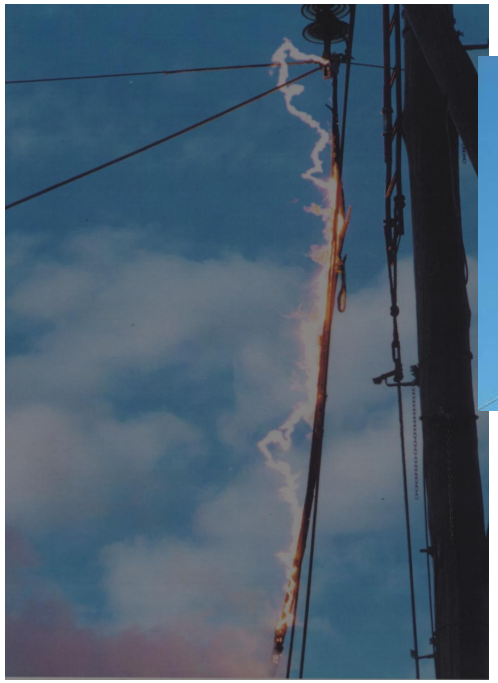
Considerations for AI in Protection

Sukumar Brahma, PhD, FIEEE
Clemson University

Overview

- Brief introduction to principles and implementation of protection.
- Hurdles in using AI in protection.

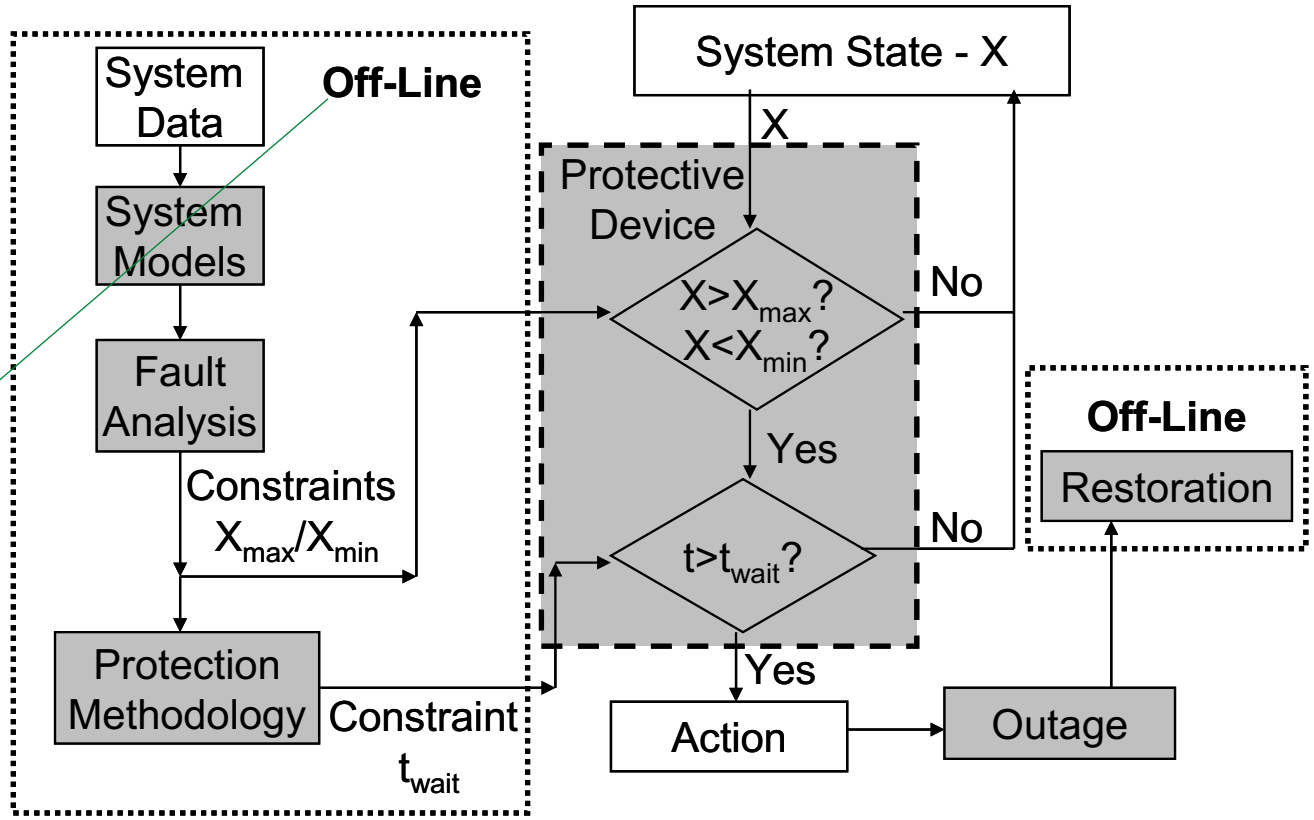
Event to Analysis



- We essentially convert these events to V&I phasors.
- Waveforms will be distorted differently for each case.
- Even for same type of fault, each fault-occurrence can produce different fundamental, different harmonics, different transient content, different decaying dc offsets (currents).
- So, protection heavily depends on filtered fundamental values – they get impacted significantly for all faults and have similar behavior for each fault-type.

Power System Protection

- Avoided at Transmission Level with Distance Relays
- Extensively used for Distribution Systems – where the grid-edge is.



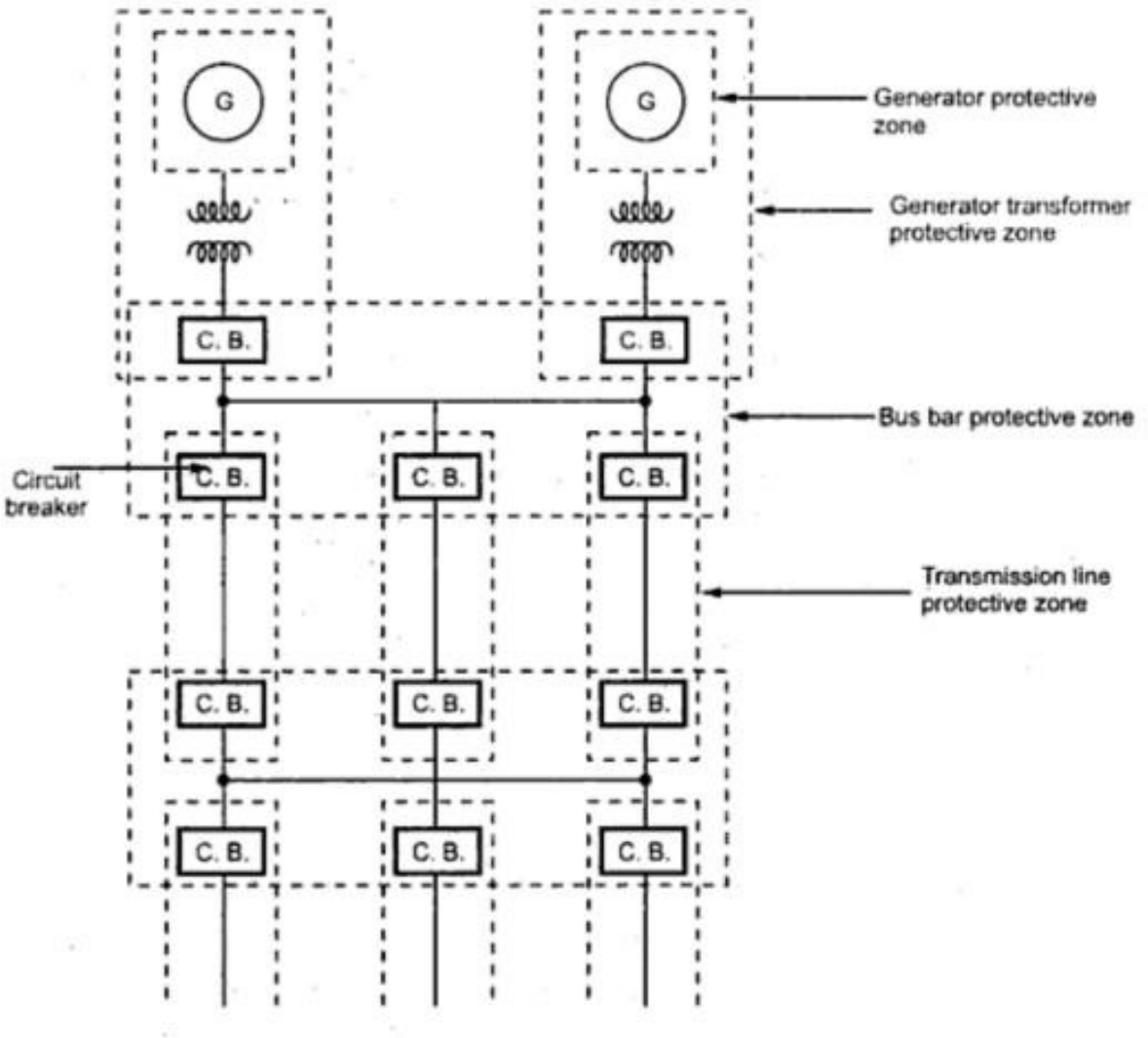
- Protection is a critical and the fastest function.
- A fault is detected by relays and cleared by circuit breakers in a total of about 3-5 cycles in transmission, up to 10 cycles in distribution.

Is Pattern Creation and Classification New to Relaying?

- Practically every relay uses a feature or a combination of features (pattern), and a rule-based classifier.
- Feature is typically frequency-domain transformation of the time-domain measurement – current, voltage, frequency, power, impedance, harmonic content……
- Pattern is the combinatory logic blocks provided in numerical relays. For example, voltage monitored overcurrent, or fault detector monitored distance element.
- Classifier typically has two-classes: Fault & No Fault.
- Separation plane is a threshold value (for feature) or a combination of threshold values (for pattern). Values and combinations are determined through
  - system analytics – e.g., fault analysis, stability analysis…
  - physics and physics-based models
  - experience

Zones of Protection and Overlap

- Zones – each zone has a primary protection, and at least one backup protection.
- Protective device must not only sense faults, but determine which zone the fault is in.
- Backup device also must be aware of the faulted zone, even for faults in adjacent zone.



https://images.app.goo.gl/ZHEoQ4GD1eHTdoUG9

Performance Metrics for Protection - I

Reliability:

- Dependability: protective device must operate during faults.

$$Dependability = \frac{\text{Number of Correct Trips}}{\text{Faults in the Protection Zone}} \times 100\%$$

- Security: Relay Must NOT operate incorrectly during faults.

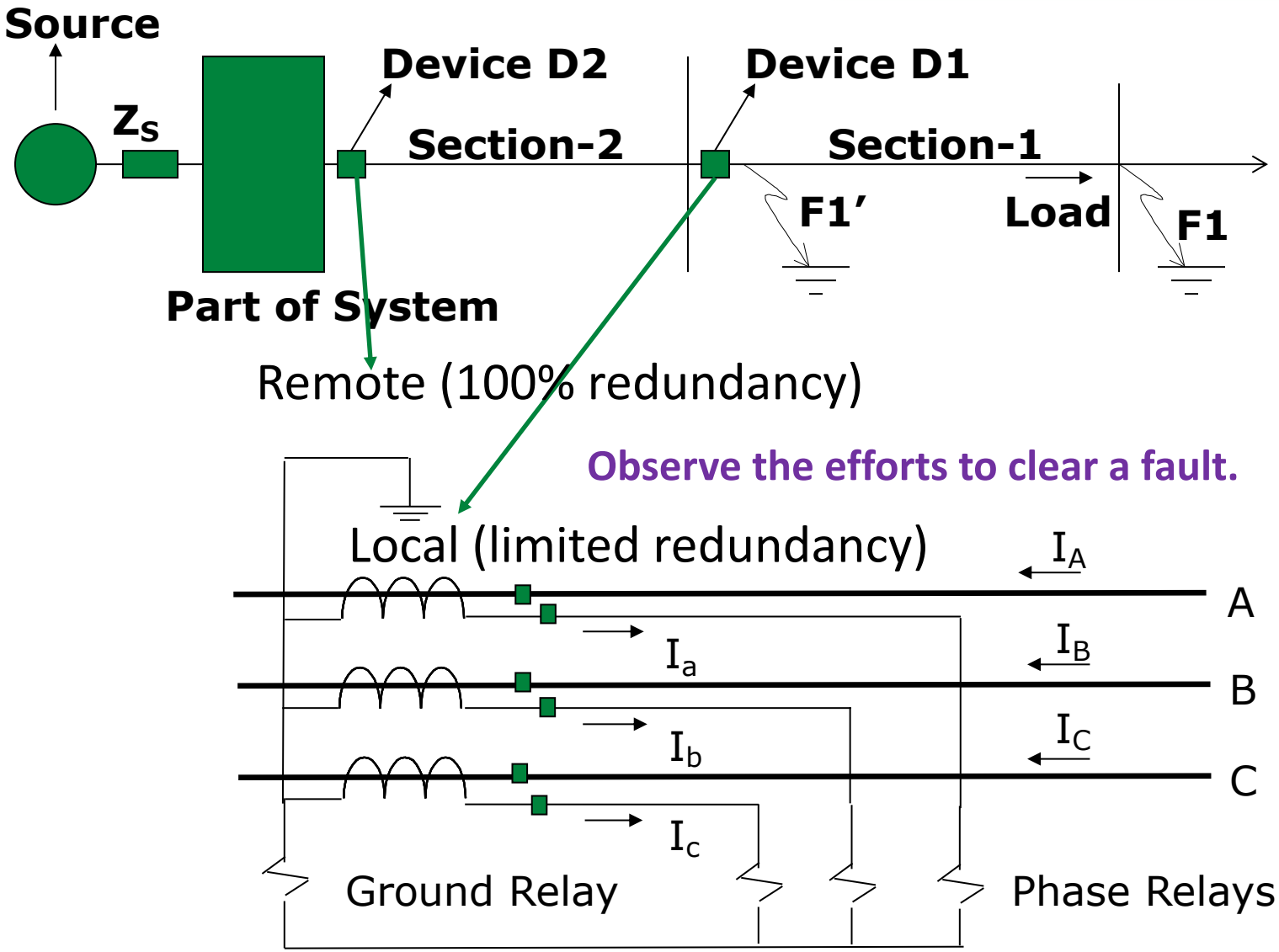
$$Security = \frac{\text{Number of Correct Restrains}}{\text{Faults outside the Protection Zone}} \times 100\%$$

  - Also, relays must not operate if there is no fault. This happens due to faulty components/devices or incorrect settings. Such "misoperations" are typically spurred by events other than the actual fault – i.e., system dynamics or overload.
  - Dependability and security are obviously contradictory terms. Engineering judgment is required here. Hardly seen in papers on ML based protection.

Performance Metrics for Protection - II

Selectivity:

- Ability to detect faults within the zone and trip circuit breakers to isolate only the faulted zone. This requires proper coordination between protection schemes employed in different zones.
  - Proper coordination of main and backup is necessary for selective and dependable protection.
  - This interdependency is critical – never addressed in published papers.



Performance Metrics for Protection - III

Speed:

- Relay must operate fast enough to avoid damage/instability and satisfy coordination with other zones.
  - For distribution systems speed is determined from thermal limits of equipment. 100 to 500 ms isolation time is not uncommon.
  - For transmission systems transient stability is the limiting criteria. It determines the critical clearing time (CCT). 3-5 cycles of isolation time typical.
  - Backup compromises the speed.

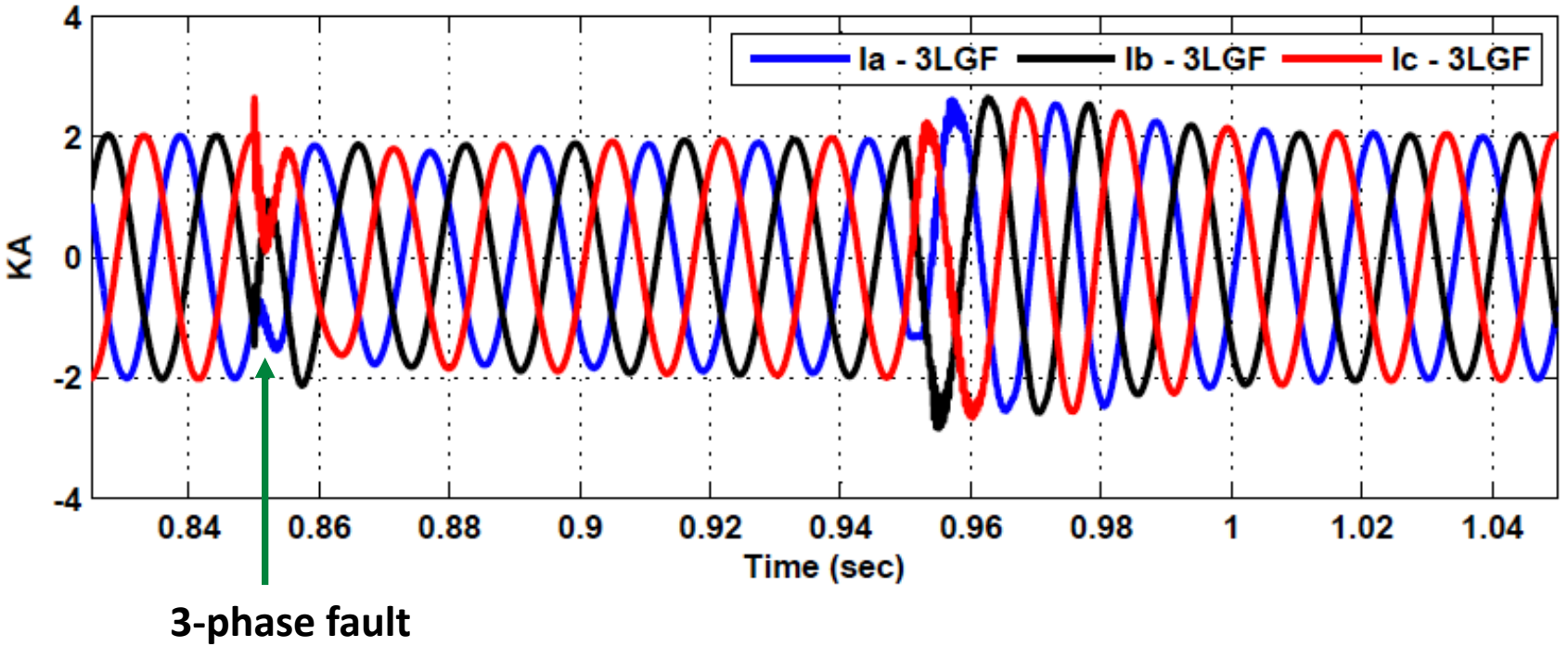
Bottom line

- It is a system that encapsulates interdependent localized schemes using physical attributes of the power system to provide safety and stability. Replacing one/few such schemes by a ML-based method does not reconcile with the holistic nature of power system protection.
- Simplicity, transparency and experience-tuned interdependency has ensured remarkably good performance over the past 100 years.
- It is not perfect, but performance baseline is extremely high.
- Even when the system fails, it often fails in predictable, understandable, and most importantly correctable ways.
- Failures are also generally limited within certain error bounds.
- Even when it fails, power system protection typically functions remarkably well – failures are limited to relatively small areas.

Replacing a Physics Based Relay with a Data-Driven Relay

- Literature is filled with papers that take this approach.
- Philosophically, why would AI perform better using the SAME features/patterns we are using to create a more dependable and secure classifier?
- If AI creates more complex features/patterns based on time-domain data, where the patterns in the transformed plane have no transparent relation to the original features, and thresholds (separation planes) are created simply by learning, why should we believe it will work better?
- Extending this thought, if a legacy protection is not working in certain system conditions, why would an AI-based method work?
  - If it uses the same patterns the legacy relay is using, or can use, applying learning to these patterns may not yield any better result, as the patterns have FAILED.
  - Do we want to take a chance with “opaque” patterns as a solution? Or go for more expensive physics-based approach?

Example – Failed Patterns – Inverter Response to Fault



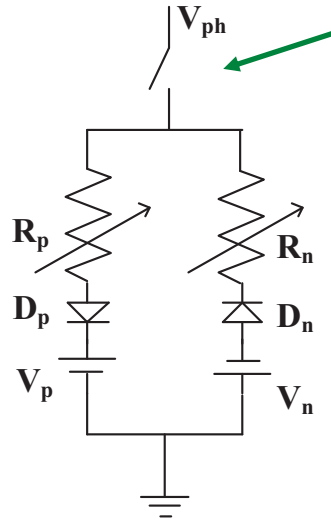
- Current does not increase in this case – phasor-based overcurrent relay fails.
- Transient seen at fault-instant heavily depends on fault instant; can also get mixed up with capacitor switching.
- Why would AI work better on fundamental phasor or high-frequency content?

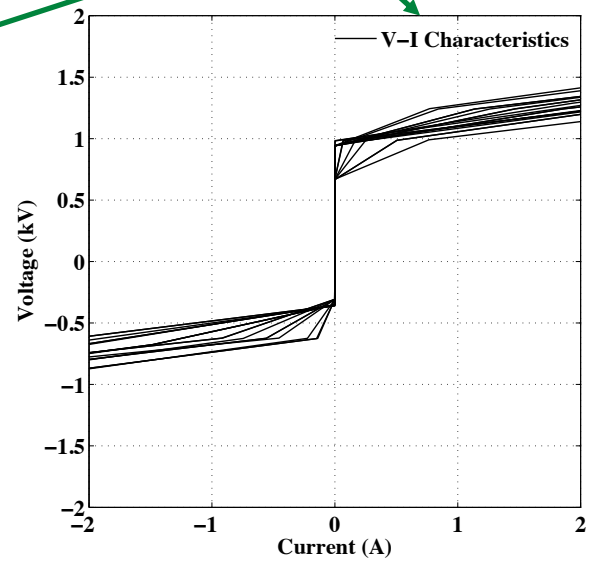
Hurdles to use of AI in Protection - I

- Reliability:
  - Even with 99.9% success rate on the network under study, dozens of daily misoperations or nonoperations would result if the technology is widely deployed across a major grid (thousands of networks).
  - Lack of backup protection in published methods exacerbates this problem.
  - Consequences of non-operation or misoperations are much dire for protection than say, for an image recognition application.
  - ML methods published to date are several orders of magnitude from achieving operational status, as standards for satisfactory security are very stringent.
- Testing with field data (if available):
  - It is unlikely that data collected at a substation would be appropriate to train devices located downstream.
  - Tested on the same network on which it is deployed – learning required for another network or for changes in topology.
  - Can you afford the training time in field?
  - Staged faults – not representative (example – High Impedance Faults)

Example – Could all these HIF be tested with the same dataset?

Theoretical Model





Hurdles to use of AI in Protection - II

- Data – very hard to get:
  - Different types of sensors will have different resolutions – phasor/waveform/harmonics
  - Even same type of sensors will have different errors.
  - The more features you create, you will more likely need different data of different resolutions – meaning diverse sensors, with different errors.
  - Remember, we need *fault data*; most datasets available publicly are steady state data.
  - Simulated data for faults are not representative of field-data.
- Divergence:
  - Faults are not well-behaved. Even field data for the same type of fault can vary. Simulated data are even less representative of real-life faults.
  - Fault resistance can vary over a range, and vary unpredictably.
  - Legacy relays do operate for such "curved balls"; ML-based techniques have a poor record. Understanding the cause of failure and correctability are lacking.

Solutions/Applications

- Conventional methods have room for improvement, and in some scenarios ML techniques can provide useful augmentation to classical techniques.
- Most academic papers propose ML methods as as a wholesale replacement - don’t throw the baby with the bathwater.
- ML Techniques that supplement existing classical protection, or in other words, **physics-aware solutions** should be sought.
- Also be aware of the systemic nature of protection.
- Look at the performance-record of legacy schemes and alternate physics-based options before opting for AI (added value).
- Pick applications that do not suit physics-based protection – detect incipient faults.
- Best applications are where no physical models are available – detect misoperations, health monitoring….

Take Away

- All information indicative of faults has been already integrated in physics-based solutions. Can AI use the same information better without being opaque?
- Physics-aware AI solutions can be explored to improve the performance.
- There are areas where protection has known weaknesses and no robust models – these are ideal for AI.

Related Publications

- Jeffrey Wischkaemper, Sukumar Brahma, “Machine Learning and Power System Protection [Viewpoint]”, *IEEE Electrification Magazine*, March 2021, pp. 108-112.
  - Talks about hurdles in more detail.
- S. Brahma, R. Kavasseri, Huiping Cao, N. R. Chaudhuri, T. Alexopoulos, and Y. Cui, “Real Time Identification of Dynamic Events in Power Systems using PMU data, and Potential Applications – Models, Promises, and Challenges”, *IEEE Trans. Power Delivery – Special Issue on Innovative Research Concepts for Power Delivery Engineering*, Vol. 32-1, pp. 294 – 301, Feb. 2017.
  - Detects relay misoperations in real time.
  - Uses field data, demonstrates the challenges in using field data (corrupt files, few ground truths), navigates through these challenges, illustrates physics enhanced solution.