IMPLEMENTING SCADA REDUNDANCY

Presenter: Justin Turner – GE Vernova

Authors: Walid Ali – GE Vernova, Justin Turner – GE Vernova

2024 Texas A&M Conference for Protective Relay Engineers

AGENDA

- Abstract
- Introduction to SCADA Redundancy
- Reliability, Maintainability, and Availability
- System Redundancy vs Network Redundancy
- System Redundancy
- Network Redundancy (Ethernet)
- Redundancy Implementation Examples
- Conclusion

ABSTRACT

Abstract

While system redundancy is a must have on a protection scheme especially on a transmission substation, redundancy is also highly desirable for substation automation. Redundancy is a balance between the criticality of a substation and equipment reliability and availability. Redundancy can enable the automation system to run flawlessly even through issues like equipment failure and cyber security concerns. This paper will explore the various types of redundancy including system redundancy with emphasis on independent dual redundancy and various types of standby redundancy and combination of both. The paper will describe different considerations when implementing redundancy in various scenarios.

INTRODUCTION TO SCADA REDUNDANCY

Introduction to SCADA Redundancy

In the domain of power system protection, redundancy emerges as an indispensable element, particularly within Transmission Substations. Its significance, however, transcends mere protection schemes, taking on paramount importance in the realm of Substation Automation. Here, redundancy delicately balances the significance of a substation with the reliability of its equipment, ensuring seamless system operation even in the face of challenges like equipment failure and cyber threats.

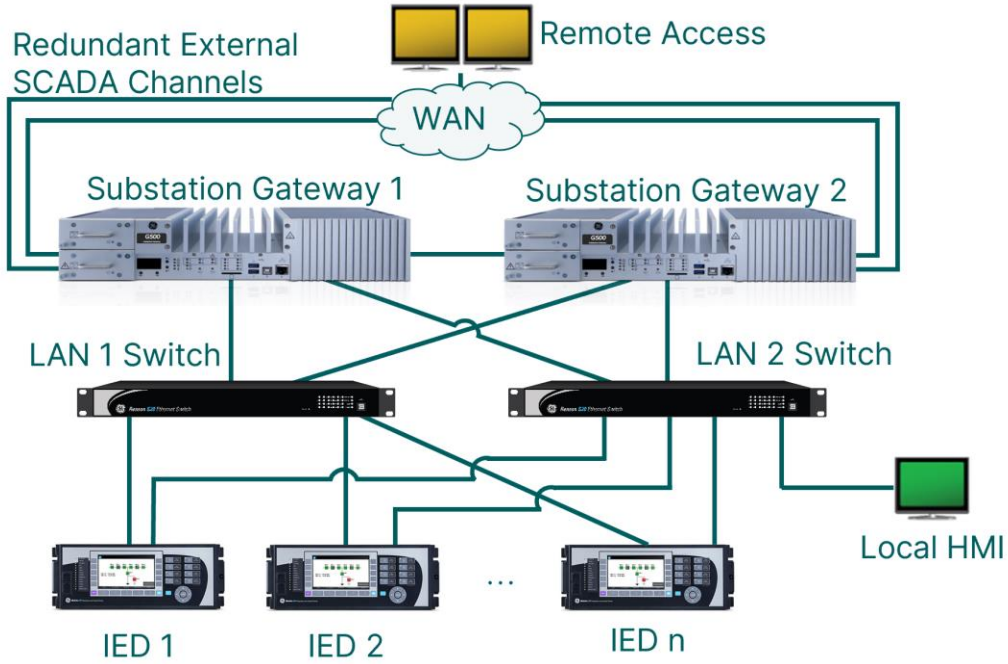
Objectives:

Consider how redundancy impacts reliability, availability, and maintainability

Investigate system redundancy in its diverse forms and their combinations

Delve into network redundancy

Explore different redundancy implementation examples



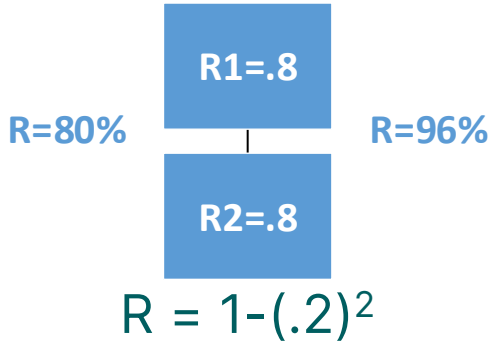
RELIABILITY, MAINTAINABILITY, AND AVAILABILITY

Reliability

- **Reliability:** The probability of the system or device will operate without any failure for a given time under the specified environment condition

- R=1–*F* where F is Failure Rate and R is reliability
  - R = 1 means perfect reliability and R = 0 implies complete failure

- When redundancy is introduced, reliability can be refined to $R= 1- (F)^2$
  - Note: This is a simplified model assuming two identical systems with the same probability and distribution of failures



Maintainability

- **Maintainability:** The probability that a failed component or system will be restored or repaired to a specified condition within a specified period
- A failed system that has a low probability of being repaired has low maintainability
- A failed system that takes a significant amount of time to repair also has low maintainability
- Redundancy may allow for a system to continue to operate while an individual component is out of service for repair or replacement with minimal system failure time

Availability

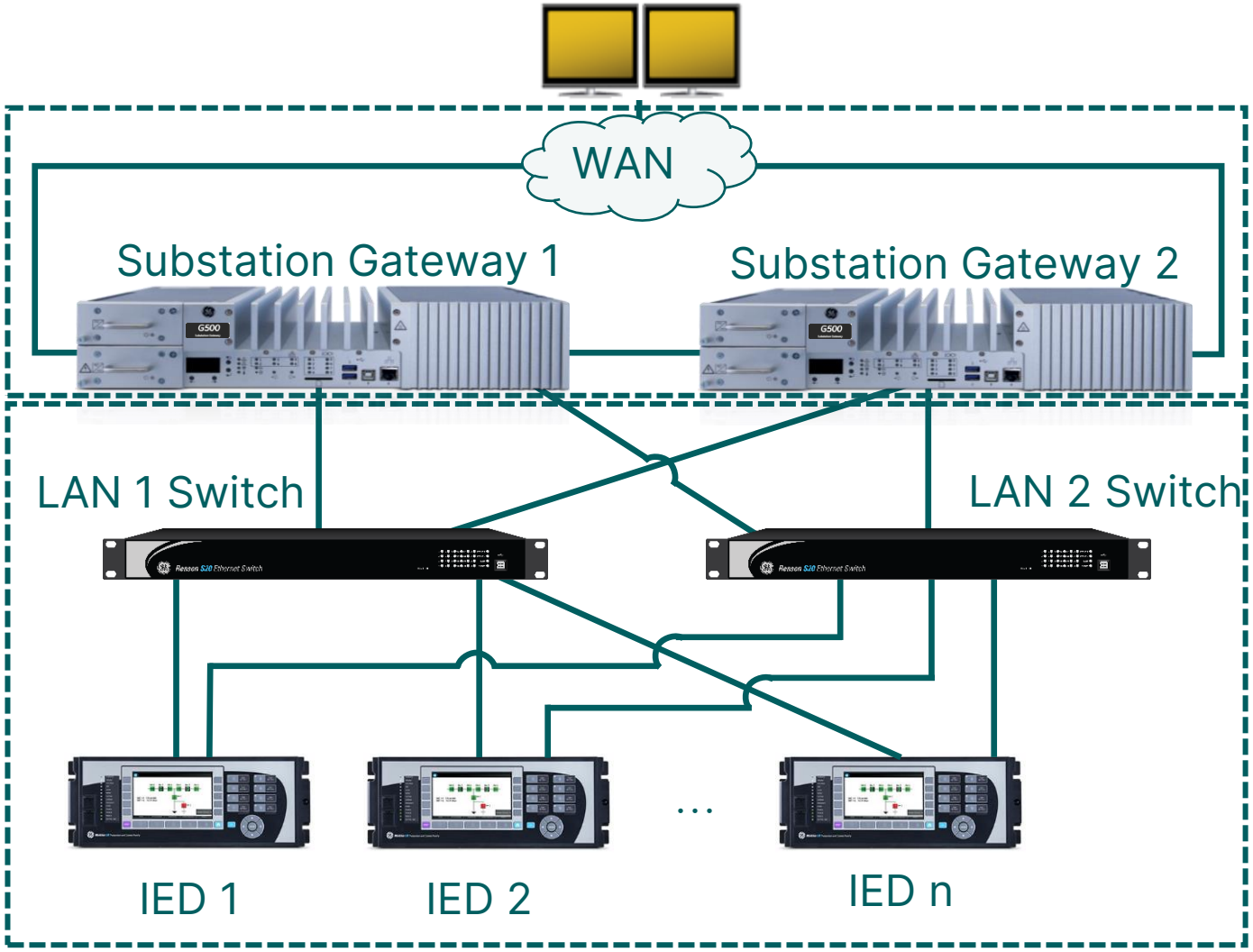
- **Availability:** The probability of the system or device to perform its functions while not in a failed state or repair state. Availability is a function of both reliability and maintainability

- Availability can be expresses as
  - A_i (Inherent Availability) = MTBF / (MTBF+MTTR)
    - MTBF is Mean Time Between Failure and MTTR is the Mean Time to Repair. Note this equation does not take into account preventive maintenance down time, logistics delay
  - A_o (Operational Availability) = Uptime / Operating Cycle
    - Ao takes into account all downtime including preventative maintenance and logistics and better reflects the real time experience the system is available
- Redundancy can bring availability from 99% to 99.99% (A = 1-(.01)2 = 99.99%) means reducing unavailability from 3.65 days per year to 50 minutes per year and conversely increasing availability

SYSTEM REDUNDANCY VS NETWORK REDUNDANCY

System vs Network Redundancy

- System redundancy refers to the duplication of one or more critical components (or sub systems) in a larger system as seen in the top dashed box
- E.g., the primary Substation Gateway 1 and the secondary Substation Gateway 2 are both connected to all downstream IEDs and in synchronization with each other
- Network redundancy involves duplicating or diversifying communications network infrastructure components and paths to ensure continuous connectivity and data transmission in the event of network failures
- E.g., each IED and Gateway has two LAN connections to different network switches as seen in the below dashed box



SYSTEM REDUNDANCY

No Redundancy

- Systems with low or no criticality may not need a redundant system
- Single purpose, low impact systems may not need redundancy if it can be easily repaired or replaced without significant impact on operations
- Systems with low operational impact and low risk of failure may justify the resources required to implement a redundant system
- Legacy systems may not support redundancy and implementing redundancy may not be feasible without replacing the legacy system and sometimes surrounding infrastructure

Primary	Secondary
Powered on	None
Active	
Processing Data	
No Secondary	

Cold Redundancy

- Secondary system or component is powered off until needed
- Secondary system is not synchronized with the primary system
- Requires manual intervention to bring the secondary system online and start processing tasks
- May be used in operations where maintaining powered secondary systems is prohibitive, likelihood of failure is low, and the downtime associated with transitioning to a secondary system is acceptable

Primary

Powered on

Active

Processing Data

No Synchronization

Secondary

Powered Off

Manual Activation

No Data Processing

No Synchronization

Warm Standby Redundancy

- Secondary system is powered on and ready to take over in case of primary system failure
- Only the primary system is processing data during normal operation
- Data synchronization between the primary system and secondary system is minimal and limited to the most critical information
- Upon primary system failure, the secondary system will automatically detect the failure and perform the failover operation to the secondary system
- Warm standby systems allow for minimal, but acceptable, downtime while transitioning from the primary system to the secondary system with only critical data, if any, synchronized between the two systems
- Some database information may be lost

Primary	Secondary
Powered on	Powered On
Active	Automatic Activation
Processing Data	No Data Processing
Minimal Synchronization	Minimal Synchronization

Hot Standby Redundancy

- Secondary system is powered on and ready to take over in case of primary system failure
- Only the primary system is processing data during normal operation
- Constant data synchronization between the primary system and secondary system
- Upon primary system failure, the secondary system will automatically detect the failure and perform the failover operation to the secondary system
- Hot standby redundancy systems are commonly used in critical applications where minimal operational downtime and minimal data loss is essential
- Minimal or no loss of database information

<u>Primary</u>

Powered on

Active

Processing Data

Constant Synchronization

<u>Secondary</u>

Powered On

Automatic Activation

No Data Processing

Constant Synchronization

Hybrid Redundancy

- A redundant system may have multiple applications which support different levels of redundancy
- More modern applications typically support higher or multiple levels of system redundancy

Example

- DNP3 hot-hot redundancy will have active communications channels on both primary and secondary systems and constant data synchronization to secondary system or simultaneous data processing on both systems
- Modbus hot standby will only have active communications on the primary system but will have constant data synchronization with the secondary system
- Third party non-standard protocol may only support warm standby with no active communications on secondary system and little to no data synchronization to secondary system

Hybrid Example

Hot – Hot: DNP3 Protocol Application

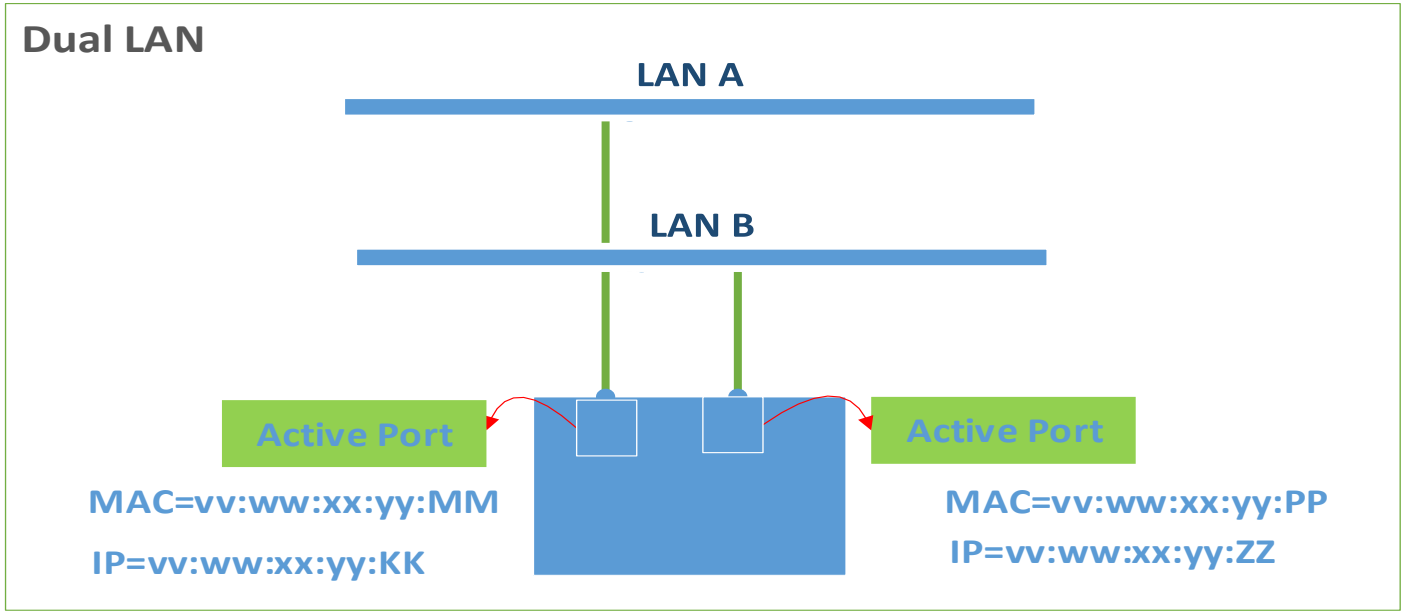
Hot Standby: Modbus Protocol Application

Warm Standby: Third Party Proprietary Protocol

NETWORK REDUNDANCY

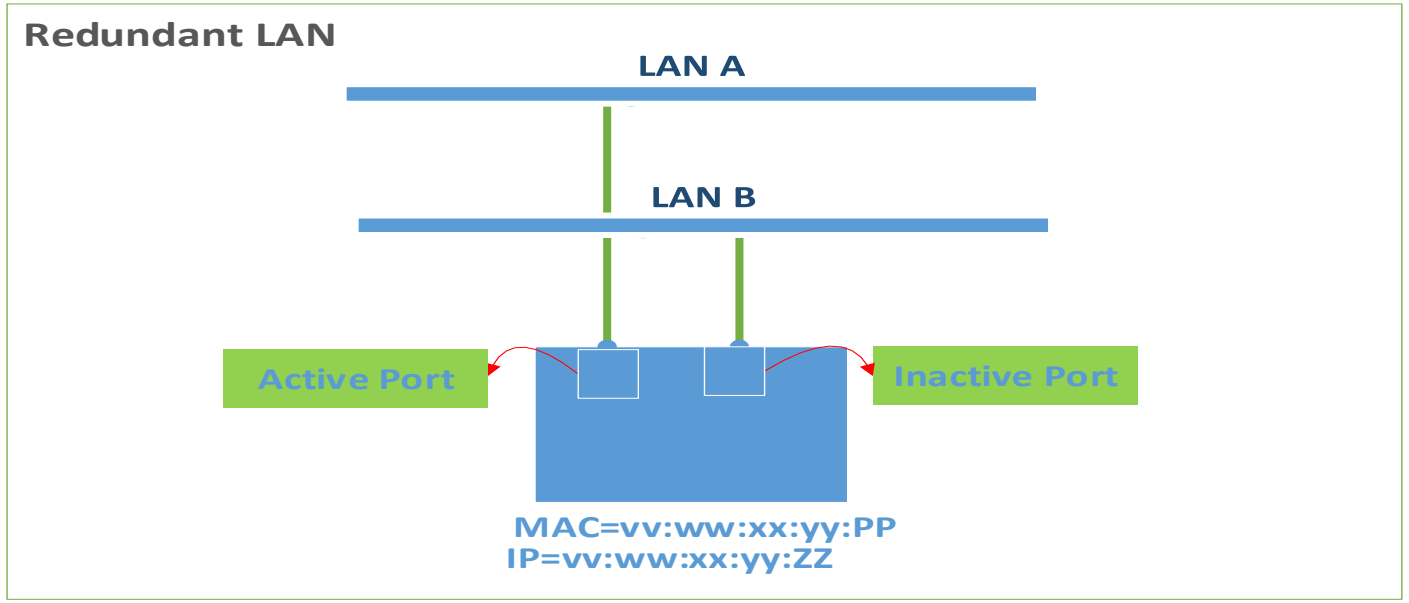
Dual LAN

- Dual LAN networks are two independent single LAN networks that connect the same devices together through different hardware and different subnets
- Two independent ethernet interfaces
- Both ports are active with separate IP addresses and subnets connected to different networks
- Redundant at the device application level and do not require any special redundancy protocol
- Failover happens in seconds
- Not suitable for highspeed communication protocols such as GOOSE messaging and Sampled Values



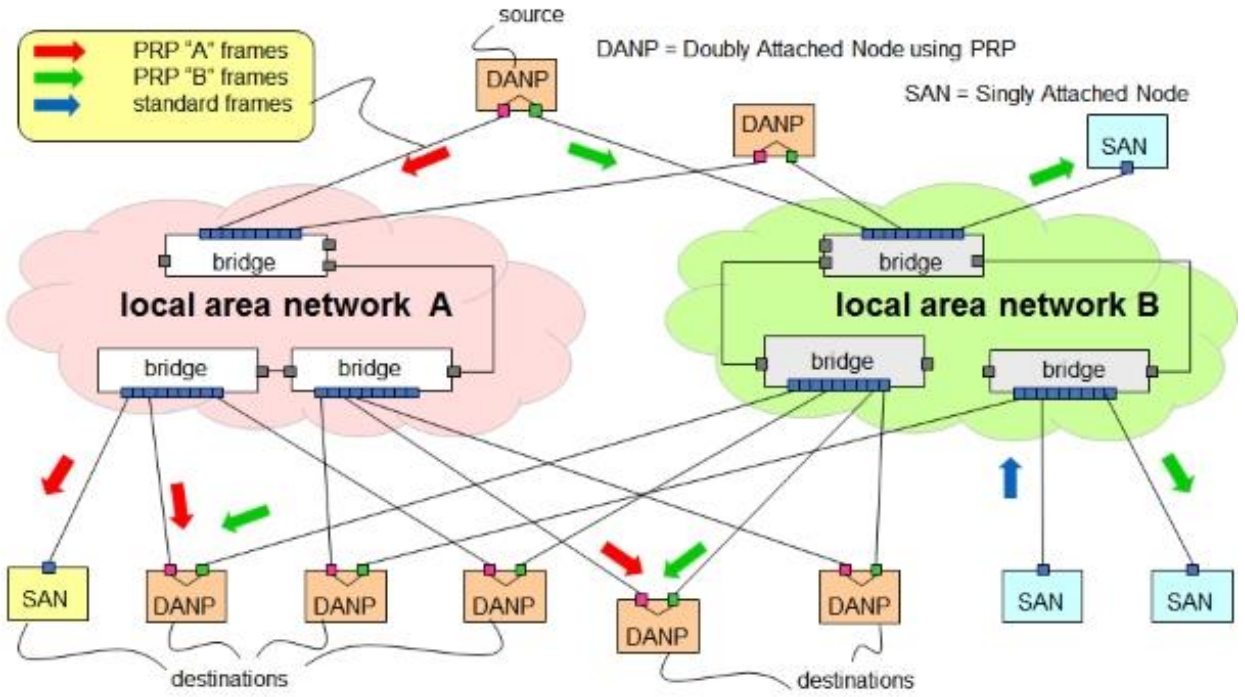
Redundant LAN

- Redundant LAN network interfaces work as a redundant pair
- Each device on the redundant LAN will need to have two ethernet interfaces that supports redundant pair
- The ethernet interfaces will share a common IP address and subnet
- Only one ethernet interface will be active at a time.
- Redundant pairs are supported at the device ethernet interface level, not the application.
- Failover happens in seconds
- Not suitable for highspeed communication protocols such as GOOSE messaging and Sampled Values



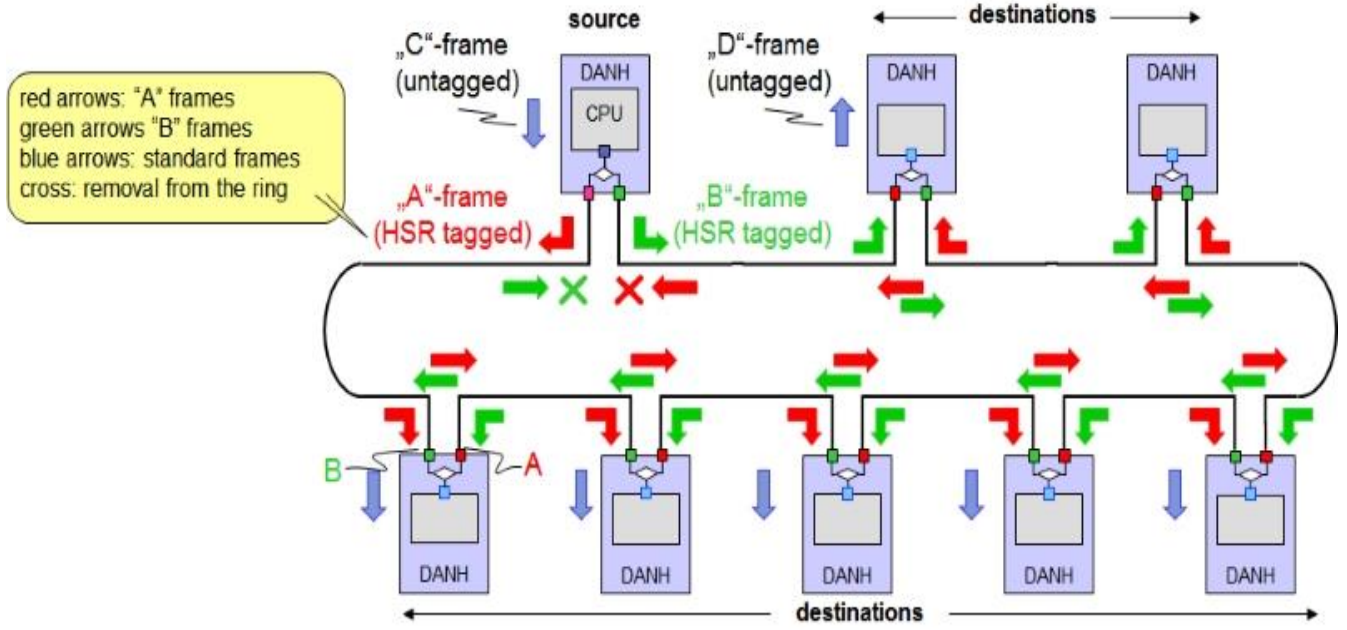
Parallel Redundancy Protocol (PRP)

- PRP is a redundancy protocol
- PRP network interfaces work as a PRP pair and each device on the PRP LAN will need to have two ethernet interfaces that support PRP
- The ethernet interfaces will share a common IP address and subnet
- Both ethernet interfaces will be active at the same time
- Ethernet frames are duplicated and sent over both network paths
- The receiving device accepts one message and discards the other message
- Failover is in microseconds
- Suitable for highspeed communication protocols such as GOOSE messaging and Sampled Values



High-availability Seamless Redundancy (HSR)

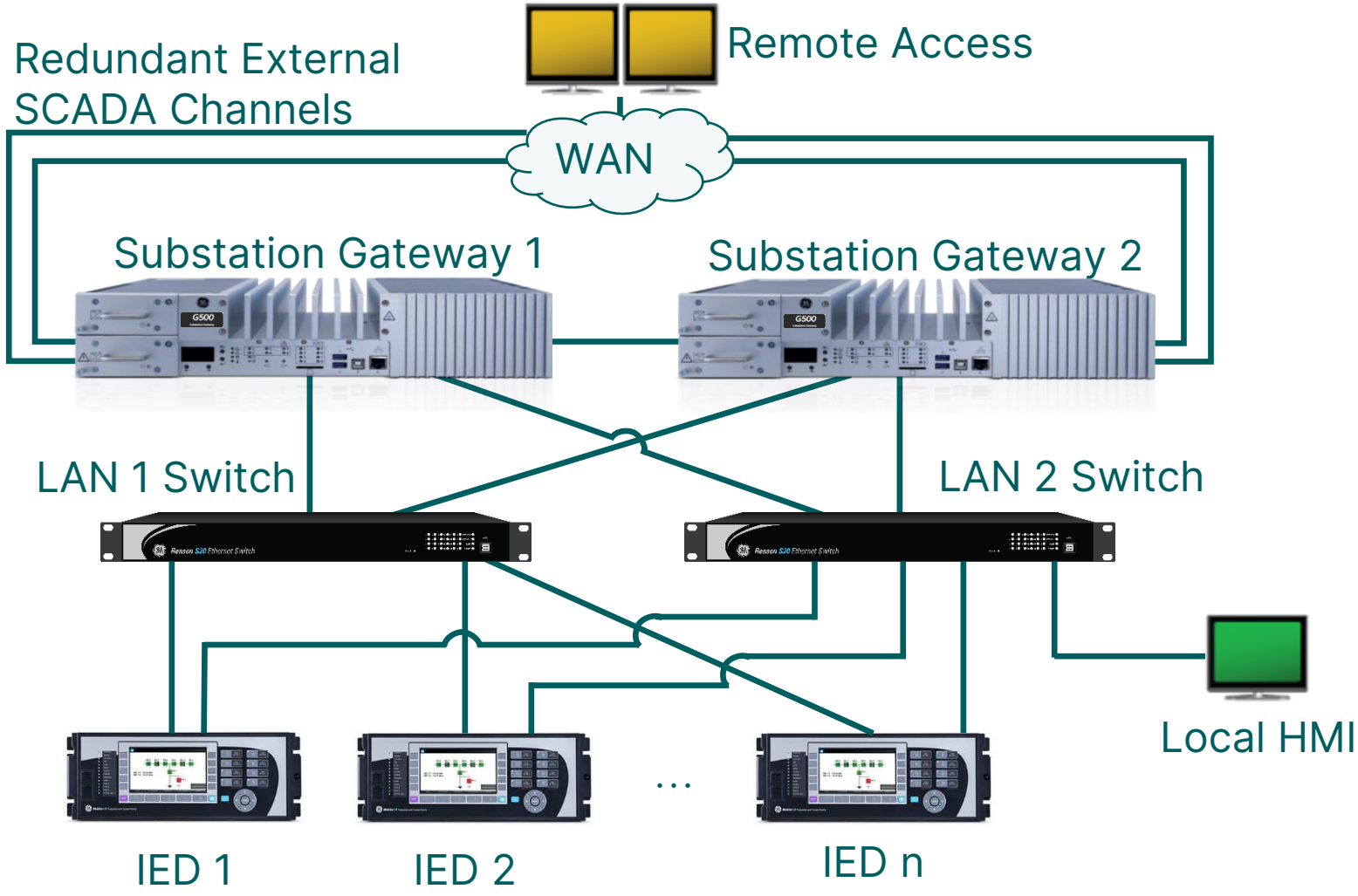
- HSR is a redundancy protocol
- HSR requires two ethernet interfaces per device that support HSR with different IP addresses
- Data is transmitted in both directions around the ring
- Each device in an HSR ring replicates and forwards ethernet frames not intended for that device from one port to the next creating two data flow rings
- Receiving devices accepts the first HSR frame and discards the duplicate frame
- HSR may require less networking resources since it employs a ring networking topology, no switches, less duplicate hardware
- HSR networks may face bandwidth constraints and device count restraints
- HSR has less networking topology flexibility, must be a ring



SCADA REDUNDANCY IMPLEMENTATION EXAMPLES

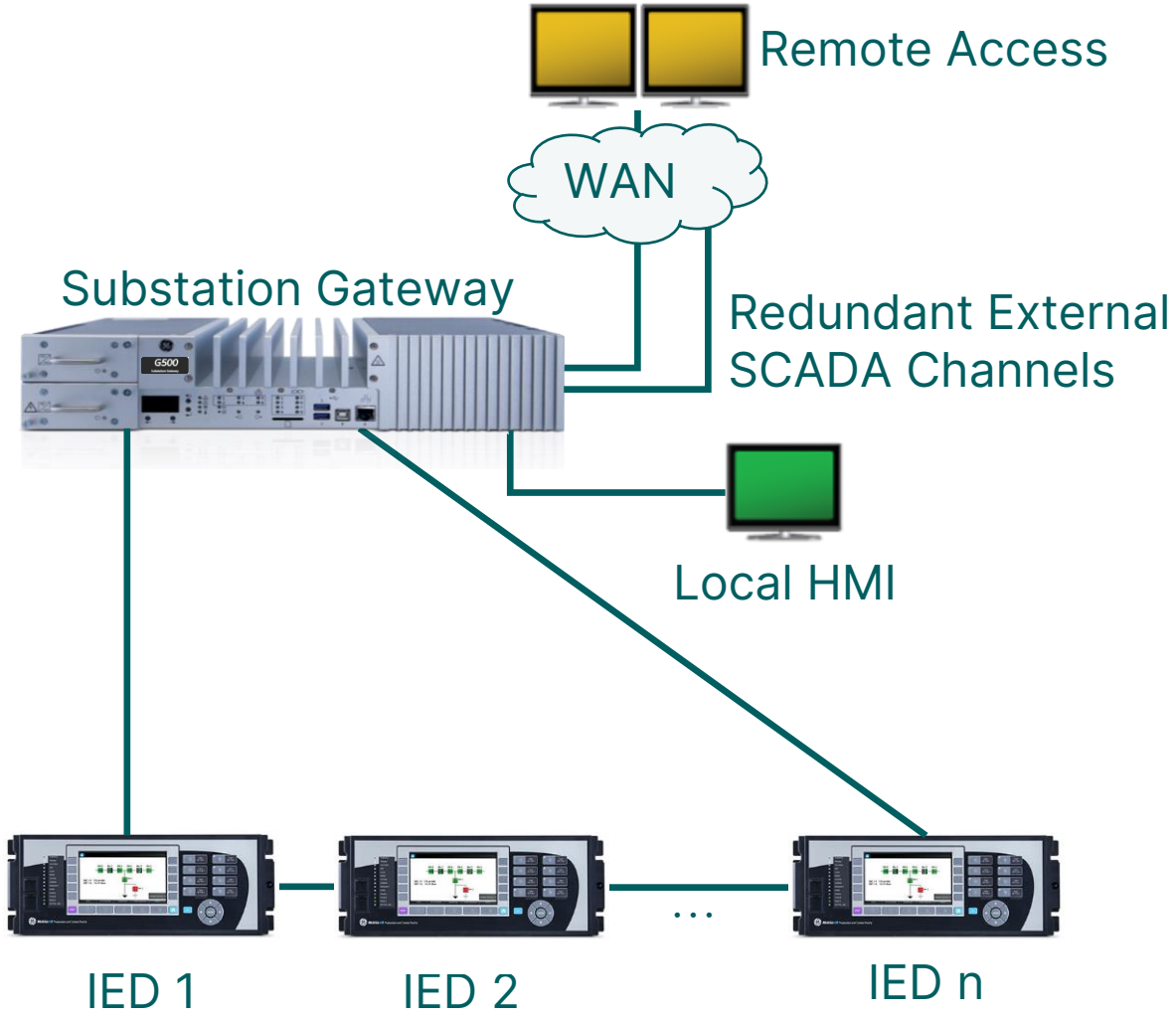
High Criticality Substation Redundancy Implementation

- Remote transmission interconnection
  - Low maintainability
  - Large impact to operations
  - Large service area
- Hot-Hot redundant system
  - Both systems powered on
  - Both comms active
  - Constant synchronization
- PRP Network Redundancy
  - High availability
  - Fast failover
  - Two independent LANs
  - High bandwidth
- Redundant external SCADA



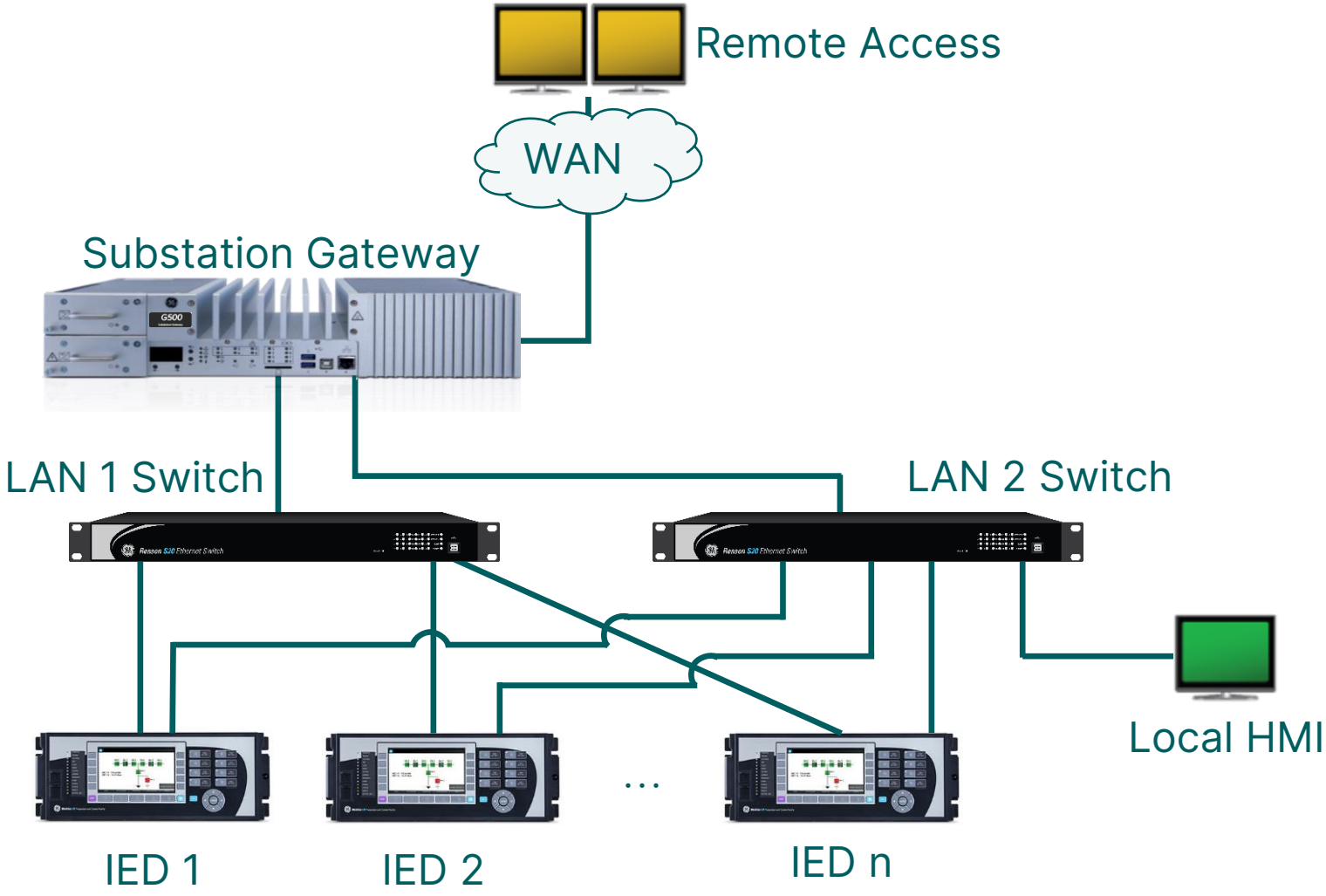
Medium Criticality Substation Redundancy Implementation

- Transmission Substation
  - Medium maintainability
  - Medium impact to operations
  - Medium service area
- No gateway system redundancy
- No switches
- HSR network redundancy
  - High availability
  - Fast failover
  - Redundant external SCADA



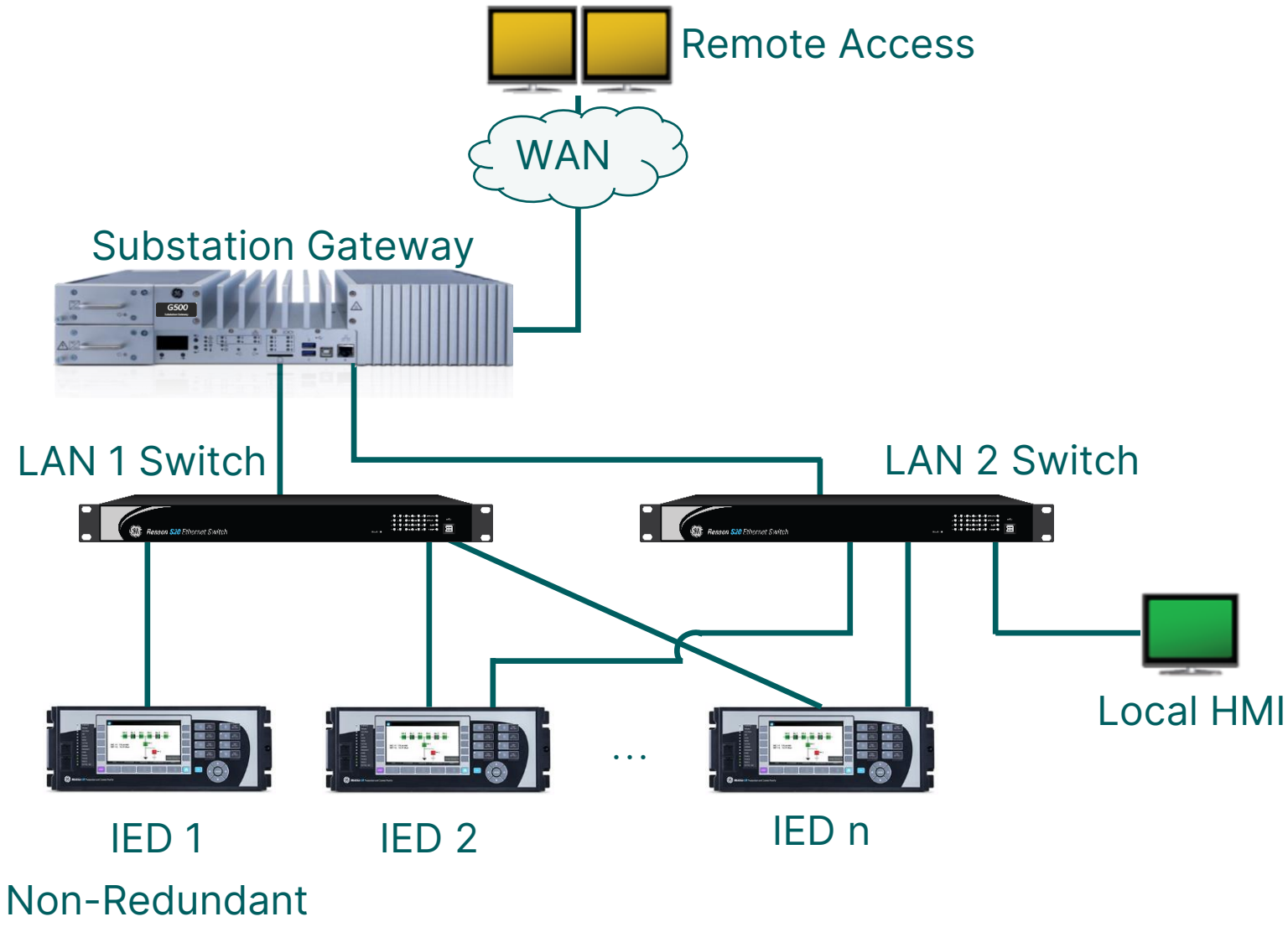
Less Critical Substation Redundancy Implementation

- Medium distribution substation
  - High maintainability
  - Medium impact to operations
  - Medium service area
- No gateway redundancy
- Redundant LAN
  - Slow failover (seconds)
  - Two independent LANs
  - High bandwidth
- No external SCADA redundancy



Non-critical Substation SCADA Redundancy Implementation

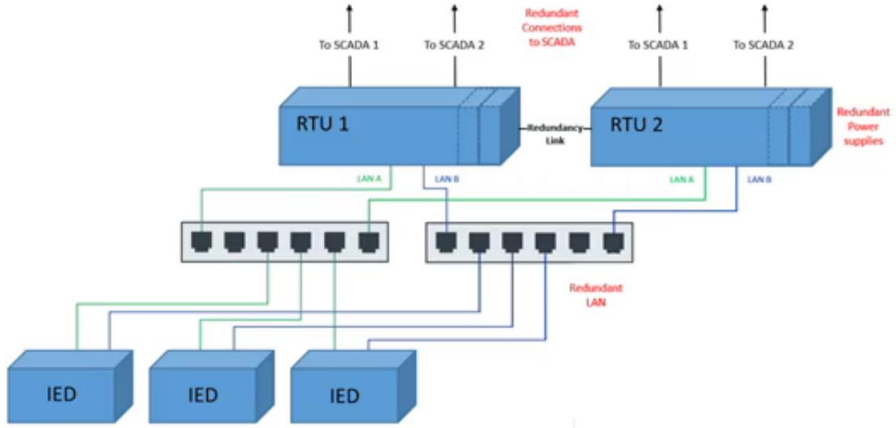
- Small Distribution Substation
  - Medium maintainability
  - Small impact to operations
  - Small service area
- No Gateway System Redundancy
- Mixed LAN
  - Redundant LAN devices and non-redundant LAN devices mix
  - Slow failover (seconds)
  - Two independent LANs
  - High bandwidth
- No external SCADA redundancy



CONCLUSION

Conclusion

- Redundancy, both at the system and network levels, emerges as a cornerstone in SCADA system reliability, availability, and maintainability
- Warm standby, hot standby, or hot-hot redundancy configurations offer distinct advantages in mitigating risks and sustaining operational resilience
- Network redundancies such as PRP, HSR, redundant LAN, and dual LAN further enhance fault tolerance and ensure seamless data acquisition and transmission, increasing overall SCADA system robustness
- By embracing the strategic deployment of redundancy strategies, engineers can navigate the complexities of modern SCADA systems, safeguarding against disruptions and implementing sustained operational excellence



QUESTIONS?