operating signal must be greater than the worst-case steady-state error in the loop voltage, E_{SS} :

$$\frac{1 - m_1}{SIR + 1} > E_{SS} \tag{15}$$

where Ess is in per unit of the nominal loop voltage.

Of course, the shorter the per-unit reach (m_1) and the lower the SIR, the higher the operating signal (the left-hand side in (15)) and the easier it becomes for the Zone 1 element to overcome the $E_{\rm SS}$ error. Security condition (15) can be written as a "maximum SIR" condition:

$$SIR < \frac{1 - m_1}{E_{SS}} - 1 \tag{16}$$

Security condition (15) can also be written as a "maximum per-unit Zone 1 reach" condition:

$$m_1 < 1 - E_{SS} \cdot (SIR + 1)$$
 (17)

Condition (16) teaches us that the shorter the Zone 1 reach and the smaller the steady-state error, the higher the maximum SIR. Condition (17) teaches us that the lower the SIR and the smaller the steady-state error, the longer the maximum Zone 1 reach. The above is exactly what we intuitively expect.

We can represent (15) graphically as straight lines on the SIR vs. m_1 plane as in Fig. 14.



Fig. 14. Zone 1 security chart considering steady-state errors.

For example, if the worst-case steady-state error is 0.025 pu and the SIR is 15, the margin for the fixed errors must be at least 40 percent of the line impedance (the reach must be below 60 percent).

Let us now turn our attention to estimating the worst-case steady-state voltage error. We assume that the individual error components accumulate (add) and never cancel (partially subtract) and write:

$$E_{SS} = E_{VT} + E_{REL} + E_{GPR} + E_{MC}$$
(18)

where (all errors are in per unit of the nominal loop voltage):

- E_{VT} is the VT error.
- E_{REL} is the relay voltage input error.
- $E_{\mbox{\scriptsize GPR}}$ is the error associated with GPR (applies in most cases).
- E_{MC} is the voltage error associated with mutual coupling (applies in rare cases).

The following subsections propose how to estimate these errors for practical applications based on the minimum amount of readily available data.

A. VT and Relay Voltage Magnitude Errors

The accuracy specifications for the VTs and the relay voltage inputs follow a similar format. In the specified measuring range, these devices exhibit a ratio error, i.e., an error that is a fixed percentage of the measured voltage. The measuring range of a VT may start as low as 10 percent of the nominal value. The measuring range of a relay may start at as low as 1 V secondary. The claimed accuracies can be on the order of half a percent.

Fig. 15 illustrates these magnitude errors by plotting the ratio error in blue (percentage of reading) and the absolute error in red (percentage of nominal).



Fig. 15. Measuring range, ratio error (blue), and absolute error (red).

As a worst-case scenario, we assume that, in applications with high SIR values, the relay voltage is outside the measuring range (below the lower limit of the range, $V_{MIN(PU)}$). Therefore, we do not have explicit data about accuracy of the VT or the relay voltage inputs for a fault that causes a very low voltage at the relay location. We know, however, that the absolute error will not increase when the voltage decreases. Therefore, we assume that the absolute error (percentage of nominal) remains constant when the voltage is below the lowest voltage of the accuracy specification (see Fig. 15).

Calculate the VT magnitude error in per unit of nominal as follows:

$$E_{VT_MAG} = \frac{E_{\%}}{100\%} \cdot V_{MIN(PU)}$$
(19)

where $E_{\%}$ is the percentage ratio error at the minimum voltage level specified, $V_{MIN(PU)}$.

Relay specifications often omit the $V_{MIN(PU)}$ value and use the convention of "[x] percentage of reading or [E_{SEC}] V secondary, whichever is greater." In such a case, calculate the relay voltage magnitude error in per unit of nominal as follows:

$$E_{\text{REL}_MAG} = \frac{E_{\text{SEC}}}{V_{\text{NOM}}}$$
(20)

where V_{NOM} is the nominal value of the voltage input (phaseto-ground voltage if using wye-connected VTs and phase-tophase voltage if using delta-connected VTs) in secondary volts.

Before using (20), review the relay accuracy specification related to the accuracy of voltage-based *protection*. Do not consider voltage *metering* accuracy because relay metering functions typically apply more filtering and are therefore more accurate than the protection functions.

Consider the following examples.

1) Example 1

Assume a VT that has a class of 0.6 percent over the range between 90 percent and 110 percent of nominal [11]. We use

 $V_{MIN(PU)} = 0.9$ pu and $E_{\%} = 0.6$ percent and calculate by using (19):

$$E_{VT_MAG} = \frac{0.6\%}{100\%} \cdot 0.9 \text{ pu} = 0.0054 \text{ pu}$$

The above result means that for voltages below 90 percent of nominal, we expect the error to be below 0.54 percent of nominal. For example, if the voltage is 4.8 percent of nominal (SIR = 20), the error is 0.54 percent of nominal, or 11 percent of the measured voltage. If the SIR is 30, the voltage is 3.2 percent of nominal and the error is 17 percent of the measured value.

2) Example 2

Assume an IEC 61869-5 Class 6P VT [7], i.e., with a maximum error of 6 percent over the range between 5 percent and 100 percent of nominal. We use $V_{MIN(PU)} = 0.05$ pu and $E_{\%} = 6$ percent and calculate by using (19):

$$E_{VT_MAG} = \frac{6\%}{100\%} \cdot 0.05 \text{ pu} = 0.0030 \text{ pu}$$

The above result means that for voltages below 5 percent of nominal, we expect the error to be below 0.3 percent of nominal. For example, if the voltage is 4.8 percent of nominal (SIR = 20), the error is 0.3 percent of nominal, or 6.3 percent of the measured value. If the SIR is 30, the voltage is 3.2 percent of nominal and the error is 9.4 percent of the measured value.

3) Example 3

Assume that a relay with a 66.4 V secondary phase-toground nominal voltage has the following voltage protection accuracy claim.

Pickup Accuracy for Phase Voltage Elements:

 $\pm (0.25\%$ of setting or 0.1 V sec, whichever is greater)

We use $E_{SEC} = 0.1 \text{ V}$ and $V_{NOM} = 66.4 \text{ V}$ and calculate by using (20):

$$E_{\text{REL}_{MAG}} = \frac{0.1 \text{ V}}{66.4 \text{ V}} = 0.0015 \text{ pu}$$

As described in this subsection, the magnitude errors apply to voltages that are measured directly (ground distance elements and phase distance elements if the relay uses deltaconnected VTs). In the next subsection, we analyze the phase voltage errors if the relay uses wye-connected VTs as is typically the case in transmission line protection.

B. VT and Relay Voltage Angle Errors

VTs and relay voltage inputs may exhibit small voltage angle errors on the order of a fraction of an electrical degree. These small errors are inconsequential even when the voltage is low, such as in high SIR applications, and can be neglected as long as the relay measures the operating voltage directly, i.e., ground distance elements and phase distance elements if the relay uses delta-connected VTs. However, we cannot neglect the angle errors when analyzing phase distance elements if the relay uses wye-connected VTs in applications where the phase SIR_{LL} is high. 12

Fig. 16 illustrates the worst-case scenario for deriving a phase-to-phase voltage from two measured phase-to-ground voltages. Because we are concerned with the Zone 1 overreach, we identify the case when the derived phase-to-phase voltage (red) appears smaller than the true phase-to-phase voltage (blue). The worst-case scenario requires the angle errors in the two measured phase-to-ground voltages to have opposite signs (shifting the two voltage phasors closer).

Further, the error in the derived phase-to-phase voltage increases when the magnitudes of the two measured phase-to-ground voltages are larger – for example, for phase-to-phase faults but not necessarily for phase-to-phase-to-ground or three-phase faults.



Fig. 16. Illustration of the measuring error in phase-to-phase voltage derived from two phase-to-ground voltages.

Calculating the exact error in the derived phase-to-phase voltage in Fig. 16 requires the magnitudes of the phase-to-ground voltages and the magnitude of the true phase-to-phase voltage. These magnitudes, however, are complex functions of SIR_{LG} and SIR_{LL}. We can simplify the analysis by making the following additional worst-case assumptions: 1) the phase-to-ground voltages did not decrease during the fault (the SIR_{LG} is low, or the fault does not involve ground) and 2) the true phase-to-ground voltages. Under these assumptions, the error in the phase-to-ground voltages. Under these assumptions, the error in the phase-to-ground voltages derived from the phase-to-ground voltages is (in per unit of nominal):

$$E_{ANG} = 2 \cdot \sin\left(\frac{\delta}{2}\right) \cong \sin(\delta)$$
 (21)

where δ is the combined phase angle error of the VT and the relay.

1) Example 4

Assume the relay angle error is 1° and the VT angle error is 0.5° . We use (21) and calculate the error in the derived phase-to-phase voltage as follows:

$$E_{ANG} = \sin(1^\circ + 0.5^\circ) = 0.0262 \text{ pu}$$

C. Combined VT and Relay Voltage Errors

We are ready now to estimate the combined VT and relay voltage input errors in per unit of nominal. Use the following formulas. Because the relay measures the operating voltage directly, the phase angle errors of the VT and the relay are inconsequential, while the VT and relay magnitude errors accumulate in the worst case. Therefore, use the following equation to calculate the combined errors of the VTs and the relay voltage inputs in per unit of nominal:

$$E_{VT} + E_{REL} = E_{VT_MAG} + E_{REL_MAG}$$
(22)

Zone 1 Phase Element if the Relay Uses Wye-Connected VTs

In this case, the angle error or the magnitude error may play the dominating role. Use the following equation to calculate the combined error of the VT and the relay in per unit of nominal, considering that the magnitude and angle errors tend to be orthogonal; and therefore, we add them by using quadrature summation:

$$E_{VT} + E_{REL} = \sqrt{(E_{VT_MAG} + E_{REL_MAG})^2 + E_{ANG}^2}$$
 (23)

Typically, the combined VT and relay voltage error, when the loop voltage is very low, is about 0.02 pu of the nominal loop voltage.

D. GPR Error

The total ground current $(3I_{0T})$ in the substation grounding resistance (R_{GPR}) creates GPR voltage. The relay measures the protected line voltage relative to the substation ground, rather than the ideal (remote) earth. We can write the voltage drop equation for a ground fault with fault resistance (R_F) and the total fault current (I_F) as follows (see Fig. 17):

$$V_{R} = Z_{L} \cdot I_{R} + R_{GPR} \cdot 3I_{0T} + R_{F} \cdot I_{F}$$
(24)

where:

V_R is the relay voltage (phase-to-substation-ground).

 I_R is the relay loop current for the Zone 1 ground element.

 Z_L is the impedance between the relay and the fault.



Fig. 17. Impact of the GPR on the ground loop distance measurement.

We use (24) to calculate the apparent impedance and obtain:

$$Z_{APP} = \frac{V_R}{I_R} = Z_L + R_{GPR} \cdot \frac{3I_{0T}}{I_R} + R_F \cdot \frac{I_F}{I_R}$$
(25)

Equation (25) informs us that if the total ground current $3I_{0T}$ and the relay loop current I_R are approximately in phase, the apparent impedance shifts horizontally to the right, similarly to that of a resistive fault (see Fig. 18). This added resistive component does not jeopardize the Zone 1 security, although it may reduce dependability, especially for short lines. However, if the network is not homogeneous, the angle of the $3I_{0T}/I_R$ ratio

may tilt the added impedance down, potentially causing an overreach. A mho Zone 1 ground element polarized with memory voltage would expand its characteristic considerably in high SIR systems. This would extend its resistive reach and can result in unexpected operation for an external fault if the GPR impedance component in Fig. 18 is tilted down. A quadrilateral Zone 1 ground element may be configured with a substantial resistive reach, and it may also overreach because of the tilted GPR impedance component.



Fig. 18. Impact of the GPR on the distance element apparent impedance in homogeneous and nonhomogeneous networks.

Typically, the GPR results in the underreaching of ground distance elements and in the degraded accuracy of single-ended impedance-based fault locators for ground faults. Because of the network nonhomogeneity, the GPR may also result in security issues for the Zone 1 ground elements.

We consider the following three cases for the Zone 1 ground distance elements:

No Grounding Path in the Substation $(3I_{0T} = 0)$

For substations without grounding banks (switching stations), neglect the impact of GPR and assume $E_{GPR} = 0$.

Inductive Grounding Path in the Substation

Assume the worst-case nonhomogeneity angle of 30 degrees (the angle between the $3I_{0T}$ and I_R). A 30-degree angle tilt results in a downward shift of the added GPR apparent impedance of half the GPR apparent impedance (see Fig. 18). Therefore, use of $E_{GPR} = 0.5 \cdot V_{GPR(PU)}$.

Inverted Grounding Path Current in the Substation Due to Autotransformers

If the substation grounding path is provided at least in part through certain autotransformers, the $3I_{0T}$ current may be significantly shifted, or even inverted, compared to the I_R current. In those cases, use $E_{GPR} = V_{GPR(PU)}$ as a precaution.

You can also simplify the GPR analysis and assume $E_{GPR} = V_{GPR(PU)}$ for all cases. Of course, the GPR error applies only to ground elements and not phase elements.

The value of the GPR voltage can be estimated based on the ratings of communications cables connecting substation equipment with facilities outside the substation. You can consider using 2 kV as a reasonable estimate of the GPR [12], but a more accurate estimate reflecting the utility's substation grounding design practices should be used, if available.

Example

Assume a typical substation grounding through power or zig-zag transformers and estimate the E_{GPR} error for two systems: 500 kV and 69 kV. We use the recommended 50 percent of the 2 kV value and calculate the following estimates.

500 kV system:

$$E_{GPR} = \frac{0.5 \cdot 2 \text{ kV}}{500 \text{ kV}/\sqrt{3}} = 0.0035 \text{ pu}$$

69 kV system:

$$E_{GPR} = \frac{0.5 \cdot 2 \text{ kV}}{69 \text{ kV}/\sqrt{3}} = 0.0251 \text{ pu}$$

As we see, the GPR impact is much smaller at higher voltages. In low SIR applications, the GPR voltage is an inconsequential fraction of the relay voltage for faults at the remote bus. In high SIR applications, the GPR voltage plays a significant role.

E. Mutual Coupling Error

A current that flows in a line that is magnetically coupled to the protected line induces a voltage in the protected line. In general, all sequence current components induce all sequence voltage components because the conductors are not spaced to perfectly cancel the relevant magnetic fields. For example, the positive-sequence current in the coupled line induces a negative-sequence voltage in the protected line. However, the zero-sequence coupling is by far the strongest (the zerosequence current in the coupled line induces zero-sequence voltage in the protected line). Practitioners are well aware of the zero-sequence mutual coupling; the short-circuit programs model it, and the ground distance elements are set to account for it. The other modes of coupling are neglected, and the shortcircuit programs do not model them.

In high SIR applications, even a small additional voltage resulting from the neglected mutual coupling can be significant when compared with the IZ - V operating signal of the Zone 1 element. This is especially the case if the coupled line carries much higher current than the protected line [1]. Additionally, while the higher current in the coupled line normally causes an underreach when considering only the zero-sequence mutual coupling, the typically neglected modes of coupling can cause overreach in high SIR applications.

One can use the line constants program to calculate the full coupling matrix for two 3-phase lines (a 6x6 matrix) and use it to calculate the impact of the coupled line currents on the loop voltages in the protected line during various fault types.

In this paper, we propose a much simpler method to approximate the impact of mutual coupling on the error in the loop voltage, E_{MC} .

We performed the following studies to obtain our formula:

• We considered a bolted fault at the remote end of the protected line with another line running in close proximity but not connected to the same buses. The

other line carries a current that is independent of the current in the protected line.

- We considered two configurations for each fault. In the first configuration, the two lines are mutually coupled. In the second configuration, the conductors of the two lines are spaced apart so that no appreciable coupling is between the lines.
- We considered the lines not transposed; each distance protection loop has a slightly different loop voltage depending on which phases are faulted (for example, AB vs. BC). We considered all 11 fault types. For phase-to-phase-to-ground faults, we considered the impact of coupling on the associated phase loop voltages and neglected the impact on the phase-to-ground voltages (distance relays measure phase apparent impedance during phase-to-phase-to-ground faults). For three-phase faults, we considered all three phase loop voltages.
- We logged the loop voltages for the cases with and without coupling and calculated the magnitude of the difference in the loop voltage.
- We logged the phase currents in the coupled line during the fault and calculated the maximum magnitude for all three phases.
- We calculated the coupling as the ratio between the effect (the change in the loop voltage) and the cause (the maximum phase current in the coupled line). We related this ratio to a unit of length of coupling (per mile or kilometer).
- For ground loops, we calculated the change in the sum of the positive- and negative-sequence components in the loop voltage. This approach removes the impact of the zero-sequence coupling.
- We repeated the test for other line configurations and logged the highest coupling for different tower and conductor configurations and different voltage levels.

We obtained the following worst-case coupling coefficient for 60 Hz systems:

0.100 V per A per mi

Our finding means that for each mile of coupling and each ampere of current in the coupled line, the coupled line can introduce an error as great as 0.1 V in the loop voltage. For example, assume that a 230 kV 10 mi line is mutually coupled to another line and the maximum fault current in that line is 5 kA. You can expect a voltage error due to coupling as great as $0.1 \cdot 5,000 \cdot 10 = 5$ kV. The 5 kV error is 5/230 =2.17 percent of the nominal voltage for the phase distance elements and $5 \cdot \sqrt{3}/230 = 3.77$ percent of the nominal voltage for the ground distance elements. The 2.17 percent and 3.77 percent errors may be inconsequential when the SIR is low. However, when the SIR is high and the relay voltage and the IZ – V operating signal is at the level of just a few percent of the nominal voltage, the induced voltage can cause security and dependability problems. Calculate the approximate voltage error in the loop voltage due to the negative- and positive-sequence mutual coupling by using the following equation:

$$E_{MC(V \text{ pri})} = X_{MC} \cdot I_{MC(A \text{ pri})} \cdot L_{MC}$$
(26)

where:

- I_{MC} is the coupled line maximum current (primary amperes); this is the highest current of all three phases for all fault types.
- $L_{\text{MC}}\,$ is the length of coupling in miles or kilometers.

 X_{MC} is the coupling coefficient as follows:

Length Units	Frequency (Hz)	
	60	50
Miles	0.100	0.083
Kilometers	0.062	0.052

Compute (26) in primary units to avoid confusion regarding the system nominal voltage levels (the protected and the coupled lines can operate at different nominal voltages) and the VT and CT ratios (the two lines can be equipped with instrument transformers of different ratios). Before you can add the E_{MC} error to the steady-state error (18), you need to express it in per unit of the nominal loop voltage of the Zone 1 element of the protected line:

$$E_{MC} = \frac{E_{MC(V \text{ pri})}}{V_{NOM(V \text{ pri})}}$$
(27)

Where $V_{NOM(V \text{ pri})}$ is the nominal system voltage in primary volts for the phase loops or $1/\sqrt{3}$ of the nominal system voltage in primary volts for the ground loops.

The approximation (26) is the worst-case scenario because it assumes no transposition along the coupled line sections. If the two lines are mutually coupled for a long distance, it is likely that the two lines are transposed within the common section, and the coupling effect will be lower.

VII. STEP-BY-STEP PROCEDURE FOR ASSESSING STEADY-STATE ZONE 1 SECURITY AND EXAMPLES

A. Step-by-Step Procedure

Follow these steps to assess the Zone 1 security for steadystate fixed errors:

- 1. By using a short-circuit program and considering all credible contingencies, obtain the highest SIR value for your application.
- 2. Obtain accuracy specifications for the VT and relay voltage inputs and calculate $E_{VT} + E_{REL}$ by using (22) for the Zone 1 ground element and (23) for the Zone 1 phase element.
- 3. Learn if the substation has "grounding sources" and if they are transformers or autotransformers. Obtain the GPR value or assume 2 kV and calculate E_{GPR} as in Subsection VI.D.
- 4. If a magnetically coupled line is present, obtain the highest faulted phase current in the coupled line for the same system configuration that results in the highest SIR for the protected line and calculate E_{MC} by

using (26) and (27). If multiple lines couple to the protected line, perform the calculations separately for each line and sum the errors.

- 5. Add the error components by using (18) and apply (15) considering your preferred Zone 1 reach setting.
- 6. If (15) is not satisfied, either reduce the reach and disable the Zone 1 element (phase and/or ground) or select system components that reduce the errors in (18).

Of course, the margin in the Zone 1 reach setting must accommodate all three categories of errors (ratio, transient, and fixed). Ensure that the margin in the final reach setting is large enough to cover all sources of error (see Section VIII).

B. Steady-State Security Zone 1 Phase Element Example

Calculate a secure Zone 1 phase element reach for a 230 kV line in a 60 Hz system with a worst-case SIR of 4 considering the following: 1) the combined VT and relay voltage error is 0.03 pu and 2) there is a mutually coupled line over 10 miles long that carries 4 kA fault current for a remote bus fault for the worst-case SIR of 4.

Using (26) with
$$X_{MC} = 0.1 \text{ V/(A·mi)}$$
, we obtain:

$$E_{MC} = \frac{0.1 \cdot 4 \text{ kA} \cdot 10 \text{ mi}}{230 \text{ kV}} = 0.0174 \text{ pu}$$

Using (17) with a total error of 0.03 pu + 0.0174 pu = 0.0474 pu, we calculate the maximum reach setting as follows:

$$m_1 < 1 - 0.0474 \cdot (4 + 1) = 0.76 \text{ pu}$$

If the line was not mutually coupled, the maximum Zone 1 phase element reach for this application would be:

$$m_1 < 1 - 0.03 \cdot (4 + 1) = 0.85 \text{ pu}$$

C. Steady-State Security Zone 1 Ground Element Example

Calculate a secure Zone 1 ground element reach for a 230 kV line with a worst-case SIR of 4 considering the following: 1) the combined VT and relay voltage error is 0.015 pu, 2) an inductive grounding path is at the substation, and 3) no mutually coupled line is in this application.

We calculate the error due to GPR as follows:

$$E_{GPR} = \frac{0.5 \cdot 2 \text{ kV}}{230 \text{ kV}/\sqrt{3}} = 0.0075 \text{ pu}$$

Using (17) with a total error of 0.015 pu + 0.0075 pu = 0.0225 pu, we calculate the maximum reach setting as follows:

$$m_1 < 1 - 0.0225 \cdot (4 + 1) = 0.89 \text{ pu}$$

VIII. COMBINING ALL SOURCES OF ERROR

We have presented methods to calculate the maximum secure Zone 1 reach considering the ratio errors [1], transient errors (Section III), and fixed steady-state errors (Section VII). We recommend that you add the security margins for all these errors to obtain the final security margin and the corresponding Zone 1 reach. Use the following formula to obtain the final Zone 1 per-unit reach:

$$m_1 = 1 - \sum margin \tag{28}$$

 $margin_{RATIO} = 1 - m_{1RATIO}$ (29a)

 $margin_{CCVT} = 1 - m_{1CCVT}$ (29b)

$$nargin_{FIXED} = 1 - m_{1FIXED}$$
(29c)

Substituting (29) into (28), we obtain the following formula for calculating the final Zone 1 reach that accounts for all three errors:

r

$$m_1 = m_{1RATIO} + m_{1CCVT} + m_{1FIXED} - 2 pu$$
 (30)

For example, if the margin for the ratio errors is 10 percent ($m_{1RATIO} = 0.90$ pu), the margin for the CCVT transients is 10 percent ($m_{1CCVT} = 0.90$ pu), the margin for the fixed errors is 20 percent ($m_{1FIXED} = 0.80$ pu), and the final Zone 1 reach is 0.60 pu. Of course, when the final reach is negative, you must disable Zone 1.

Fig. 19 shows an example of the maximum reach setting vs. the SIR by using (31) that combines a 10 percent ratio error ($m_{1RATIO} = 90$ percent) with a range of fixed steady-state error values.



Fig. 19. Example Zone 1 security chart considering 10 percent ratio error and a range of fixed steady-state errors.

IX. IEEE C37.113 AND FIELD EXPERIENCE

Typically, a Zone 1 element is not set much greater than 80 percent of the line impedance. We know from experience that with the 80 percent setting, there are no Zone 1 security issues if the system is strong, and that one should expect security issues if the system is weak. The IEEE C37.113 Line Protection Guide uses an SIR of 0.5 as the upper limit for a strong system (definition of a "long line") and an SIR of 4 as the lower limit of a weak system (definition of a "short line"). We apply our findings to explain the origins of the SIR of 0.5 and SIR of 4 in IEEE C37.113.

Assume that half of the 20 percent margin covers the ratio and fixed errors, and the other half covers CCVT transient errors.

Consider the CCVT transient errors and assume that the CCVT envelope is always below 40 percent, even for a very poorly performing CCVT [2]. We use (13) and calculate the

highest SIR for a secure Zone 1 application, assuming the margin of 10 percent $(1 - m_1 = 0.1 \text{ pu})$, and obtain SIR < 0.63. This SIR value is close to the arbitrary value of 0.5 in IEEE C37.113, and it confirms our field experience that in strong systems, a typically set Zone 1 element will not have any security issues due to the CCVT transients, even with CCVTs that have a very poor transient response.

Assume the system is not impacted by GPR or mutual coupling, and consider the combined ratio and fixed error of 0.025 pu. We use (16) and calculate the highest SIR for a secure Zone 1 application, assuming the margin of 10 percent $(1 - m_1 = 0.1 \text{ pu})$, and obtain SIR < 3. This SIR value is close to the arbitrary value of 4 in IEEE C37.113, and it confirms our field experience that in weak systems, a typically set Zone 1 element may have security issues, especially when the CCVT transients erode the initial 20 percent security margin.

X. CONCLUSIONS

We have presented an engineering method for quantifying the foremost factors that impact the Zone 1 security in high SIR applications, including the CCVT transients, VT and relay measuring errors, GPR, and mutual coupling. We have shown how to use the error estimates to verify the Zone 1 security and how to change the application parameters to ensure security.

Our approach looks at three different classes of factors that impact the Zone 1 security: a) ratio measurement errors, b) CCVT transients, and c) steady-state voltage errors that are independent of the measured voltages and currents.

The ratio measurement errors are proportional to the measured voltage and current. They are best accommodated by following a standard practice and shortening the Zone 1 reach to provide a percentage margin that is greater than the sum of the percentage ratio errors in the measured voltage, measured current, and line impedance. In applications to strong systems, you need to account for only the ratio errors and the zero-sequence mutual coupling. In applications to weak systems, you should consider the other two less-known classes of errors.

We have introduced a novel method to assess the impact of CCVT transient errors on the Zone 1 security. Our method brings together all the key factors that impact transient Zone 1 security: the SIR, the CCVT transient response, and Zone 1 inherent operating time, reach, and additional time delay, if applied. You can use the Zone 1 security criterion to both evaluate the Zone 1 security and calculate the reach setting and additional time delay to ensure security. You can also calculate the SIR limits for a secure Zone 1 application with desired settings given the relay and CCVT makes and models. You can also use the security criterion to specify the CCVT transient response that would ensure a secure Zone 1 application for a particular SIR, relay make and model, and Zone 1 settings.

We have introduced a method to estimate the worst-case steady-state voltage errors that are independent of the measured voltage and current, and we have shown how to use these errors to verify the Zone 1 security. These errors include voltage measurement errors for high SIR conditions when 1) the relay voltages are very low and therefore outside the specified measurement range, and the measurement error is no longer a ratio error, 2) a GPR component is in the phase-to-ground voltages, or 3) the voltages are induced by lines that are mutually coupled with the protected line. We explain which data to collect and how to use them to verify the Zone 1 security.

If we expect to set the Zone 1 reach to 80 percent of the line impedance but want to avoid finding any CCVT and relay data and instead assume the worst-case CCVT transients, we can apply the Zone 1 element if the SIR is below 0.63, assuming the steady-state errors require a margin that is less than 10 percent (see Section IX).

If we expect to set the Zone 1 reach to 80 percent of the line impedance and assume the total steady-state voltage error is below 2.5 percent of nominal (VT and relay errors, no GPR or mutual coupling to a line that carries significant current), we can apply the Zone 1 element when the SIR is less than 3, assuming the transient errors require a margin that is less than 10 percent (see Section IX).

We can state the following:

- It is very unlikely that in systems with SIR values below about 0.63, a typically set Zone 1 element (an 80 percent reach setting) would overreach because of the CCVT transients, regardless of the CCVT and relay makes and models.
- It is very unlikely that in systems with SIR values below about 3, and without significant GPR or mutual coupling, a typically set Zone 1 element (an 80 percent reach setting) would overreach because of steady-state errors, regardless of the VT and relay makes and models.

These SIR values (0.63 and 3) are similar to the limits in the IEEE C37.113 Line Protection Guide (0.5 and 4). Our paper connects heuristic SIR values with the application data. An SIR of 0.5 (the loop voltage for the remote bus fault is 2/3 of the nominal voltage) is the upper limit for dismissing the impact of the CCVT transients on the Zone 1 security. An SIR of 4 (the loop voltage for the remote bus fault of 1/5 of the nominal voltage) is the upper limit for dismissing the impact of steady-state errors in the relay voltage on the Zone 1 security.

We have also proposed a new method for specifying the security of Zone 1 elements in terms of transient overreach (Section V). This method is much more nuanced than today's relay specifications and is harmonized with the concept of CCVT classes that the IEC and IEEE standards have introduced.

XI. REFERENCES

- B. Kasztenny, "Settings Considerations for Distance Elements in Line Protection Applications," proceedings of the 74th Annual Conference for Protective Relay Engineers, College Station, TX, USA, 2021.
- [2] B. Kasztenny, D. Sharples, V. Asaro, and M. Pozzuoli, "Distance Relays and Capacitive Voltage Transformers – Balancing Speed and Transient Overreach," proceedings of the 54th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, USA, 2000.
- [3] IEEE Std C37.113-2015, *IEEE Guide for Protective Relay Applications to Transmission Lines.*

- [4] H. J. Altuve Ferrer and E. O. Schweitzer, III (eds.), Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems, Schweitzer Engineering Laboratories, Inc., Pullman, WA, USA, 2010.
- [5] P. G. Mysore and J. U. Berzins, "Impact of Voltage Transients and System Impedance Ratio on Zone 1 Distance Relay Reach," proceedings of the 56th Annual Minnesota Power Systems Conference, Saint Paul, MN, USA, 2020.
- [6] M. Thompson, D. Heidfeld, and D. Oakes, "Transmission Line Setting Calculations – Beyond the Cookbook Part II," proceedings of the 48th Annual Western Protective Relay Conference, Spokane, WA, USA, 2021.
- [7] IEC 61869-5:2011, Instrument Transformers Part 5: Additional Requirements for Capacitor Voltage Transformers.
- [8] IEEE Std PC57.13.9, IEEE Draft Standard for Power-Line Carrier Coupling Capacitors and Coupling Capacitor Voltage Transformers.
- [9] B. Kasztenny, W. J. Premerlani, and I. Raducanu, "Self-adjusting voltage filtering technique compensating for dynamic errors of capacitive voltage transformers," U.S. Patent 7,567,881, July 2009.
- [10] IEC 60255-121:2014, Measuring Relays and Protection Equipment Part 121: Functional Requirements for Distance Protection.
- [11] IEEE Std C57.13-2016, IEEE Standard Requirements for Instrument Transformers.
- [12] ANSI/IEEE Std 487-1980, Guide for the Protection of Wire-Line Communication Facilities Serving Electric Power Stations.

XII. BIOGRAPHIES

Bogdan Kasztenny has over 30 years of experience in power system protection and control. In his decade-long academic career (1989-1999), Dr. Kasztenny taught power system and digital signal processing courses at several universities and conducted applied research for several relay manufacturers. In 1999, Bogdan left academia for relay manufacturers where he has since designed, applied, and supported protection, control, and fault-locating products with their global installations numbering in the thousands. Bogdan is an IEEE Fellow, an IET Fellow, a Senior Fulbright Fellow, a Distinguished CIGRE Member, and a registered professional engineer in the province of Ontario. Bogdan has served as a Canadian representative of the CIGRE Study Committee B5 (2013-2020) and on the Western Protective Relav Conference Program Committee (2011-2020). In 2019, Bogdan received the IEEE Canada P. D. Ziogas Electric Power Award. Bogdan earned both the Ph.D. (1992) and D.Sc. (Dr. habil., 2019) degrees, has authored over 220 technical papers, holds over 60 U.S. patents, and is an associate editor of the IEEE Transactions on Power Delivery.

Ritwik Chowdhury received his BS degree in engineering from the University of British Columbia and his MS degree in engineering from the University of Toronto. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2012, where he is presently a senior engineer in research and development. Ritwik holds over 10 patents and has helped author over 25 technical papers. He was recognized as an exceptional reviewer for *IEEE Transactions on Power Delivery* for three years. He is the chair of the Protection and Control Practices Subcommittee (I-SC) of the IEEE Power System Relaying and Control (PSRC) Committee, the chair of two IEEE Standards Working Groups, and the recipient of the 2021 PSRC Outstanding Young Engineer Award. Ritwik is a senior member of IEEE, a member of CIGRE, and a registered professional engineer in the province of Ontario.