Speed and Security Considerations for Protection Channels

Shankar V. Achanta, Ryan Bradetich, and Ken Fodero

Schweitzer Engineering Laboratories, Inc.

Brief History of Pilot Protection

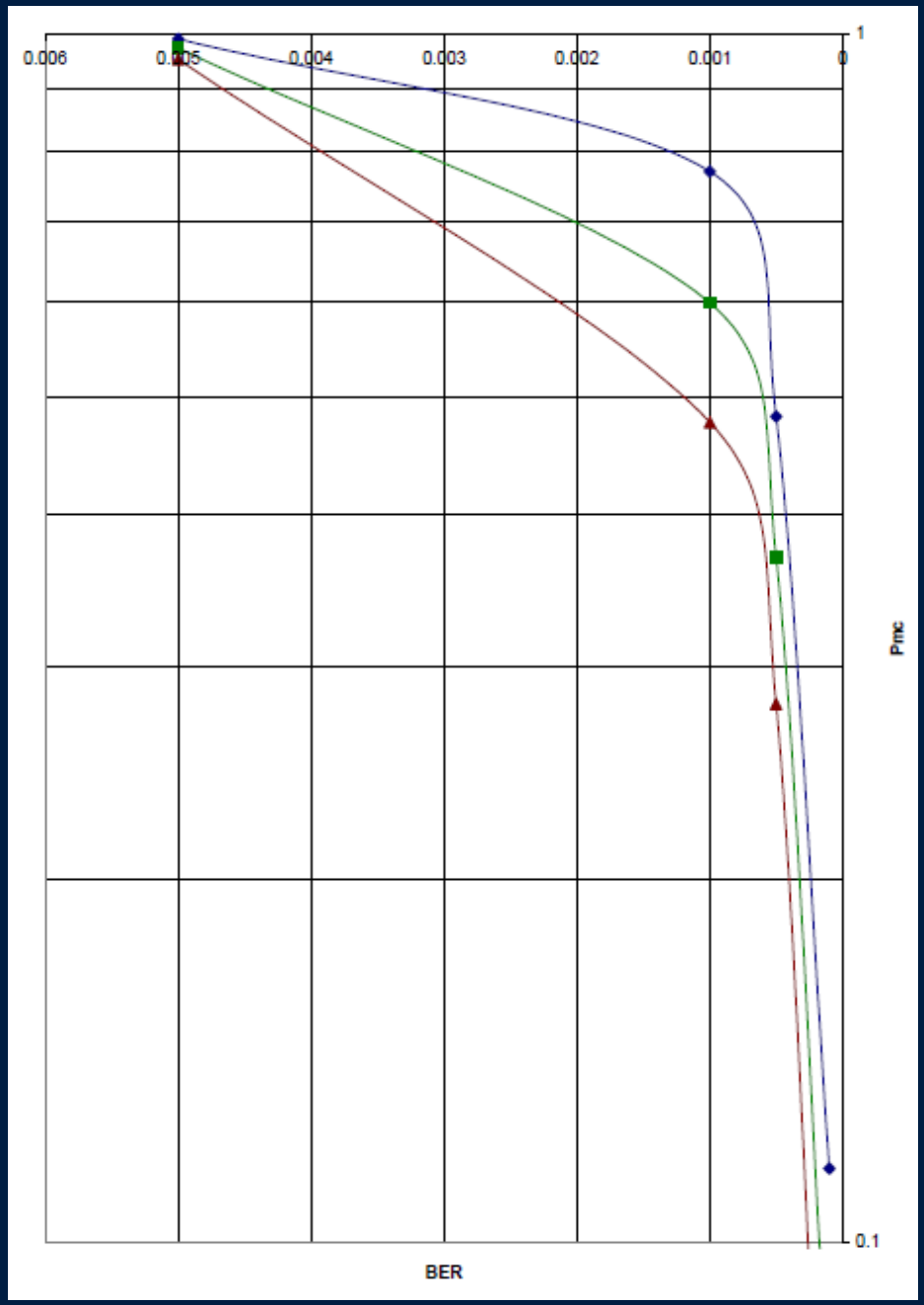
- Pilot protection schemes have been in service since 1940s
- In late 1960s, solid-state audio tone systems, leased four-wire circuits, and analog microwave increased pilot protection availability
- In 1980s, digital communications operating on fiber-optic medium began to appear

Cybersecurity Considerations

- Pilot protection systems are point-to-point
- Spoofing and tampering have minimal effect on bulk electric system
- Pilot protection systems are typically isolated from external networks

Teleprotection Is Standards-Based

- Environmental – IEEE C37.90, IEEE 1613
- Audio tones – IEEE C37.93
- Teleprotection – IEC 60834-1
- Power line carrier (PLC) – ANSI C93.5

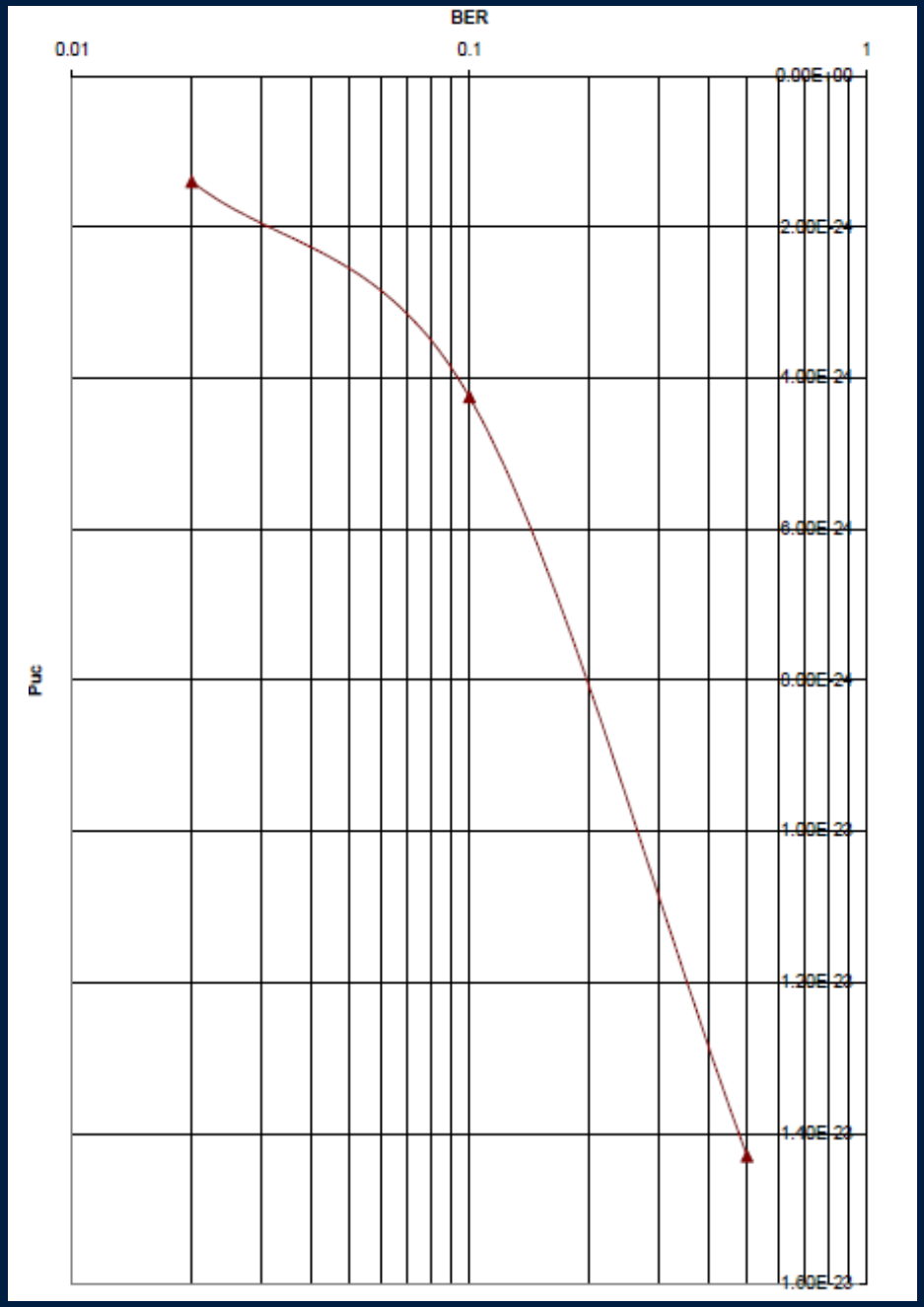


Security and Dependability

IEC 60834-1

Probability of missing command (dependability)

$$P_{MC} \approx \frac{N_T - N_R}{N_T} = 1 - \frac{N_R}{N_T}$$



Security and Dependability

IEC 60834-1

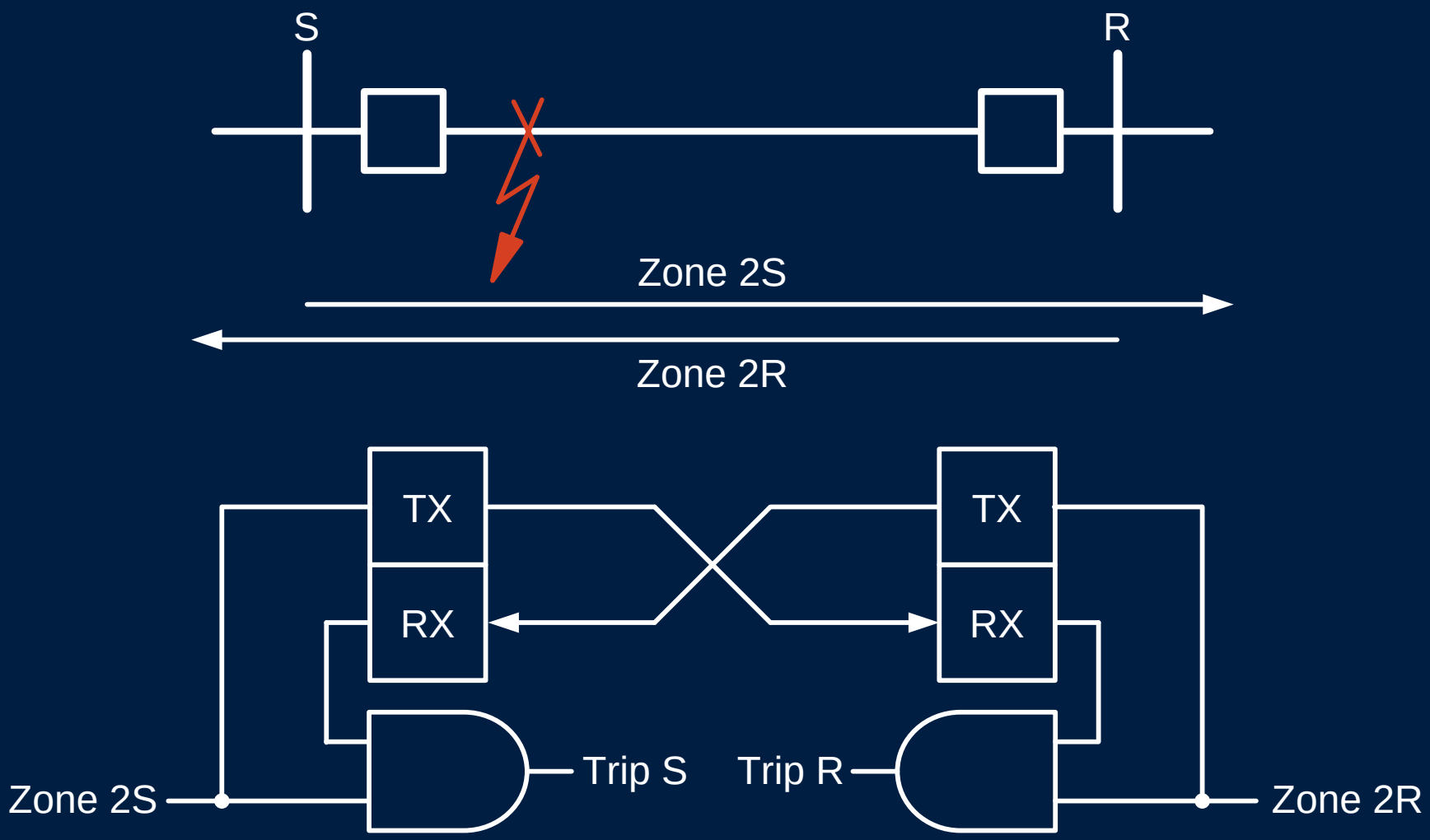
Probability of unwanted command (security)

$$P_{UC} \approx \frac{N_{UC}}{P_B}$$

Pilot Protection Relay Schemes

- Permissive overreaching transfer trip (POTT)
- Directional comparison unblocking (DCUB)
- Directional comparison blocking (DCB)
- Direct transfer trip (DTT)
- Line current differential

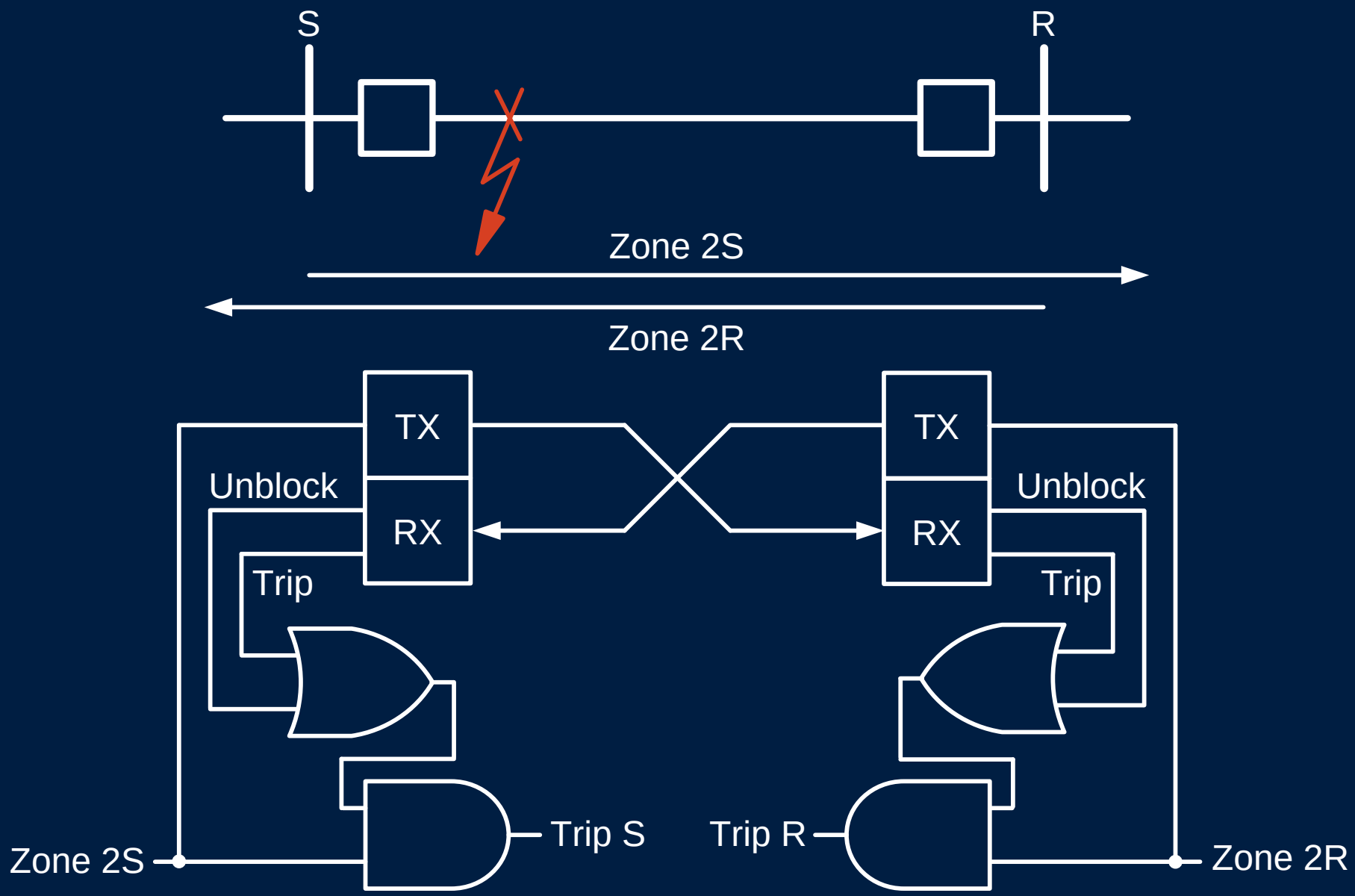
POTT Teleprotection



POTT Channel Requirements

- POTT schemes are inherently tolerant of propagation delay and channel asymmetry
- POTT teleprotection needs to provide high security and high speed (4–8 ms is typical)

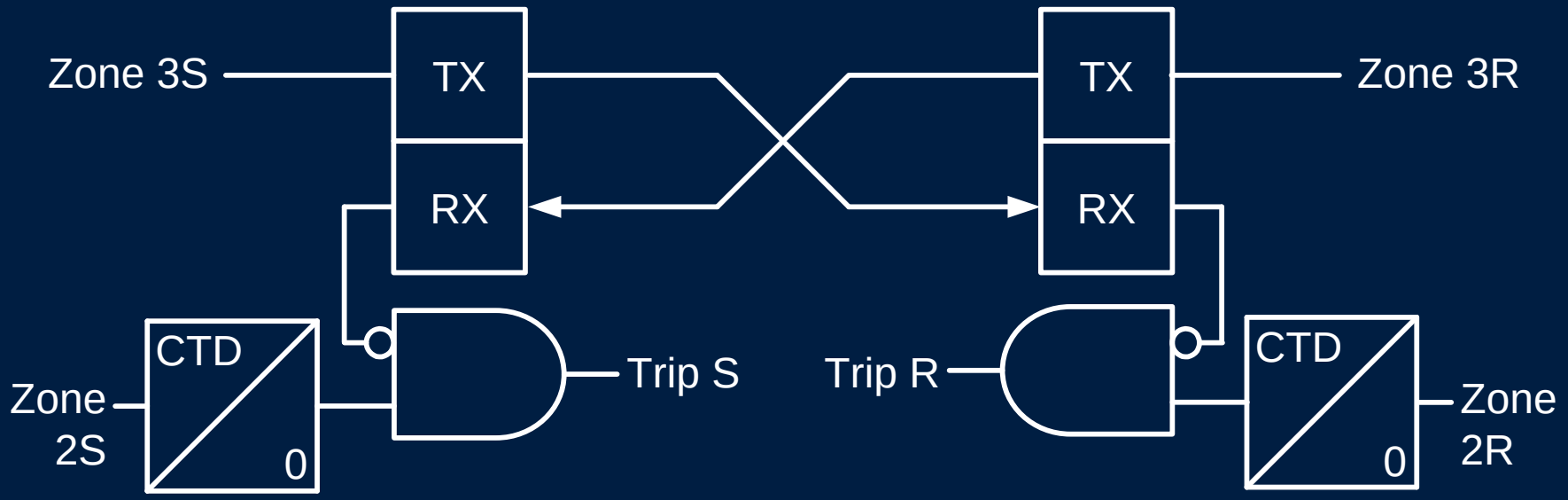
DCUB Teleprotection



DCUB Channel Requirements

- DCUB is POTT scheme adapted for use with PLC systems
- Unblock logic permits tripping if channel failure is caused by fault on power line
- DCUB teleprotection needs to provide high security and high speed (4–8 ms is typical)

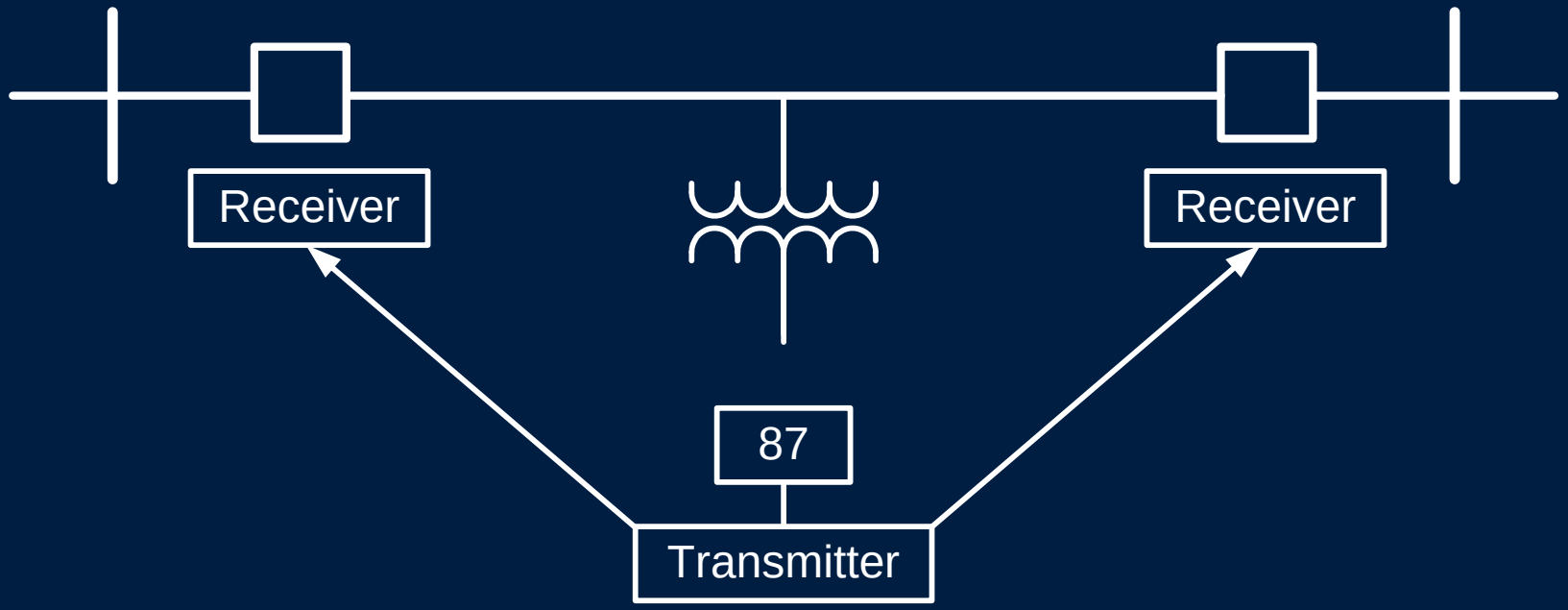
DCB Teleprotection



DCB Channel Requirements

- DCB schemes are intended for use with on/off PLC systems
- Teleprotection signal is sent to prevent tripping
- DCB teleprotection needs to provide high dependability and ultra high speed (1.5–5 ms is typical)

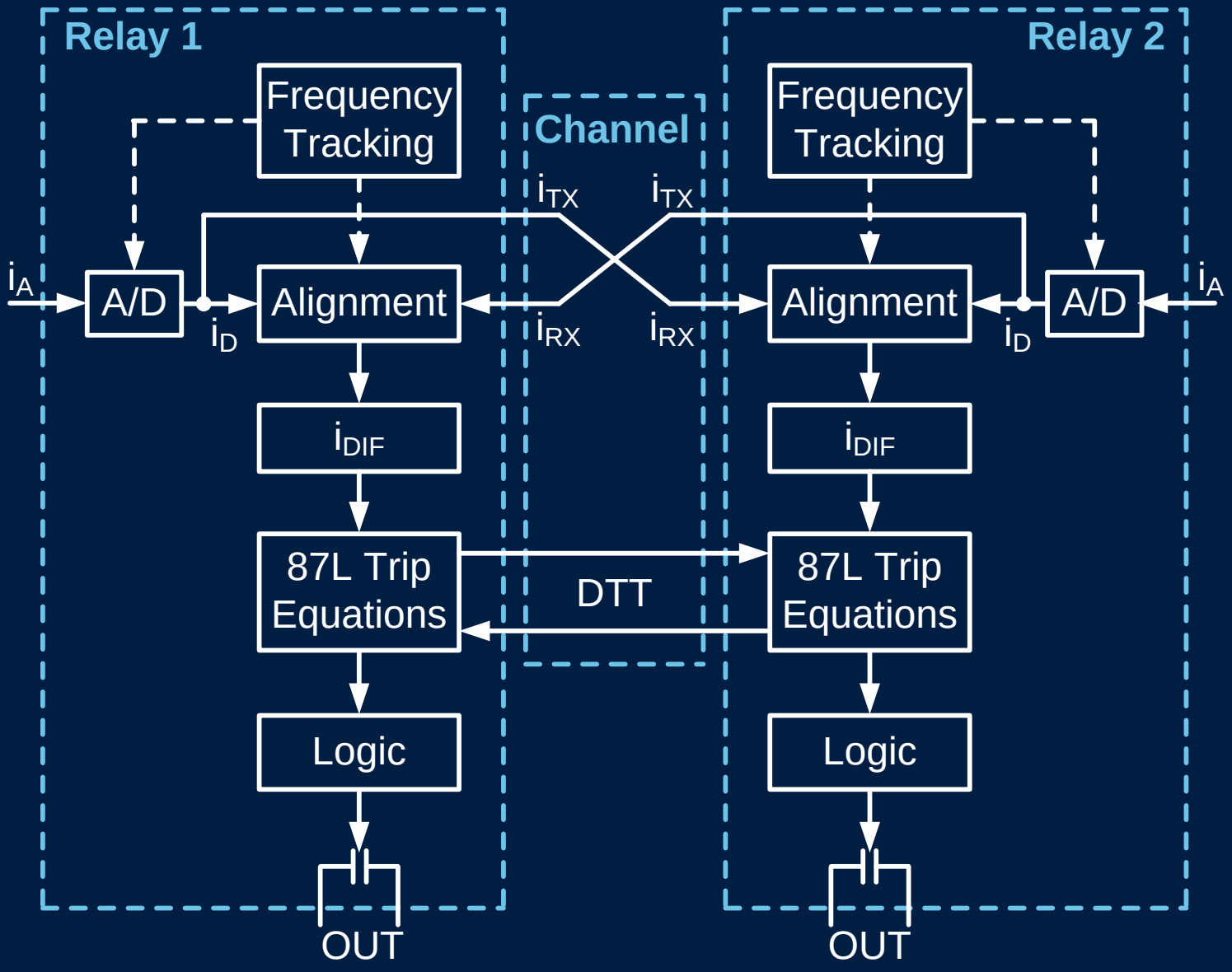
DTT Teleprotection



DTT Channel Requirements

- DTT schemes are typically used for breaker failure schemes and for remote equipment protection
- Teleprotection signal trips circuit breaker directly
- DTT teleprotection needs to provide high security and medium speed (8–12 ms is typical)

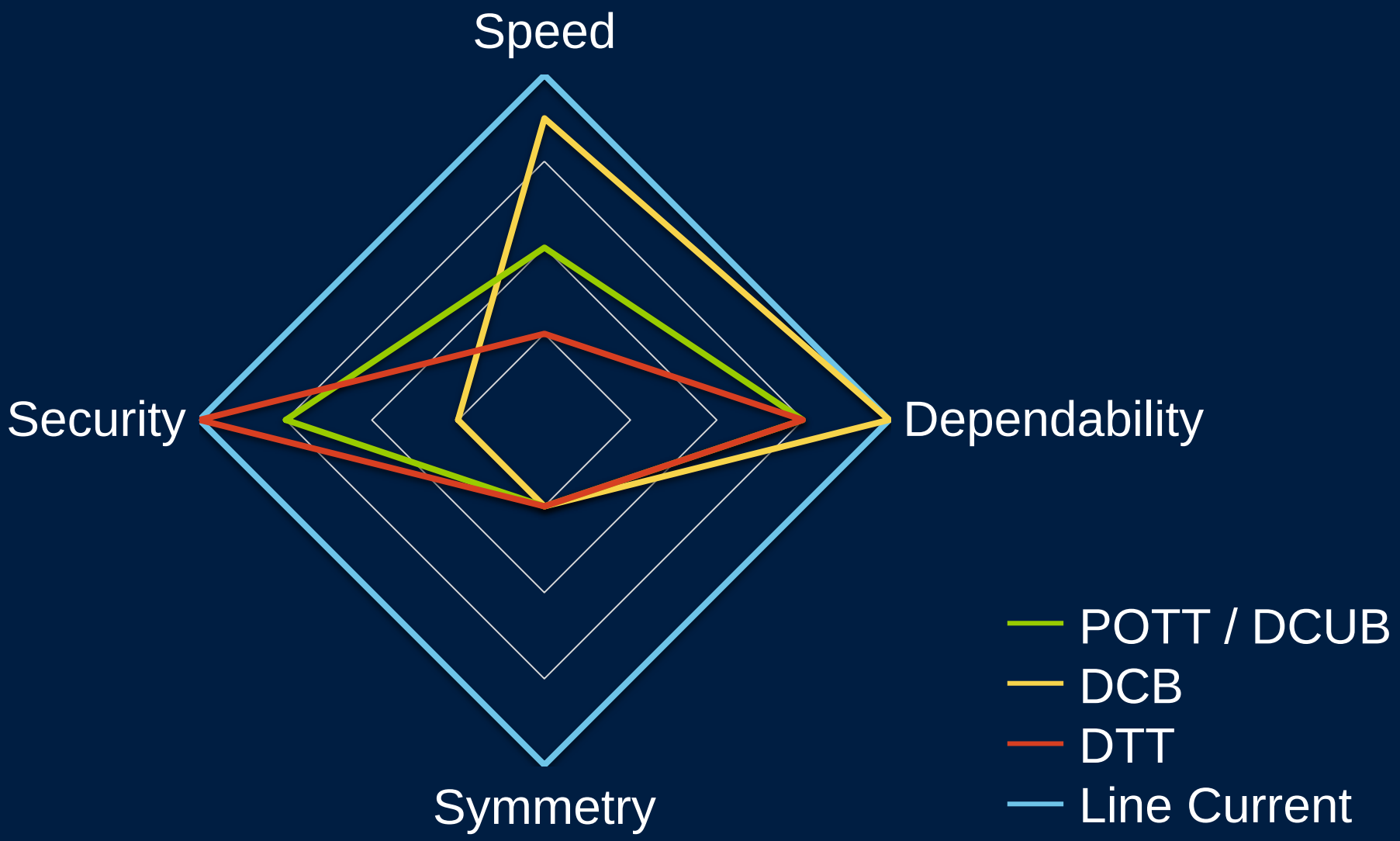
Line Current Differential



Line Current Differential Channel Requirements

- Line current differential is communications-dependent protection scheme
- Scheme provides high availability, ultra high speed (1–2 ms), low asymmetry (<4 ms), and deterministic latency

It’s Not Just About Speed



It’s Not One-Size-Fits-All

- Requirements are different for extra-high-voltage protection verses subtransmission protection
- Ultimately, effect on system stability, equipment through-fault tolerance, and other system performance requirements dictate speed requirements

Performance Varies by Technology

- Direct fiber
- PLC
- Microwave
- Unlicensed radio
- Time-division multiplexer (TDM)
- Ethernet transport

Transport Technology Challenges

Each transport system technology change has presented new advantages and challenges for traditional teleprotection systems

Speed Is Not Only Priority

- We need to get back to first principles
- Speed is important but not at expense of security and dependability of teleprotection
- Reliability of transport system is just as important

Transport Technology Is Changing

- There is migration toward using Ethernet for substation communications
- This introduces challenge of running TDM-based teleprotection across packet-based networks

Merging IT and OT

- There is drive to merge corporate core network with substation control and automation network
- Merger of these two networks exposes OT network to IT events, potentially affecting protection system performance
- OT network is no longer isolated, exposing it to greater cybersecurity risks

Conclusion

- We need to understand
  - Performance and failure modes of modern Ethernet transport systems
  - Impacts of combining IT and OT networks
- This will ensure that we maintain reliability of existing teleprotection systems

Questions?