PWROG
PWR Owners Group

Global Expertise • One Voice

Lessons Learned in PRA Modeling of Digital Instrumentation and Control Systems

Richard Rolland (Westinghouse / PWROG)
Raymond Schneider (Westinghouse / PWROG)

Probabilistic Safety Assessment and Management
PSAM 16

June 26th, 2022 – July 1st, 2022

PWROG
PWR Owners Group

Topics

- Introduction / Background
- Overview of System
- Failure Modes and Effects Analysis
- Hardware Failure Rates of Digital Components
- Hardware Common Cause Failure and Software Failure
- Model Incorporation and Results
- Summary, Contact Information, and Q&A

Introduction / Background

PWROG Background

- PWROG Risk Management Committee (RMC) has identified digital instrumentation and control (DI&C) system modeling as an important effort for the industry to support risk-informed applications and meet the as-built, as-operated requirements for PRA applications.

- A project was completed to identify the best practices and lessons learned for DI&C system with current methodologies and data available.

- A pilot plant was used which modeled the safety features sequencer (SFS).

- Improvements have been identified for DI&C PRA modeling and future work is planned.

Overview of System

DI&C Improvements

- DI&C systems provide for additional system redundancy, including redundancy within a train or within an individual component.

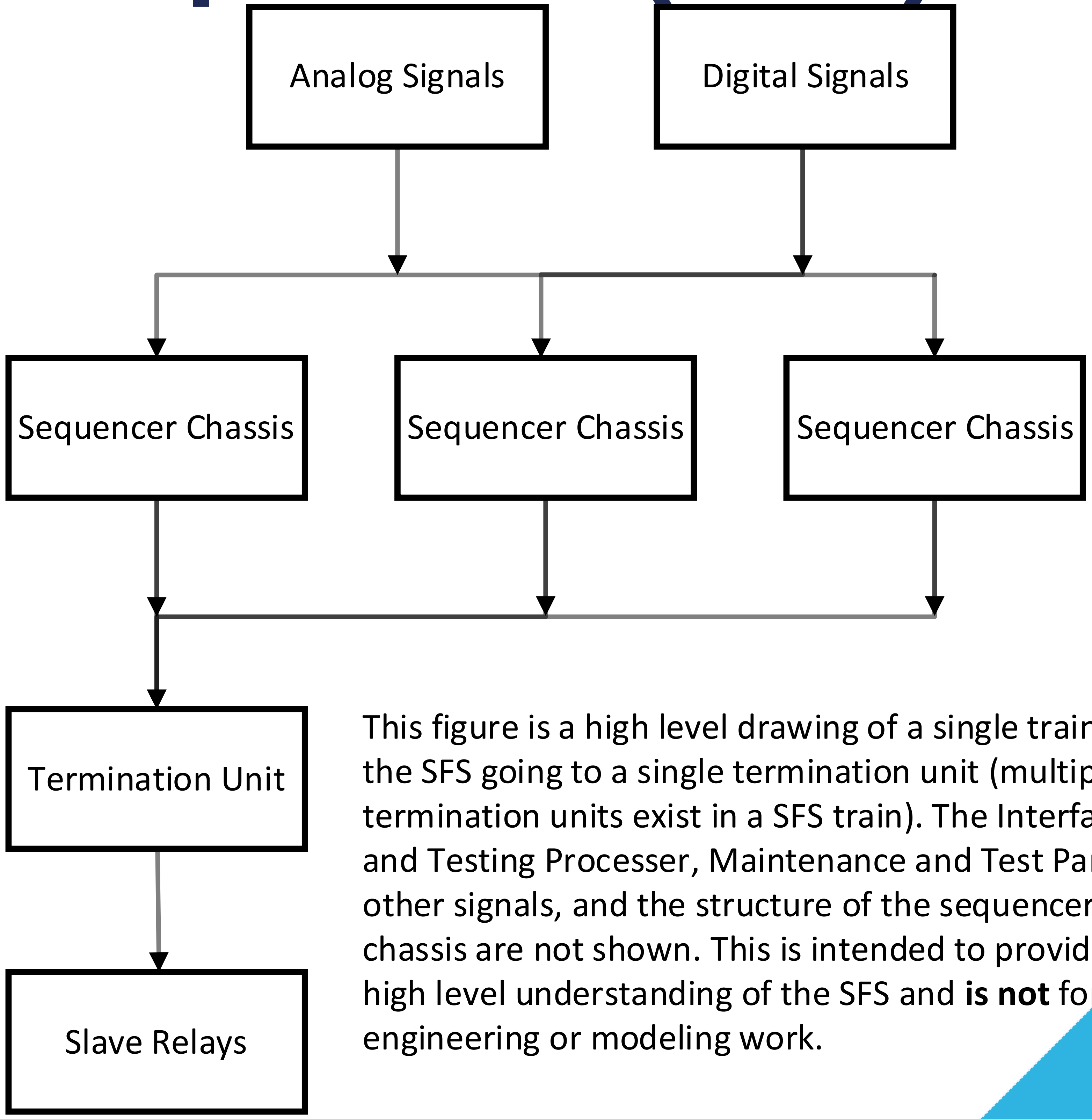
- DI&C systems may provide for online self-diagnostics including the ability to detect local failures.
  - Intended to enhance system reliability and reduce out of service time.

- Although there are benefits to DI&C systems, there is a reliance on common software throughout the system.
  - A software error can lead to a failure of all trains (e.g., same inputs leading to same software error).

DI&C Safety Features Sequencer (SFS)

- Provides actuation of diesel generator if loss of offsite power (LOSP) occurs and/or safety injection (SI) signal is received.

- Provides for proper load-shed and sequencing of engineered safety features (ESF) equipment in scenario of LOSP and/or SI signal to prevent overloading diesel generators.

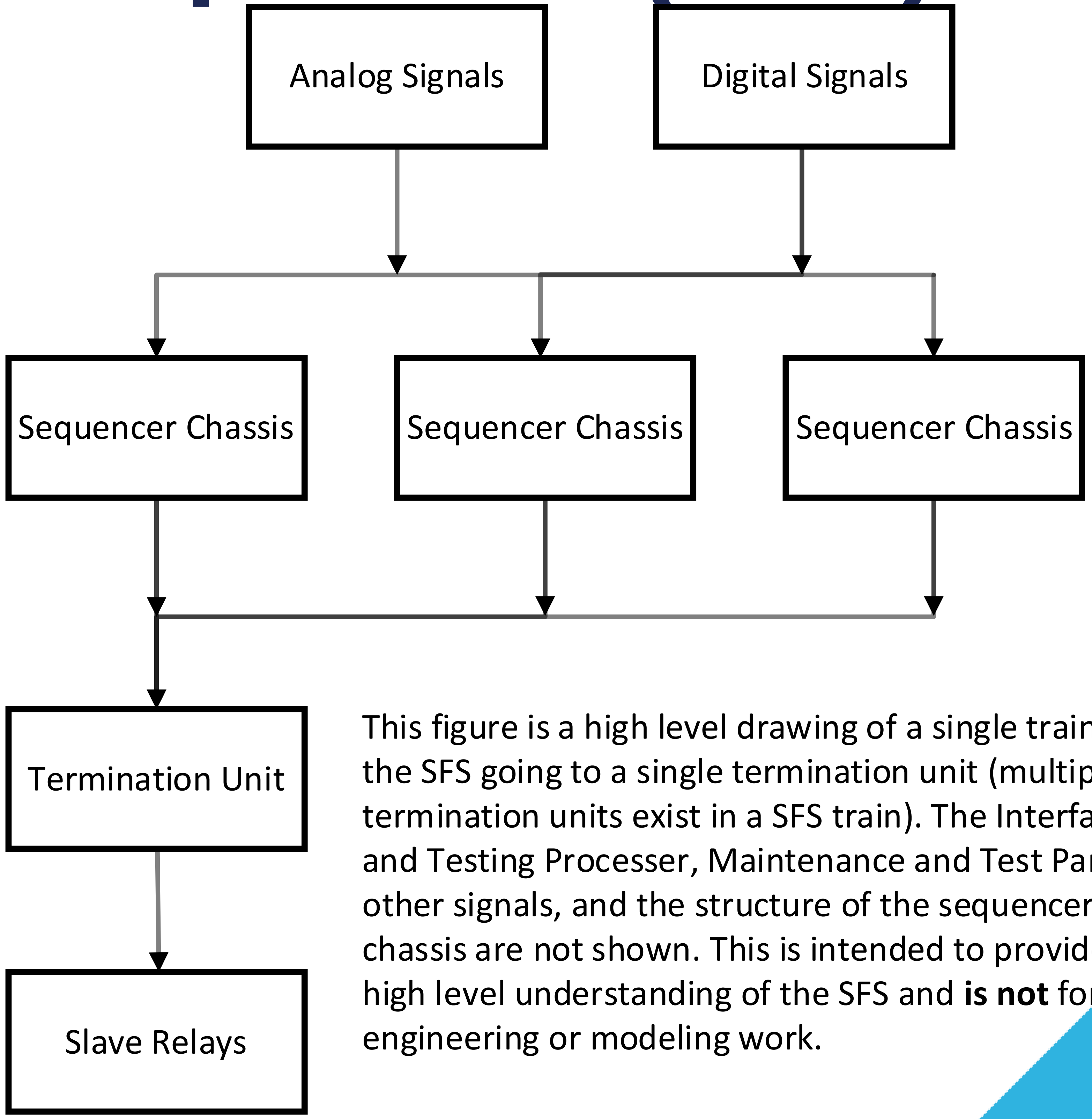


This figure is a high level drawing of a single train of the SFS going to a single termination unit (multiple termination units exist in a SFS train). The Interface and Testing Processer, Maintenance and Test Panel, other signals, and the structure of the sequencer chassis are not shown. This is intended to provide a high level understanding of the SFS and **is not** for engineering or modeling work.

DI&C Safety Features Sequencer (SFS)

- Signals evaluated in redundant sequencer chassis which then sends output signal to termination unit.

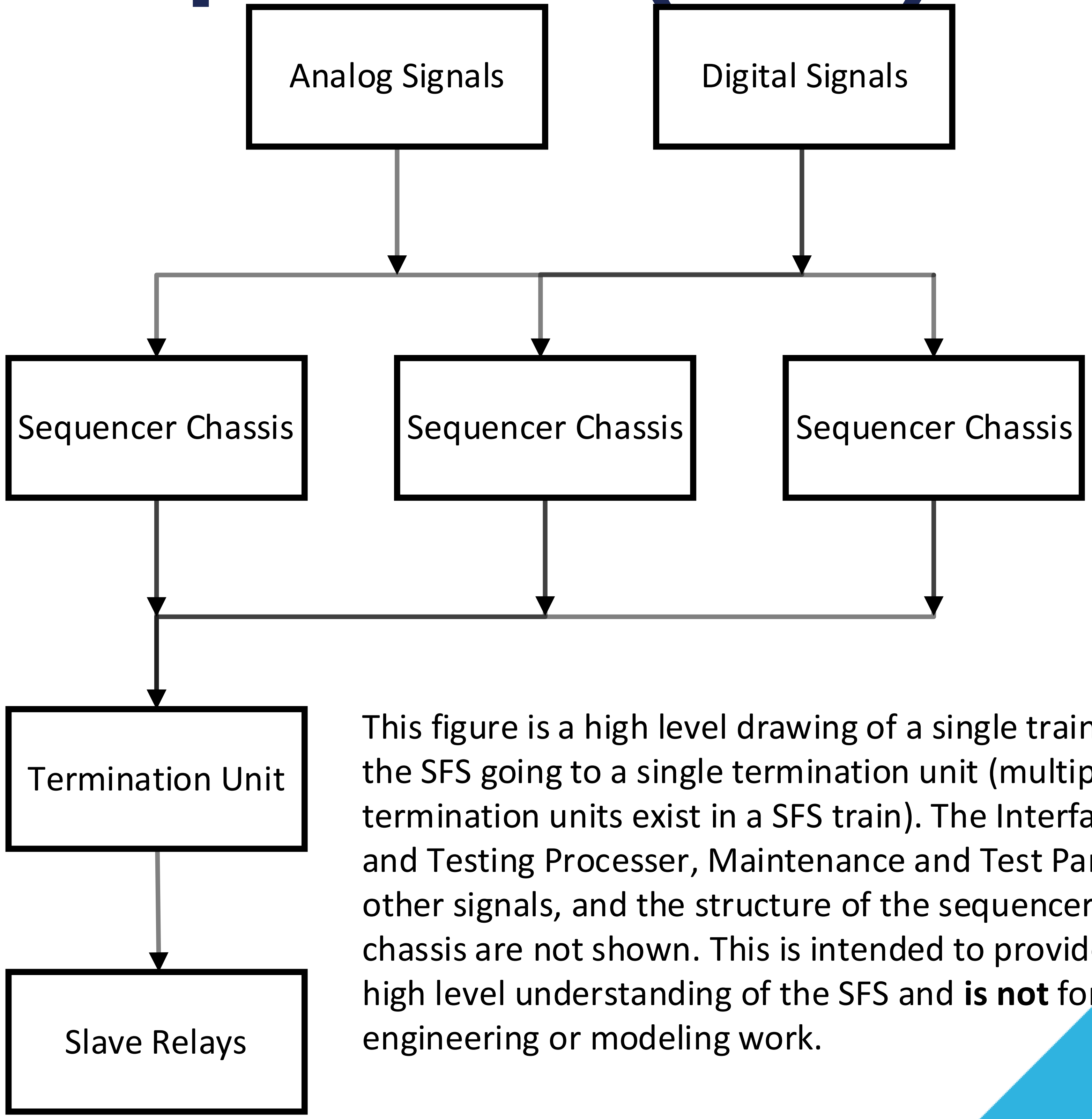
- Termination units complete voting logic to determine if signal should be sent to slave relays.



This figure is a high level drawing of a single train of the SFS going to a single termination unit (multiple termination units exist in a SFS train). The Interface and Testing Processer, Maintenance and Test Panel, other signals, and the structure of the sequencer chassis are not shown. This is intended to provide a high level understanding of the SFS and **is not** for engineering or modeling work.

DI&C Safety Features Sequencer (SFS)

- SFS has an interface and test processor, and maintenance and test panel that provides online testing, alarming, and maintenance capabilities.



This figure is a high level drawing of a single train of the SFS going to a single termination unit (multiple termination units exist in a SFS train). The Interface and Testing Processer, Maintenance and Test Panel, other signals, and the structure of the sequencer chassis are not shown. This is intended to provide a high level understanding of the SFS and **is not** for engineering or modeling work.

Failure Modes and Effects Analysis

Failure Modes and Effects Analysis

- FMEA provides a comprehensive assessment on the failure modes of the components within the digital system being examined.
- FMEA can be used to identify components that impact the safety functions of the SFS.
- FMEA can be used to identify if a component should be divided further into sub-components based on redundancy within the sub-components.
  - For example, should a termination unit be separated into multiple sub-components.

PWROG
PWR Owners Group

Failure Modes and Effects Analysis

- **Binning of Components in FMEA**
  - Identification of components that support safety functions from FMEA.
  - Helps to improve understanding of the DI&C system for further discussion with I&C system engineers on failure pathways.
  - Bin components in groups based on whether they support safety functions by themselves, with other component failures, or if the component failure does not contribute to a safety function failing.

Failure Modes and Effects Analysis

- **FMEA identifies testing capabilities within the SFS and its failure modes**
  - Can be used to identify appropriate way to model the SFS with regards to testing features.
  - Important to take these into account since they provide for realistic assessment of the DI&C system availability to respond to events.
  - I&C vendors generally collect information on the chance of failure of these automatic testing functions in detecting specific component failures.
  - These values, along with the mean time to repair, can be used to identify component unavailability.

Failure Modes and Effects Analysis

- **FMEA identifies the level of redundancy within the DI&C system**
  - Redundancies should be considered based on the level of benefit they provide (e.g., modeling at the sub-component level for specific channels rather than the component level that handles all channels).
  - Consider if the increased modeling complexity significantly impact risk insights of the model?
  - Example: A component may process several channels and each channel may be evaluated by a specific set of sub-components. If these sub-components are the main failure pathway for the component, sub-division to the channel level may have a significant impact on the failure rate of the system.

Failure Modes and Effects Analysis

- **Temperature Limits of DI&C Systems are Identified**
  - DI&C systems are more susceptible to temperatures.
  - Provides information on the necessary equipment (e.g., fans) required to maintain the system within operating temperature parameters.
  - Some components (e.g., fans) may not be required for successful operation of the DI&C system and the system may still remain in its operating conditions.
  - Temperature impacts can matter for performance of the DI&C components.

Hardware Failure Rates of Digital Components

Hardware Failure Rates

- **Challenges with DI&C Data**
  - Limited data compared to AI&C (fewer hours of operation).
  - Advantageous to discuss with I&C vendor on data available for their system and components (including temperature dependence).
  - Hardware vs. software failure identification from data collected can be difficult to always identify (e.g., replacing a part also may reboot the system).
    - Hardware data would be conservatively bounded if included several software failures.
    - Data has been improving.

Hardware Failure Rates

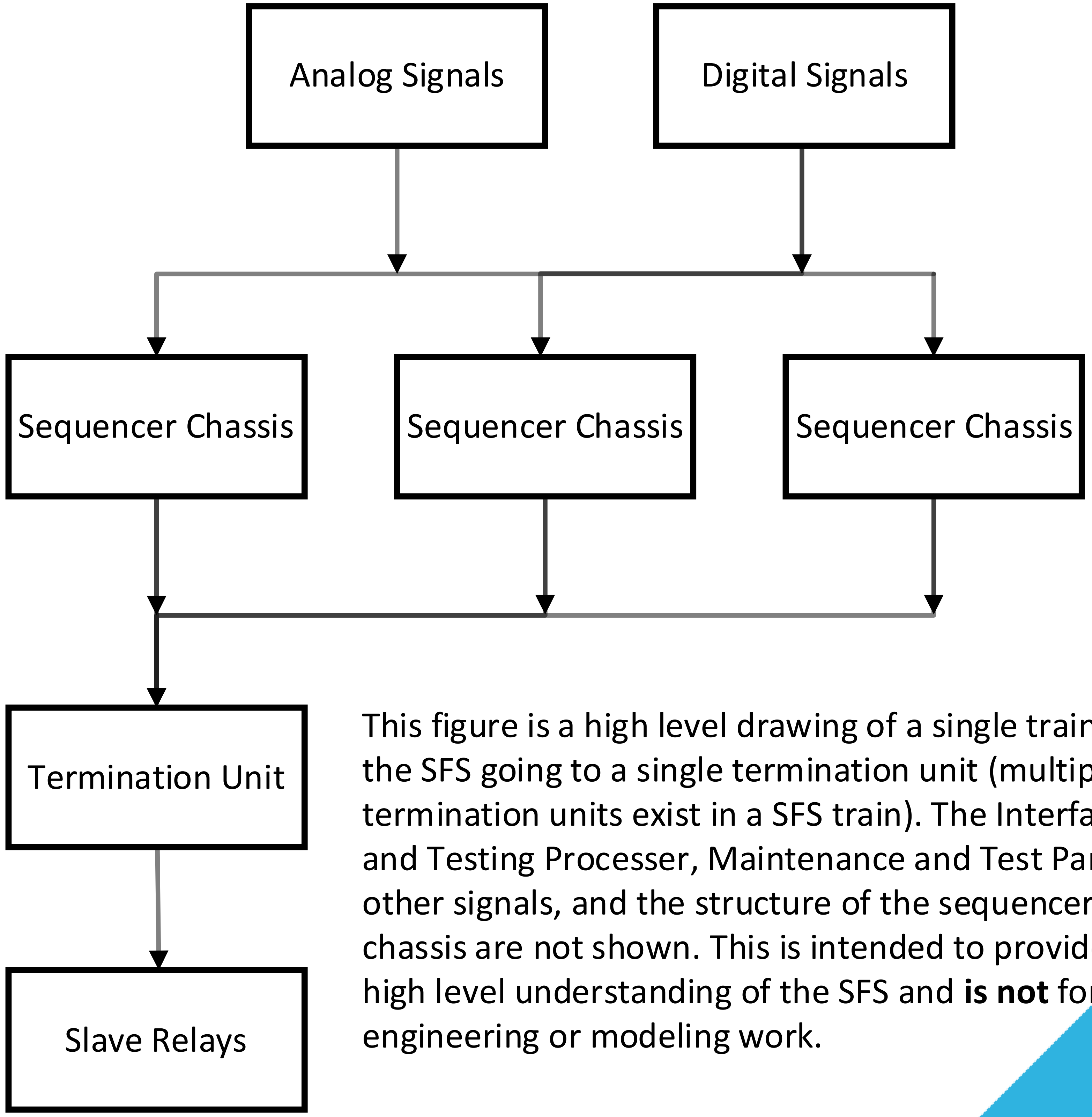
- **Temperature Effects on Digital Component Failure Rates**
  - Temperature can affect long-term reliability of hardware components in DI&C systems.
  - Bounding estimates of temperature values experienced can be used to avoid underestimating the failure rates caused by temperatures.
  - I&C vendors generally have maximum temperature operating limits and failure rates associated with specific temperatures.
  - Pilot conservatively assumed a higher operating temperature in order to identify failure rates that would meet operating conditions within the SFS.
- **Unavailability of components can be identified to account for testing features that detect failures, repair times, failure rate, etc. This provides a more encompassing view of failures in the SFS.**

Hardware Failure Rates

- **Redundancy within components**
  - Digital components are a collection of individual sub-components that when combined provide the functions desired for the component.
  - Software programs can be used to estimate an overall failure rate of these components if limited data exists.
    - The parts count method is a simplistic method that assumes all components are in series and any sub-component failure leads to a system failure.
    - Detailed modeling of these sub-components by sub-dividing out the component into sub-trains can provide improvements in risk insights.
    - Detailed modeling should only be done if there is a significant contribution to risk in order to avoid increasing the size of the model unnecessarily.

Hardware Failure Rates

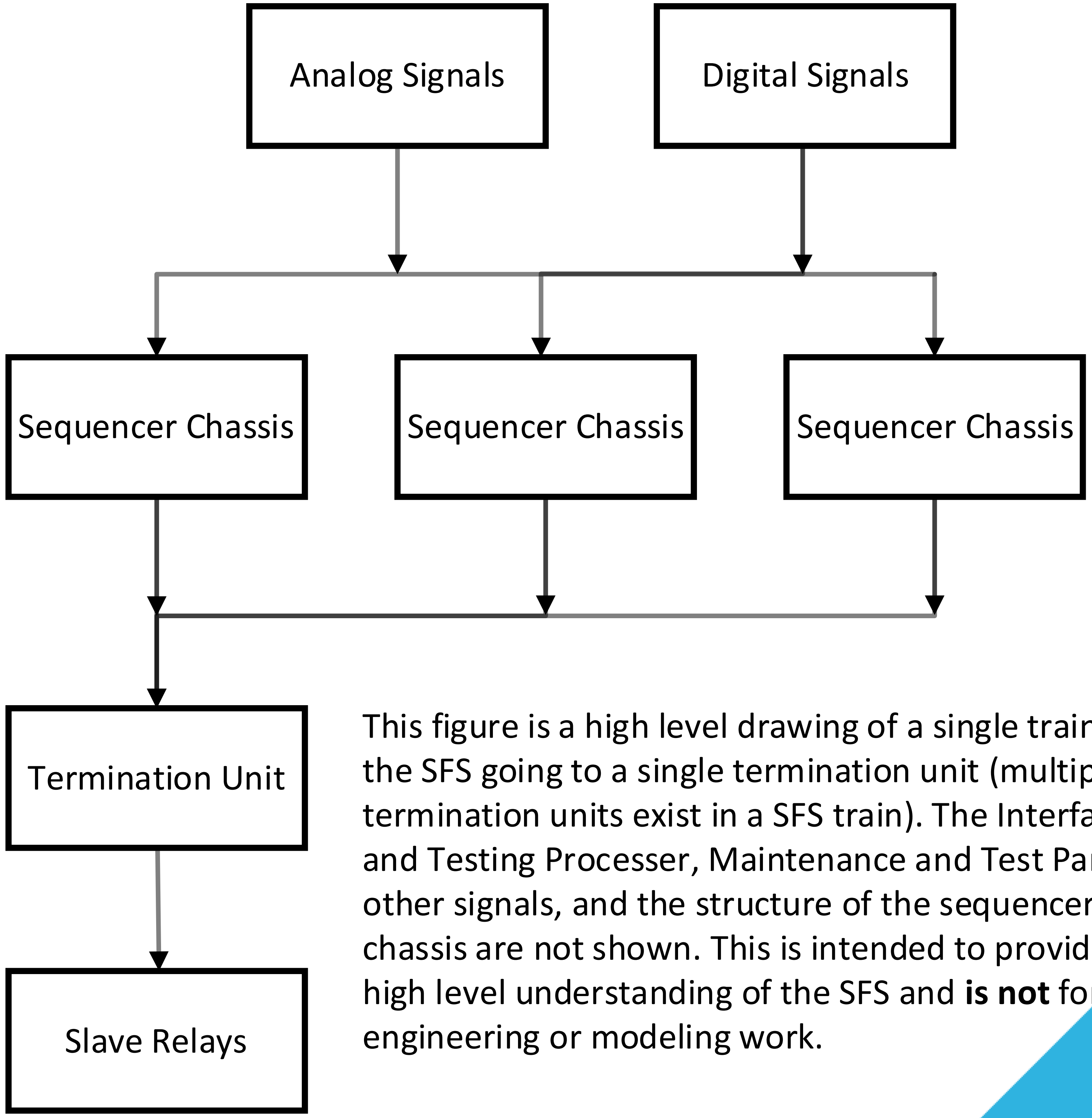
- **Redundancy within components**
  - Detailed Modeling Example.
    - Termination unit uses the parts count method.
    - The termination unit receives multiple redundant SFS chassis signals that are provided to it.
    - A termination unit evaluates each one of these based on redundant voting logic within the termination.
    - Multiple channels are present within the termination unit.



This figure is a high level drawing of a single train of the SFS going to a single termination unit (multiple termination units exist in a SFS train). The Interface and Testing Processer, Maintenance and Test Panel, other signals, and the structure of the sequencer chassis are not shown. This is intended to provide a high level understanding of the SFS and **is not** for engineering or modeling work.

Hardware Failure Rates

- **Redundancy within components**
  - Detailed Modeling Example.
    - Determination that sub-components that are significant contributor to overall termination unit risk were associated with all channels, but each were only supporting a single redundant voter within the termination unit.
    - Sub-dividing a termination unit into “sub-trains” where all redundant voter units are AND rather than OR can reduce the failure rates associated with the overall termination unit.



This figure is a high level drawing of a single train of the SFS going to a single termination unit (multiple termination units exist in a SFS train). The Interface and Testing Processer, Maintenance and Test Panel, other signals, and the structure of the sequencer chassis are not shown. This is intended to provide a high level understanding of the SFS and **is not** for engineering or modeling work.

Hardware Failure Rates

- Further evaluation on lessons learned and best practices for sub-component modeling is planned for future PWROG work.

Hardware Common Cause Failure and Software Failure

Hardware Common Cause Failure

- **Hardware CCF**
  - DI&C components have limited available common cause failures data.
    - Benefits – Limited common cause failures identified.
    - Drawback – Limited data.
  - IEC 61508 has identified approaches for approximating CCF based on available DI&C system information / characteristics.

Hardware Common Cause Failure

- **Hardware CCF**
  - Beta factor method
    - The beta factor method is the simplistic method that is used to identify CCF (all fail).
    - A methodology has been developed in IEC 61508 to approximate a beta CCF with available information on the DI&C system design.
    - In this pilot, we had limited data available for CCF (expected to be similar with other newer DI&C systems). Beta factor was used based on limited data available.
    - Can lead to conservative results.

Hardware Common Cause Failure

- **Hardware CCF**
  - "Shock model" (binomial failure rate) CCF method
    - Limited or no data available for DI&C systems makes proper estimation of CCF difficult. Beta factor approximation leads to conservative results.
    - IEC 61508 has an approximation of "shock model" CCF method using the Beta factor as input along with other assumptions.
    - Process needs to be examined in further detail and evaluation for acceptability of the assumptions used to approximate the factors in the "shock model" CCF method for the ASME/ANS PRA Standard needs to be determined.

Hardware Common Cause Failure

- **Hardware CCF**
  - "Shock model" (binomial failure rate) CCF method
    - Expected to significantly reduce the impact of hardware CCF on the system.
    - Planned future PWROG work will examine the impact of moving to the "shock model" CCF method and the acceptability of the assumptions in IEC 61508 with regards to the ASME/ANS PRA Standard.

Software Common Cause Failure

- **Software CCF**
  - Software failures can lead to common cause failure based on similar functions being provided. Since the software is the same for all like-SSCs, similar inputs are expected to send out similar outputs.
  - Software failures may also not be collected in data based on the issue being solved with a system reboot (may not be logged directly as a software failure).
  - The pilot system made an assumption that a software failure would lead to an overall failure of the SFS based on the safety integrity level (SIL) of the SFS.
    - SFS is safety related and meets requirements of SIL 4 (highest integrity level).
    - IEC 61508 has identified approximations of software failures based on each SIL.
    - Assumed software failure leads to failure of entire system based on limited data.

Software Common Cause Failure

- **Software CCF**
  - Realistic treatment of software failures is a complex issue and ongoing work is being completed with regards to this.
  - PWROG is planning to collaborate with U.S. DoE to determine realistic identification and quantification of software failures.
    - Initial evaluation of DoE methods have identified this as a potential path forward in estimation of software failure.
    - One ongoing topic is to determine the best way to identify software failures on the system-wide, multiple train, or component level (e.g., does the software failure have a high likelihood of impacting the entire system) in planned future PWROG work.

Model Incorporation and Results

Model Incorporation

- **Pilot plant incorporated model**
  - High number of DI&C modeling links for the SFS pilot.
  - AI&C has multiple system links for specific channels / signals from the DI&C system.
  - Leads to time commitment for model incorporation.
  - As building system models for DI&C systems, it is important to realize the modeling links and to make sure to identify level of detail to not overly complicate the DI&C system model.
    - Example: Modeling at higher levels (if appropriate) may provide for benefits in model incorporation scope of work.

Results

- **Pilot Results**
  - Pilot results and the conservatisms identified with DI&C modeling led to conservative CDF and LERF results.
  - Proposed improvements have been identified.
  - Further lessons learned and best practices are planned to be piloted in future PWROG work, including:
    - Use of the “shock model” with limited data (use assumed beta factor as an input with additional assumptions to develop “shock model”) with IEC-61508 method. Evaluate method for use in future PRA modeling and provide best practices and lessons learned.
    - Evaluation of a detailed software failure approach (e.g., DoE research) and determine proper separation of CCF to realistically evaluate software failure.
    - Best practices on detail modeling of specific components that have redundancy within them.

Summary, Contact Information, and Q&A

Summary

- PWROG has been focusing on identifying best practices and lessons learned for modeling DI&C systems.

- Pilot application identified best practices and lessons learned and additional improvements that could be made to the process.

- Additional improvements are planned to be piloted in future project revisions.

Contact Information

PWROG Management Contact Information

Michael Powell, P.E.
PWROG Chairman &
Chief Operating Officer
623-393-6864
Michael.powell@aps.com

Brad Dolan
PWROG Risk Management Committee
Chairman
423-751-2139
bwdolan@tva.gov

Jim Lynde
PWROG Procedures Committee
Chairman
815-406-2201
james.lynde@constellation.com

Damian Mirizio
PWROG Risk Management Committee
Program Director
412-374-3494
mirizids@pwrog.com

Laura Genutis
PWROG Procedures Committee
Program Director
412-374-4553
genutill@westinghouse.com

Contact Information

Author Contact Information

Richard Rolland
Westinghouse Senior Engineer
860-731-6447
rollanrw@westinghouse.com

Raymond Schneider
Westinghouse Fellow Engineer
860-731-6461
schneire@westinghouse.com

Thank you for your Attention!

Questions?